ODATV SORUŞTURMASI DİJİTAL ADLİ ANALİZ RAPORU

24 AĞUSTOS 2012

Hazırlayanlar

Osman PAMUK
Ünal TATAR
Emin ÇALIŞKAN

İÇİNDEKİLER

1 KONU

Kapsam

T.C. 16. Ağır Ceza Mahkemesinin 2011/14 dosya No'lu 09.03.2012 tarihli yazısına istinaden gerçekleştirilen dijital adli analiz çalışması ve sonuçlarını içermektedir.

Analiz Soruları

09.03.2012 tarihinde teslim alınan müzekkerede bulunan 14 soru ile müzekkere ekinde bulunan dilekçelerdeki sorulara ilişkin cevapları içermektedir.

İncelenen Deliller

ODATV'de yapılan arama sonucunda elde edilen Seagate Marka "ST3120827AS_4MS1TF89" seri numaralı bilgisayar hard diski, sanık Barış PEHLİVAN'ın evinde yapılan arama sonucunda elde edilen Fujitsu Marka "MHV2060BHNW18T6229459" seri numaralı hard disk ve sanık Müyesser Uğur YILDIZ'ın evinde yapılan aramada elde edilen Samsung Marka "S17HJ90Q816726" seri numaralı harddisk incelenmiştir. Raporda bulunan bazı yorumlarda; ODATV'den elde edilen ST3120827AS_4MS1TF89 seri numaralı imaj için **Delil 1,** Barış PEHLİVAN'dan elde edilen MHV2060BHNW18T6229459 seri numaralı imaj için **Delil 2**, Müyesser Uğur YILDIZ'dan elde edilen imaj için **Delil 3** numaralandırması yapılmıştır.

2 İNCELEME

Kullanılan araçlar

Disklerin incelenmesi için AccessData® FTK® Imager 3.1.0.1514[1], Encase 6.18.0.59[2], Encase 7.03.01.203, SIFT 2.13 Linux İşletim Sistemi[3], R-Studio[4], Mount Image Pro[5], LiveView[6] vb. dijital adli analiz araçları kullanılmıştır.

Metodoloji

Müzekkerede ve müzekkere ekine iliştirilen dilekçelerde bulunan sorulara yönelik araştırmalar yapılmış, hard disk imajları adli analiz araçlarıyla detaylı tetkik edilmiş, zararlı yazılım incelemesine yönelik statik ve dinamik analizler yapılmıştır.

[1] http://accessdata.com/
[2] http://www.guidancesoftware.com/encase-forensic.htm
[3] http://computer-forensics.sans.org/community/downloads
[4] http://www.r-studio.com/
[5] http://www.mountimage.com/
[6] http://liveview.sourceforge.net/

3 MÜZEKKERE SORULARI

Soru 1.)

Yapılan arama ve el koyma işlemi sırasında belirtilen hard disklerden imaj alma (CMK'nın 134 Md. göre bilgisayar kayıtlarından kopya çıkartılması) işleminin teknik olarak usulüne uygun yapılıp yapılmadığı, imaj alma işlemi sırasında kullanılan programların ve kullanılan donanımın bu iş için uygun ve güvenilir bulunup bulunmadığı? Kullanılan programların uluslararası geçerliliğinin bulunup bulunmadığının açıklanması?

Cevap 1.)

İlgili müzekkerede belirtilen ve tarafımıza teslim edilen imajların teknik olarak usulüne uygun alınıp alınmadığının tespiti, imaj alma işlemleri için kullanılan donanımların ve programların geçerliliğinin denetlenmesi ve bu araçların teknik olarak usulüne uygun kullanılıp kullanılmadığının ortaya çıkarılması ile mümkün olabilmektedir.

Yapılan inceleme ve tetkiklerde, imaj alma işlemleri için Tableu[7] ürününün kullanıldığı tespit edilmiştir. ABD merkezli GuidanceSoftware şirketinin bir ürünü olan Tableu, bir dijital adli analiz aracı olarak imaj alma işlemleri için kullanılan, yazılım ve donanım halde komple bir üründür.

Tableu, imaj alma işlemleri için gerek adli merciler ve kolluk kuvvetleri, gerekse bilişim uzmanları tarafından kullanılan ve bu alanda sıkça karşılaşılan bir üründür. Write-blocker (yazma korumalı) donanımsal özelliğiyle imajı alınan dijital verilerin değişmezliğini ve bütünlüğünü tesis etme amacında bir yazılım-donanım ürünüdür.

Tarafımıza ulaşan dijital adli delillerin, Tableu ürününe ait Tableau Forensic Duplicator Model TD1 modeliyle kopyalandığı anlaşılmıştır. Genelde Tableu ürünleri, özelde ise TD1 versiyonuyla ilgili yapılan araştırmalarda, ürünün uluslararası geçerliliğine dair hazırlanmış çeşitli raporlara ulaşmak mümkündür. Bunlardan en geçerlisi ve göze çarpanı, Amerika Birleşik Devletleri Adalet Bakanlığının, Teknoloji ve Standartlar Ulusal Enstitüsü'ne (NIST)[8] yaptırdığı dijital adli analiz araçlarının güvenliği konusundaki analiz raporudur.

[7] Tableu. Üretici firma web adresi:*http://www.guidancesoftware.com* Ürün web adresi: *http://www.tableau.com*
[8] http://www.cftt.nist.gov/

Tableu ürününün bu alanda aldığı rapora, şirketin web adresinden ulaşmak mümkündür.[9] Test kapsamı, değerlendirme kriterleri ve gerçekleştirilen analizler için NIST'in web adresi ziyaret edilebilir.[10] İlgili raporlara ulaşmak için bağlantı adresi verilen referanslar incelenebilir.

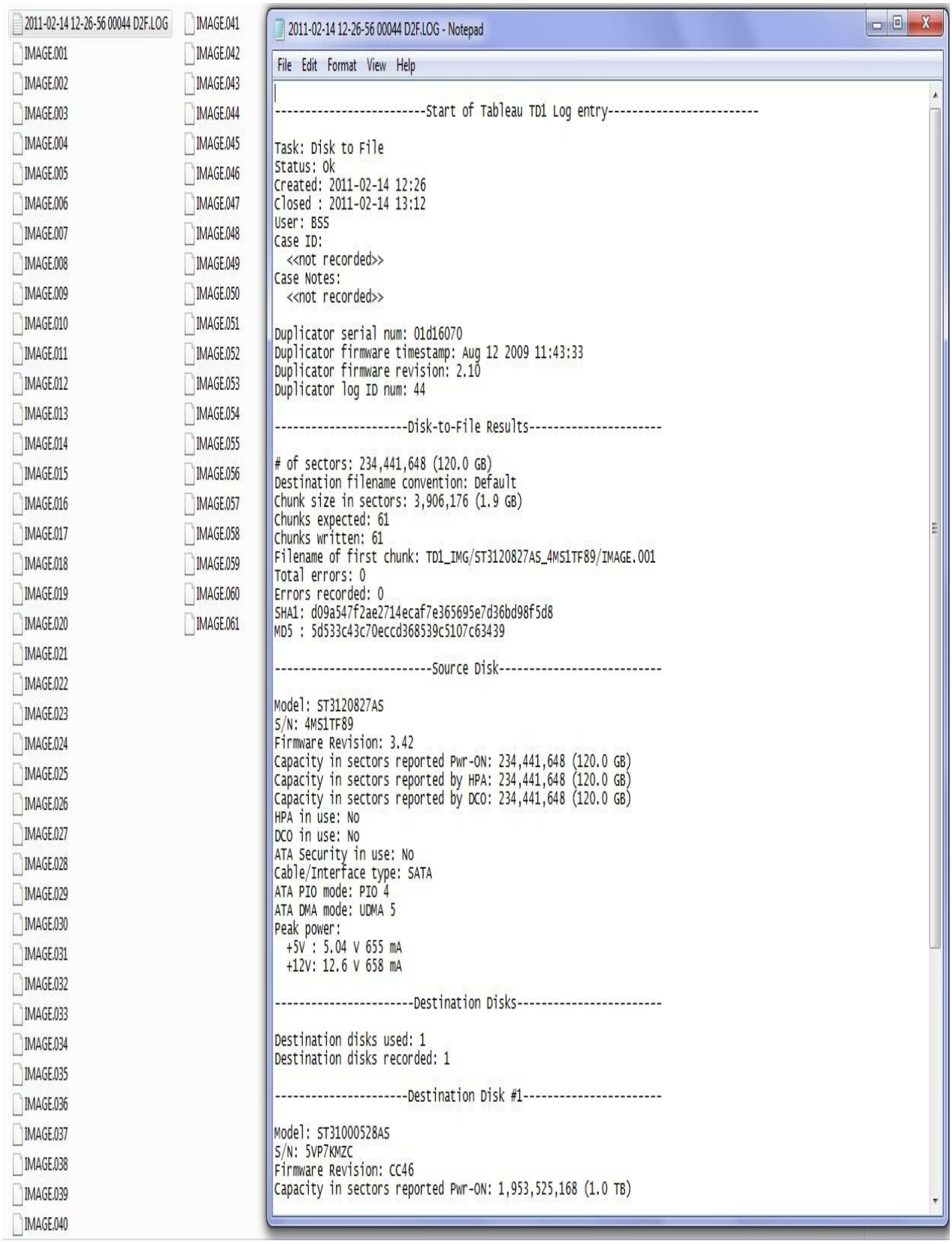
Müzekkerede tarafımıza yöneltilen sorulardan "dijital delillerden imaj alınması amacıyla çalıştırılan araçların teknik olarak usulüne uygun kullanılıp kullanılmadığının tespiti", ilgili araçların yönergelerine ve kullanma kılavuzlarına uygun şekilde hareket edildiğinin, doğru ve tutarlı şekilde imaj kopyalarının alındığının kontrolüyle mümkün olabilir.

Kullanılan Tableu ürününün imaj alma işlemleri sonrası oluşturduğu loglar ve dosyalar incelenerek yorum yapılabilir.

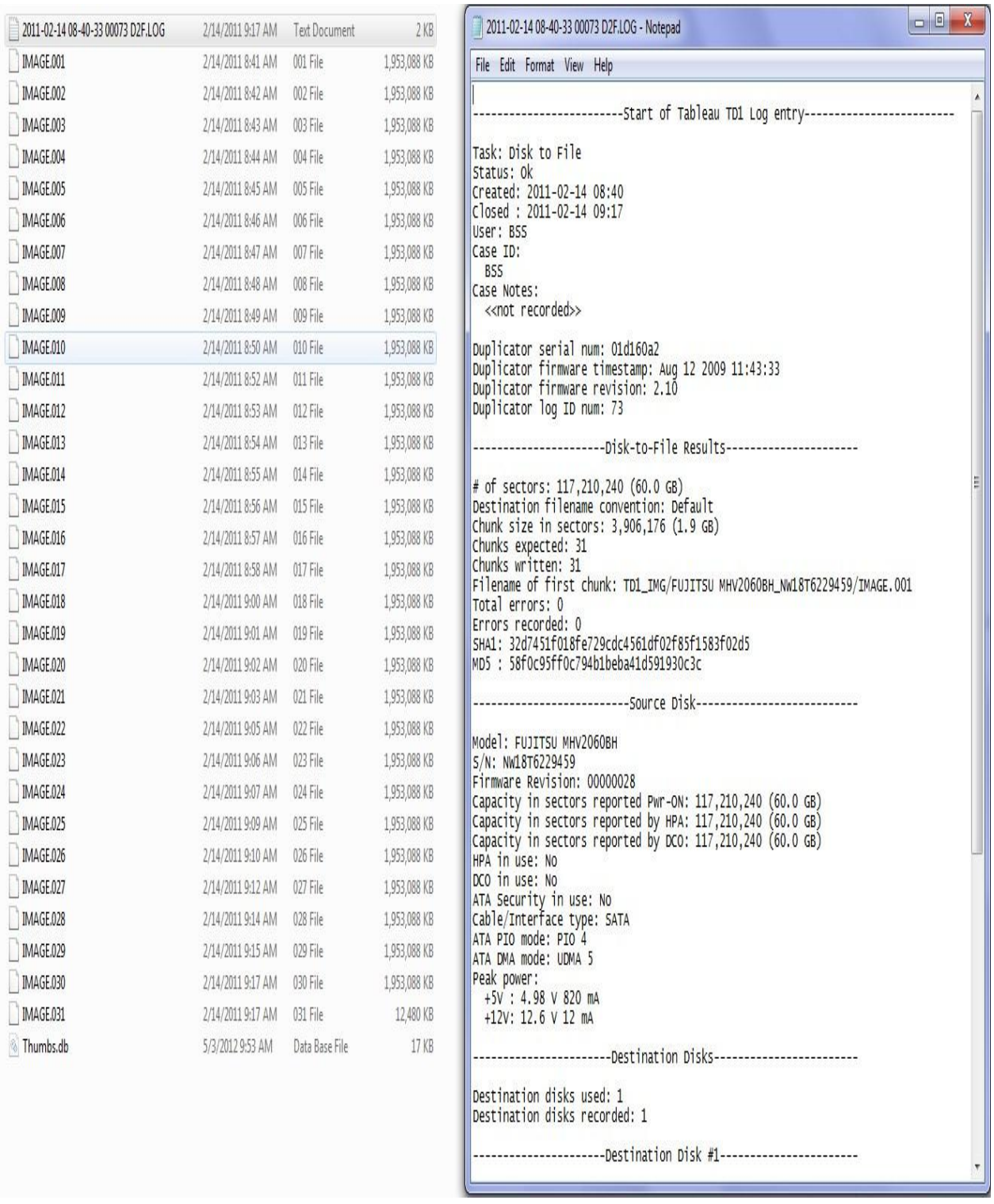
09.03.2012 tarihinde, soruşturma kapsamında görevli 16. Ağır Ceza Mahkemesi'nden imza karşılığı teslim alınan imajlara ait dosyalar ve kayıt loglarına ait ekran kopyaları aşağıda verilmiştir. Oluşan loglar ve dosyalar incelendiğinde herhangi bir tutarsızlık veya yanlışlık görünmemektedir.

Detayı açıklanan ve referansları verilen bu araştırmalar ve tetkikler neticesinde, soruşturma kapsamında kullanılan ve yukarda detay bilgisi geçen dijital adli analiz araçlarının gerekli ve yeterli güven seviyesine sahip olduğu, bu araçların uluslararası alanda kabul görüp geçerli sayıldığı, bu araçlar kullanılarak soruşturma kapsamında gerçekleştirilmiş imaj alma işlemler süreçlerinin de teknik olarak usulune uygun yürütüldüğü belirtilebilir.

[9] http://www.tableau.com/pdf/en/Test_Report_NIST_TD1.pdf
[10] http://www.cftt.nist.gov/fmp-atp-pc-01.pdf

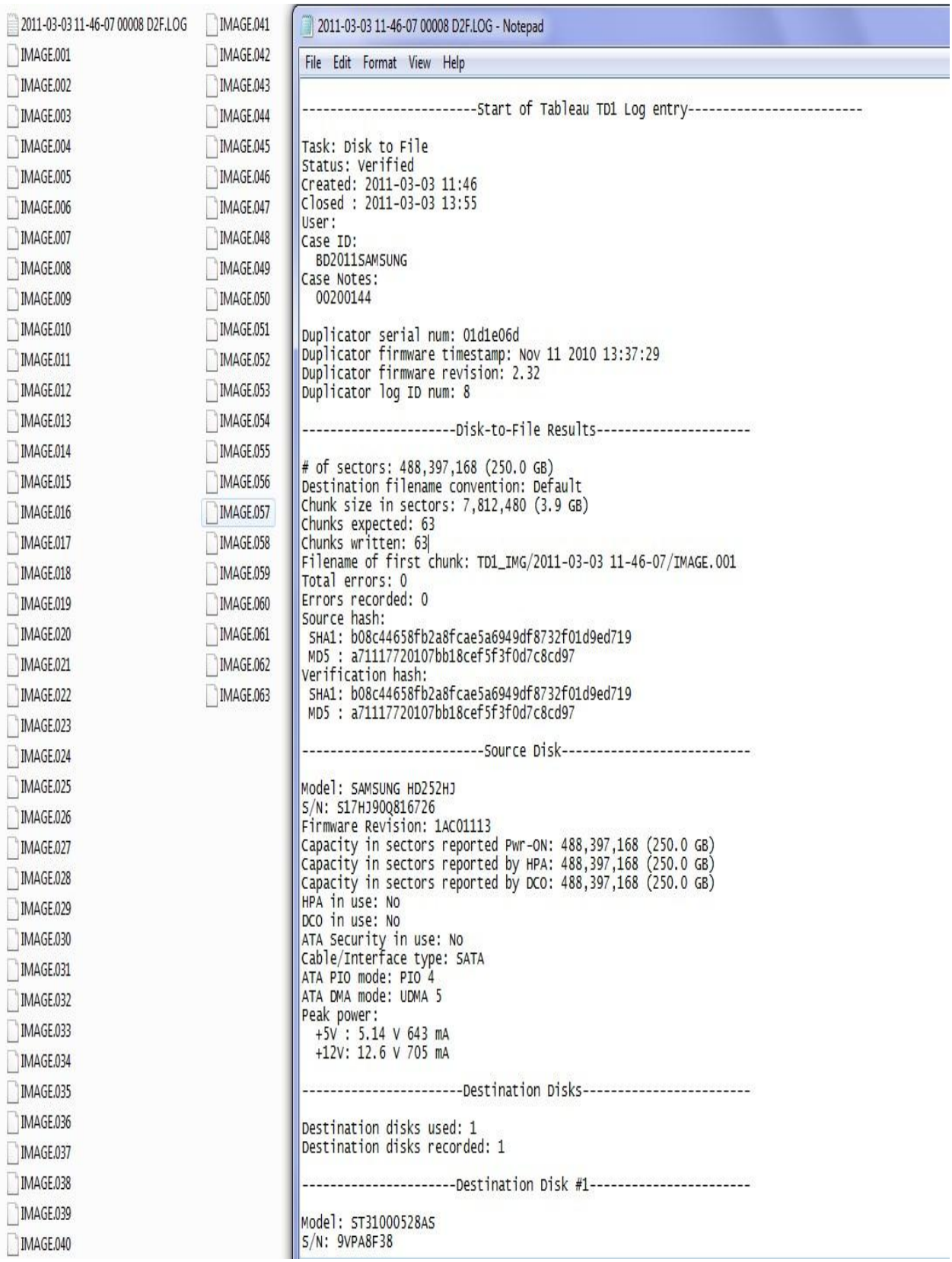


Şekil 1 - 5VP7KMZC Seri No'lu İmaj Dosyaları ve Logu



2011-02-14 08-40-33 00073 D2F.LOG	2/14/2011 9:17 AM	Text Document	2 KB
IMAGE.001	2/14/2011 8:41 AM	001 File	1,953,088 KB
IMAGE.002	2/14/2011 8:42 AM	002 File	1,953,088 KB
IMAGE.003	2/14/2011 8:43 AM	003 File	1,953,088 KB
IMAGE.004	2/14/2011 8:44 AM	004 File	1,953,088 KB
IMAGE.005	2/14/2011 8:45 AM	005 File	1,953,088 KB
IMAGE.006	2/14/2011 8:46 AM	006 File	1,953,088 KB
IMAGE.007	2/14/2011 8:47 AM	007 File	1,953,088 KB
IMAGE.008	2/14/2011 8:48 AM	008 File	1,953,088 KB
IMAGE.009	2/14/2011 8:49 AM	009 File	1,953,088 KB
IMAGE.010	2/14/2011 8:50 AM	010 File	1,953,088 KB
IMAGE.011	2/14/2011 8:52 AM	011 File	1,953,088 KB
IMAGE.012	2/14/2011 8:53 AM	012 File	1,953,088 KB
IMAGE.013	2/14/2011 8:54 AM	013 File	1,953,088 KB
IMAGE.014	2/14/2011 8:55 AM	014 File	1,953,088 KB
IMAGE.015	2/14/2011 8:56 AM	015 File	1,953,088 KB
IMAGE.016	2/14/2011 8:57 AM	016 File	1,953,088 KB
IMAGE.017	2/14/2011 8:58 AM	017 File	1,953,088 KB
IMAGE.018	2/14/2011 9:00 AM	018 File	1,953,088 KB
IMAGE.019	2/14/2011 9:01 AM	019 File	1,953,088 KB
IMAGE.020	2/14/2011 9:02 AM	020 File	1,953,088 KB
IMAGE.021	2/14/2011 9:03 AM	021 File	1,953,088 KB
IMAGE.022	2/14/2011 9:05 AM	022 File	1,953,088 KB
IMAGE.023	2/14/2011 9:06 AM	023 File	1,953,088 KB
IMAGE.024	2/14/2011 9:07 AM	024 File	1,953,088 KB
IMAGE.025	2/14/2011 9:09 AM	025 File	1,953,088 KB
IMAGE.026	2/14/2011 9:10 AM	026 File	1,953,088 KB
IMAGE.027	2/14/2011 9:12 AM	027 File	1,953,088 KB
IMAGE.028	2/14/2011 9:14 AM	028 File	1,953,088 KB
IMAGE.029	2/14/2011 9:15 AM	029 File	1,953,088 KB
IMAGE.030	2/14/2011 9:17 AM	030 File	1,953,088 KB
IMAGE.031	2/14/2011 9:17 AM	031 File	12,480 KB
Thumbs.db	5/3/2012 9:53 AM	Data Base File	17 KB

Şekil 2 - 5VP7L1TN Seri No'lu İmaj Dosyaları ve Logu



Şekil 3 - 9VPA8F38 Seri No'lu İmaj Dosyaları ve Logu

Soru 2.)

Arama ve el koyma işlemi sırasında, imaj alma işlemi sonucunda dijital medyaya (Hard Disk) ait hash değerlerinin doğru olarak arama ve el koyma tutanağında belirtilip belirtilmediği, farklılık var ise nedenleri, farklılık yok ise bunun nasıl bir anlam ifade edeceğinin açıklanması?

Cevap 2.)

Müzekkere eklerinde tarafımıza iletilen dijital hard disk imajlarının hash değerlerine ait arama-el koyma tutanağında belirtilen veriler aşağıdaki gibidir.

Delil Seri Numarası	Disk Markası	Kapasite	Disk Seri No	Dava Dosyasında Konumu
ST3120927AS_4MS1TF89	Seagate	120 GB	5VP7KMZC	Klasör 2 - Sayfa 216
MHV2060BH_NW18T6229459	Fujitsu	60 GB	5VP7L1TN	Klasör 8 - Sayfa 241
S17HJ90Q816726	Samsung	250 GB	9VPA8F38	Klasör 25 - Sayfa 119

Tablo 1 - Dijital İmajların Dava Dosyasındaki Konumları

ST3120927AS_4MS1TF89 Seri Numaralı Disk

ST3120927AS_4MS1TF89 seri numaralı diske ait arama el koyma tutanakları, dava dosyalarından 2. klasörde 216. sayfada bulunmaktadır. Elde edilen imaj ile ilgili tutanaklarda belirtilmiş olan SHA1 ve MD5 hash değerleri aşağıdaki gibidir.

SHA1: d09a547f2ae2714ecaf7e365695e7d36bd98f5d8

MD5: 5d533c43c70eccd368539c5107c63439

4) Seagate marka 5VP7KMZC seri numaralı 1TB kapasiteli sabit disk içerisine;

a) Koridorun sonunda soldaki odanın pencere kenarındaki sol köşede bulunan masanın altındaki siyah renkli bilgisayar kasası içerisinden çıkan Seagate marka 9QZ5XN3K seri numaralı 80GB kapasiteli sabit diskin imajı alınmış ve hash bilgisi:
SHAİ: 4ff90ae608d8927f50901e3aeedbfb041bc27d32
MD5 : 425da6942262f977a9f3572bafd4a5db olarak tespit edilmiştir.

b) Koridorun sonunda soldaki odanın girişe göre soldaki ortadaki masanın altında bulunan bilgisayar kasası içerisinden çıkan Seagate marka 4MS1TE98 seri numaralı 120GB kapasiteli sabit diskin imajı alınmış ve hash bilgisi:
SHAİ: 988df76803d17b0fabbddf0efc445e7dddeb23d8
MD5 : a7ca2965d4188c5d490e10fa0d8ea549 olarak tespit edilmiştir.

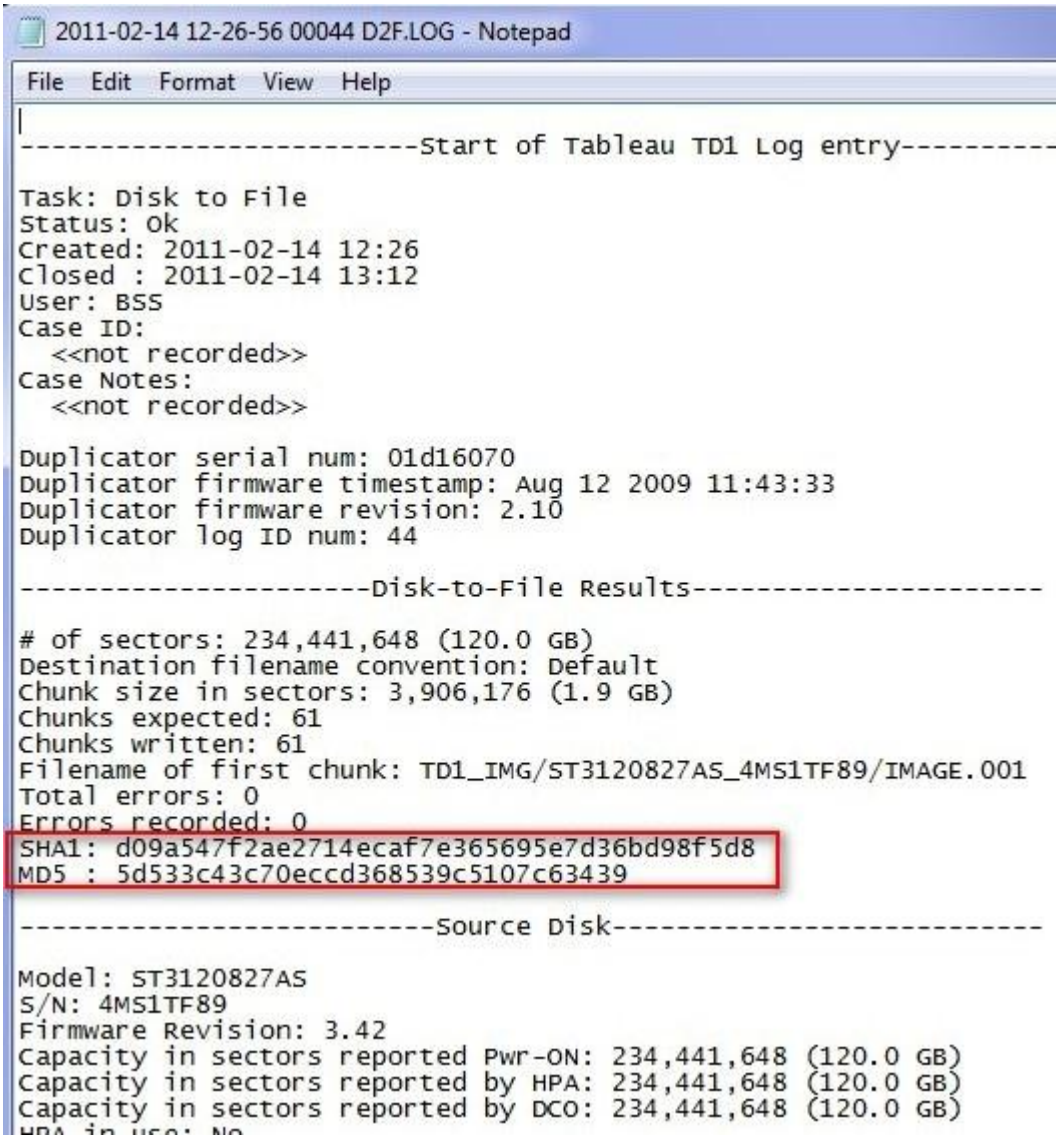
c) Koridorun sonunda soldaki odanın girişe göre sağda pencerenin yanındaki masadaki Exper marka bilgisayar kasasının içerisinden çıkan 2 adet sabit diskten birisi olan Seagate marka 4MS1TF89 seri numaralı 120GB kapasiteli sabit diskin imajı alınmış ve hash bilgisi:
SHAİ: d09a547f2ae2714ecaf7e365695e7d36bd98f5d8
MD5 : 5d533c43c70eccd368539c5107c63439 olarak tespit edilmiştir.

d) Koridorun sonunda soldaki odanın girişe göre sol karşıdaki masada bulunan HP marka bilgisayar kasası içerisinden çıkan 3 adet sabit diskten birisi olan Seagate marka 9QG4Z3ZF seri numaralı 500GB kapasiteli sabit diskin imajı alınmış ve hash bilgisi:
SHAİ: 2f6e39a5d84edd9b5595f5978d2e33c2a4a01918
MD5 : 48334415f99b4792400e5222ab5476df olacak tespit edilmiştir.

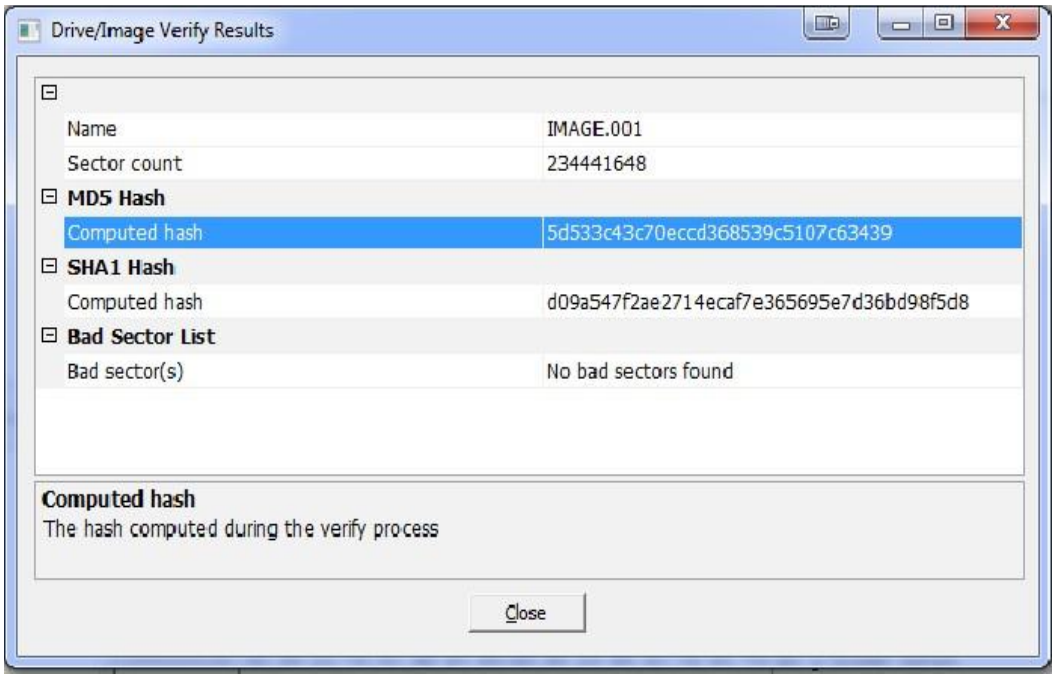
2/4

Şekil 4 - ST3120927AS_4MS1TF89 Seri No'lu İmajın Tutanaklardaki Kaydı

ST3120927AS_4MS1TF89 seri numaralı diskin imaj alma işlemleri sonrasında oluşan ve Tableu ürününün çıktısı olan TD1 logunda da aynı değerler görünmektedir. İlgili hash değerleri için aşağıdaki ekran kopyası incelenebilir.



Şekil 5 - ST3120927AS_4MS1TF89 Seri No'lu İmajın TD1 Loglarındaki Kaydı



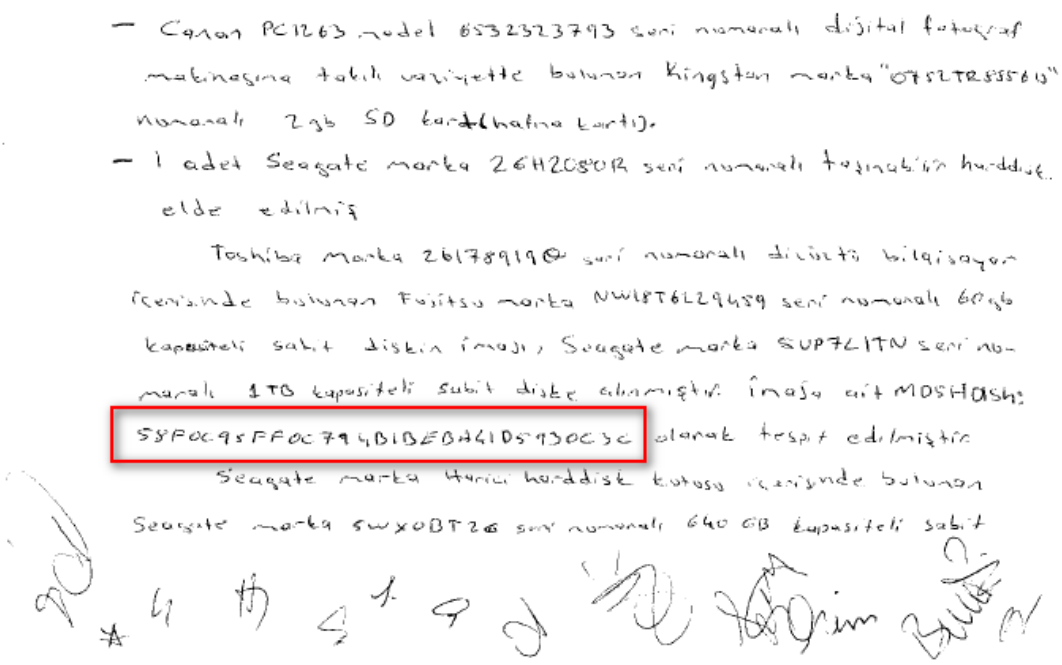
Şekil 6 - Tarafımıza iletilen ST3120927AS_4MS1TF89 Seri No'lu İmajın Hash Değerleri

İncelenen *ST3120927AS_4MS1TF89* seri nolu imaja ait hash değerlerinin tarafımıza iletilen hard disk imajlarıyla tutarlılık göstermesi, arama-el koyma sırasında kopyası çıkarılan orijinal hard disk ile bizlere iletilen hard disk kopyasının aynı olduğunu gösterir.

MHV2060BH_NW18T6229459 Seri Numaralı Disk

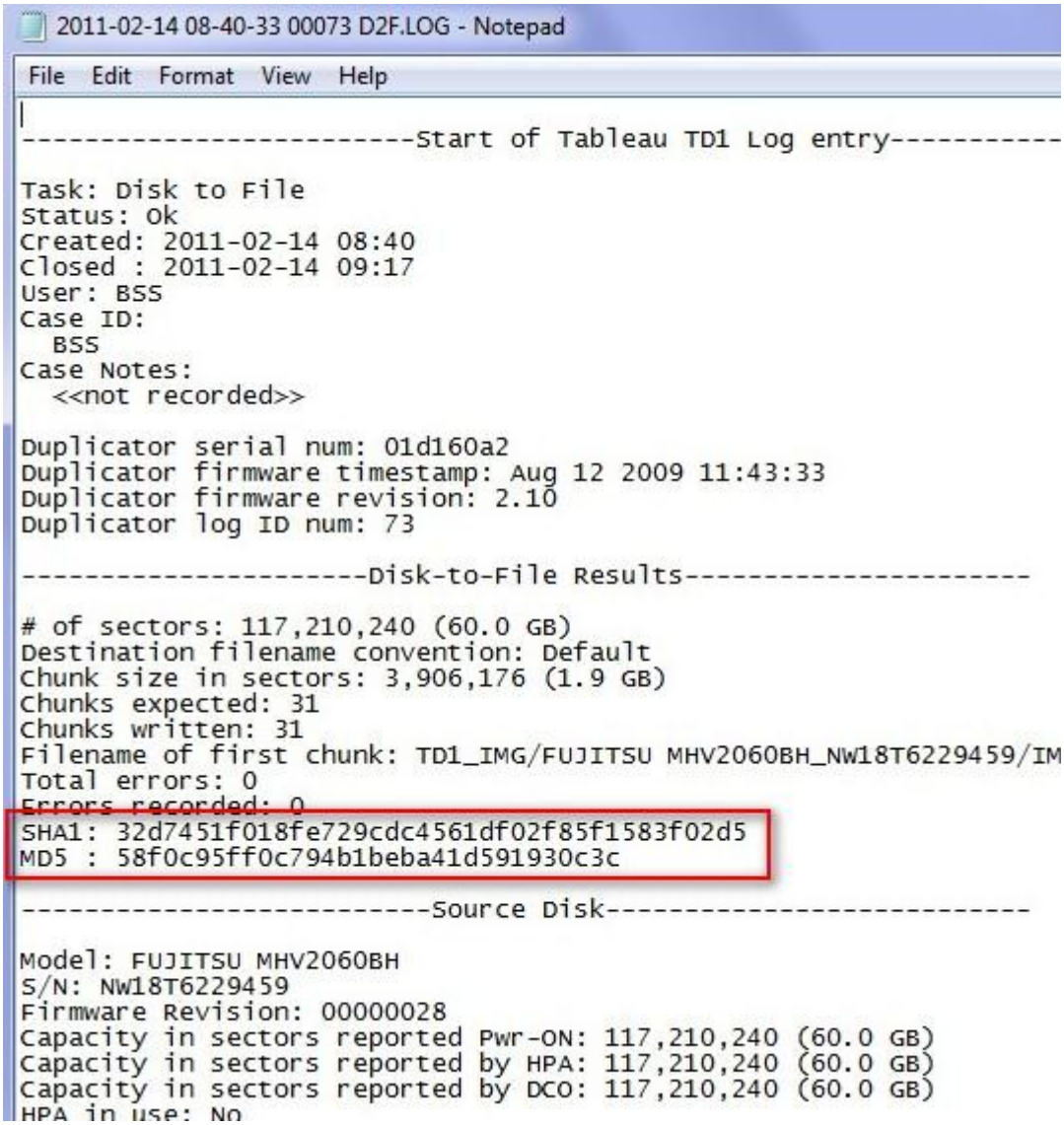
MHV2060BH_NW18T6229459 seri numaralı diske ait arama el koyma tutanakları, dava dosyalarından 8. klasörde 241. sayfada bulunmaktadır. Elde edilen imaj ile ilgili tutanaklarda belirtilmiş olan MD5 hash değeri aşağıdaki gibidir.

MD5: 58f0c95ff0c794b1beba41d5930c3c

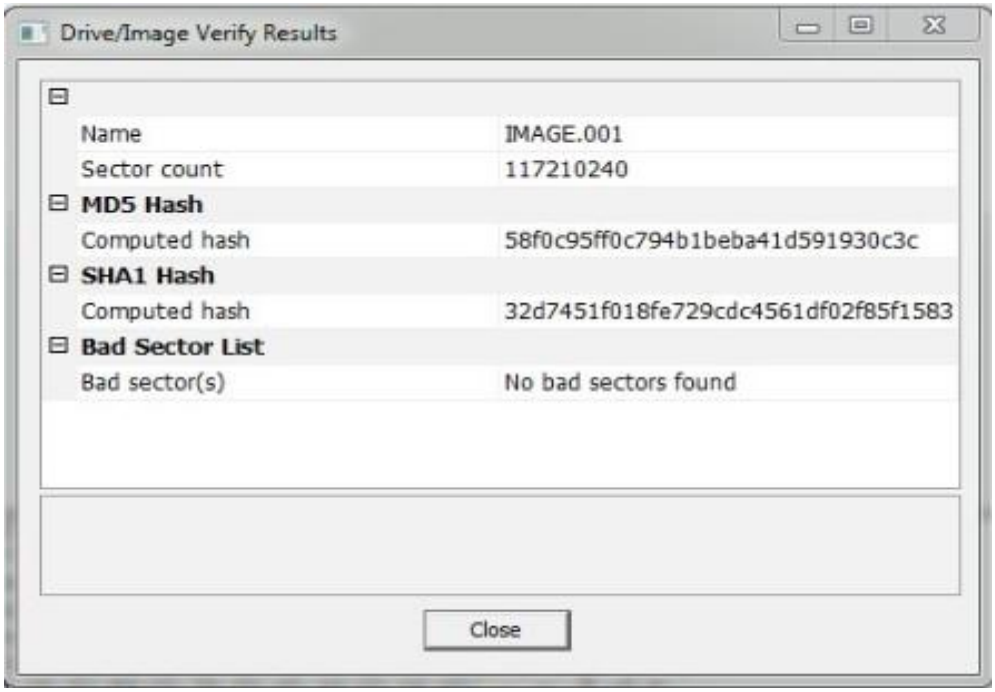


Şekil 7 - MHV2060BH_NW18T6229459 Seri No'lu İmajın Tutanaklardaki Kaydı

MHV2060BH_NW18T6229459 seri numaralı diskin imaj alma işlemleri sonrasında oluşan ve Tableu ürününün çıktısı olan TD1 logunda da aynı değerler görünmektedir. İlgili hash değerleri için aşağıdaki ekran kopyası incelenebilir.



Şekil 8 - MHV2060BH_NW18T6229459 Seri No'lu İmajın TD1 Loglarındaki Kaydı



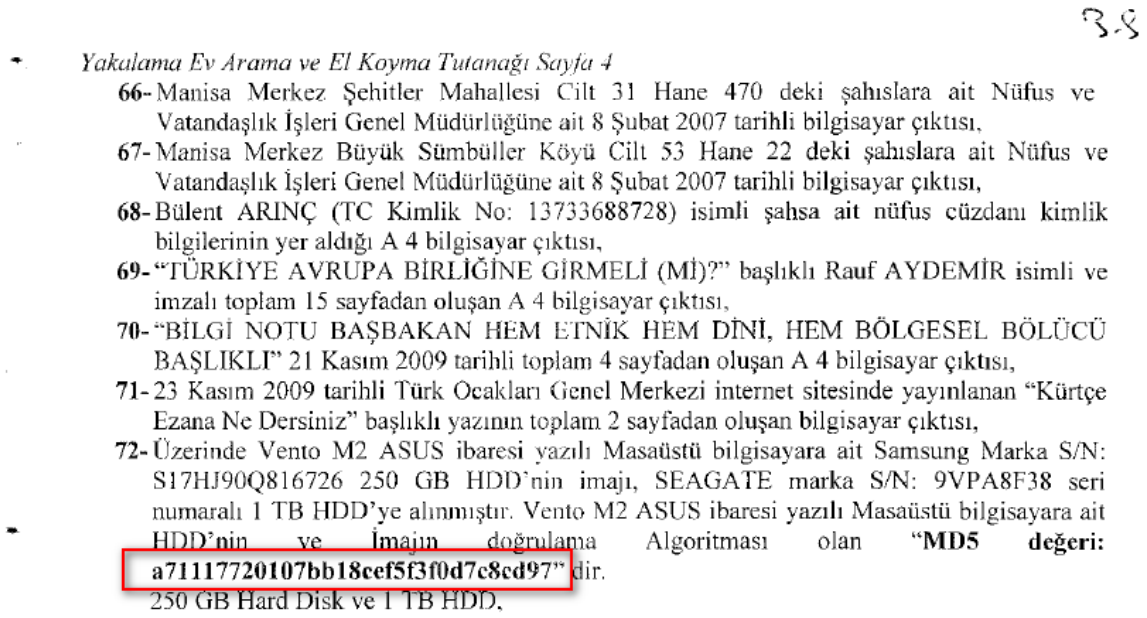
Şekil 9 – Tarafımıza iletilen MHV2060BH_NW18T6229459 Seri No'lu İmajın Hash Değerleri

İncelenen *MHV2060BH_NW18T6229459* seri nolu imaja ait hash değerlerinin tarafımıza iletilen hard disk imajlarıyla tutarlılık göstermesi, arama-el koyma sırasında kopyası çıkarılan orijinal hard disk ile bizlere iletilen hard disk kopyasının aynı olduğunu gösterir.

S17HJ90Q816726 Seri Numaralı Disk

S17HJ90Q816726 seri numaralı diske ait arama el koyma tutanakları, dava dosyalarından 25. klasörde 119. sayfada bulunmaktadır. Elde edilen imaj ile ilgili tutanaklarda belirtilmiş olan MD5 hash değeri aşağıdaki gibidir.

MD5: a71117720107bb18cef5f3f0d7c8cd97



38

Yakalama Ev Arama ve El Koyma Tutanağı Sayfa 4

66- Manisa Merkez Şehitler Mahallesi Cilt 31 Hane 470 deki şahıslara ait Nüfus ve Vatandaşlık İşleri Genel Müdürlüğüne ait 8 Şubat 2007 tarihli bilgisayar çıktısı,

67- Manisa Merkez Büyük Sümbüller Köyü Cilt 53 Hane 22 deki şahıslara ait Nüfus ve Vatandaşlık İşleri Genel Müdürlüğüne ait 8 Şubat 2007 tarihli bilgisayar çıktısı,

68- Bülent ARINÇ (TC Kimlik No: 13733688728) isimli şahsa ait nüfus cüzdanı kimlik bilgilerinin yer aldığı A 4 bilgisayar çıktısı,

69- "TÜRKİYE AVRUPA BİRLİĞİNE GİRMELİ (Mİ)?" başlıklı Rauf AYDEMİR isimli ve imzalı toplam 15 sayfadan oluşan A 4 bilgisayar çıktısı,

70- "BİLGİ NOTU BAŞBAKAN HEM ETNİK HEM DİNİ, HEM BÖLGESEL BÖLÜCÜ BAŞLIKLI" 21 Kasım 2009 tarihli toplam 4 sayfadan oluşan A 4 bilgisayar çıktısı,

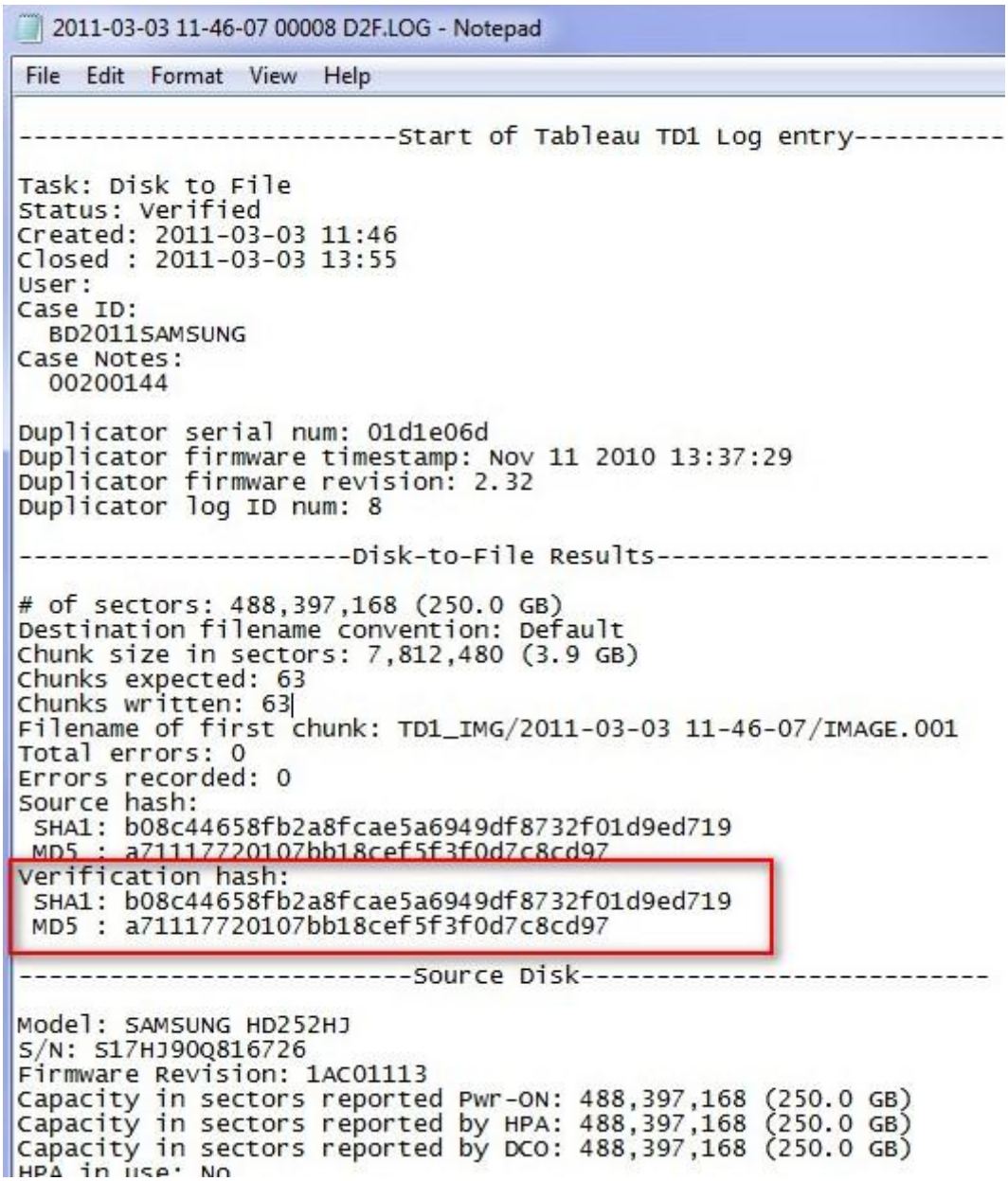
71- 23 Kasım 2009 tarihli Türk Ocakları Genel Merkezi internet sitesinde yayınlanan "Kürtçe Ezana Ne Dersiniz" başlıklı yazının toplam 2 sayfadan oluşan bilgisayar çıktısı,

72- Üzerinde Vento M2 ASUS ibaresi yazılı Masaüstü bilgisayara ait Samsung Marka S/N: S17HJ90Q816726 250 GB HDD'nin imajı, SEAGATE marka S/N: 9VPA8F38 seri numaralı 1 TB HDD'ye alınmıştır. Vento M2 ASUS ibaresi yazılı Masaüstü bilgisayara ait HDD'nin ve İmajın doğrulama Algoritması olan **"MD5 değeri: a71117720107bb18cef5f3f0d7c8cd97"** dir.

250 GB Hard Disk ve 1 TB HDD,

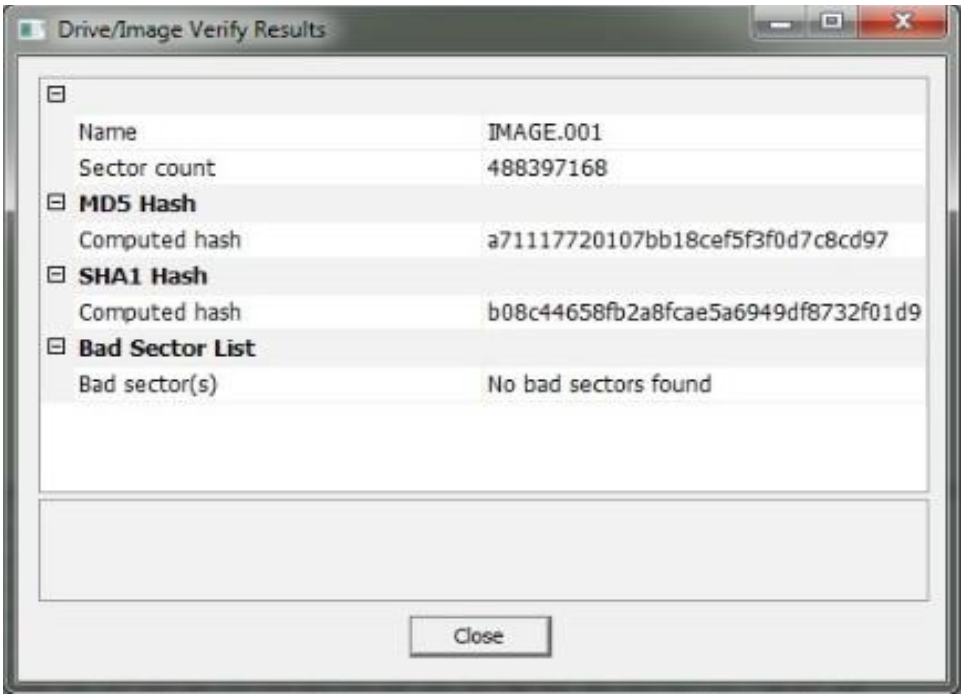
Şekil 10 - S17HJ90Q816726 Seri No'lu İmajın Tutanaklardaki Kaydı

S17HJ90Q816726 seri numaralı diskin imaj alma işlemleri sonrasında oluşan ve Tableu ürününün çıktısı olan TD1 logunda da aynı değerler görünmektedir. İlgili hash değerleri için aşağıdaki ekran kopyası incelenebilir.



Şekil 11 - S17HJ90Q816726 Seri No'lu İmajın TD1 Loglarındaki Kaydı

Yaptığımız incelemelerde, ilgili hard disk imajına ait tutanaklarda belirtilmiş olan hash değerleri ve imaj alma işlemleri esnasında oluşan TD1 loglarındaki hash değerleri ile, müzekkere ekinde tarafımıza teslim edilen hard disk imajının hash değerlerinin uyumlu olduğu gözlenmiştir.



Şekil 12 – Tarafımıza İletilen S17HJ90Q816726 Seri No'lu İmajın Hash Değerleri

İncelenen *S17HJ90Q816726* seri nolu imaja ait hash değerlerinin tarafımıza iletilen hard disk imajlarıyla tutarlılık göstermesi, arama-el koyma sırasında kopyası çıkarılan orijinal hard disk ile bizlere iletilen hard disk kopyasının aynı olduğunu gösterir.

Soru 3.)

Bilgisayar hard diskinde kayıtlı bir dijital verinin o bilgisayara veya bilgisayar kullanıcısına aidiyetinin nasıl belirleneceğinin ayrıntılı bir şekilde açıklanması?

Cevap 3.)

Bir bilgisayar sabit diskinde kayıtlı bir dijital verinin o bilgisayara ait olup olmadığı, o sabit diske adli analiz kurallarına uyarak el konulması ile garanti altına alınabilir. Sabit diskteki kayıtlı bir dijital verinin belli bilgisayar kullanıcısına aidiyeti konusunda ise; ilgili dijital verinin bilgisayarda oluşturduğu çeşitli izler, üstveriler, ilgili dijital veriyi çalıştıran bilgisayar programında oluşan kayıt verileri ve bu programın bilgisayarda yüklü olan diğer program ve uygulamalarla olan ilişkisine dair kayıt verileri analiz edilerek bir yorum yapılabilir. Bütün bu inceleme ve analizler, dijital verilerin aidiyeti noktasında fikir oluşturmakla birlikte, kesinlik içeren ifadelerin kullanılması da mümkün olmamaktadır.

Örnek vermek gerekirse, incelenecek dijital veri word, excel vs. gibi bir Microsoft Office dosyası ise; Office uygulamalarının gerek kurulum gerekse kullanım esnasında kullanıcıdan istediği ve kaydettiği yazar ismi, şirket ismi vb. üstveriler (metadata) ilgili bilgisayar kullanıcısına ait bilgi verebilir. İlgili dijital veriye ait yazar (author), son kaydeden kullanıcı (last saved by) gibi bilgiler incelenebilir. Bu bilgilerin girilmemiş olması halinde ise Microsoft Office uygulamasının atadığı öntanımlı (default) değerler görünecektir.

Bilgisayarlar, işletim sisteminin kurulumu esnasında bir kullanıcı adı girilmesini ister. Bu kullanıcı adı verisi (username), o bilgisayarda yapılacak birçok işlem için referans olarak kullanılır. Bilgisayarda bulunan birçok dijital veri de bu kullanıcı adını *"dosya sahibi"* olarak kendi üstverisine kaydeder. İşte bu işletim sisteminin kurulumu esnasında girilmiş ve çeşitli dijital verilerde iz bırakan kullanıcı adı bilgisi kullanılarak, dijital verilerin o bilgisayara ve bilgisayar kullanıcısına aidiyeti noktasında bilgi edinilebilir.

Bu durumun yanı sıra bir dijital verinin ilgili bilgisayar kullanıcısına ait olup olmadığı; incelenen dijital verinin bulunduğu bilgisayarda o dijital veriyi işleyecek bir programın var olup olmaması ve varsa versiyon uyumlulukları ile analiz edilebilir. Dijital veriyi işleyebilecek program ile o dijital verinin versiyon bilgisinin uyumsuzluğu, o dijital verinin ilgili bilgisayara ait olmadığını düşündürebileceği gibi, uyumlu olması da o bilgisayar ve bilgisayar kullanıcısına ait olduğunu düşündürebilir.

Dijital veriler, türlerine ve kullanım alanlarına göre bilgisayarlarda farklı izler ve üstveriler bırakabilir. Bir diğer örnek olarak, *pst* uzantılı bir dijital veri, Microsoft firmasına ait Outlook ürününün kullandığı ve e-posta dosyalarını içeren bir veriyi işaret eder. Bu durumda, ilgili

dosyada bulunan e-postaların incelenmesi ile dijital verinin aidiyeti noktasında fikir sahibi olunabilir. Buna benzer şekilde bilgisayarda kayıtlı olan anında mesajlaşma (IM) programlarının ürettiği veriler de analiz edilebilir. İncelenecek dijital veriye ait izlere internet geçmişi, çerez, arşivlenmiş bilgiler, kayıtlı kısayollar vb. yerlerde rastlanılması halinde ise analiz bu alanda yoğunlaştırılabilir ve o dijital verinin ilgili bilgisayardaki geçmişi incelebilir. Bu ve buna benzer örnekler çoğaltılabilmektedir. Buradan hareketle, dijital verilerin sahiplik bilgilerinin incelenmesinin çok farklı yollarının olduğu, incelenecek dijital veriye göre çeşitli yaklaşımlar ve farklı analiz tekniklerinin mümkün olduğu söylenebilir.

Soru 4.)

Bilgisayarda oluşturulan bir dijital dosyanın kim tarafından hangi bilgisayarda oluşturulduğunun nasıl belirleneceğinin açıklanması?

Cevap 4.)

Bilgisayarlarda bulunan dijital dosyaların kim tarafından oluşturulduğunun açığa çıkarılması için, incelenmek istenen dosyalara ait üstverilerin ve sistem kayıtlarının analiz edilmesi işlemleri uygulanabilir. Dosya sahipliğinin tespiti ile ilgili yöntemler 3. Soru'da detaylı şekilde cevaplanmıştır.

Bir dijital dosyanın hangi bilgisayarda oluşturulduğunun tespiti için ise, bir önceki soruda belirtilen üstverilerinin incelenmesi yeterli olmayacaktır. Bazı dijital dosyalar, üretildikleri bilgisayara ait *Bilgisayar Adı, MAC Adresi* gibi verileri saklarlar. Bu gibi üstverilerin kullanılıyor olması, incelemesi yapılan dijital dosyanın hangi bilgisayarda üretildiğine dair fikir verse de, bu bilgilerin kesinliğinden söz edilemez. Sebebi ise bu üstverilerin çeşitli tekniklerle değiştirilebilmesinin mümkün olmasıdır.

Ancak bununla birlikte, dijital dosyanın hangi bilgisayarda oluşturulduğunun tespiti hakkında incelenebilecek başka durumlar söz konusudur. Bunun için o dijital dosyanın bilgisayara nasıl geldiği konusunda araştırma yapılabilir. Bilgisayarda tespit edilen elektronik posta kayıtları, anlık mesajlaşma (MSN vb. programlar) yazışmaları gibi dosya transfer programlarının ürettiği bilgiler incelenebilir. Başka bilgisayarda oluşturulduğu düşünülen ya da analiz edilmek istenen dosyalar için, bu dosyaların metaveri bölümlerinde bulunan bilgiler ile dosyanın transfer yoluyla gönderildiğinden şüphelenilen bilgisayarın kullanıcı bilgileri karşılaştırılabilir. Bu bilgiler, o dosyaların üstverilerinde bulunan *Yazar(Author), Son Değiştiren Kullanıcı (Last Modified By)* vb. gibi bilgiler olabilir. Bunun yanı sıra; elektronik imza ve mobil imza gibi ıslak imza yerine kullanılabilen teknolojilerle imzalanmış elektronik postaların kullanılmasının tespiti durumunda, dijital dosyaların hangi bilgisayarda oluşturulduğu ve iletildiği hakkında daha kesin ifadelerle yorum yapılabilir. Ayrıca, tespit edilen dijital dosyaların, o bilgisayarda kurulu olan ve o dijital dosyayı açmak için ilişkilendirilen programla olan uyumuna da bakılabilir. Sözgelimi Microsoft Word metin editörü programına ait bir dosyanın üstverileri 2007 versiyonuna aitse, ancak bilgisayarda kurulu olan Microsoft Office'in versiyonu 2010 olarak tespit edilmişse, o dijital verinin başka bir bilgisayarda oluşturulduğu düşünülebilir. Ancak aksi bir durumun olabileceği, o bilgisayar kullanıcısının daha önce Microsoft Office 2007 kullanarak o dosyayı oluşturduğu ihtimali de değerlendirilmelidir. İşte bu ve buna benzer veri analizleri ile, dijital dosyaların oluşturulması için hangi bilgisayarların kullanıldığı hakkında fikir sahibi olunabilir.

Dijital dosyaların kim tarafından ve hangi bilgisayarda oluşturulduğunun tespiti, yukarıda izahı yapıldığı üzere çeşitli analizler ve araştırmaların sonucunda yorumlanabilir. Ancak bu değerlendirmeler, bilişim teknolojilerinin yapısı gereği kesinlik ifadeleriyle yapılamaz. Tespit edilen bir dijital dosyanın o bilgisayarda üretildiği hakkında kesin bir ifade kullanılamadığı gibi, başka bir bilgisayarda oluşturulup o bilgisayara taşındığı konusunda da kesin bir ifadeyle yorum yapılamaz. İnceleme ve analizler, sınırlı sayıda dijital dosya analizinden ziyade kişi veya kişilerin kullandığı bütün bilgisayarlar değerlendirilerek yapılırsa bu konuda daha net ifadelerle yorum yapılabilir.

Soru 5.)

Ek-1 listede belirtilen dijital dosyaların, her biri için ayrı ayrı olarak belirtilmesi sureti ile, kullanıcı bilgilerinin belirtilmesi, dosyaların hangi bilgisayarda oluşturulduğu, imajı alınan bilgisayarda oluşturulup oluşturulmadığı, dosyalara ait oluşturulma, değiştirilme, ulaşılma tarih bilgilerinin neler olduğu, başka bir bilgisayarda oluşturulup imajı alınan bilgisayara kopyalanıp kopyalanmadığı, tarih açısından uyumsuzluk ve çelişki bulunup bulunmadığı, virüs, trojen vb. gibi zararlı yazılımlarla oluşturulup oluşturulmadığının ayrıntılı bir şekilde açıklanması?

Cevap 5.)

EK-1 listede belirtilen dijital dosyaların, müzekkere ekinde teslim edilen hard disk imajlarından elde edilen bilgileri bu bölümde ayrıntılı olarak incelenmiştir. Bu bilgiler soruda belirtilen "kullanıcı bilgileri, oluşturulma, değiştirilme ve erişim tarihleri" başlıklarını içermektedir. Tespit edilen tarih verilerinden hareketle, dosyalarda herhangi bir uyumsuzluk olup olmadığı da yorumlanmıştır.

Dosyaların hangi bilgisayarda kim tarafından oluşturulduğu ve kime ait olduğu ile ilgili değerlendirmeler cevap 3 ve cevap 4'te verilmiştir. Ek-1 listede bulunan ve aşağıda sıralanan her bir dosya için; işletim sistemi ve dosya sistemi üzerindeki izler, dosya üstveri tutarlılığı, dosya sistemi üstveri tutarlılığı incelenmiş ve raporlanmıştır. Cevap 12'de ilgili imajlarda zararlı yazılımların olası etkileri incelenmiştir. Bu değerlendirmeler ve incelemeler sonucunda ek-1 listede belirtilen dosyaların imajı alınan bilgisayarda oluşturulmuş olma ihtimali veya nasıl ilgili bilgisayarlara gelmiş olabileceği hakkındaki tespitlerimiz her dosya için ayrı ayrı belirtilmiştir.

EK-1 dosyaların **$MFT** kayıtlarından ve **Belge Üstverileri'**nden alınan verilere ilişkin açıklamalar aşağıda yer almaktadır. EK-1 dosya listesi için yazılan ve yine aşağıda sıralanan raporlar incelenirken bu açıklamalardan faydalanmak yerinde olacaktır.

Belge Üstverileri: Bu başlık altında ilgili dosyaya ilişkin üstverilere ait bilgiler bulunmaktadır. Belge Üstverileri, incelenmek istenen dosyanın diskteki konumu tespit edilerek ortaya çıkarılır. Bu alandaki veriler, dosyanın içerik bilgisiyle birlikte tutulur ve dosya tipine özel olarak çeşitlenebilir. Örnek vermek gerekirse; Microsoft Office Word uygulamasına ait bir dosyanın üstverilerinde *Yazar*, *Yönetici*, *Karakter Sayısı* vb. uygulamaya özgü veriler tutulurken, çalıştırılabilir EXE tipinde bir dosya için *makine tipi* ve *Dosya İşletim Sistemi* üstverileri tutulmaktadır. Benzer şekilde PDF tipinde bir dosya için de, *PDF Oluşturma Tarihi* verisi ayrıca tutulmaktadır.

EK-1 dosya listesindeki veriler Office Word, Office Excel ve PDF tiplerinde olduğu için, dosya üstverilerinde bu uygulamalara ilişkin bilgiler bulunmaktadır.

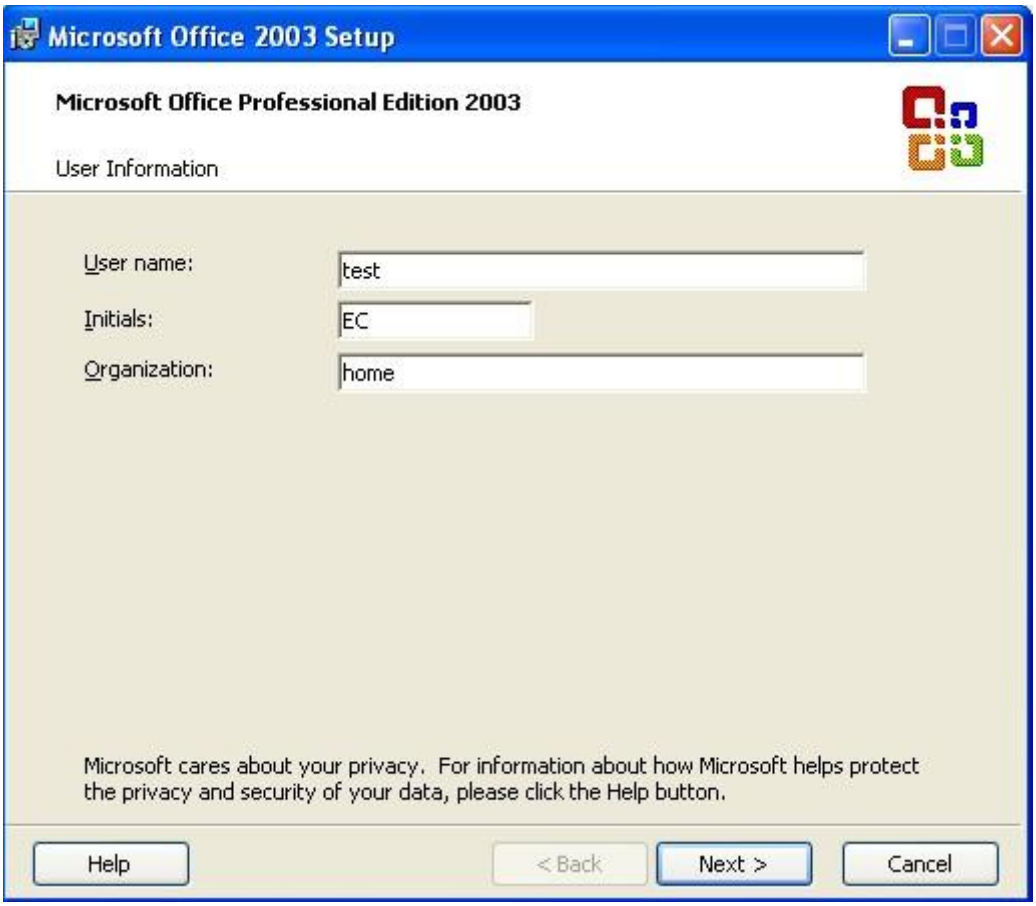
Dosya Adı (FileName): Dosya adı bilgisini içerir.

Dosya Konumu (FileLocation): Dosyanın hangi konumda bulunduğu bilgisinin içerir.

Dosya Durumu (State): Dosyanın kullanıcı tarafından silinip silinmediği bilgisini verir. Bir dosyanın kullanıcı tarafından silinmiş olması, o dosyanın diskte bulunamayacağı veya ortaya çıkarılamayacağı anlamına gelmez. Bu bilgilere çeşitli profesyonel araçlarla ulaşılabilir. Ancak silinmiş olan dosyalar, disk üzerinde zaman içinde tahrifata uğrayabilir. Bilgisayarda bulunan işletim sistemi, zaman içinde bu silinmiş verilerin olduğu disk bölümünün bir kısmının üzerine başka veriler yazabilir. Bu durumda dosyanın bir kısmı veya tamamı geri döndürülemez hale gelebilmektedir.

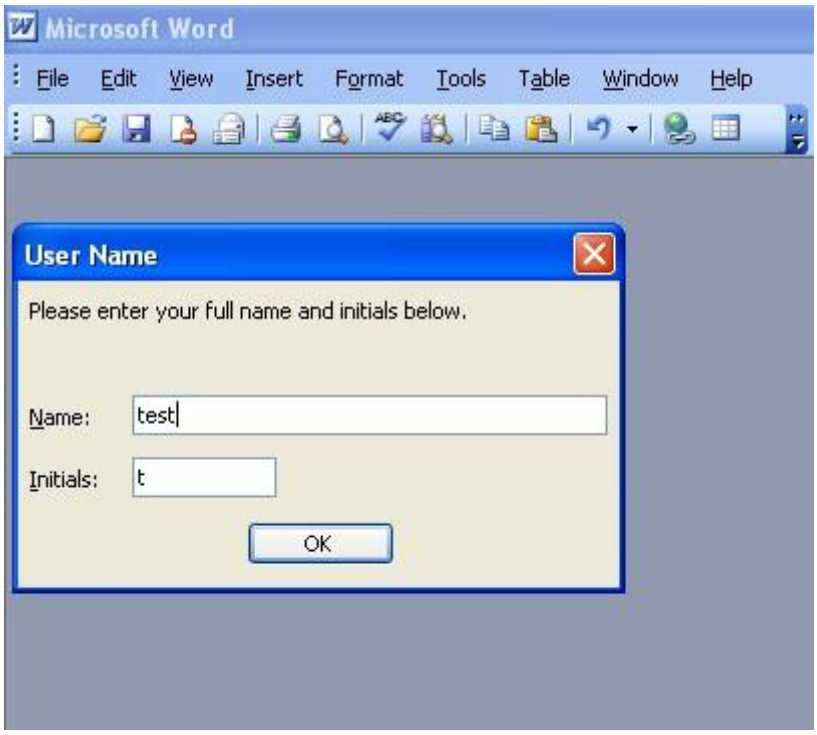
EK-1 listede verilen ve aşağıdaki gibi sıralanan dosyaların bir kısmı silinmemiş halde tespit edilmiştir. Bir diğer kısmı silinmiş, bu silinenlerin bir kısmı da ciddi tahrifata uğramıştır. Ancak bütün olarak okunamayacak şekilde tahrifata uğramış bile olsa, ilgili dosyaların bir kısmı okunabilir ve ortaya çıkarılabilir. Bu durum bu gibi dosyalar için detaylı şekilde açıklanmıştır.

Yazar (Author): Yazar verisi, Microsoft Office dokümanlarında saklanan üstverilerden biridir. Dosyanın ilk oluşturulduğu bilgisayarda, Office uygulamasının yazar bilgisini verir. Microsoft Office uygulaması, kurulum esnasında kullanıcıdan yazar bilgisi ister. Bu bilgi öntanımlı olarak o bilgisayardaki işletim sistemi kullanıcısı olarak gelir. Kullanıcı başka bir veri girerek değiştirmezse yazar bilgisi kullanıcı adı ile aynı olur. Konuyla ilgili ekran kopyası için Şekil 13 - Office Kurulumu Kullanıcı Metaverileri incelenebilir. İşletim sistemi kullanıcısı “test” olan kullanıcı için, “username” alanı da test olarak gelmiştir.



Şekil 13 - Office Kurulumu Kullanıcı Metaverileri

Office uygulamasının kurulumu esnasında bu değerler girilmezse, kurulum sonrası açılacak ilk Office uygulamasında bu değerler tekrar sorulacaktır. Bilgisayarda yeni bir kullanıcı oluşturulduğunda, o kullanıcının açacağı ilk Office uygulamasında da aynı pencere gelecektir. Bu penceredeki veriler de silinse ve hiçbir kullanıcı adı girilmese bile, Office uygulaması işletim sistemi kullanıcısını "Yazar" olarak kaydedecektir. İlgili ekran kopyası Şekil 14 - Office İlk Açıldığında İstenen Verilerde görülmektedir.



Şekil 14 - Office İlk Açıldığında İstenen Veriler

Yazar bilgisi ve altta sıralanan diğer Office üstverileriyle ilgili üretici firma Microsoft'un yayımladığı makale için referanstaki bağlantı incelenebilir.[11]

Son Değiştiren Kullanıcı (LastModifiedBy): Dosyayı en son değiştiren kullanıcının adını verir. Bu veri, dosyanın son değiştirildiği bilgisayardaki Office uygulamasının "yazar" verisidir. Office uygulamasının kurulumu esnasında değiştirilmediği müddetçe, yazar bilgisi işletim sistemi kullanıcısı ile aynı olmaktadır.

Yönetici (Manager): Dosyaya ilişkin yönetici kullanıcı adının verir.

Şirket (Company): Dosyaya ilişkin şirket verisini gösterir. Bu bilgi Office uygulamasının kurulumu esnasında belirlenmektedir. Kullanıcının girdiği değer şirket verisi olmaktadır. Konuyla ilgili ekran kopyası için Şekil 13 - Office Kurulumu Kullanıcı Metaverileri incelenebilir.

Nesne Tipi (CompObjUserType): Dosyanın tipini gösterir.

Yazılım Tipi (Software): Office uygulamasında dosyanın oluşturulduğu uygulumanın versiyonu hakkında bilgi verir.

Karakter Tipi (CodePage): Dosyanın hangi karakter tipi kullanılarak oluşturulduğunu belirtir.

[11] http://office.microsoft.com/en-us/help/inspect-documents-for-hidden-data-and-personal-information-HA010074435.aspx

Karakter Sayısı (CharCountWithSpaces): Dosyanın kaç karakterden oluştuğunun sayısını verir.

Uygulama Versiyonu (AppVersion): Üretici firmanın verdiği uygulama versiyon seri numarasını gösterir.

Dosya Boyutu (FileSize): Dosyanın disk üzerinde kapladığı alanı belirtir.

Toplam Değiştirme Süresi (TotalEditTime): Dosyanın ne kadar süre değişikliğe uğradığını gösterir. Kullanıcının dosyayı açık tuttuğu sürelerin toplamıyla hesaplanır.

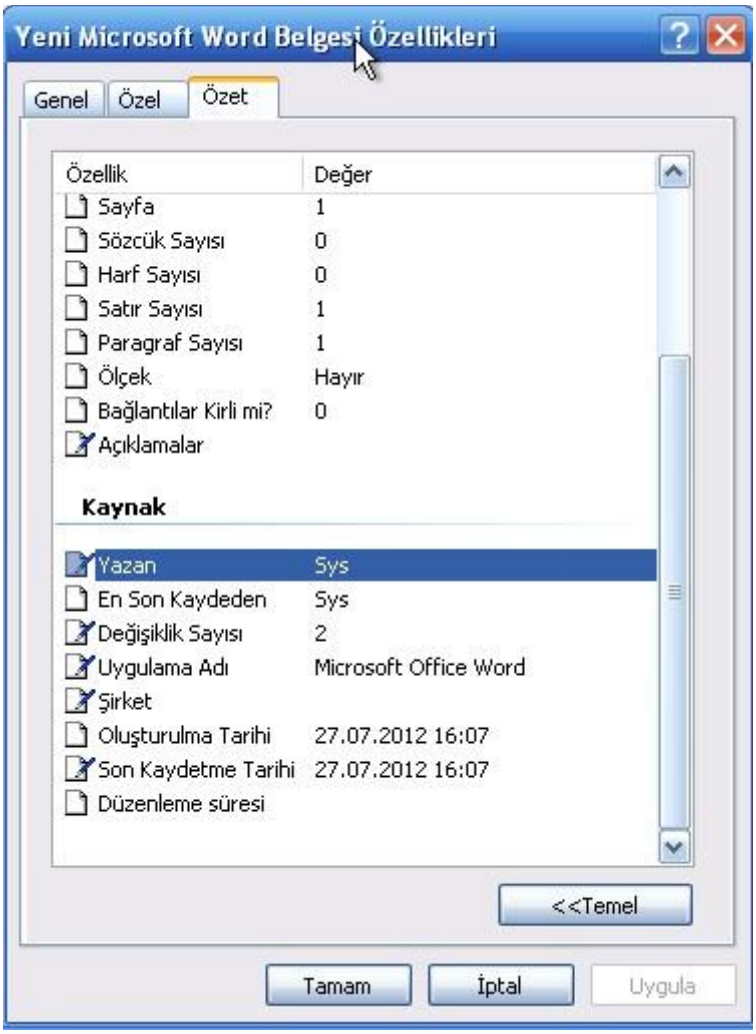
Revizyon Numarası (RevisionNumber): Dosyanın kaç kez açılıp değişiklik yapılarak ve kaydedilerek kapatıldığını gösterir.

Belge Oluşturma Tarihi (CreateDate): Belgenin oluşturulduğu tarihi gösterir.

Belge Değiştirme Tarihi (ModifyDate): Belgenin en son değiştirildiği tarihi gösterir.

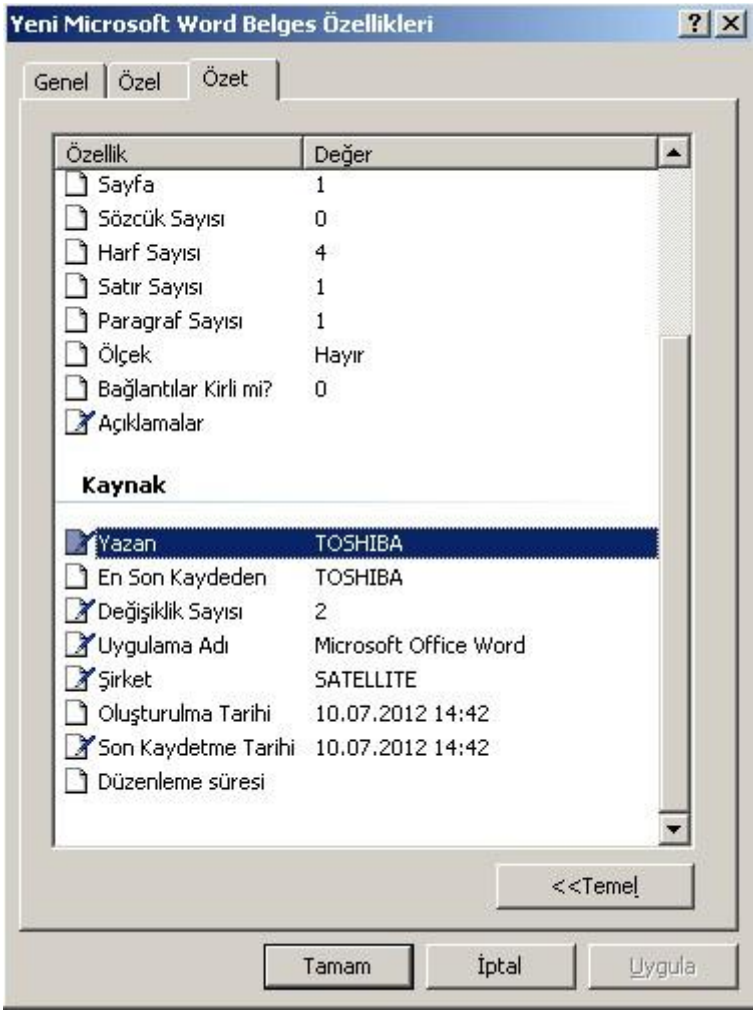
EK-1 dosya listesini yukarıdaki veriler ışığında yorumlarken, adli analizi yapılan imajlarda Office dosya metaverilerinin öntanımlı olarak hangi kullanıcı isimleriyle saklandığı incelenebilir.

ST3120927AS_4MS1TF89 seri numaralı imajda yeni bir office dosyası oluşturulduğunda kullanıcı verileri aşağıdaki gibi olmaktadır.



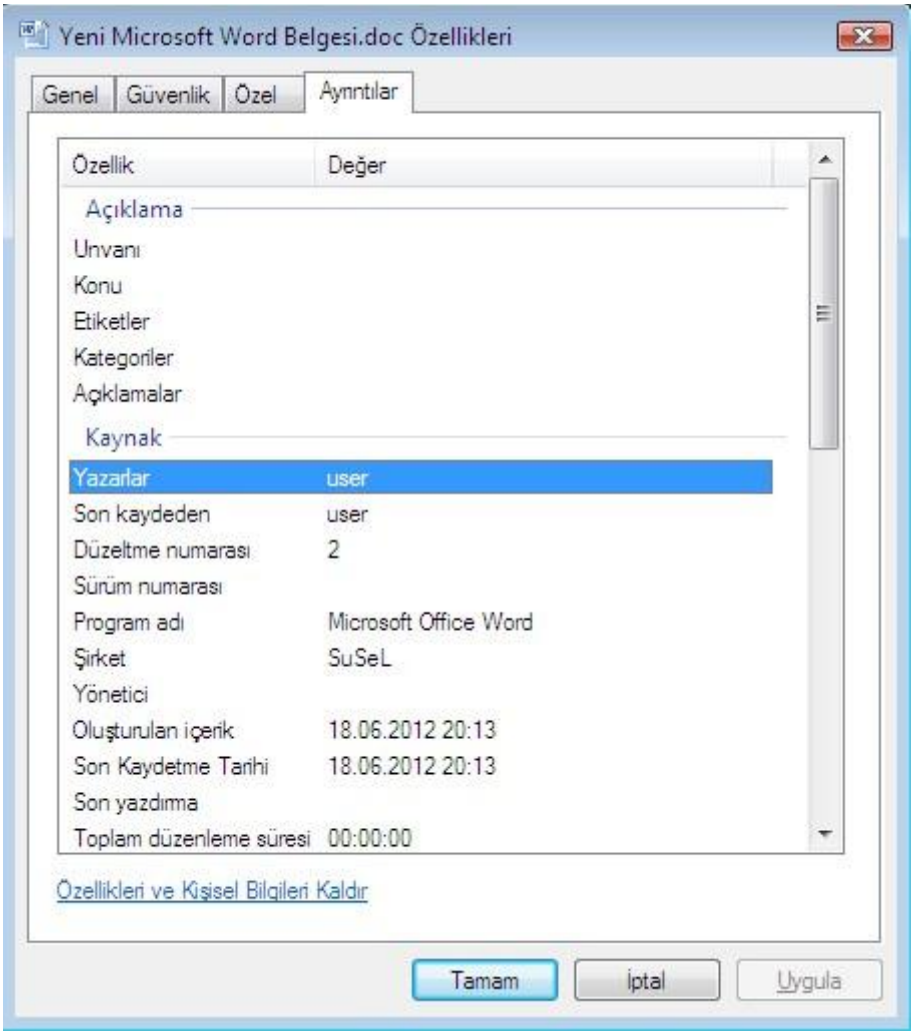
Şekil 15 - ST3120927AS_4MS1TF89 Seri Numaralı ODATV İmajı Office Üstverileri

MHV2060BH_NW18T6229459 seri numaralı imajda yeni bir office dosyası oluşturulduğunda kullanıcı verileri aşağıdaki gibi olmaktadır.



Şekil 16 - MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN İmajı Office Üstverileri

S17HJ90Q816726 seri numaralı imajda yeni bir office dosyası oluşturulduğunda kullanıcı verileri aşağıdaki gibi olmaktadır.



Şekil 17 - S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur İmajı Office Üstverileri

Dosya Sistemi Zaman Üstverileri: Dosya sistemi üstverileri ve bu verilerin tutulduğu MFT (Master File Table); bir bilgisayarda bulunan bütün dosyaların o bilgisayardaki ilgili diskin hangi bölümünde yer aldığını, boyutunun ne kadar olduğunu, dosyanın oluşturulma, değiştirilme, erişim ve kayıt değiştirme zamanlarının ne olduğunu verisini ihtiva eder. Tutulan bu üstverilerin Microsoft işletim sistemi üretici firması tarafından nasıl açıklandığı detaylı incelemek için ilgili referans incelenebilir.[12]

Talep kapsamında incelememiz istenilen ek-1 listesindeki bütün dosyalara ait tarih verileri, bu başlık altında incelenmiştir.

Std Oluşturma Zamanı: "Standart Information" üstveri bölümünden elde edilen dosya oluşturulma zamanını gösterir.

[12] http://msdn.microsoft.com/en-us/library/bb470206%28v=vs.85%29.aspx

Std Değiştirme Zamanı: "Standart Information" üstveri bölümünden elde edilen dosya değiştirilme zamanını gösterir.

Std Erişim Zamanı: "Standart Information" üstveri bölümünden elde edilen dosya erişim zamanını gösterir.

Std MFT Kaydı Değişim Zamanı: "Standart Information" üstveri bölümünden elde edilen dosya MFT kaydı değişim zamanını gösterir.

FN Oluşturma Zamanı: "Filename" üstveri bölümünden elde edilen dosya oluşturulma zamanını gösterir.

FN Değiştirme Zamanı: "Filename" üstveri bölümünden elde edilen dosya değiştirilme zamanını gösterir.

FN Erişim Zamanı: "Filename" üstveri bölümünden elde edilen dosya erişim zamanını gösterir.

FN MFT Kaydı Değişim Zamanı: "Filename" üstveri bölümünden elde edilen dosya MFT kaydı değişim zamanını gösterir.

Yukarıda açıklanan zaman tarih verilerinin yorumlanmasına geçmeden önce, mahkeme tarafından teslim edilmiş olan ilgili disklerdeki **NTFS** dosya sisteminin tarih verilerini nasıl kaydettiğini incelemekte fayda bulunmaktadır.

NTFS dosya sistemiyle ilgili bilgi almak için aşağıda verilen bağlantı incelenebilir.[13] NTFS dosya sistemi, dosyaların zaman tarih bilgilerini çeşitli kurallara göre günceller ve bu güncellemeler sonrasında dosya **Oluşturma Tarihi, Değiştirme Tarihi, Erişim Tarihi sıralaması değişebilir.** Bu tarihler sıralı olmak zorunda değildir.

Bu nedenle bilgisayarda normal bir kullanıcı davranışıyla oluşturulan bir dosyanın **değiştirme tarihi, oluşturma tarihinden önce olabilir.** Örnek vermek gerekirse, NTFS dosya sistemi bulunan bir bilgisayarda oluşturduğumuz bir dosyayı, başka bir klasöre kopyaladığımızda oluşturma tarihi, kopyalama işlemini yaptığımız tarih olacaktır. Ancak değiştirme tarihi, dosyayı ilk değiştirdiğimiz tarih olarak kalır. Bu işlem dizisine göre değiştirme tarihi, oluşturma tarihinden önce görünecektir. $MFT tablosunda dosyaların ne zaman ve ne şekilde güncellendiği konusunda aşağıdaki tablo yol gösterici olacaktır.[14]

[13] http://computer-forensics.sans.org/blog/2009/12/18/ntfs-an-introduction/
[14] http://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf

Müzekkere ekinde teslim edilen EK-1 dosyasındaki verilerin oluşturma-değiştirme-erişim tarihleri yorumlanırken bu verilerden hareket edilebilir.

Windows NTFS Zaman Kuralları								
$STDINFO								
Zamanlar	Dosya İsim Değişikliği	Yerel Dosya Taşıma	Bölüm Dosya Taşıma	Dosya Kopyalama	Dosya Erişim	Dosya Değiştirme	Dosya Oluşturma	Dosya Silme
Değiştirme Zamanı						Değişir	Değişir	
Erişim Zamanı			Değişir	Değişir	Değişir (XP)		Değişir	
Oluşturma Zamanı		*		Değişir			Değişir	
MFT Kaydı Değişim Zamanı	Değişir	Değişir	Değişir	Değişir	Değişir (her zaman değil)	Değişir (her zaman değil)	Değişir	*
$FILENAME								
Zamanlar	Dosya İsim Değişikliği	Yerel Dosya Taşıma	Bölüm Dosya Taşıma	Dosya Kopyalama	Dosya Erişim	Dosya Değiştirme	Dosya	Dosya Silme
Değiştirme Zamanı	*	Değişir	Değişir (XP)	Değişir			Değişir	*
Erişim Zamanı	*		Değişir	Değişir			Değişir	
Oluşturma Zamanı	*		Değişir (XP)	Değişir			Değişir	
MFT Kaydı Değişim	*	Değişir	Değişir (XP)	Değişir			Değişir	*
*	Değişip değişmediği test edilmesi gerekir							

Şekil 18 - Windows NTFS Zaman Değişim Kuralları

Dosyaların zaman tarih bilgileri yorumlanırken dikkat edilmesi gereken diğer bir konu zaman dilimleridir. Türkiye UTC/GMT +2 saat diliminde yer alır. Bu nedenle yerel saat UTC(Coordinated Universal Time)'ye göre 2 saat ileridedir. Yaz saati uygulaması nedeniyle yaz aylarında bu zaman farkı +3 saate çıkmaktadır. Kış aylarında tekrar +2 olmaktadır.

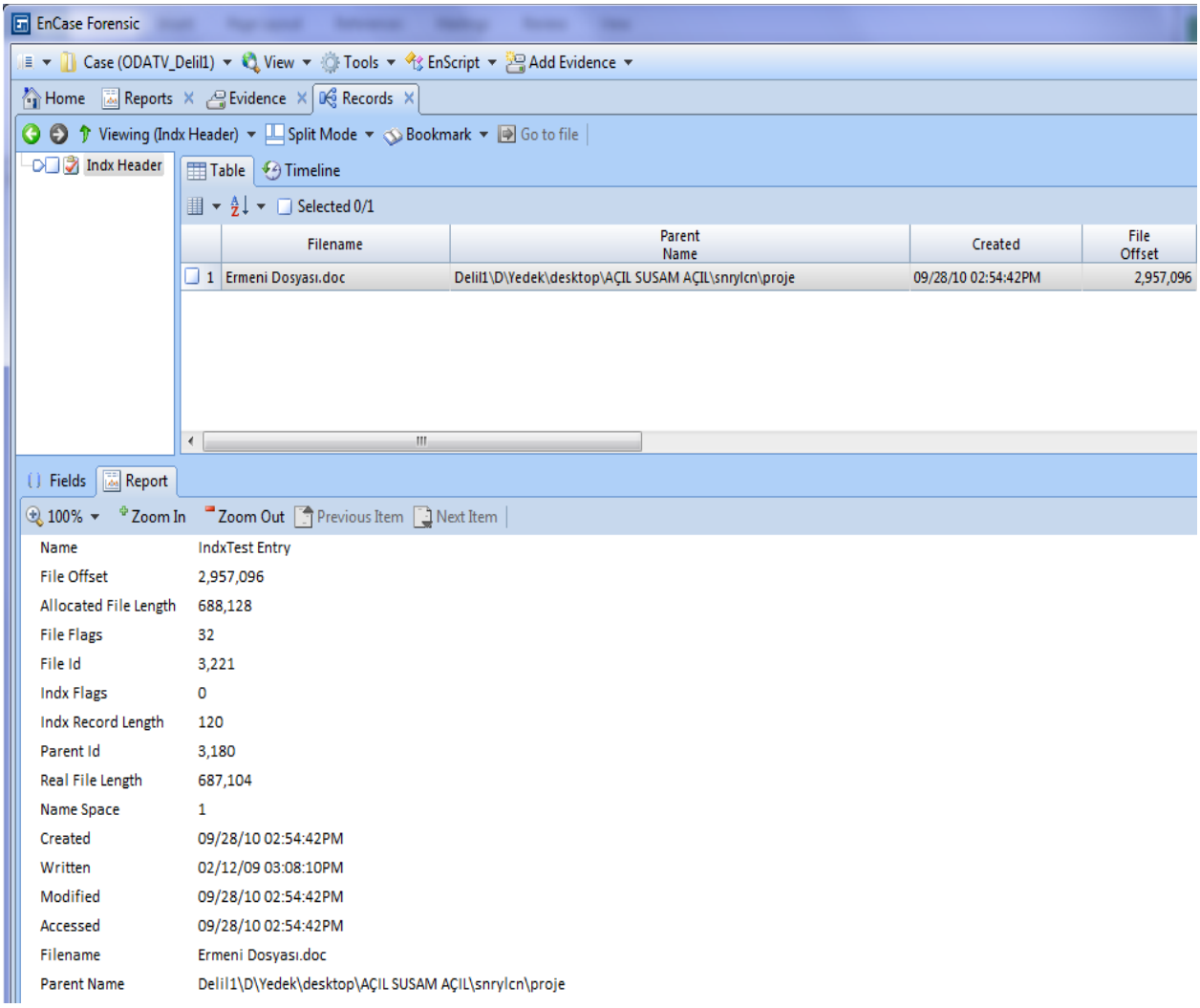
Bilgisayarlar yerel saatlerini bu hesaplamayla ayarlayarak kullanıcıya gösterir. Ancak dosya sistemi, saat bilgilerini UTC'ye göre tutmaktadır. Bazı adli analiz araçları UTC'ye göre rapor oluştururken, bazıları yerel saati hesaplayarak rapor oluşturur. Bu nedenle adli analiz araçlarından çıkan veriler yerel saat zaman farkı dikkate alınmadan yorumlanırsa, işlemin yapıldığı Türkiye saatine göre 2-3 saatlik bir farklılık oluşabilmektedir. Dava kapsamında çalışma yapan bazı bilirkişilerin raporları arasındaki birkaç saatlik zaman farkının nedeni budur. Dikkat edilirse bu fark saat hanesinde bulunmaktadır, dakika ve saniye haneleri aynıdır. Raporumuzda EK-1 listedeki dosyalar için hazırlanmış olan tablolarda bulunan veriler UTC'ye göre raporlanmıştır. Bununla birlikte, Encase gibi bazı dijital adli analiz araçları ve Windows işletim sisteminin saatini referans alarak çalışan diğer bazı uygulamalar yerel saate göre çıktı üretmektedir. Dolayısıyla raporda yer alan Encase vb. uygulamalara ait çıktılarda görünen saat verisiyle dosya üstverilerinin bulunduğu tablolar arasında birkaç saatlik fark olabilmektedir, bu durum herhangi bir tutarsızlığı işaret etmez.

1.) Ermeni Dosyası.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	Ermeni Dosyası.doc
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\Ermeni Dosyası.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor.
Yazar	OPEY A.
Son Değiştiren Kullanıcı	OPEY A.
Yönetici	OĞUZTAN
Şirket	STRATEJİ
Nesne Tipi	Microsoft Word Belgesi
Yazılım Tipi	Microsoft Word 8.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	274519
Uygulama Versiyonu	8.3814
Dosya Boyutu	672 KB
Toplam Değiştirme Süresi	8.1 saat
Revizyon Numarası	271
Belge Oluşturma Tarihi	
Belge Değiştirme Tarihi	
Dosya Sistemi Tarih Üstverileri	
Std Info Oluşturma Tarihi	2010-09-28 11:54:42.453125
FN Oluşturma Zamanı	2010-09-28 11:54:42.453125
Std Info Değiştirme Tarihi	2009-02-12 13:08:10
FN Değiştirme Zamanı	2010-09-28 11:54:42.453125
Std Info Erişim Tarihi	2010-09-28 11:54:42.500000
FN Info Erişim Tarihi	2010-09-28 11:54:42.453125
Std Info Giriş Tarihi	2010-09-28 11:54:42.500000
FN Info Giriş Tarihi	2010-09-28 11:54:42.453125

İlgili dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (Index Artifact) kayıtlarında da rastlanılmıştır.



Şekil 19 - Ermeni Dosyası.doc Dosyasına Ait Logfile (Index Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

"Ermeni Dosyası.doc" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış

olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

Ancak bununla beraber silinmiş durumunda olan ve bu sebeple ne dosyası olduğu anlaşılamayan, açılmış bir internet sitesi ya da okunmuş bir dokümanda bu dosyanın ismi geçmektedir. Dosya isminin disk üzerindeki aramalarda bu şekilde bir doküman ya da internet geçmişinde çıkmış olması, bu dosyanın bu disk üzerinde bulunduğuna dair net bir bilgi vermemektedir.

Dosya isminin geçtiği cluster ve sektör adresleri aşağıdaki gibidir:

CL 13247262 SO 254, CL 13247874 SO 194, CL 13247858 SO 224, CL 526246 SO 194, CL 526230 SO 224, CL 525634 SO 254, CL 14538942 SO 254, CL 14539538 SO 224, CL 14539554 SO 194

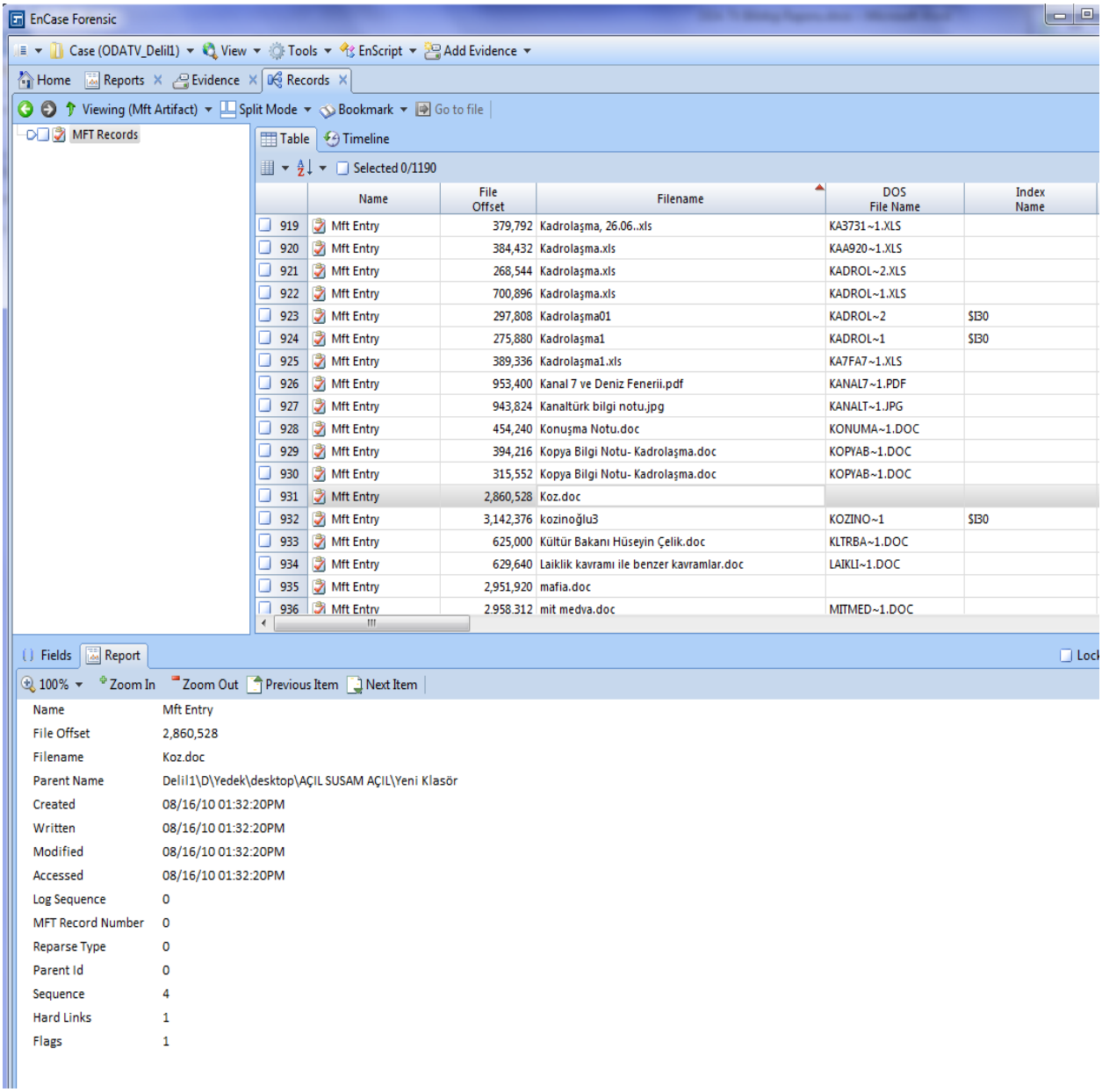
2.) Koz.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	Koz.doc
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\Koz.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor.
Yazar	soner
Son Değiştiren Kullanıcı	soner
Yönetici	
Şirket	Conqueror
Nesne Tipi	Microsoft Word Document
Yazılım Tipi	Microsoft Word 10.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	178
Uygulama Versiyonu	10,2605
Dosya Boyutu	24 kB
Toplam Değiştirme Süresi	1.0 dakika
Revizyon Numarası	8
Belge Oluşturma Tarihi	2010:08:04 09:48:00
Belge Değiştirme Tarihi	2010:08:04 09:49:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-08-16 10:32:20.031248
FN Oluşturma Zamanı	2010-08-16 10:32:20.031248
Std Değiştirme Zamanı	2010-08-04 10:49:56
FN Değiştirme Zamanı	2010-08-16 10:32:20.031248
Std Erişim Zamanı	2010-08-16 10:32:20.031248
FN Erişim Zamanı	2010-08-16 10:32:20.031248
Std Giriş Zamanı	2010-08-16 10:32:20.031248
FN Giriş Zamanı	2010-08-16 10:32:20.031248

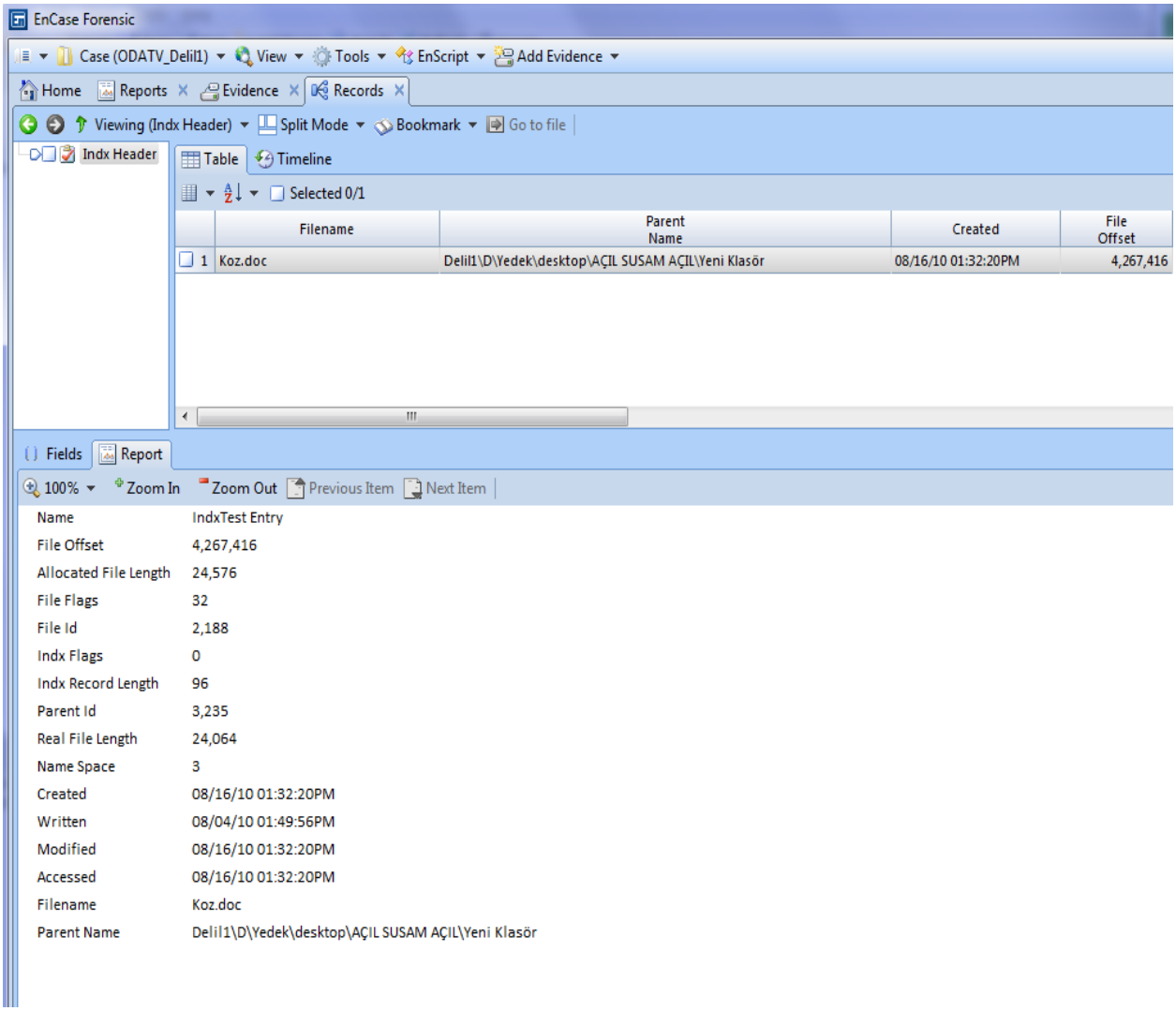
Yapılan incelemelerde diskin Logfile alanında farklı konumlarda bu dosyaya ait kayda rastlanılmıştır. $Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının

oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.



Şekil 20 - Koz.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

İlgili dosyayla ilişkili bir diğer kayıt ise $LogFile (Index Artifact) alanında görülmüştür.



Şekil 21 - Koz.doc Dosyasına Ait Logfile (Index Artifact) Kaydı

$Logfile'da kaydinin olmasi bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

“Koz.doc” dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

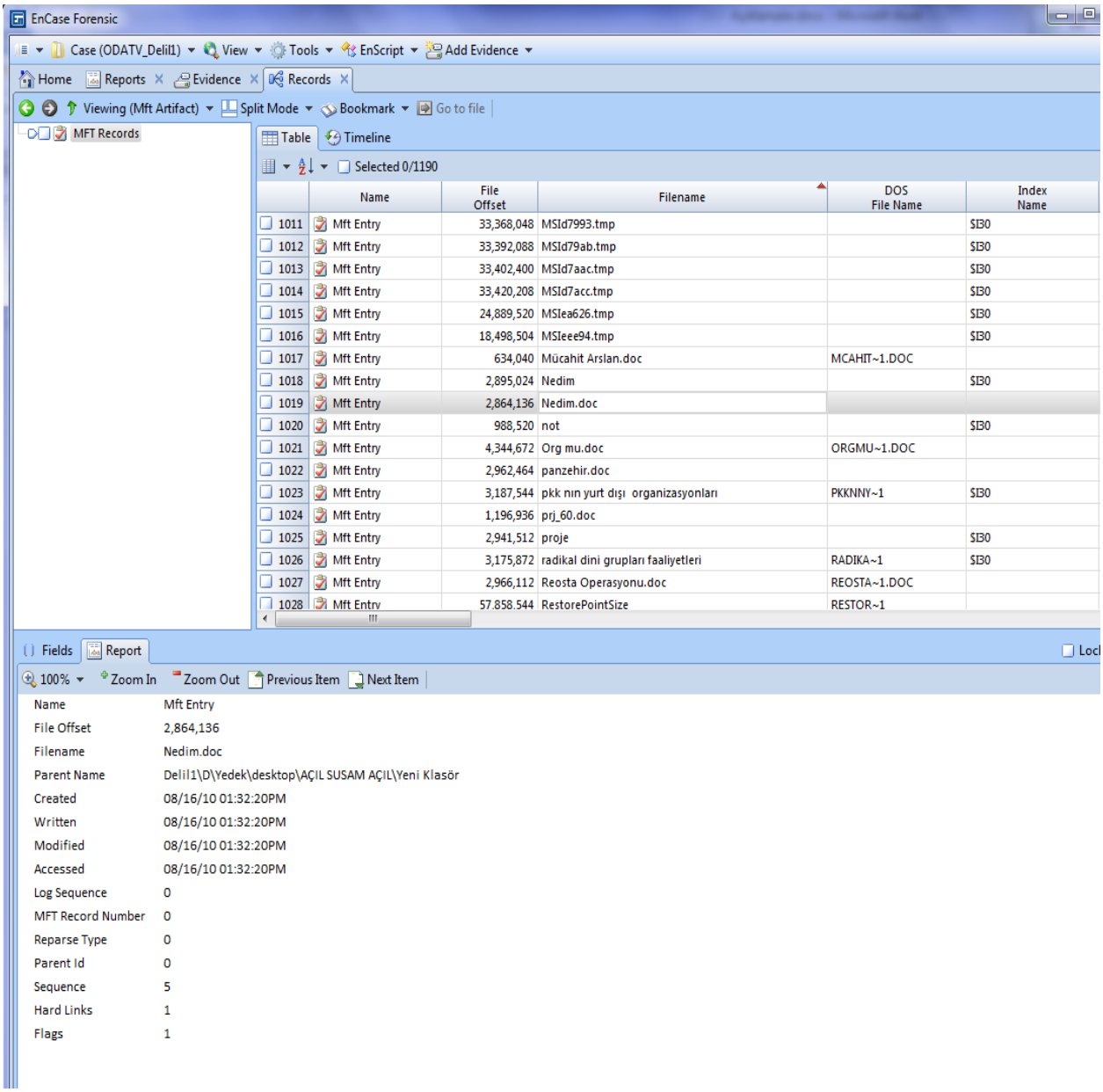
Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

3.) Nedim.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	Nedim.doc
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\Nedim.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor.
Yazar	Soner
Son Değiştiren Kullanıcı	Soner
Yönetici	
Şirket	Conqueror
Nesne Tipi	Microsoft Word Document
Yazılım Tipi	Microsoft Word 10.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	494
Uygulama Versiyonu	10,2605
Dosya Boyutu	24 kB
Toplam Değiştirme Süresi	3.0 dakika
Revizyon Numarası	7
Belge Oluşturma Tarihi	2010:08:09 05:32:00
Belge Değiştirme Tarihi	2010:08:09 05:35:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-08-16 10:32:20.046875
FN Oluşturma Zamanı	2010-08-16 10:32:20.046875
Std Değiştirme Zamanı	2010-08-09 06:35:18
FN Değiştirme Zamanı	2010-08-16 10:32:20.046875
Std Erişim Zamanı	2010-08-16 10:32:20.046875
FN Erişim Zamanı	2010-08-16 10:32:20.046875
Std Giriş Zamanı	2010-08-16 10:32:20.046875
FN Giriş Zamanı	2010-08-16 10:32:20.046875

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (MFT Artifact) kayıtlarında da rastlanılmıştır.



Şekil 22 - Nedim.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

"Nedim.doc" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.

- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

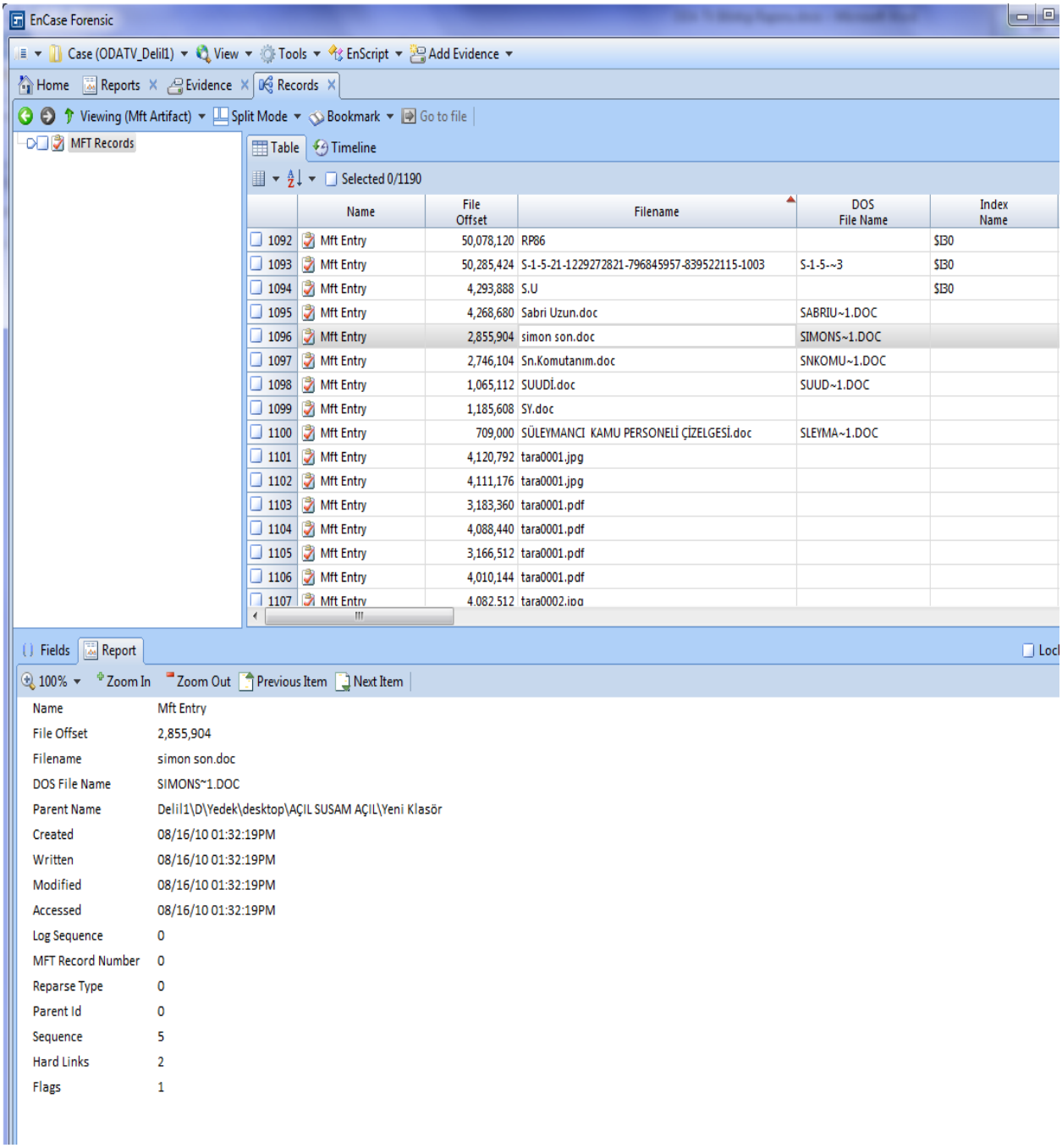
S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

4.) simon son.doc

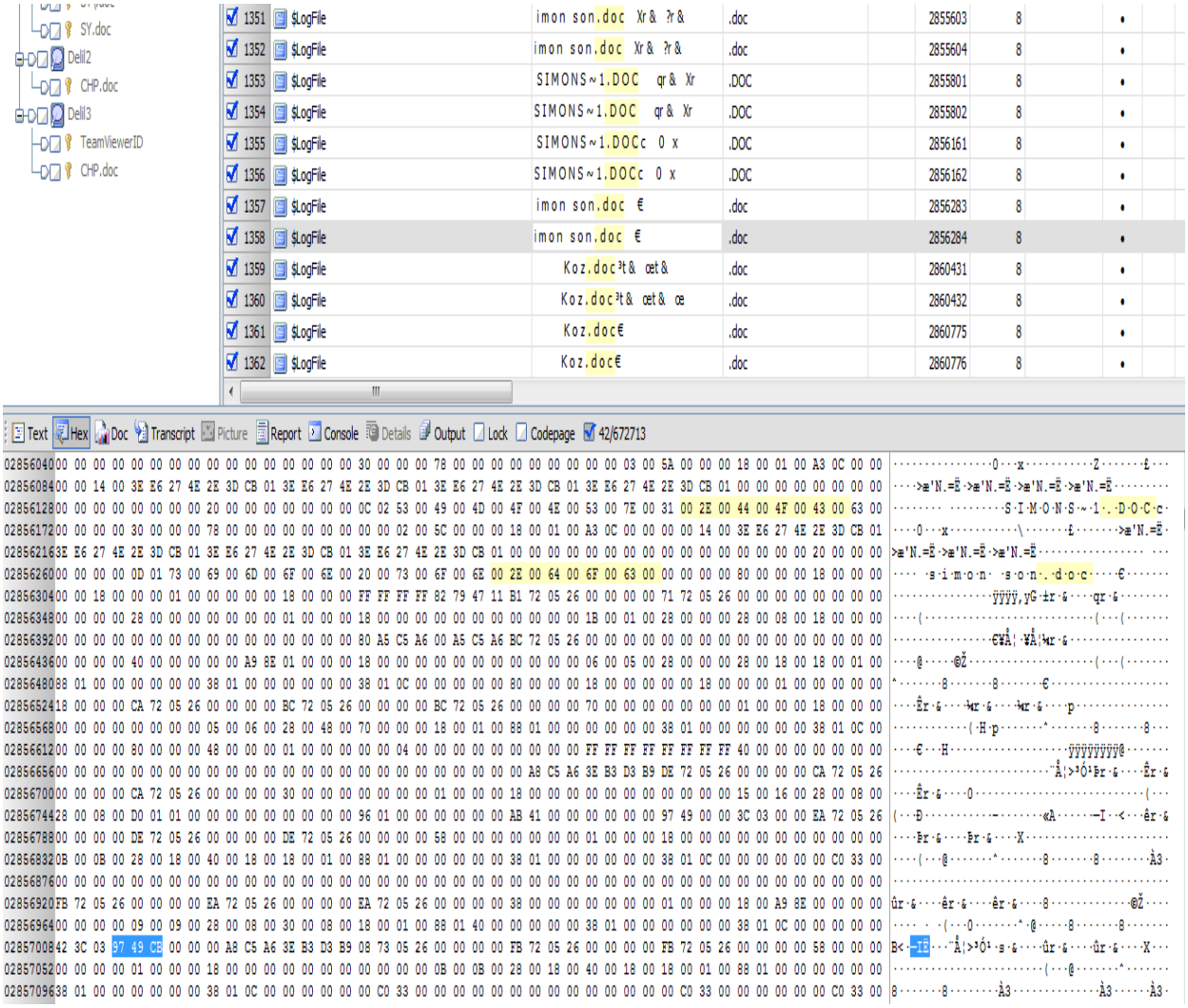
ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

İlgili dosyanın silinmiş olduğu ve $MFT kaydının bulunmadığı tespit edilmiştir. Ancak dosya unallocated clusters alanında tespit edilmiştir ve görüntülenmiştir. İlgili dosyaya ait Logfile alanında kayda rastlanılmıştır. $Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.



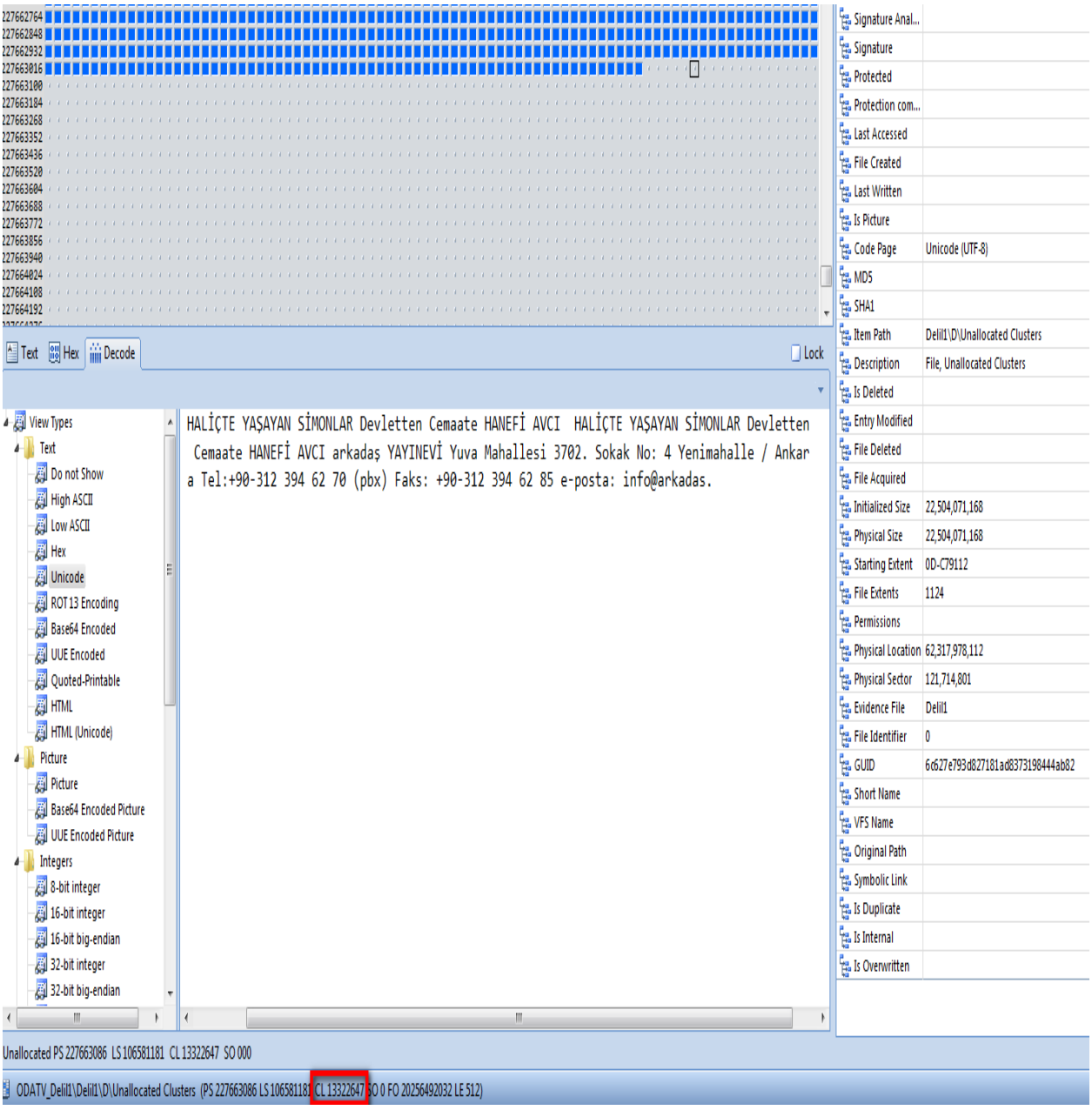
Şekil 23 - simon son.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

Logfile'dan elde edilen değerler kullanılarak dosyanın başlangıç cluster adresi tespit edilmiştir.



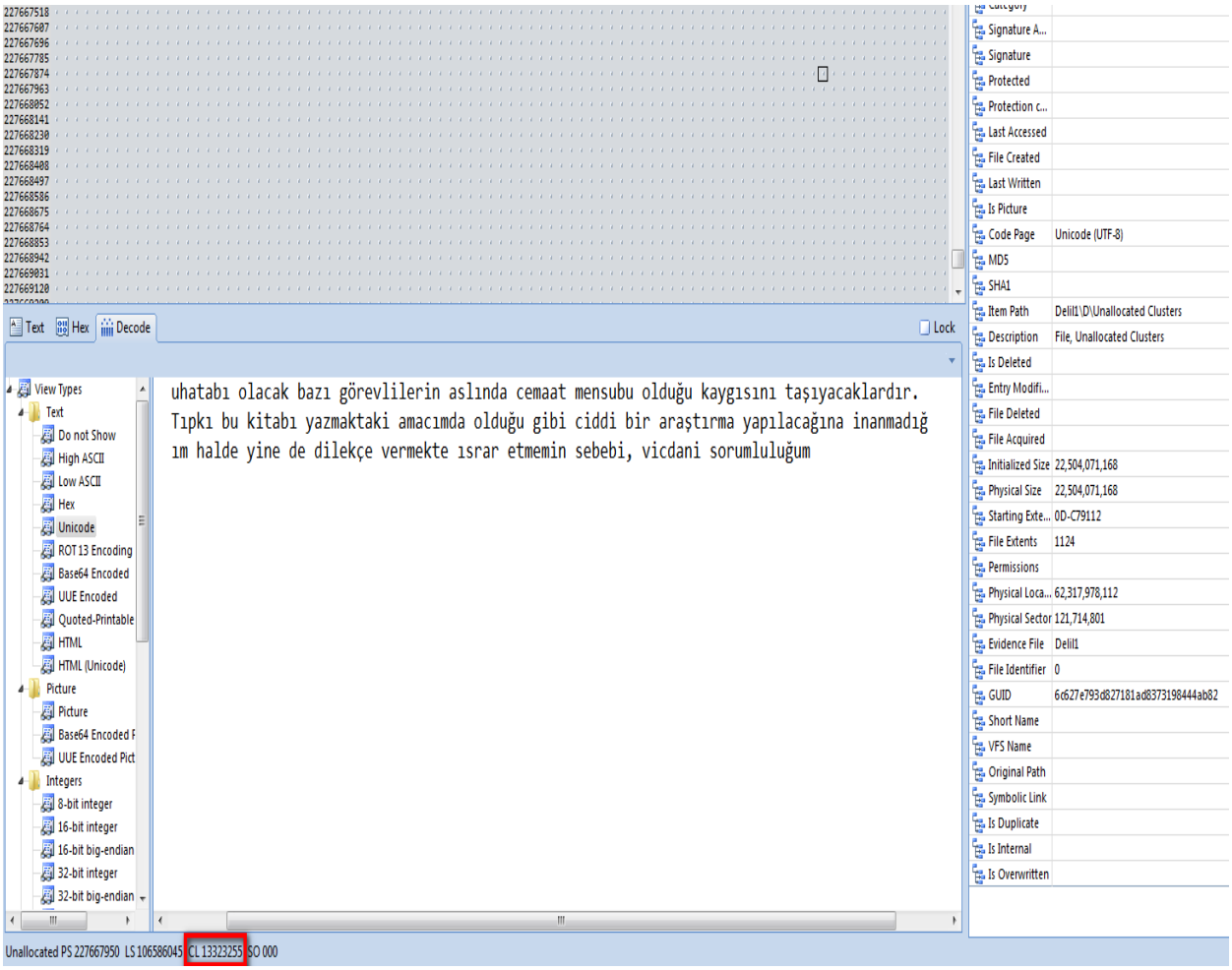
Şekil 24 - simon son.doc dosyasının başlangıç cluster değeri

Başlangıç adresi 9749CB00 olan dosyanın bulunduğu cluster olan 13322647 (10'luk tabanda karşılığı) adresine gidildiğinde aşağıdaki veriler elde edilmiştir.



Şekil 25 - simon son.doc dosyasının silinmiş alanda (unallocated cluster) tespit edilen bölümü -1

Bu sektörden başlayarak toplam 4864 sektörde doküman kalıntıları görüntülenebilmiştir. Tespit edilen son bölüme ait ekran kopyası aşağıdadır.



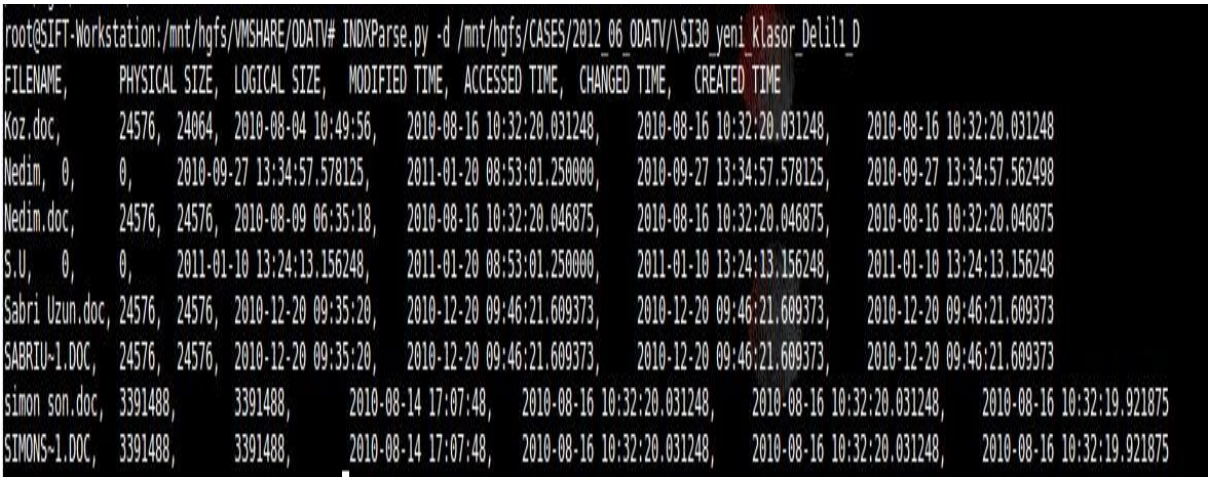
Şekil 26 - simon son.doc dosyasının silinmiş alanda (unallocated cluster) tespit edilen son bölümü

Tespit edilen ve görüntülenebilen simon son.doc dosyasına ait metaverilerden bir kısmı R-Studio[15] adli analiz aracıyla kurtarılabilmiştir. R-Studio, $MFT kaydı silinmiş ancak unallocated clusters alanında bulunmaya devam eden dosyaları metaverileriyle birlikte kurtarabilen bir üründür.

Simon son.doc dosyası ile ilgili ayrıca $I30 Index dosyasında kayda rastlanmıştır. $I30 dosyası, silinmiş veriler için zaman bilgisi başta olmak üzere çeşitli üstverilerin geri dönüşümü için kullanılabilecek sistem dosyalarından biridir.[16] $I30 Index verilerinden elde

[15] http://www.r-studio.com/
[16] http://computer-forensics.sans.org/blog/2011/09/20/ntfs-i30-index-attributes-evidence-of-deleted-and-overwritten-files

edilen zaman tarih bilgileri, Std zamanlarını vermektedir.



Şekil 27 - $I30 Index İle Elde Edilen Veriler

Yukarıda bahsedilen tekniklerle elde edilen metaveriler için alttaki tablo incelenebilir.

Belge Üstverileri	
Dosya Adı	simon son.doc
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\simon son.doc
Dosya Durumu	Silinmiş, $MFT kaydı yok,unallocated clusterda bulunuyor
Yazar	
Son Değiştiren Kullanıcı	
Yönetici	
Şirket	
Nesne Tipi	Microsoft Office Word Belgesi
Yazılım Tipi	Microsoft Word Word
Karakter Tipi	Unicode (UTF-8)
Karakter Sayısı	977727
Uygulama Versiyonu	11.5606
Dosya Boyutu	3.2 MB
Toplam Değiştirme Süresi	
Revizyon Numarası	
Belge Oluşturma Tarihi	2010-08-14 16:05:00
Belge Değiştirme Tarihi	2010-08-14 16:07:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-08-16 10:32:20
FN Oluşturma Zamanı	
Std Değiştirme Zamanı	2010-08-14 17:07:48

FN Değiştirme Zamanı	
Std Erişim Zamanı	2010-08-16 10:32:20
FN Erişim Zamanı	
Std Giriş Zamanı	2010-08-16 10:32:20
FN Giriş Zamanı	

Elde edilen metaverilerden hareketle, bu dosyanın ilk olarak 14 Ağustos 2010 tarihinde oluşturulduğu ve aynı tarihte değiştirildiği görülmüştür. Şekil 23 - simon son.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı ekran kopyasında ve yukarıdaki tabloda bulunan Std zamanlarında görüntülendiği gibi, ilgili dosya 16 Ağustos 2010 tarihinde de dosya sistemi metaverilerine yansımıştır. Bu durum dosyanın o tarihte işlem gördüğüne işaret eden bir durumdur.

"simon son.doc" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydına ulaşılamadığından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılamamaktadır. Fakat "dizin girdileri" analizi yapılarak bu dosyanın silinmeden önce bulunduğu dizinin "index" girdilerinden dosya sistemi zaman bilgilerinden bir kısmına ulaşılabilmiştir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD

dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

5.) ABDULKADIR AYGAN.pdf

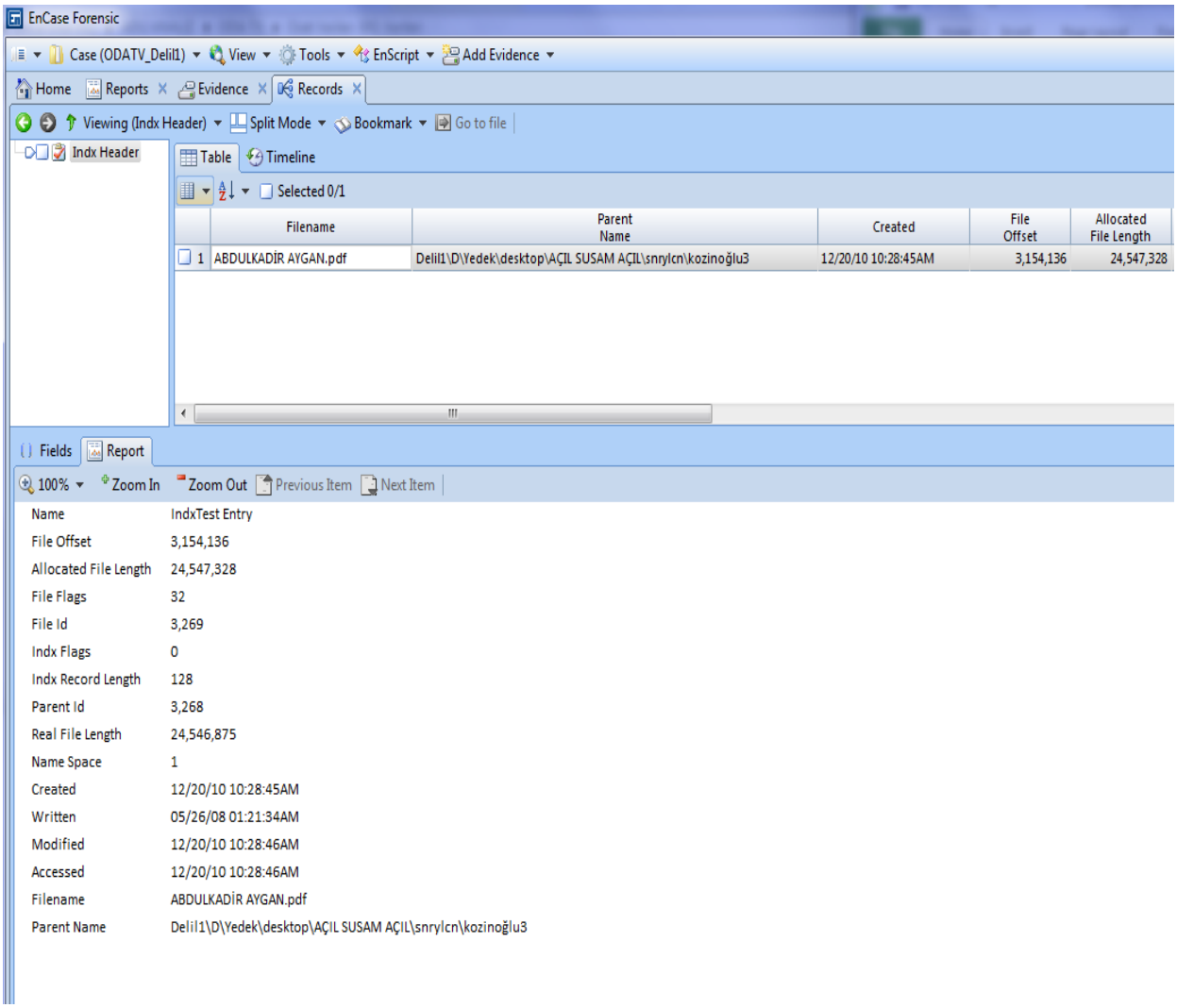
ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	ABDULKADIR AYGAN.pdf
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\kozinoğlu3\ABDULKADİR AYGAN.pdf
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor
Yazar	
Son Değiştiren Kullanıcı	
Yönetici	
Şirket	
Nesne Tipi	
Yazılım Tipi	
Karakter Tipi	
Karakter Sayısı	
Uygulama Versiyonu	
Dosya Boyutu	23 MB
Toplam Değiştirme Süresi	
Revizyon Numarası	
Belge Oluşturma Tarihi	
Belge Değiştirme Tarihi	

Dosya Sistemi Tarih Üstverileri

Std Oluşturma Zamanı	2010-12-20 08:28:45.281248
FN Oluşturma Zamanı	2010-12-20 08:28:45.281248
PDF Oluşturma Tarihi	2008-05-26 00:21:33+03:00
Std Değiştirme Zamanı	2008-05-25 22:21:34
FN Değiştirme Zamanı	2010-12-20 08:28:45.281248
Std Erişim Zamanı	2010-12-20 08:28:46.765625
FN Erişim Zamanı	2010-12-20 08:28:45.281248
Std Giriş Zamanı	2010-12-20 08:28:46.765625
FN Giriş Zamanı	2010-12-20 08:28:45.281248

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (Index Artifact) kayıtlarında da rastlanılmıştır.



Şekil 28 - ABDULKADIR AYGAN.pdf Dosyasına Ait Index Artifact Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

"ABDULKADIR AYGAN.pdf" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış

olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

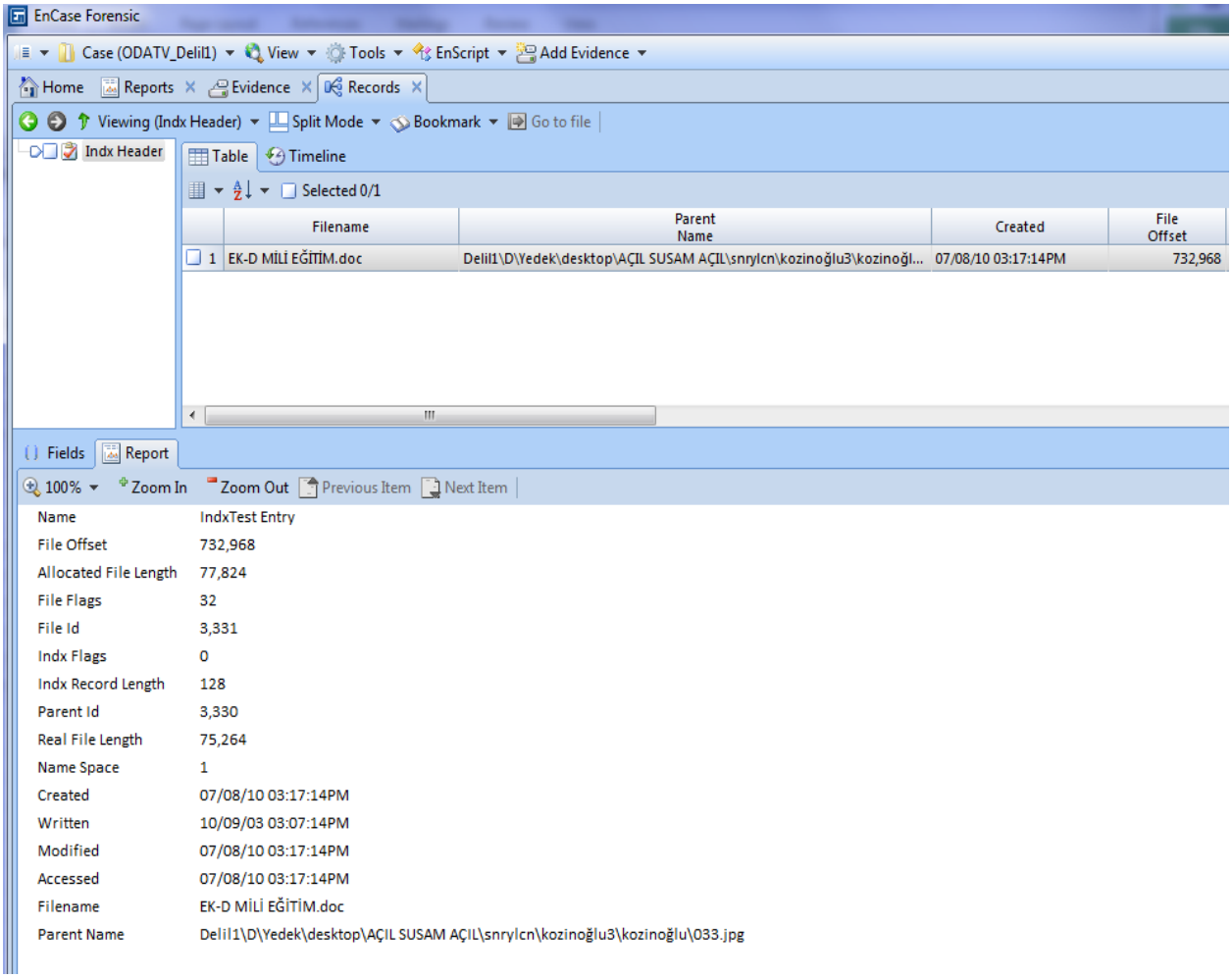
Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

6.) EK-D MİLİ EĞİTİM.doc

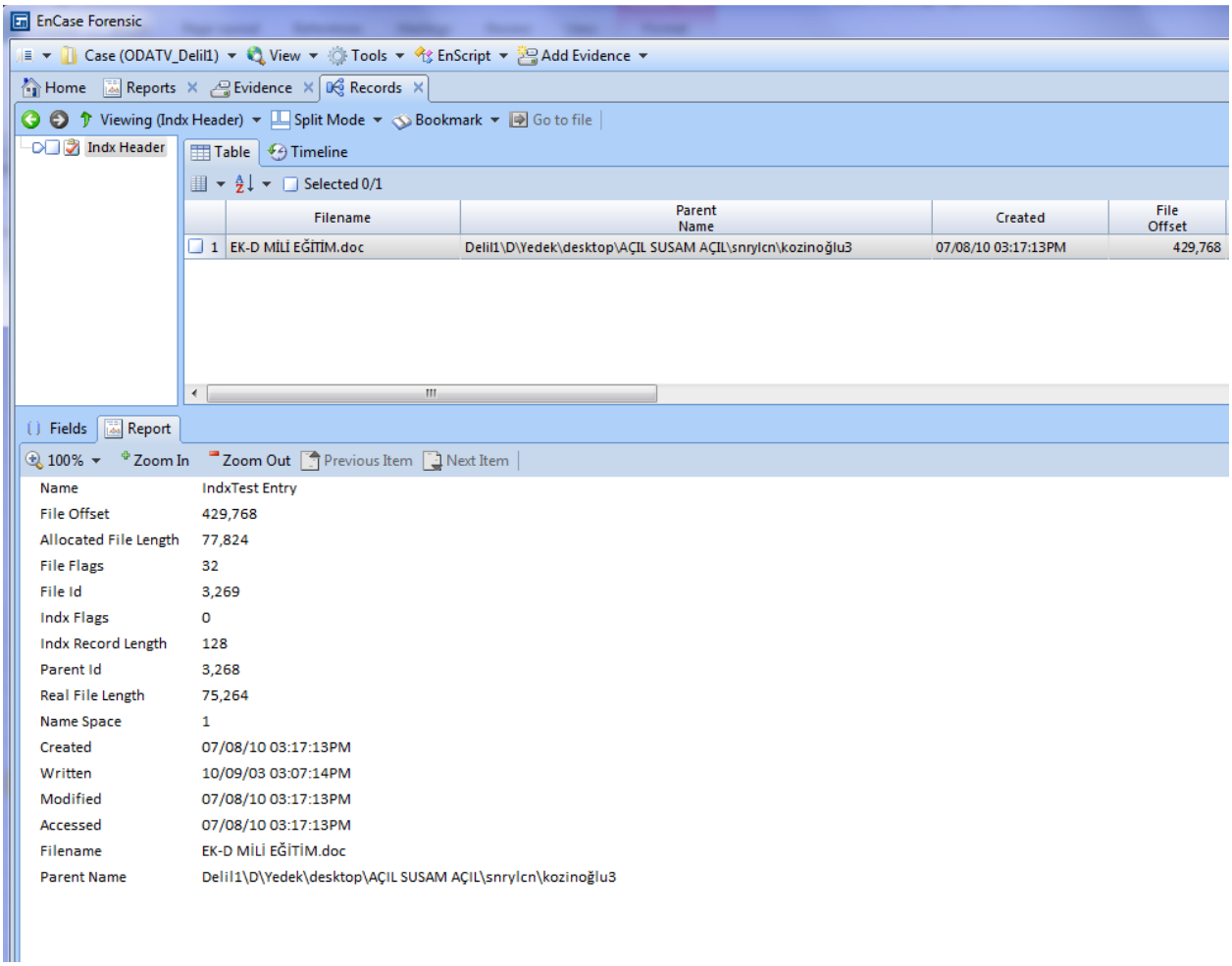
ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

İlgili dosyanın silinmiş olduğu ve $MFT kaydının bulunmadığı tespit edilmiştir. Bununla beraber dosya unallocated clusters alanında tespit edilebilmiş ve görüntülebilmiştir.

İlgili dosyaya ait 2 farklı $LogFile (Index Artifact) kaydı tespit edilmiştir.



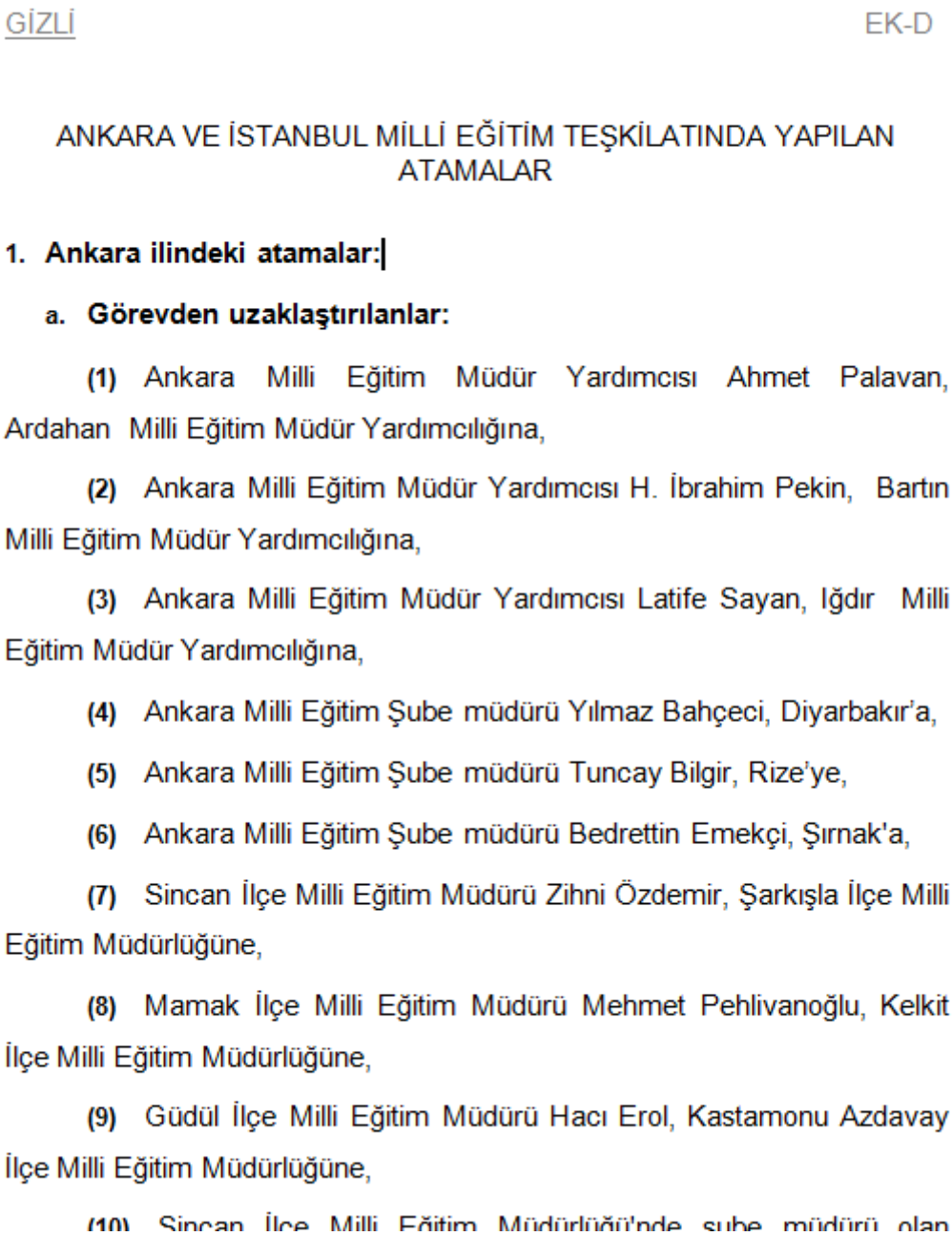
Şekil 29 - EK-D MİLLİ EĞİTİM.doc Dosyasına Ait Index Artifact Kaydı -1



Şekil 30 - EK-D MİLLİ EĞİTİM.doc Dosyasına Ait Index Artifact Kaydı -2

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

Yapılan tetkikler neticesinde unallocated clusters alanından bu dosya olduğu düşünülen bir doküman kurtarılabilmiştir. Milli Eğitim ile ilgili olan ve üsteri olarak **EK-D** işareti bulunan belge aşağıdaki gibidir.



GİZLİ EK-D

ANKARA VE İSTANBUL MİLLİ EĞİTİM TEŞKİLATINDA YAPILAN ATAMALAR

1. Ankara ilindeki atamalar:

a. Görevden uzaklaştırılanlar:

(1) Ankara Milli Eğitim Müdür Yardımcısı Ahmet Palavan, Ardahan Milli Eğitim Müdür Yardımcılığına,

(2) Ankara Milli Eğitim Müdür Yardımcısı H. İbrahim Pekin, Bartın Milli Eğitim Müdür Yardımcılığına,

(3) Ankara Milli Eğitim Müdür Yardımcısı Latife Sayan, Iğdır Milli Eğitim Müdür Yardımcılığına,

(4) Ankara Milli Eğitim Şube müdürü Yılmaz Bahçeci, Diyarbakır'a,

(5) Ankara Milli Eğitim Şube müdürü Tuncay Bilgir, Rize'ye,

(6) Ankara Milli Eğitim Şube müdürü Bedrettin Emekçi, Şırnak'a,

(7) Sincan İlçe Milli Eğitim Müdürü Zihni Özdemir, Şarkışla İlçe Milli Eğitim Müdürlüğüne,

(8) Mamak İlçe Milli Eğitim Müdürü Mehmet Pehlivanoğlu, Kelkit İlçe Milli Eğitim Müdürlüğüne,

(9) Güdül İlçe Milli Eğitim Müdürü Hacı Erol, Kastamonu Azdavay İlçe Milli Eğitim Müdürlüğüne,

(10) Sincan İlçe Milli Eğitim Müdürlüğü'nde şube müdürü olan

Şekil 31 - EK-D Mili Eğitim dosya içeriği

Tespit edilen dosyaya ait belge üstverileri aşağıdaki gibidir.

Belge Üstverileri	
Dosya Adı	EK-D MİLİ EĞİTİM.doc
Dosya Konumu	Unallocated Clusters
Dosya Durumu	Silinmiş, $MFT kaydı yok, unallocated clusterda bulunuyor
Yazar	KARA KUVVETLERI KOMUTANLIGI
Son Değiştiren Kullanıcı	bim
Yönetici	

Şirket	tsk
Nesne Tipi	
Yazılım Tipi	Microsoft Word 9.0
Karakter Tipi	
Karakter Sayısı	3478
Uygulama Versiyonu	
Dosya Boyutu	76 kB
Toplam Değiştirme Süresi	6.0 dakika
Revizyon Numarası	3
Belge Oluşturma Tarihi	2003-10-08 16:45:00
Belge Değiştirme Tarihi	2003-10-09 12:07:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	
FN Oluşturma Zamanı	
Std Değiştirme Zamanı	
FN Değiştirme Zamanı	
Std Erişim Zamanı	
FN Erişim Zamanı	
Std Giriş Zamanı	
FN Giriş Zamanı	

Office Word dokümanlarının bazı versiyonlarında bulunan "Son 10 Kullanıcı Bilgisi" üstverisi incelendiğinde, dosyanın daha önce "**MİLİ EĞİTİM EK-D**" ismiyle kayıtlı olduğu tespit edilmiştir. Son 10 kullanıcıya ait bilgiler aşağıda sıralanmıştır.

Son Kullanıcı Üstveri Bilgileri		
No	**Yazar**	**Lokasyon**
1	KARA KUVVETLERI KOMUTANLIGI	L:\2220-ICISTIHBARATSUBE\Belgeler\3 ncü k1s1m\z Çali_malar\Durum deerlendirmeleri\36 HD 12-18 Eylül 2003\36 HD 12-18 Eylül 2003 ^.Md.düzeltmeli.doc
2	KARA KUVVETLERI KOMUTANLIGI	C:\Documents and Settings\61431048\Application Data\Microsoft\Word\Otomatik Kurtarma kayd136 HD 12-18 Eylül 2003 ^.Md
3	KARA KUVVETLERI KOMUTANLIGI	L:\2220-ICISTIHBARATSUBE\Belgeler\3 ncü k1s1m\z Çali_malar\Durum deerlendirmeleri\36 HD 12-18 Eylül 2003\36 HD 12-18 Eylül 2003 ^.Md.düzeltmeli.doc
4	KARA KUVVETLERI KOMUTANLIGI	L:\2220-ICISTIHBARATSUBE\Belgeler\3 ncü k1s1m\z Çali_malar\Durum deerlendirmeleri\36 HD 12-18 Eylül 2003\36 HD 12-18 Eylül 2003 ^.Md.düzeltmeli.doc

5	KARA KUVVETLERI KOMUTANLIGI	C:\Documents and Settings\61431048\Application Data\Microsoft\Word\Otomatik Kurtarma kayd1EK-A atamalar111.asd
6	KARA KUVVETLERI KOMUTANLIGI	L:\2220-ICISTIHBARATSUBE\Belgeler\3 ncü k1s1m\z Çali_malar\Durum deerlendirmeleri\36 HD 12-18 Eylül 2003\EK-A atamalar111.doc
7	bim	K:\Belgeler\KUB0LAY\EK-A atamalar111.doc
8	bim	C:\Documents and Settings\63752024\Application Data\Microsoft\Word\Otomatik Kurtarma kayd1EK-A atamalar111.asd
9	bim	**K:\Belgeler\KUB0LAY\EK-D MİLİ EĞİTİM.doc**
10	bim	**K:\Belgeler\KUB0LAY\EK-D MİLİ EĞİTİM.doc**

Tablo 2 - EK-D Mili Eğitim Son Kullanıcı Üstverileri

Tespit edilen veriler ışığında, silinmiş alandan kurtarılan bu dosyanın EK-D Mili Eğitim.doc olduğu düşünülmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Belge Üstverileri	
Dosya Adı	EK-D MİLLİ EĞİTİM.doc
Dosya Konumu	\D\Lost Files\001 AKP-KADROLASMA ÇALISMALARI\EK-D MILLI EGITIM.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunmuyor
Yazar	
Son Değiştiren Kullanıcı	
Yönetici	
Şirket	
Nesne Tipi	
Yazılım Tipi	
Karakter Tipi	
Karakter Sayısı	
Uygulama Versiyonu	
Dosya Boyutu	76 kB
Toplam Değiştirme Süresi	
Revizyon Numarası	
Belge Oluşturma Tarihi	
Belge Değiştirme Tarihi	
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-07-08 20:20:48.198875
FN Oluşturma Zamanı	2010-07-08 20:20:48.198875
Std Değiştirme Zamanı	2003-10-09 11:07:14

FN Değiştirme Zamanı	2010-07-08 20:20:48.198875
Std Erişim Zamanı	2010-07-08 20:20:48.198875
FN Erişim Zamanı	2010-07-08 20:20:48.198875
Std Giriş Zamanı	2010-07-08 20:20:48.198875
FN Giriş Zamanı	2010-07-08 20:20:48.198875

Belge Üstverileri	
Dosya Adı	EK-D MİLLİ EĞİTİM.doc
Dosya Konumu	\D\Lost Files\Kadrolaşma\Kadrolaşma GPP Çalışması\EK-D MİLİ EĞİTİM.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunmuyor
Yazar	
Son Değiştiren Kullanıcı	
Yönetici	
Şirket	
Nesne Tipi	
Yazılım Tipi	
Karakter Tipi	
Karakter Sayısı	
Uygulama Versiyonu	
Dosya Boyutu	76 kB
Toplam Değiştirme Süresi	
Revizyon Numarası	
Belge Oluşturma Tarihi	
Belge Değiştirme Tarihi	
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-07-08 20:20:45.308249
FN Oluşturma Zamanı	2010-07-08 20:20:45.308249
Std Değiştirme Zamanı	2003-10-09 11:07:14
FN Değiştirme Zamanı	2010-07-08 20:20:45.308249
Std Erişim Zamanı	2010-07-08 20:20:45.323875
FN Erişim Zamanı	2010-07-08 20:20:45.308249
Std Giriş Zamanı	2010-07-08 20:20:45.323875
FN Giriş Zamanı	2010-07-08 20:20:45.308249

Bu dosya ilgili imajda silinmiş olarak bulunmuştur. Bu dosyaya aynı zamanda LogFile kayıtlarında da rastlanılmıştır. LogFile kayıtlarında bulunan dosyalar aşağıda görülmektedir.

Bu dosya ile ilişkili olarak, LogFile kayıtlarında tespit edilen ve **\D\BARIS YEDEK 11122009\DEKSTOP\özel** dizini altında bulunan **08_07(2).rar** dosyasının kaydı düştükten

sonra çok sayıda benzer içerikli dosyanın da kaydının düştüğü görülmektedir. Bu kayıtlara bakarak **08_07.rar** dosyasının iki defa indirildiği, daha sonra da sıkıştırılmış dosyadan aşağıda belirtilen dosyaların çıkarıldığı düşünülmektedir. Bu sıkıştırılmış dosyanın iki defa indirilmiş olduğu düşüncesi, dosya adının sonundaki parantezin içinde (2) geçmesinden kaynaklanmaktadır. E-posta eklentisi,web sitesi vb. gibi internet kaynaklarından dosya indirildiği zaman bu şekilde bir isimlendirme yapılmaktadır.

Bununla birlikte, 08_07(2).rar dosyanın kullanıcı tarafından bu şekilde isimlendirilmiş olma ihtimali de mevcuttur.

08_07.rar sıkıştırılmış dosyasının içinde bulunan dosyaların listesi aşağıdaki gibidir. **EK-D MİLİ EĞİTİM.doc** dosyası da bu kayıtlardan biri olarak görünmektedir.

Dosya Adı	Oluşturma Tarihi	Giriş Tarihi	Değiştirme Tarihi	Erişim Tarihi
08_07(2).rar	08.07.2010 23:14:53	08.07.2010 23:14:53	08.07.2010 23:14:53	08.07.2010 23:14:53
KADROLAŞMA KONUŞMA NOTU(OCAK 2004).doc	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**
Kadrolaşma en son 0610170003.doc	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**
KADROLAŞMA EK-C.doc	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**
KADROLAŞMA EK-A.doc	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**
Kadrolaşma Bilgi Notu (Ocxak 2004).doc	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**
EK-E AKP'NİN ATAMALARI.xls	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**
EK-D MİLİ EĞİTİM.doc	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**	**08.07.2010 23:20:45**
Kadrolaşma GPP Çalışması	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kadrolaşma1.xls	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kadrolaşma.xls	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kadrolaşma, 26.06..xls	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kadrolaşma özeti.doc	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45

Kadrolaşma temaları.doc	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kadrolaşma son.xls	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kadrolaşma listeye ilave edilecek.xls	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kadrolaşma eski.xls	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kadrolaşma eski.xls	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Bilgi Notu- Kadrolaşma.doc	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kadrolaşma Konuşma Notu 0611.doc	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kadrolaşma 21.07.03.xls	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kadrolaşma.xls	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kadrolaşma1	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kadrolaşma	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kopya Bilgi Notu- Kadrolaşma.doc	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45	08.07.2010 23:20:45
Kadrolaşma.xls	08.07.2010 23:20:48	08.07.2010 23:20:48	08.07.2010 23:20:48	08.07.2010 23:20:48
EK-D MİLİ EĞİTİM.doc	08.07.2010 23:20:48	08.07.2010 23:20:48	08.07.2010 23:20:48	08.07.2010 23:20:48
Kadrolaşma 21.07.03.xls	08.07.2010 23:20:48	08.07.2010 23:20:48	08.07.2010 23:20:48	08.07.2010 23:20:48
Kadrolaşma Bilgi Notu (OCAK 2004).doc	08.07.2010 23:20:48	08.07.2010 23:20:48	08.07.2010 23:20:48	08.07.2010 23:20:48
Kadrolaşma eski ufuğa verilen üzerine eilave ettikleri.xls	08.07.2010 23:20:48	08.07.2010 23:20:48	08.07.2010 23:20:48	08.07.2010 23:20:48
KADROLAŞMA KONUŞMA NOTU(OCAK 2004).doc	08.07.2010 23:20:48	08.07.2010 23:20:48	08.07.2010 23:20:48	08.07.2010 23:20:48

Tablo 3 - 08_07(2).rar Sıkıştırılmış Dosyasında Bulunan Kayıtlar

EK-1 listesinde bulunan dosyalar yukarıdaki tabloda koyu renkte gösterilmiştir.

“EK-D MİLİ EĞİTİM.doc” dokümanı Delil2 diskinde silinmiş ama $MFT kaydı kurtarılabilir durumda bulunmaktadır. Ayrıca bu dosyanın Delil1 diskinde "unallocated cluster" üzerinde bir kopyasına rastlanmış ve veri kurtarma programları yardımıyla kurtarılabilmiştir. Delil1 üzerinde bulunan dosyadan sadece dosya üstverilerine, Delil2 den ise sadece dosya sistemi

üstverilerine ulaşılabilmiştir. Delil2 de bu dosyanın bulunduğu iki ayrı dizin için $Logfile kayıtlarına ulaşılmıştır. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.

- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

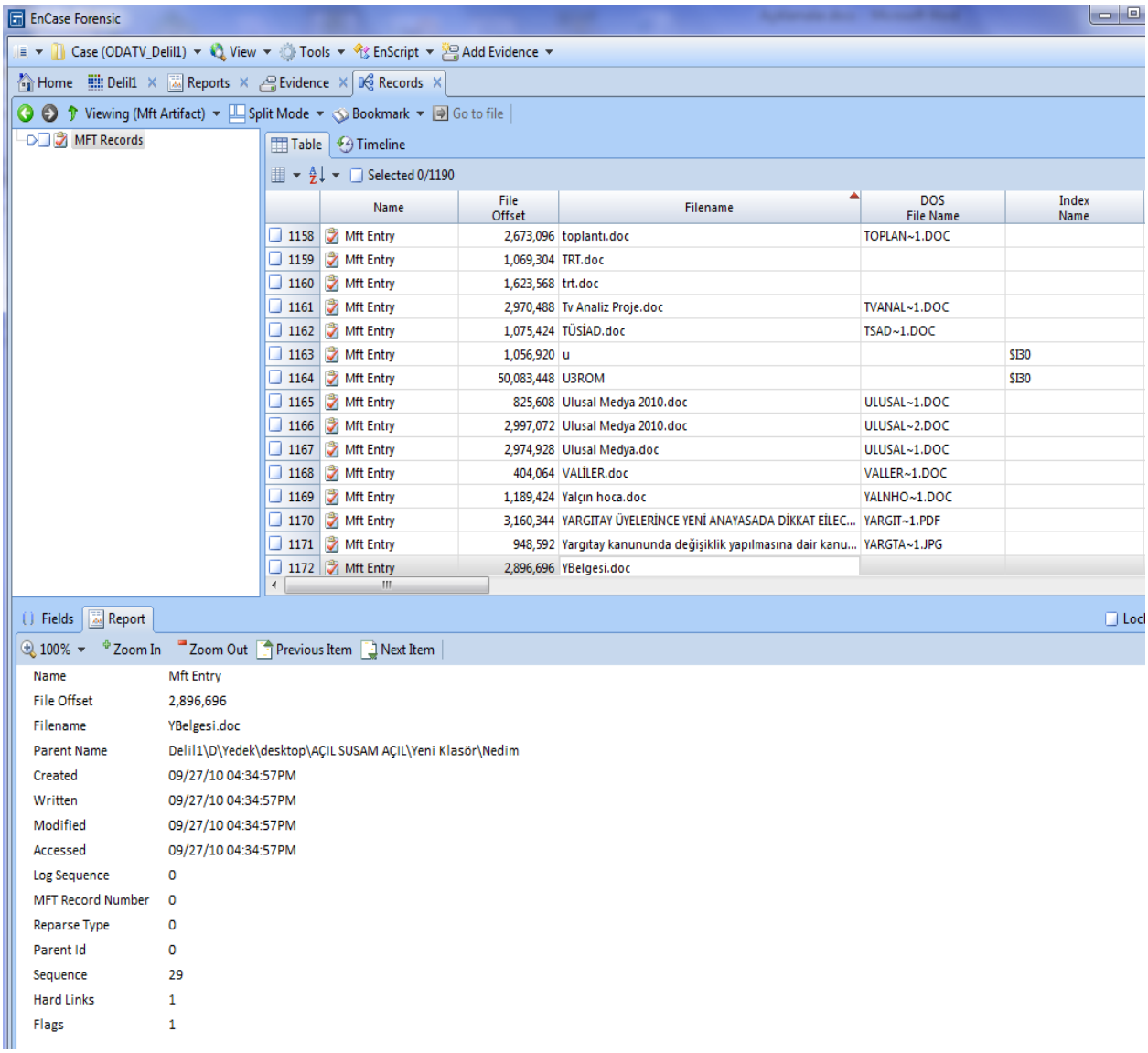
Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

7.) YBelgesi.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	YBelgesi.doc
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\Nedim\YBelgesi.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor.
Yazar	nsener
Son Değiştiren Kullanıcı	nsener
Yönetici	
Şirket	
Nesne Tipi	Microsoft Office Word Belgesi
Yazılım Tipi	Microsoft Office Word
Karakter Tipi	Windows Turkish
Karakter Sayısı	352803
Uygulama Versiyonu	11,5606
Dosya Boyutu	1680 kB
Toplam Değiştirme Süresi	1.7 gün
Revizyon Numarası	130
Belge Oluşturma Tarihi	2009:04:08 15:15:00
Belge Değiştirme Tarihi	2009:05:15 12:19:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-09-27 13:34:57.578125
FN Oluşturma Zamanı	2010-09-27 13:34:57.578125
Std Değiştirme Zamanı	2009-07-09 12:20:00
FN Değiştirme Zamanı	2010-09-27 13:34:57.578125
Std Erişim Zamanı	2010-09-27 13:34:57.640625
FN Erişim Zamanı	2010-09-27 13:34:57.578125
Std Giriş Zamanı	2010-09-27 13:34:57.640625
FN Giriş Zamanı	2010-09-27 13:34:57.578125

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (Index Artifact) kayıtlarında da rastlanılmıştır.



Şekil 32 - YBelgesi.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

"YBelgesi.doc" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.

- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

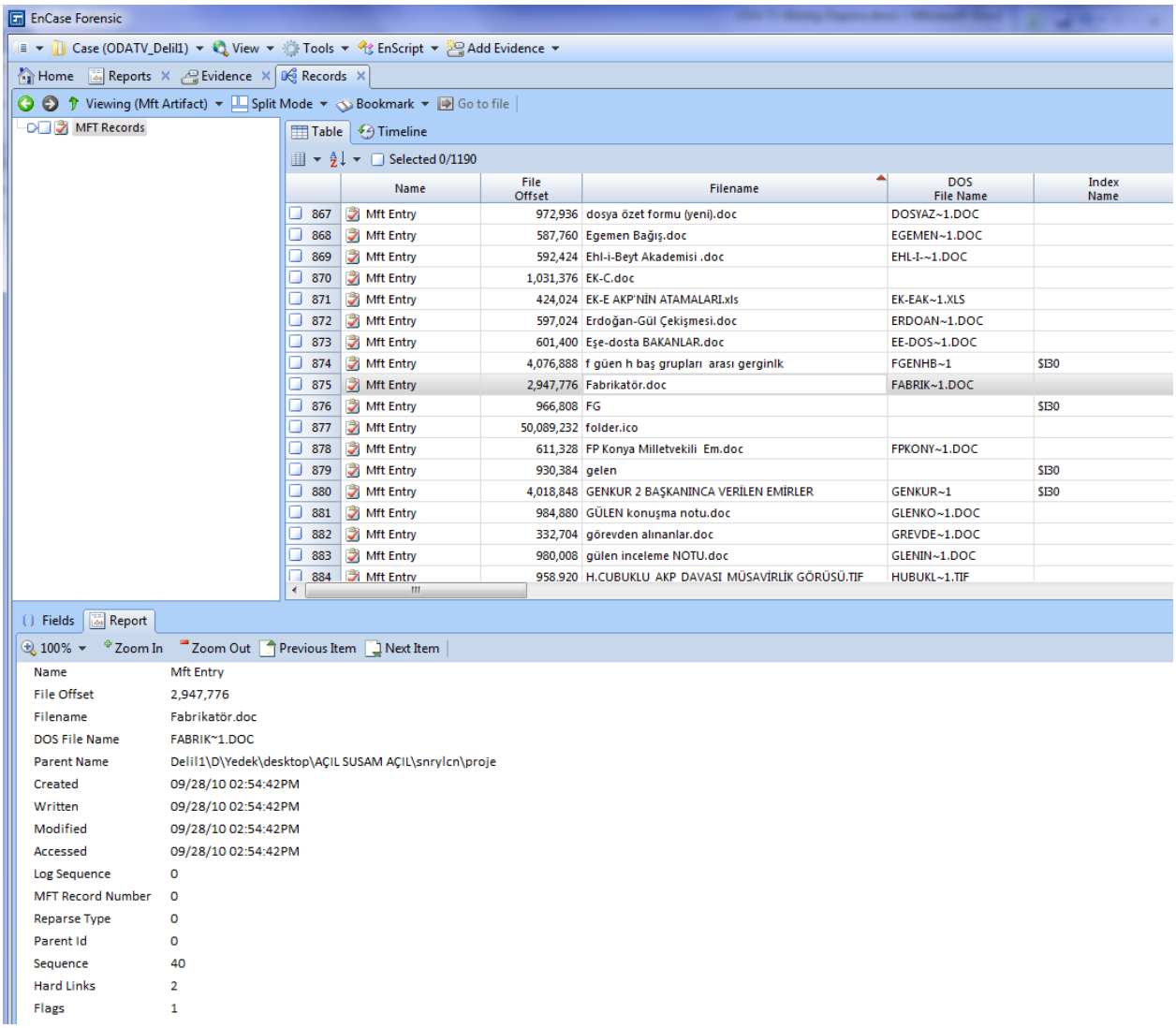
Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

8.) Fabrikatör.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	Fabrikatör.doc
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\Fabrikatör.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor.
Yazar	OPEY A.
Son Değiştiren Kullanıcı	OPEY A.
Yönetici	OĞUZTAN
Şirket	STRATEJİ
Nesne Tipi	Microsoft Word Belgesi
Yazılım Tipi	Microsoft Word 8.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	53762
Uygulama Versiyonu	8,3814
Dosya Boyutu	240 kB
Toplam Değiştirme Süresi	13.3 saat
Revizyon Numarası	789
Belge Oluşturma Tarihi	2000:02:12 10:00:00
Belge Değiştirme Tarihi	2000:03:31 16:11:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-09-28 11:54:42.500000
FN Oluşturma Zamanı	2010-09-28 11:54:42.500000
Std Değiştirme Zamanı	2009-02-12 13:08:10
FN Değiştirme Zamanı	2010-09-28 11:54:42.500000
Std Erişim Zamanı	2010-09-28 11:54:42.500000
FN Erişim Zamanı	2010-09-28 11:54:42.500000
Std Giriş Zamanı	2010-09-28 11:54:42.500000
FN Giriş Zamanı	2010-09-28 11:54:42.500000

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (MFT Artifact) kayıtlarında da rastlanılmıştır.



Şekil 33 - Fabrikatör.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

"Fabrikatör.doc" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

Ancak bununla beraber silinmiş durumunda olan ve bu sebeple ne dosyası olduğu anlaşılamayan, açılmış bir internet sitesi ya da okunmuş bir dokümanda bu dosyanın ismi geçmektedir. Dosya isminin disk üzerindeki aramalarda bu şekilde bir doküman ya da internet geçmişinde çıkmış olması, bu dosyanın bu disk üzerinde bulunduğuna dair net bir bilgi vermemektedir.

Dosya isminin geçtiği cluster ve sektör adresleri aşağıdaki gibidir:

CL 13247262 SO 254, CL 13247874 SO 194, CL 13247858 SO 224, CL 526246 SO 194, CL 526230 SO 224, CL 525634 SO 254, CL 14538942 SO 254, CL 14539538 SO 224, CL 14539554 SO 194

9.) Ulusal Medya.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	Ulusal Medya.doc
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\Ulusal Medya.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor.
Yazar	OPEY A.
Son Değiştiren Kullanıcı	OPEY A.
Yönetici	
Şirket	STRATEJİ
Nesne Tipi	Microsoft Word Belgesi
Yazılım Tipi	Microsoft Word 8.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	33990
Uygulama Versiyonu	8,3814
Dosya Boyutu	156 kB
Toplam Değiştirme Süresi	6.3 saat
Revizyon Numarası	296
Belge Oluşturma Tarihi	2000:12:15 12:45:00
Belge Değiştirme Tarihi	2001:01:27 13:46:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-09-28 11:54:42.562498
FN Oluşturma Zamanı	2010-09-28 11:54:42.562498
Std Değiştirme Zamanı	2009-02-12 13:08:12
FN Değiştirme Zamanı	2010-09-28 11:54:42.562498
Std Erişim Zamanı	2010-09-28 11:54:42.562498
FN Erişim Zamanı	2010-09-28 11:54:42.562498
Std Giriş Zamanı	2010-09-28 11:54:42.562498
FN Giriş Zamanı	2010-09-28 11:54:42.562498

"Ulusal Medya.doc" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

Ancak bununla beraber silinmiş durumunda olan ve bu sebeple ne dosyası olduğu anlaşılamayan, açılmış bir internet sitesi ya da okunmuş bir dokümanda bu dosyanın ismi geçmektedir. Dosya isminin disk üzerindeki aramalarda bu şekilde bir doküman ya da internet geçmişinde çıkmış olması, bu dosyanın bu disk üzerinde bulunduğuna dair net bir bilgi vermemektedir.

Dosya isminin geçtiği cluster ve sektör adresleri aşağıdaki gibidir:

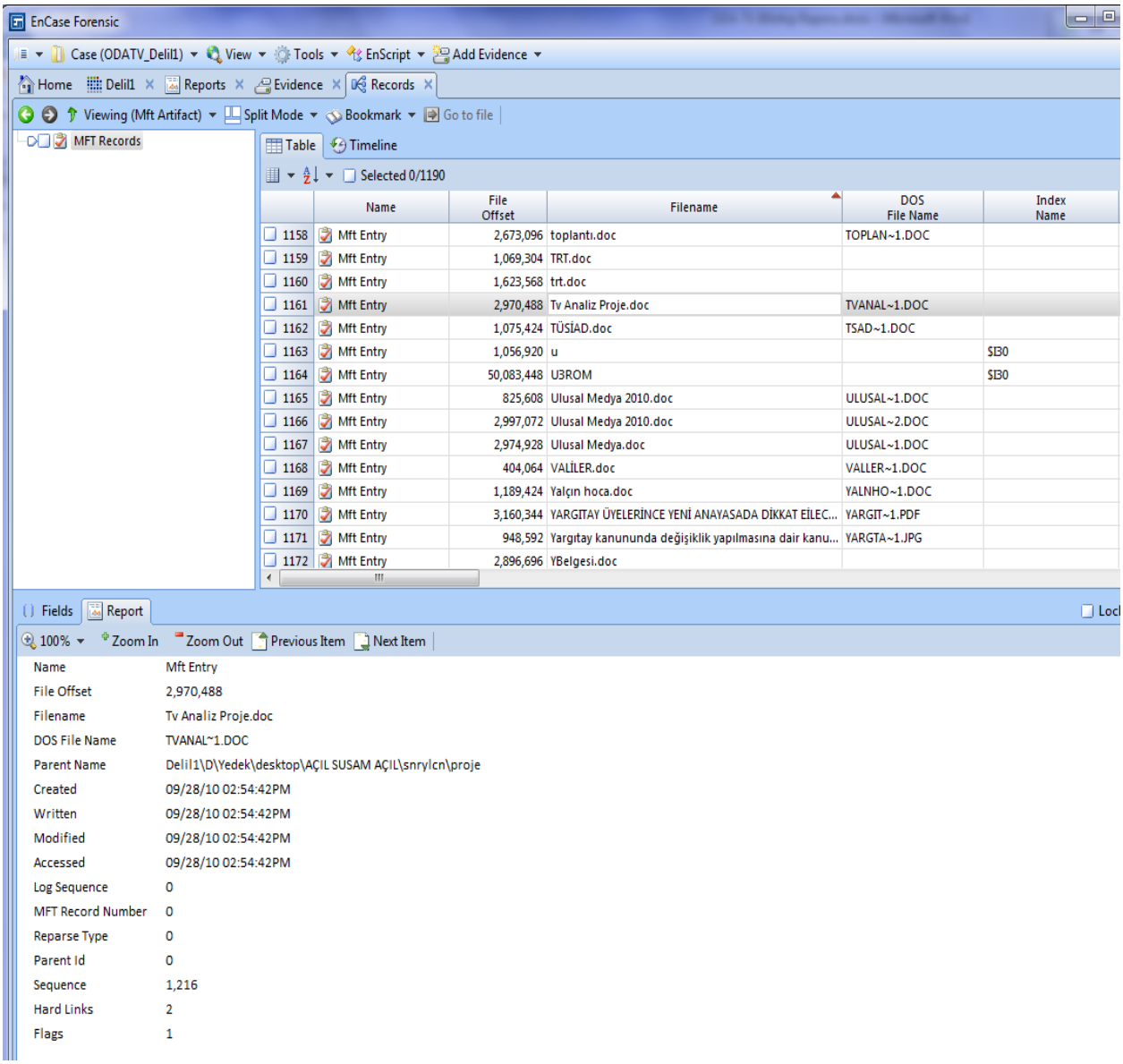
CL 13247262 SO 456, CL 13247875 SO 444, CL 526247 SO 444, CL 525634 SO 456, CL 14538942 SO 456, CL 14539555 SO 444

10.) Tv Analiz Proje.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	Tv Analiz Proje.doc
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\Tv Analiz Proje.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor.
Yazar	Ümit OĞUZTAN
Son Değiştiren Kullanıcı	OPEY A.
Yönetici	
Şirket	COMPAQ
Nesne Tipi	Microsoft Word Belgesi
Yazılım Tipi	Microsoft Word 8.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	84120
Uygulama Versiyonu	8,3814
Dosya Boyutu	240 kB
Toplam Değiştirme Süresi	2.1 saat
Revizyon Numarası	180
Belge Oluşturma Tarihi	2000:07:23 08:23:00
Belge Değiştirme Tarihi	2000:07:23 20:42:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-09-28 11:54:42.546875
FN Oluşturma Zamanı	2010-09-28 11:54:42.546875
Std Değiştirme Zamanı	2009-02-12 13:08:12
FN Değiştirme Zamanı	2010-09-28 11:54:42.546875
Std Erişim Zamanı	2010-09-28 11:54:42.562498
FN Erişim Zamanı	2010-09-28 11:54:42.546875
Std Giriş Zamanı	2010-09-28 11:54:42.562498
FN Giriş Zamanı	2010-09-28 11:54:42.546875

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (Index Artifact) kayıtlarında da rastlanılmıştır.



Şekil 34 - Tv Analiz Proje.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

"Tv Analiz Proje.doc" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.

- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

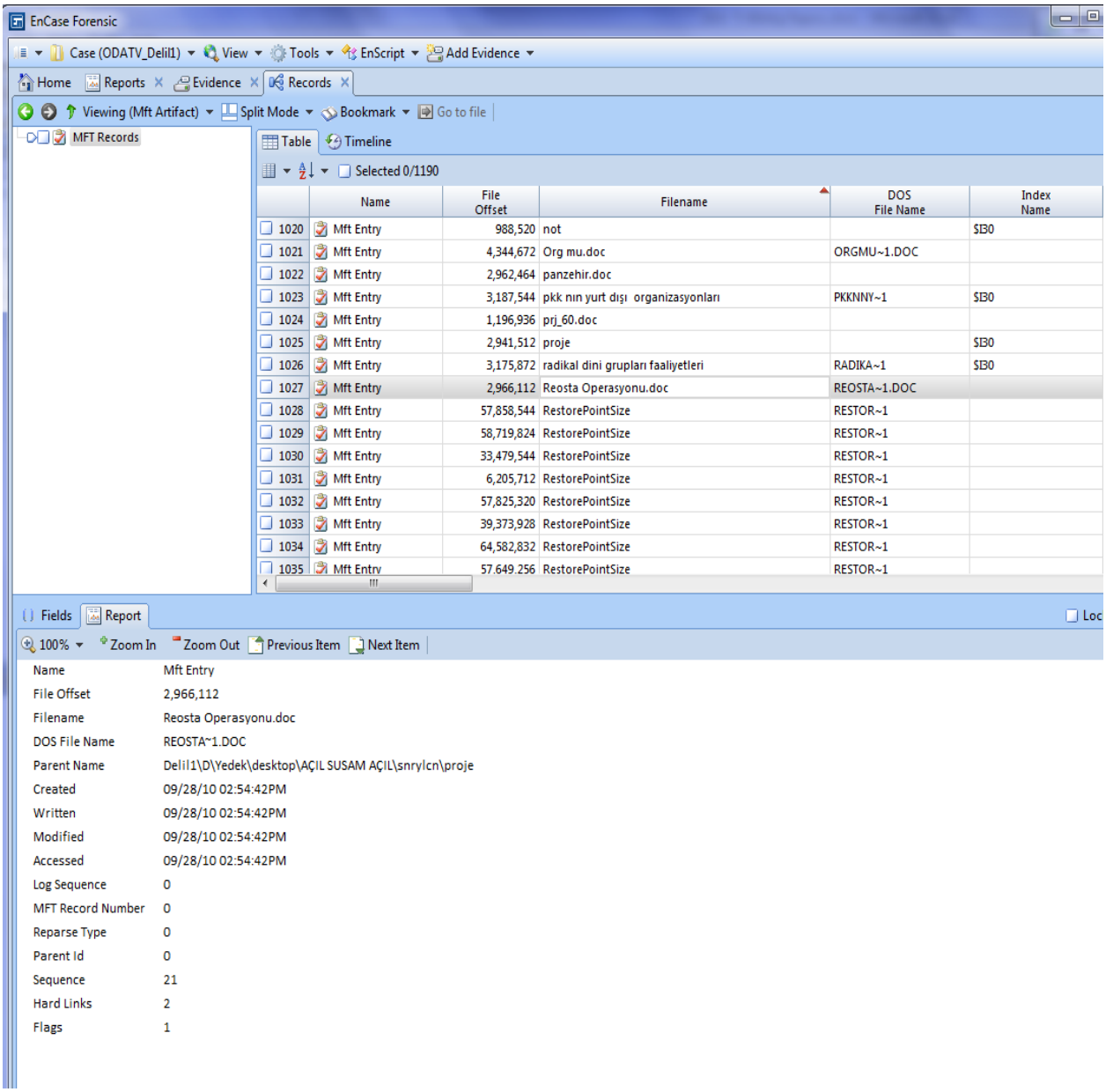
Ancak bununla beraber silinmiş durumunda olan ve bu sebeple ne dosyası olduğu anlaşılamayan, açılmış bir internet sitesi ya da okunmuş bir dokümanda bu dosyanın ismi geçmektedir. Dosya isminin disk üzerindeki aramalarda bu şekilde bir doküman ya da internet geçmişinde çıkmış olması, bu dosyanın bu disk üzerinde bulunduğuna dair net bir bilgi vermemektedir.

11.) Reosta Operasyonu.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	Reosta Operasyonu.doc
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\Reosta Operasyonu.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor.
Yazar	OPEY A.
Son Değiştiren Kullanıcı	OPEY A.
Yönetici	OĞUZTAN
Şirket	STRATEJİ
Nesne Tipi	Microsoft Word Belgesi
Yazılım Tipi	Microsoft Word 8.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	72847
Uygulama Versiyonu	8,3814
Dosya Boyutu	200 kB
Toplam Değiştirme Süresi	1.2 saat
Revizyon Numarası	804
Belge Oluşturma Tarihi	2000:05:02 19:50:00
Belge Değiştirme Tarihi	2003:07:25 23:36:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-09-28 11:54:42.546875
FN Oluşturma Zamanı	2010-09-28 11:54:42.546875
Std Değiştirme Zamanı	2009-02-12 13:08:12
FN Değiştirme Zamanı	2010-09-28 11:54:42.546875
Std Erişim Zamanı	2010-09-28 11:54:42.546875
FN Erişim Zamanı	2010-09-28 11:54:42.546875
Std Giriş Zamanı	2010-09-28 11:54:42.546875
FN Giriş Zamanı	2010-09-28 11:54:42.546875

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (Index Artifact) kayıtlarında da rastlanılmıştır.



Şekil 35 - Reosta Operasyonu.doc Dosyasına Ait Logfile (Index Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

"Reosta Operasyonu.doc" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

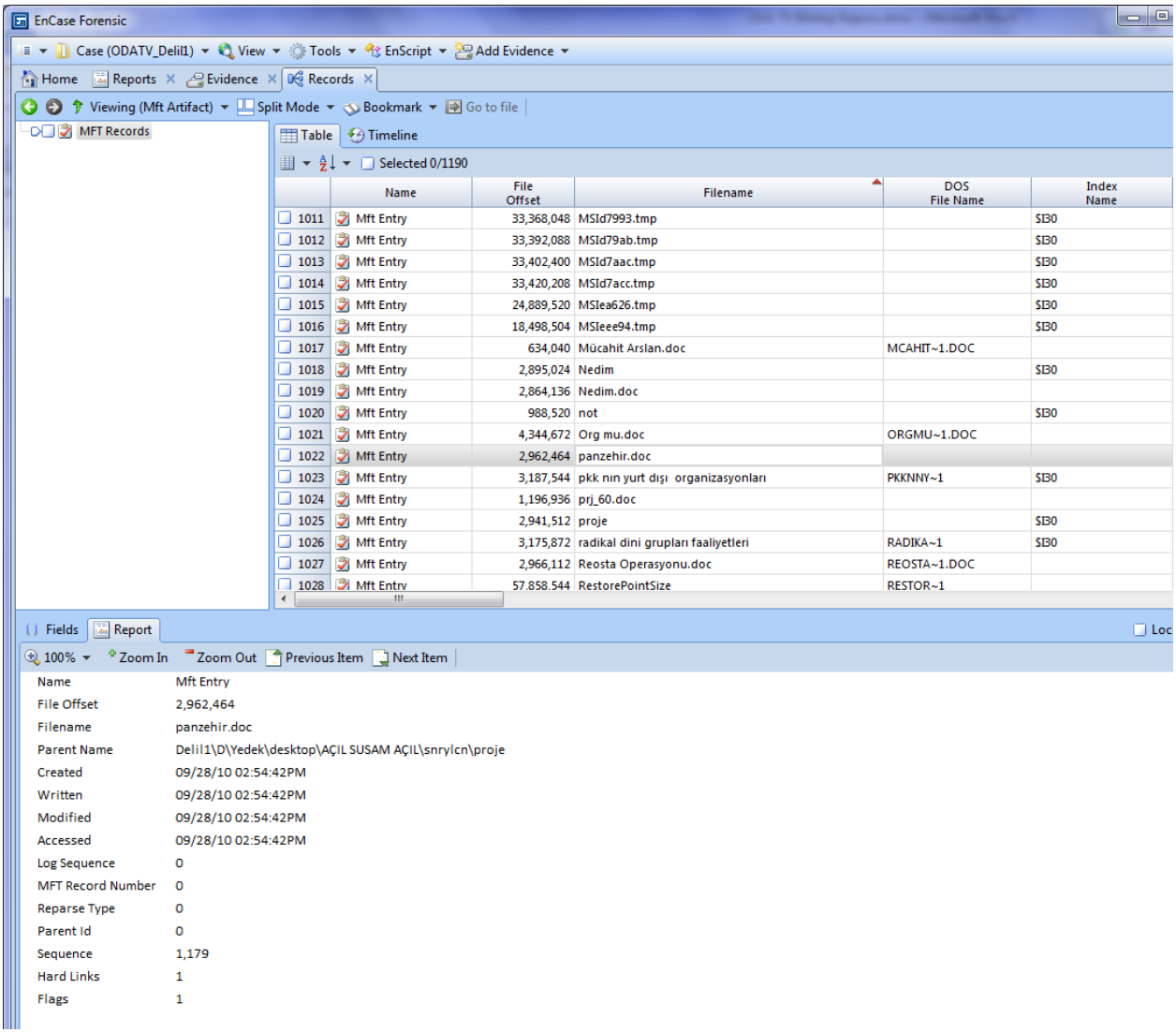
Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

12.) panzehir.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	panzehir.doc
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\panzehir.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor.
Yazar	OPEY A.
Son Değiştiren Kullanıcı	OPEY A.
Yönetici	OĞUZTAN
Şirket	STRATEJİ
Nesne Tipi	Microsoft Word Belgesi
Yazılım Tipi	Microsoft Word 8.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	71095
Uygulama Versiyonu	8,3814
Dosya Boyutu	228 kB
Toplam Değiştirme Süresi	7.4 saat
Revizyon Numarası	310
Belge Oluşturma Tarihi	2000:04:25 10:57:00
Belge Değiştirme Tarihi	2000:12:15 19:00:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-09-28 11:54:42.531248
FN Oluşturma Zamanı	2010-09-28 11:54:42.531248
Std Değiştirme Zamanı	2009-02-12 13:08:12
FN Değiştirme Zamanı	2010-09-28 11:54:42.531248
Std Erişim Zamanı	2010-09-28 11:54:42.531248
FN Erişim Zamanı	2010-09-28 11:54:42.531248
Std Giriş Zamanı	2010-09-28 11:54:42.531248
FN Giriş Zamanı	2010-09-28 11:54:42.531248

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (MFT Artifact) kayıtlarında da rastlanılmıştır



Şekil 36 - panzehir.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

“panzehir.doc” dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

Ancak bununla beraber silinmiş durumunda olan ve bu sebeple ne dosyası olduğu anlaşılamayan, açılmış bir internet sitesi ya da okunmuş bir dokümanda bu dosyanın ismi geçmektedir. Dosya isminin disk üzerindeki aramalarda bu şekilde bir doküman ya da internet geçmişinde çıkmış olması, bu dosyanın bu disk üzerinde bulunduğuna dair net bir bilgi vermemektedir.

Dosya isminin geçtiği cluster ve sektör adresleri aşağıdaki gibidir:

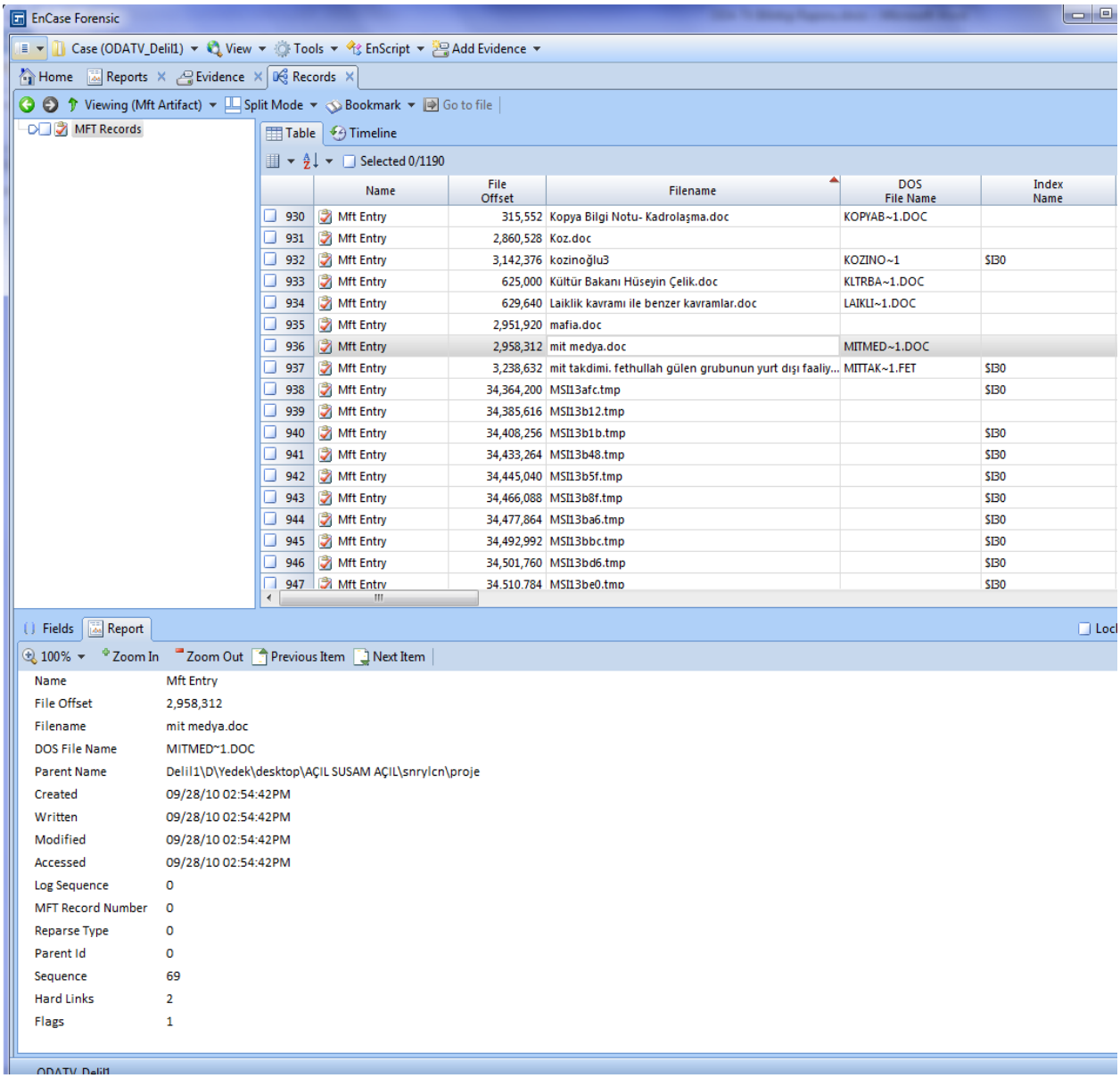
CL 13247875 SO 124, CL 13247858 SO 230, CL 13247858 SO 468, CL 13247262 SO 062, CL 14539555 SO 124, CL 14539538 SO 230, CL 14539538 SO 468, CL 14538942 SO 062, CL 526247 SO 124, CL 526230 SO 230, CL 526230 SO 468, CL 525634 SO 062

13.) mit medya.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	mit medya.doc
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\mit medya.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor.
Yazar	OPEY A.
Son Değiştiren Kullanıcı	OPEY A.
Yönetici	
Şirket	STRATEJİ
Nesne Tipi	Microsoft Word Belgesi
Yazılım Tipi	Microsoft Word 8.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	89208
Uygulama Versiyonu	8,3814
Dosya Boyutu	324 kB
Toplam Değiştirme Süresi	6.6 saat
Revizyon Numarası	351
Belge Oluşturma Tarihi	2000:12:12 18:29:00
Belge Değiştirme Tarihi	2001:01:04 08:23:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-09-28 11:54:42.515625
FN Oluşturma Zamanı	2010-09-28 11:54:42.515625
Std Değiştirme Zamanı	2009-02-12 13:08:10
FN Değiştirme Zamanı	2010-09-28 11:54:42.515625
Std Erişim Zamanı	2010-09-28 11:54:42.515625
FN Erişim Zamanı	2010-09-28 11:54:42.515625
Std Giriş Zamanı	2010-09-28 11:54:42.515625
FN Giriş Zamanı	2010-09-28 11:54:42.515625

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (MFT Artifact) kayıtlarında da rastlanılmıştır.



Şekil 37 - mit medya.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

“mit medya.doc” dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.

- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

Ancak bununla beraber silinmiş durumunda olan ve bu sebeple ne dosyası olduğu anlaşılamayan, açılmış bir internet sitesi ya da okunmuş bir dokümanda bu dosyanın ismi geçmektedir. Dosya isminin disk üzerindeki aramalarda bu şekilde bir doküman ya da internet geçmişinde çıkmış olması, bu dosyanın bu disk üzerinde bulunduğuna dair net bir bilgi vermemektedir.

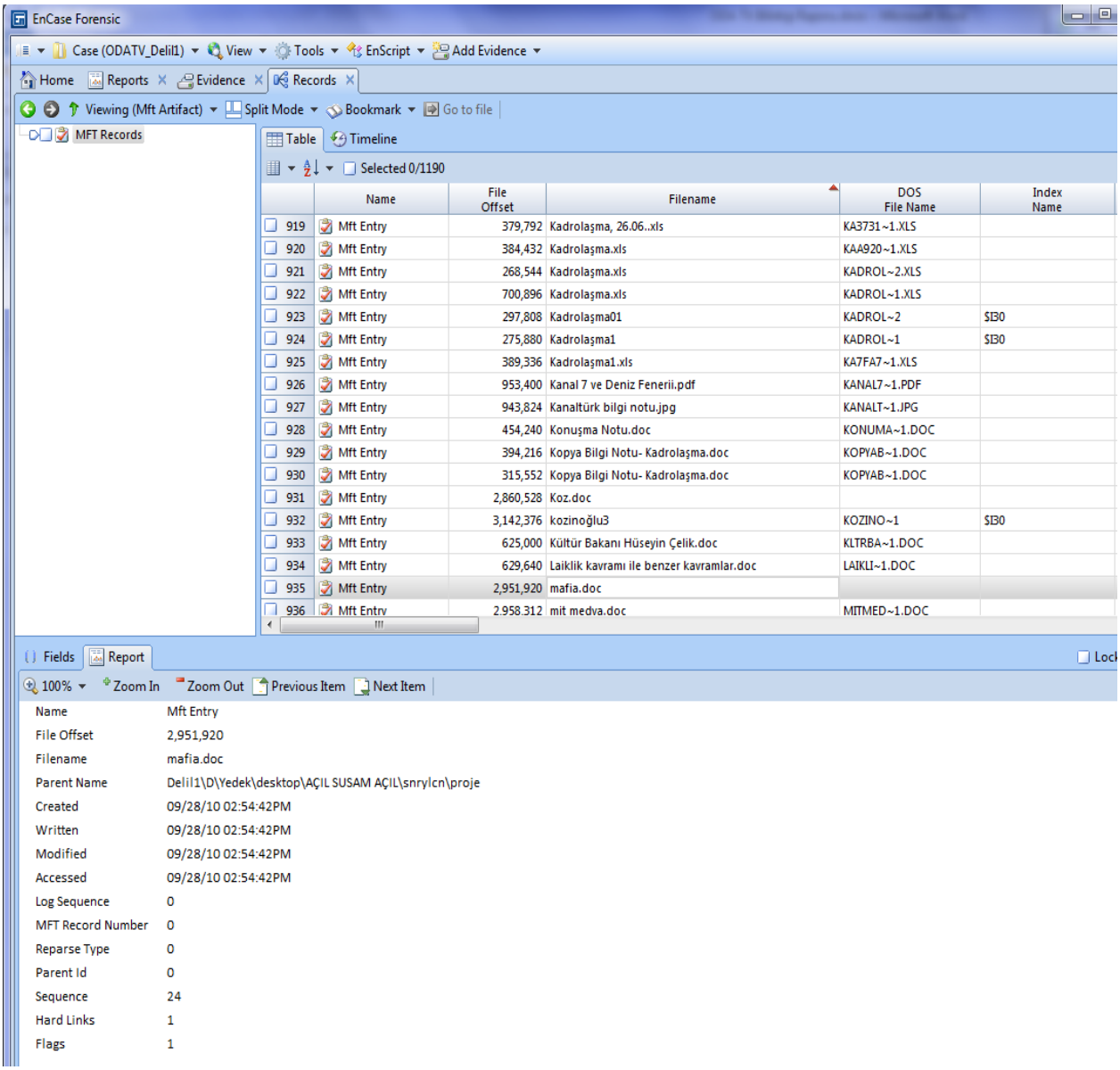
Dosya isminin geçtiği cluster ve sektör adresleri aşağıdaki gibidir:
CL 13247874 SO 444,CL 13247262 SO 094,CL 13247858 SO 214,CL 525634 SO 094,CL 526246 SO 444,CL 14538942 SO 094,CL 14539554 SO 444

14.) mafia.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	mafia.doc
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\mafia.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor.
Yazar	OPEY A.
Son Değiştiren Kullanıcı	OPEY A.
Yönetici	
Şirket	STRATEJİ
Nesne Tipi	Microsoft Word Belgesi
Yazılım Tipi	Microsoft Word 8.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	68512
Uygulama Versiyonu	8,3814
Dosya Boyutu	200 kB
Toplam Değiştirme Süresi	15.3 saat
Revizyon Numarası	596
Belge Oluşturma Tarihi	2000:09:11 08:18:00
Belge Değiştirme Tarihi	2003:07:25 22:46:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-09-28 11:54:42.500000
FN Oluşturma Zamanı	2010-09-28 11:54:42.500000
Std Değiştirme Zamanı	2009-02-12 13:08:10
FN Değiştirme Zamanı	2010-09-28 11:54:42.500000
Std Erişim Zamanı	2010-09-28 11:54:42.515625
FN Erişim Zamanı	2010-09-28 11:54:42.500000
Std Giriş Zamanı	2010-09-28 11:54:42.515625
FN Giriş Zamanı	2010-09-28 11:54:42.500000

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (MFT Artifact) kayıtlarında da rastlanılmıştır.



Şekil 38 - mafia.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

"mafia.doc" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış

olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

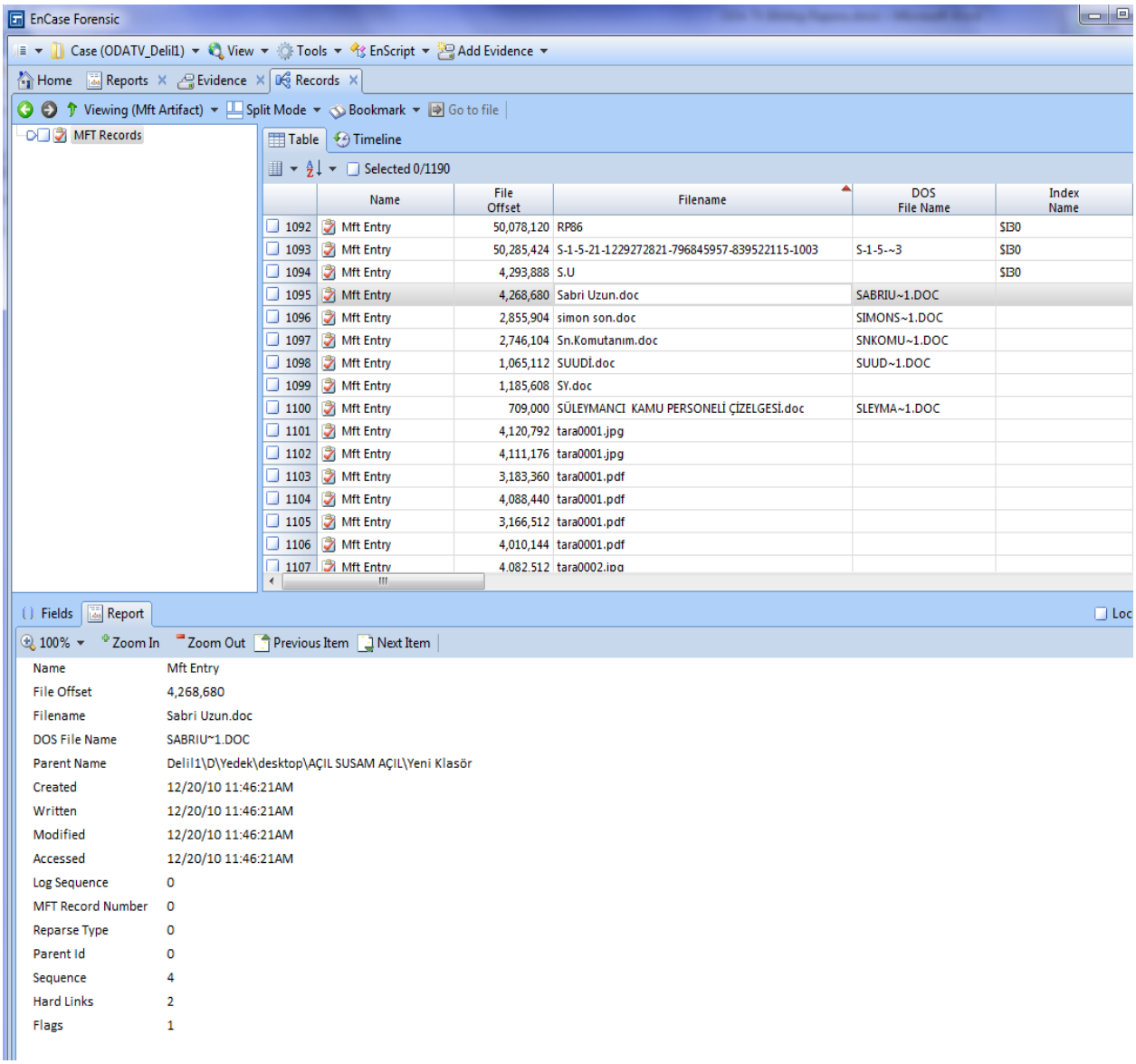
Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

15.) Sabri Uzun.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	Sabri Uzun.doc
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\Sabri Uzun.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor.
Yazar	soner
Son Değiştiren Kullanıcı	soner
Yönetici	
Şirket	Conqueror
Nesne Tipi	Microsoft Word Document
Yazılım Tipi	Microsoft Word 10.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	442
Uygulama Versiyonu	10,2605
Dosya Boyutu	24 kB
Toplam Değiştirme Süresi	6.0 dakika
Revizyon Numarası	5
Belge Oluşturma Tarihi	2010:12:20 09:29:00
Belge Değiştirme Tarihi	2010:12:20 09:35:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-12-20 09:46:21.609373
FN Oluşturma Zamanı	2010-12-20 09:46:21.609373
Std Değiştirme Zamanı	2010-12-20 09:35:20
FN Değiştirme Zamanı	2010-12-20 09:46:21.609373
Std Erişim Zamanı	2010-12-20 09:46:21.609373
FN Erişim Zamanı	2010-12-20 09:46:21.609373
Std Giriş Zamanı	2010-12-20 09:46:21.609373
FN Giriş Zamanı	2010-12-20 09:46:21.609373

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (Index Artifact) kayıtlarında da rastlanılmıştır.



Şekil 39 - Sabri Uzun.doc Dosyasına Ait Logfile (Index Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

"Sabri Uzun.doc" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.

- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

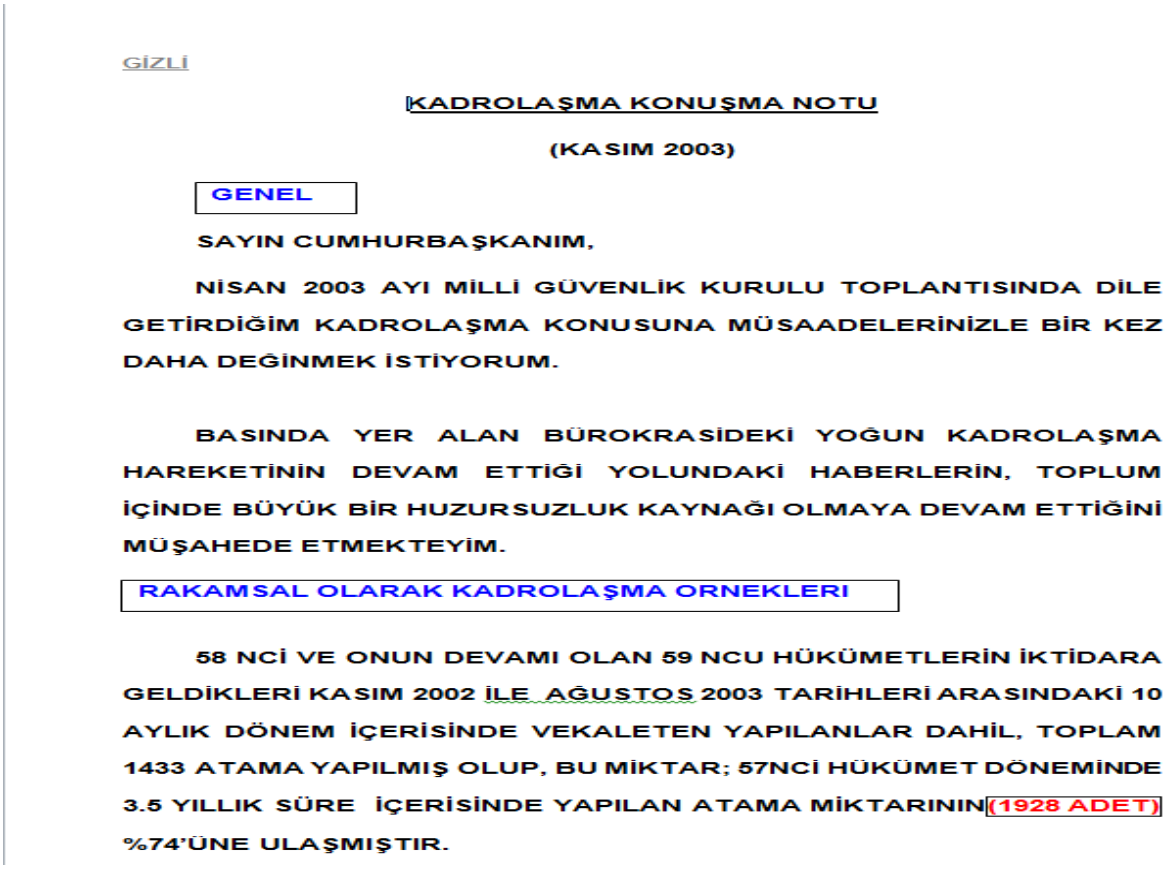
Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

16.) Konuşma Notu.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

İlgili dosyanın silinmiş olduğu tespit edilmiştir. Ancak unallocated clusters alanında içeriği bulunan ve bu dosya olduğu düşünülen bir dosya kurtarılmıştır.

Dosya içeriği aşağıdaki gibidir.



GİZLİ

KADROLAŞMA KONUŞMA NOTU

(KASIM 2003)

GENEL

SAYIN CUMHURBAŞKANIM,

NİSAN 2003 AYI MİLLİ GÜVENLİK KURULU TOPLANTISINDA DİLE GETİRDİĞİM KADROLAŞMA KONUSUNA MÜSAADELERİNİZLE BİR KEZ DAHA DEĞİNMEK İSTİYORUM.

BASINDA YER ALAN BÜROKRASİDEKİ YOĞUN KADROLAŞMA HAREKETİNİN DEVAM ETTİĞİ YOLUNDAKİ HABERLERİN, TOPLUM İÇİNDE BÜYÜK BİR HUZURSUZLUK KAYNAĞI OLMAYA DEVAM ETTİĞİNİ MÜŞAHEDE ETMEKTEYİM.

RAKAMSAL OLARAK KADROLAŞMA ORNEKLERI

58 NCİ VE ONUN DEVAMI OLAN 59 NCU HÜKÜMETLERİN İKTİDARA GELDİKLERİ KASIM 2002 İLE AĞUSTOS 2003 TARİHLERİ ARASINDAKİ 10 AYLIK DÖNEM İÇERİSİNDE VEKALETEN YAPILANLAR DAHİL, TOPLAM 1433 ATAMA YAPILMIŞ OLUP, BU MİKTAR; 57NCİ HÜKÜMET DÖNEMİNDE 3.5 YILLIK SÜRE İÇERİSİNDE YAPILAN ATAMA MİKTARININ(1928 ADET) %74'ÜNE ULAŞMIŞTIR.

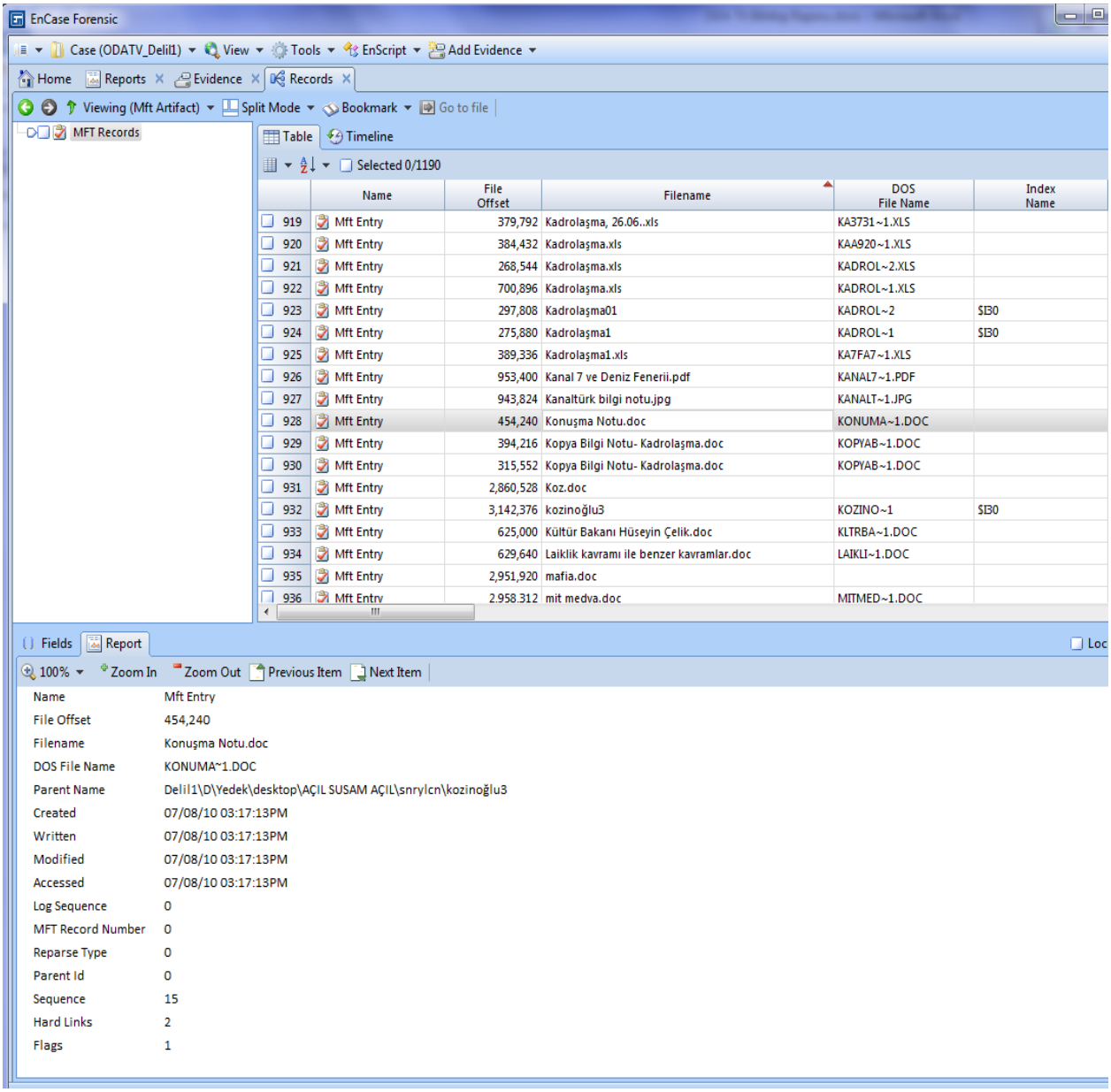
Şekil 40 - Konuşma Notu.doc içerikli dosya

Tespit edilen ve görüntülenebilen Konuşma Notu.doc dosyası tamamen kurtarılabilmiştir. Kurtarılan dosyadan elde edilen metaveriler aşağıdaki gibidir.

Belge Üstverileri	
Dosya Adı	Konuşma Notu.doc
Dosya Konumu	
Dosya Durumu	Silinmiş, $MFT kaydı yok,unallocated clusterda bulunuyor.

Yazar	KARA KUVVETLERİ KOMUTANLIĞI
Son Değiştiren Kullanıcı	Celalettin BACANLI
Yönetici	
Şirket	KARA KUVVETLERI KOMUTANLIGI
Nesne Tipi	Microsoft Word Belgesi
Yazılım Tipi	Microsoft Word 9.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	2812
Uygulama Versiyonu	9.2812
Dosya Boyutu	34 kB
Toplam Değiştirme Süresi	0 dakika
Revizyon Numarası	2
Belge Oluşturma Tarihi	2003:12:26 15:57:00
Belge Değiştirme Tarihi	2003:12:26 15:57:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	
FN Oluşturma Zamanı	
Std Değiştirme Zamanı	
FN Değiştirme Zamanı	
Std Erişim Zamanı	
FN Erişim Zamanı	
Std Giriş Zamanı	
FN Giriş Zamanı	

Konuşma Notu.doc dosyasının bu imajda bulunduğuna dair Logfile (MFT Artifact) kaydına da rastlanmıştır.



Şekil 41 - Konuşma Notu.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Belge Üstverileri	
Dosya Adı	Konuşma Notu.doc
Dosya Konumu	\D\Lost Files\Kadrolasma\Kadrolasma GPP Çalismasi\Konusma Notu.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunmuyor.
Yazar	
Son Değiştiren Kullanıcı	
Yönetici	
Şirket	
Nesne Tipi	
Yazılım Tipi	
Karakter Tipi	
Karakter Sayısı	
Uygulama Versiyonu	
Dosya Boyutu	28 kB
Toplam Değiştirme Süresi	
Revizyon Numarası	
Belge Oluşturma Tarihi	
Belge Değiştirme Tarihi	
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-07-08 20:20:45.370750
FN Oluşturma Zamanı	2010-07-08 20:20:45.370750
Std Değiştirme Zamanı	2004-01-08 14:43:54
FN Değiştirme Zamanı	2010-07-08 20:20:45.370750
Std Erişim Zamanı	2010-07-08 20:20:45.386374
FN Erişim Zamanı	2010-07-08 20:20:45.370750
Std Giriş Zamanı	2010-07-08 20:20:45.386374
FN Giriş Zamanı	2010-07-08 20:20:45.370750

“Konusma Notu.doc” dokümanı Delil2 diskinde silinmiş ama $MFT kaydı kurtarılabilir durumda bulunmaktadır. Ayrıca bu dosyanın Delil1 diskinde "unallocated cluster" üzerinde bir kopyasına rastlanmış ve veri kurtarma programları yardımıyla kurtarılabilmiştir. Delil1 üzerinde bulunan dosyadan sadece belge üstverilerine, Delil2 den ise sadece dosya sistemi üstverilerine ulaşılabilmiştir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

17.) KADROLAŞMA KONUŞMA NOTU(OCAK 2004) .doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

İlgili dosyanın silinmiş olduğu tespit edilmiştir. Ancak unallocated clusters alanında içeriği tespit edilen ve bu dosya olduğu düşünülen bir dosya kurtarılmıştır.

Dosya içeriği aşağıdaki gibidir.

GİZLİ

KADROLAŞMA KONUŞMA NOTU

(OCAK 2004)

GENEL

SAYIN CUMHURBAŞKANIM,

NİSAN 2003 AYI MİLLİ GÜVENLİK KURULU TOPLANTISINDA DİLE GETİRDİĞİM KADROLAŞMA KONUSUNA MÜSAADELERİNİZLE BİR KEZ DAHA DEĞİNMEK İSTİYORUM.

BASINDA YER ALAN BÜROKRASİDEKİ YOĞUN KADROLAŞMA HAREKETİNİN DEVAM ETTİĞİ YOLUNDAKİ HABERLERİN, TOPLUM İÇİNDE BÜYÜK BİR HUZURSUZLUK KAYNAĞI OLMAYA DEVAM ETTİĞİNİ MÜŞAHEDE ETMEKTEYİM.

RAKAMSAL OLARAK KADROLAŞMA ÖRNEKLERİ

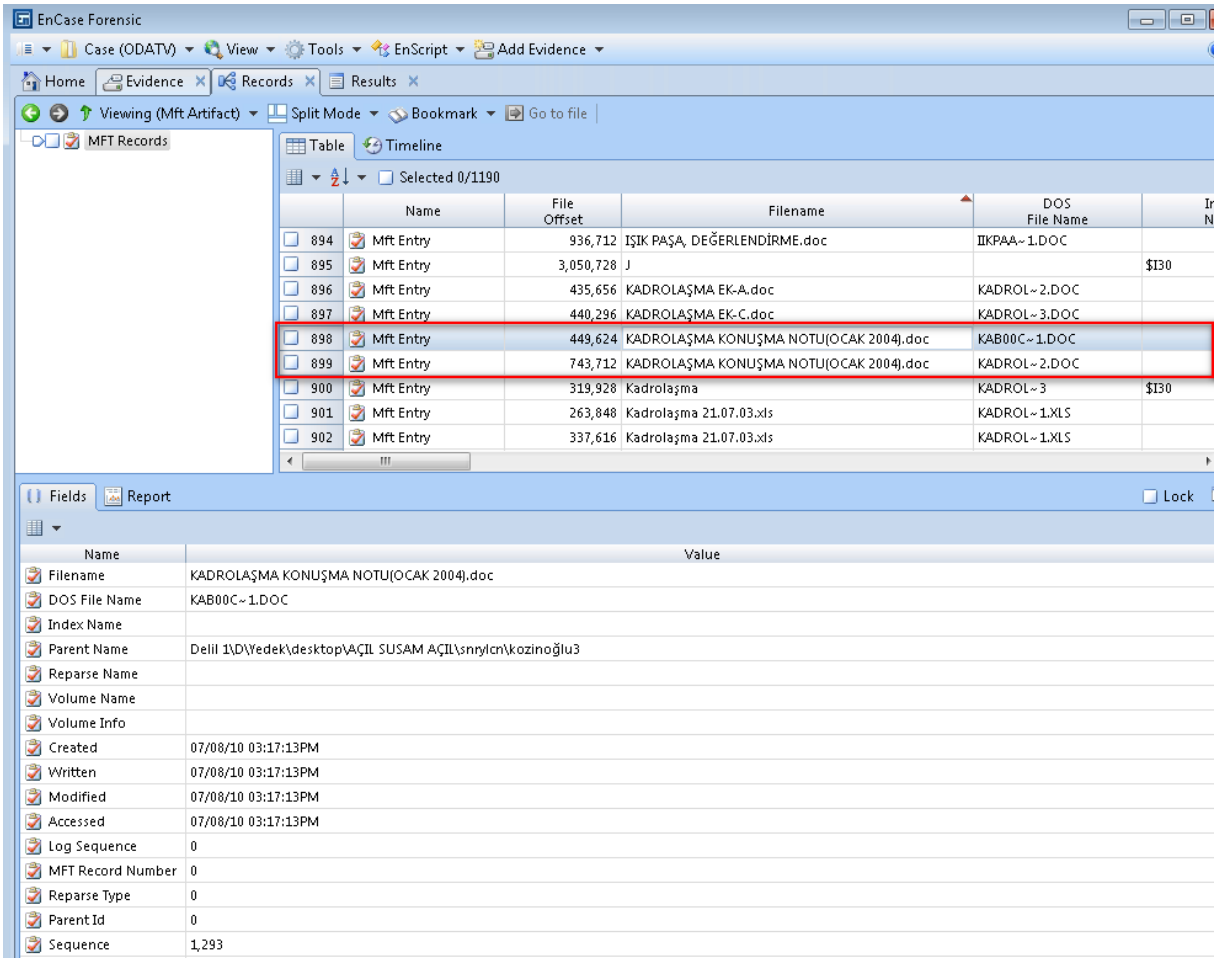
58 NCİ VE ONUN DEVAMI OLAN 59 NCU HÜKÜMETLERİN İKTİDARA GELDİKLERİ KASIM 2002 İLE ARALIK 2003 TARİHLERİ ARASINDAKİ 14 AYLIK DÖNEM İÇERİSİNDE VEKALETEN YAPILANLAR DAHİL, TOPLAM 1689 ATAMA YAPILMIŞ OLUP, BU MİKTAR; 57NCİ HÜKÜMET DÖNEMİNDE 3.5 YILLIK SÜRE İÇERİSİNDE YAPILAN ATAMA MİKTARININ (1928 ADET) %87,6'SINA ULAŞMIŞTIR.

Şekil 42 - KADROLAŞMA KONUŞMA NOTU(OCAK 2004) içerikli dosya

Tespit edilen ve görüntülenebilenKADROLAŞMA KONUŞMA NOTU(OCAK 2004).doc dosyası tamamen kurtarılabilmiştir. Kurtarılan dosyadan elde edilen metaveriler aşağıdaki gibidir.

Belge Üstverileri	
Dosya Adı	KADROLAŞMA KONUŞMA NOTU(OCAK 2004).doc
Dosya Konumu	
Dosya Durumu	Silinmiş, $MFT kaydı yok,unallocated clusterda bulunuyor.
Yazar	KARA KUVVETLERI KOMUTANLIGI
Son Değiştiren Kullanıcı	KARA KUVVETLERI KOMUTANLIGI
Yönetici	
Şirket	KARA KUVVETLERI KOMUTANLIGI
Nesne Tipi	Microsoft Word Belgesi
Yazılım Tipi	Microsoft Word 9.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	2900
Uygulama Versiyonu	9.4402
Dosya Boyutu	28 kB
Toplam Değiştirme Süresi	30.0 dakika
Revizyon Numarası	6
Belge Oluşturma Tarihi	2004:01:08 15:10:00
Belge Değiştirme Tarihi	2004:01:08 15:40:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	
FN Oluşturma Zamanı	
Std Değiştirme Zamanı	
FN Değiştirme Zamanı	
Std Erişim Zamanı	
FN Erişim Zamanı	
Std Giriş Zamanı	
FN Giriş Zamanı	

KADROLAŞMA KONUŞMA NOTU(OCAK 2004).doc dosyasının bu imajda bulunduğuna dair Logfile (MFT Artifact) kaydına da rastlanmıştır.



Şekil 43 - KADROLAŞMA KONUŞMA NOTU(OCAK 2004).doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Belge Üstverileri	
Dosya Adı	KADROLAŞMA KONUŞMA NOTU(OCAK 2004) .doc
Dosya Konumu	\D\Lost Files\Kadrolasma\Kadrolasma GPP Çalismasi\KADROLASMA KONUSMA NOTU(OCAK 2004).doc
Dosya Durumu	Silinmiş
Yazar	
Son Değiştiren Kullanıcı	
Yönetici	

Şirket	
Nesne Tipi	
Yazılım Tipi	
Karakter Tipi	
Karakter Sayısı	
Uygulama Versiyonu	
Dosya Boyutu	28 kB
Toplam Değiştirme Süresi	
Revizyon Numarası	
Belge Oluşturma Tarihi	
Belge Değiştirme Tarihi	
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-07-08 20:20:45.355124
FN Oluşturma Zamanı	2010-07-08 20:20:45.355124
Std Değiştirme Zamanı	2004-01-08 14:40:14
FN Değiştirme Zamanı	2010-07-08 20:20:45.355124
Std Erişim Zamanı	2010-07-08 20:20:45.370750
FN Erişim Zamanı	2010-07-08 20:20:45.355124
Std Giriş Zamanı	2010-07-08 20:20:45.370750
FN Giriş Zamanı	2010-07-08 20:20:45.355124

Belge Üstverileri	
Dosya Adı	KADROLAŞMA KONUŞMA NOTU(OCAK 2004) .doc
Dosya Konumu	\D\Lost Files\001 AKP-KADROLASMA ÇALISMALARI\KADROLASMA KONUSMA NOTU(OCAK 2004).doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunmuyor.
Yazar	
Son Değiştiren Kullanıcı	
Yönetici	
Şirket	
Nesne Tipi	
Yazılım Tipi	
Karakter Tipi	
Karakter Sayısı	
Uygulama Versiyonu	
Dosya Boyutu	28 kB
Toplam Değiştirme Süresi	
Revizyon Numarası	
Belge Oluşturma Tarihi	
Belge Değiştirme Tarihi	
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-07-08 20:20:48.230124
FN Oluşturma Zamanı	2010-07-08 20:20:48.230124

Std Değiştirme Zamanı	2004-01-08 14:40:14
FN Değiştirme Zamanı	2010-07-08 20:20:48.230124
Std Erişim Zamanı	2010-07-08 20:20:48.230124
FN Erişim Zamanı	2010-07-08 20:20:48.230124
Std Giriş Zamanı	2010-07-08 20:20:48.230124
FN Giriş Zamanı	2010-07-08 20:20:48.230124

Bu dosyanın da daha önce bahsi geçen Tablo 3 - 08_07(2).rar Sıkıştırılmış Dosyasında Bulunan Kayıtlar isimli sıkıştırılmış dosyadan çıkarıldığı düşünülmektedir.

"KADROLAŞMA KONUŞMA NOTU(OCAK 2004).doc" dokümanı Delil2 diskinde silinmiş ama $MFT kaydı kurtarılabilir durumda bulunmaktadır. Ayrıca bu dosyanın Delil1 diskinde "unallocated cluster" üzerinde bir kopyasına rastlanmış ve veri kurtarma programları yardımıyla kurtarılabilmiştir. Delil1 üzerinde bulunan dosyadan sadece dosya üstverilerine, Delil2 den ise sadece dosya sistemi üstverilerine ulaşılabilmiştir. Delil2 de bu dosyanın bulunduğu iki ayrı dizin için $Logfile kayıtlarına ulaşılmıştır. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.

- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

- Delil2 deki ikinci kopyanın (oluşturma zamanı 3 dk ileride olan), ilk dosyanın başka bir dizine kopyalanması ile oluşturulduğu düşünülmektedir. Bunun sebebi de zaman bilgisi ileride olan dosyanın STD oluşturma, STD erişim, STD MFT kaydı değişim zamanları ile FN zamanlarının tümünün aynı değerde olmasıdır.

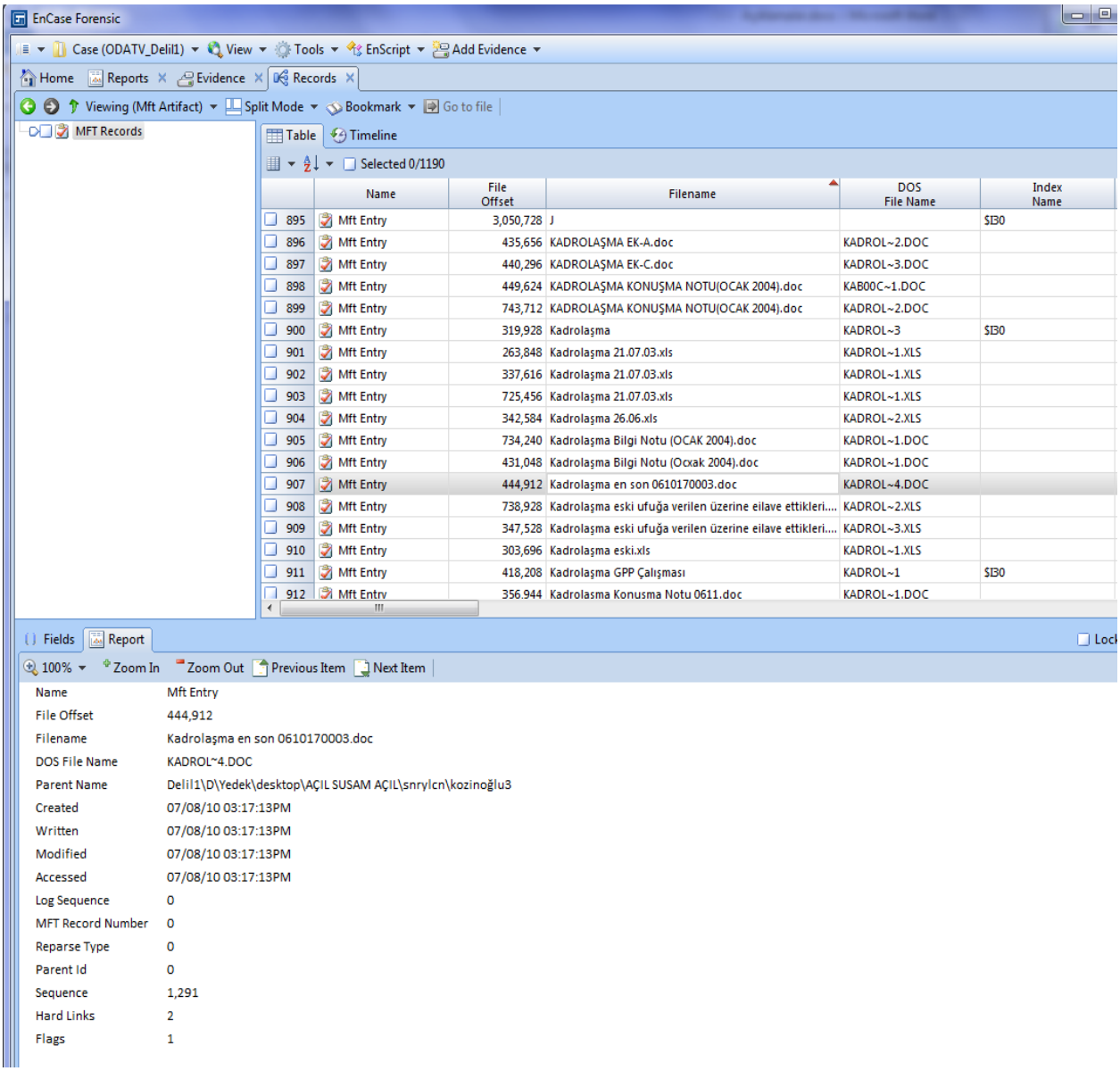
S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

18.) Kadrolaşma en son0610170003.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Yapılan incelemelerde diskin Logfile alanında bu dosyaya ait kayda rastlanılmıştır. $Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.



Şekil 44 - Kadrolaşma en son0610170003.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

Gerçekleştirilen detaylı tetkikler neticesinde, unallocated clusters alanında bu dosya olduğu düşünülen bir dosya kurtarılmıştır. Dosya içeriği aşağıdaki gibidir.

GİZLİ

DEVLETTE KADROLAŞMA
BİLGİ NOTU
(EKİM 2003)

1. ÖNCESİ :

a. Genel :

AKP; Kasım 2002- Ekim 2003 tarihleri arasında geçen 11 aylık süre içerisinde hükümet etmeye başladığı günden itibaren sürekli ve sistemli olarak Devletin tüm kurum ve kuruluşları içerisinde, üst düzey bürokratlardan başlamak üzere en alt seviyedeki memura kadar kadrolaşma gayreti içerisindedir. Hükümet mevcut sistemi hemen yıkmak yerine, devlet yapısıyla çatışmayacak şekilde kadrolaşmak suretiyle, zaman içerisinde Devletin stratejik kurum ve kuruluşlarının içine sızmayı, bu kurum ve kuruluşları ele geçirmeyi ya da kontrol etmeyi benimsemektedir.

Hükümet arzu ettiği kadrolaşmayı gerçekleştirmek maksadıyla çeşitli yöntemler uygulamaktadır. Bu yöntemler;

- Üst düzey bürokratları üçlü kararname ile asaleten atamak,
- Asaleten atamanın yapılamadığı durumlarda (Cumhurbaşkanının onaylamaması, atanan kişiye ait yasal engellerin bulunması, görevin gerektirdiği şartlara haiz olamama durumu vb) vekaleten atama veya geçici

Şekil 45 - Kadrolaşma en son0610170003.doc Dosyası İçeriği

Dosya kurtarma çalışmaları neticesinde, dokumana ait belge üstverileri de elde edilmiştir. Detaylı bilgi için aşağıdaki tablo incelenebilir.

Belge Üstverileri	
Dosya Adı	Kadrolaşma en son0610170003.doc
Dosya Konumu	Unallocated Clusters
Dosya Durumu	Silinmiş, $MFT kaydı yok, unallocated clusterda bulunuyor.
Yazar	bim

Son Değiştiren Kullanıcı	bim
Yönetici	
Şirket	kkk
Nesne Tipi	Microsoft Word Belgesi
Yazılım Tipi	Microsoft Word 9.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	20469
Uygulama Versiyonu	
Dosya Boyutu	76 kB
Toplam Değiştirme Süresi	1 saat
Revizyon Numarası	12
Belge Oluşturma Tarihi	2003-10-11 06:33:00
Belge Değiştirme Tarihi	2003-10-13 06:27:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	
FN Oluşturma Zamanı	
Std Değiştirme Zamanı	
FN Değiştirme Zamanı	
Std Erişim Zamanı	
FN Erişim Zamanı	
Std Giriş Zamanı	
FN Giriş Zamanı	

Office Word dokümanlarının bazı versiyonlarında bulunan “Son 10 Kullanıcı Bilgisi” üstverisi incelendiğinde, dosyanın daha önce “Kadrolaşma en son0610170003.doc” ismiyle kayıtlı olduğu tespit edilmiştir. Son 10 kullanıcıya ait bilgiler aşağıda sıralanmıştır.

Son Kullanıcı Üstveri Bilgileri		
No	**Yazar**	**Lokasyon**
1	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc
2	bim	C:\Documents and Settings\63752024\Application Data\Microsoft\Word\Otomatik Kurtarma kayd1Kadrolaşma en son 0610170003.asd

3	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc
4	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc
5	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc
6	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc
7	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc
8	bim	C:\Documents and Settings\63752024\Application Data\Microsoft\Word\Otomatik Kurtarma Kadrolaşma en son 0610170003.asd
9	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc
10	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc

Tablo 4 - Kadrolaşma en son0610170003.doc Son Kullanıcı Üstverileri

Tespit edilen veriler ışığında, silinmiş alandan kurtarılan bu dosyanın Kadrolaşma en son 0610170003.doc olduğu düşünülmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Belge Üstverileri	
Dosya Adı	Kadrolaşma en son0610170003.doc
Dosya Konumu	\D\Lost Files\Kadrolasma\Kadrolasma GPP Çalismasi\Kadrolasma en son 0610170003.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunmuyor.
Yazar	
Son Değiştiren Kullanıcı	
Yönetici	
Şirket	
Nesne Tipi	

Yazılım Tipi	
Karakter Tipi	
Karakter Sayısı	
Uygulama Versiyonu	
Dosya Boyutu	76 kB
Toplam Değiştirme Süresi	
Revizyon Numarası	
Belge Oluşturma Tarihi	
Belge Değiştirme Tarihi	
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-07-08 20:20:45.355124
FN Oluşturma Zamanı	2010-07-08 20:20:45.355124
Std Değiştirme Zamanı	2003-10-13 05:27:14
FN Değiştirme Zamanı	2010-07-08 20:20:45.355124
Std Erişim Zamanı	2010-07-08 20:20:45.355124
FN Erişim Zamanı	2010-07-08 20:20:45.355124
Std Giriş Zamanı	2010-07-08 20:20:45.355124
FN Giriş Zamanı	2010-07-08 20:20:45.355124

Bu dosyanın da daha önce bahsi geçen Tablo 3 - 08_07(2).rar Sıkıştırılmış Dosyasında Bulunan Kayıtlar isimli sıkıştırılmış dosyadan çıkarıldığı düşünülmektedir.

“Kadrolaşma en son0610170003.doc” dokümanı Delil2 diskinde silinmiş ama $MFT kaydı kurtarılabilir durumda bulunmaktadır. Ayrıca bu dosyanın Delil1 diskinde "unallocated cluster" üzerinde bir kopyasına rastlanmış ve veri kurtarma programları yardımıyla kurtarılabilmiştir. Delil1 üzerinde bulunan dosyadan sadece belge üstverilerine, Delil2 den ise sadece dosya sistemi üstverilerine ulaşılabilmiştir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.

- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir

yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

• Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

• Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

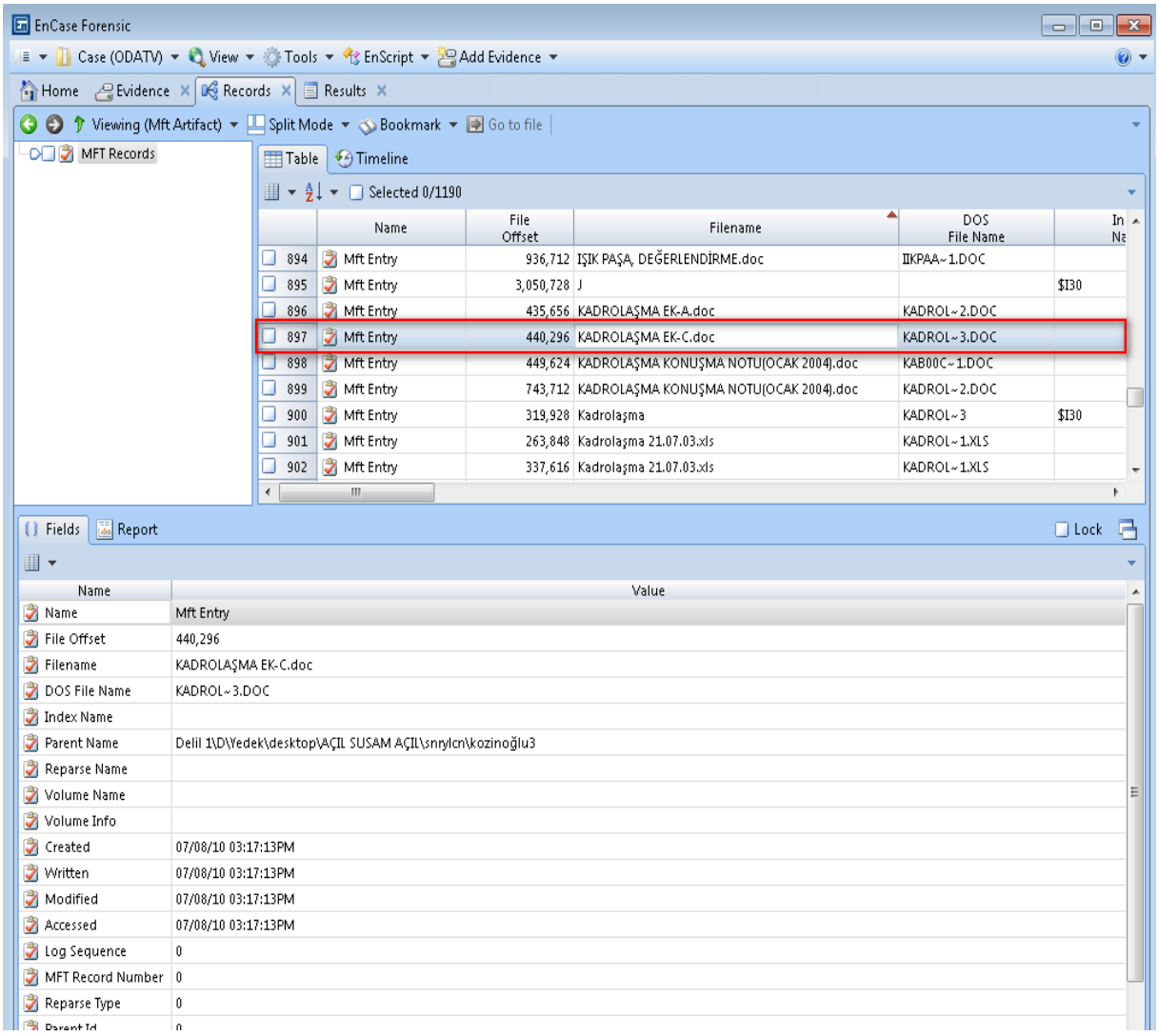
S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

19.) KADROLAŞMA EK-C.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Yapılan incelemelerde diskin Logfile alanında bu dosyaya ait kayda rastlanılmıştır. $Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.



Şekil 46 - KADROLAŞMA EK-C.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

Bununla beraber dosyanın kendisine ulaşılamamıştır. Dosyanın kendisinin bulunamayıp LogFile kayıtlarının tespit edilmesi, dosyanın silinmiş ve dosyanın bulunduğu disk alanının üzerine başka bir dosyanın verilerinin yazılmış olduğuna işaret etmektedir

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Belge Üstverileri	
Dosya Adı	KADROLAŞMA EK-C.doc
Dosya Konumu	\D\Lost Files\Kadrolasma\Kadrolasma GPP Çalismasi\KADROLASMA EK-C.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunmuyor.
Yazar	
Son Değiştiren Kullanıcı	
Yönetici	
Şirket	
Nesne Tipi	
Yazılım Tipi	
Karakter Tipi	
Karakter Sayısı	
Uygulama Versiyonu	
Dosya Boyutu	28 kB
Toplam Değiştirme Süresi	
Revizyon Numarası	
Belge Oluşturma Tarihi	
Belge Değiştirme Tarihi	
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-07-08 20:20:45.339500
FN Oluşturma Zamanı	2010-07-08 20:20:45.339500
Std Değiştirme Zamanı	2003-10-09 11:04:20
FN Değiştirme Zamanı	2010-07-08 20:20:45.339500
Std Erişim Zamanı	2010-07-08 20:20:45.355124
FN Erişim Zamanı	2010-07-08 20:20:45.339500
Std Giriş Zamanı	2010-07-08 20:20:45.355124
FN Giriş Zamanı	2010-07-08 20:20:45.339500

Bu dosyanın da daha önce bahsi geçen Tablo 3 - 08_07(2).rar Sıkıştırılmış Dosyasında Bulunan Kayıtlar isimli sıkıştırılmış dosyadan çıkarıldığı düşünülmektedir.

"KADROLAŞMA EK-C.doc" dokümanı Delil2 diskinde silinmiş ama $MFT kaydı kurtarılabilir durumda bulunmaktadır. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

• İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

• Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

• Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

• Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

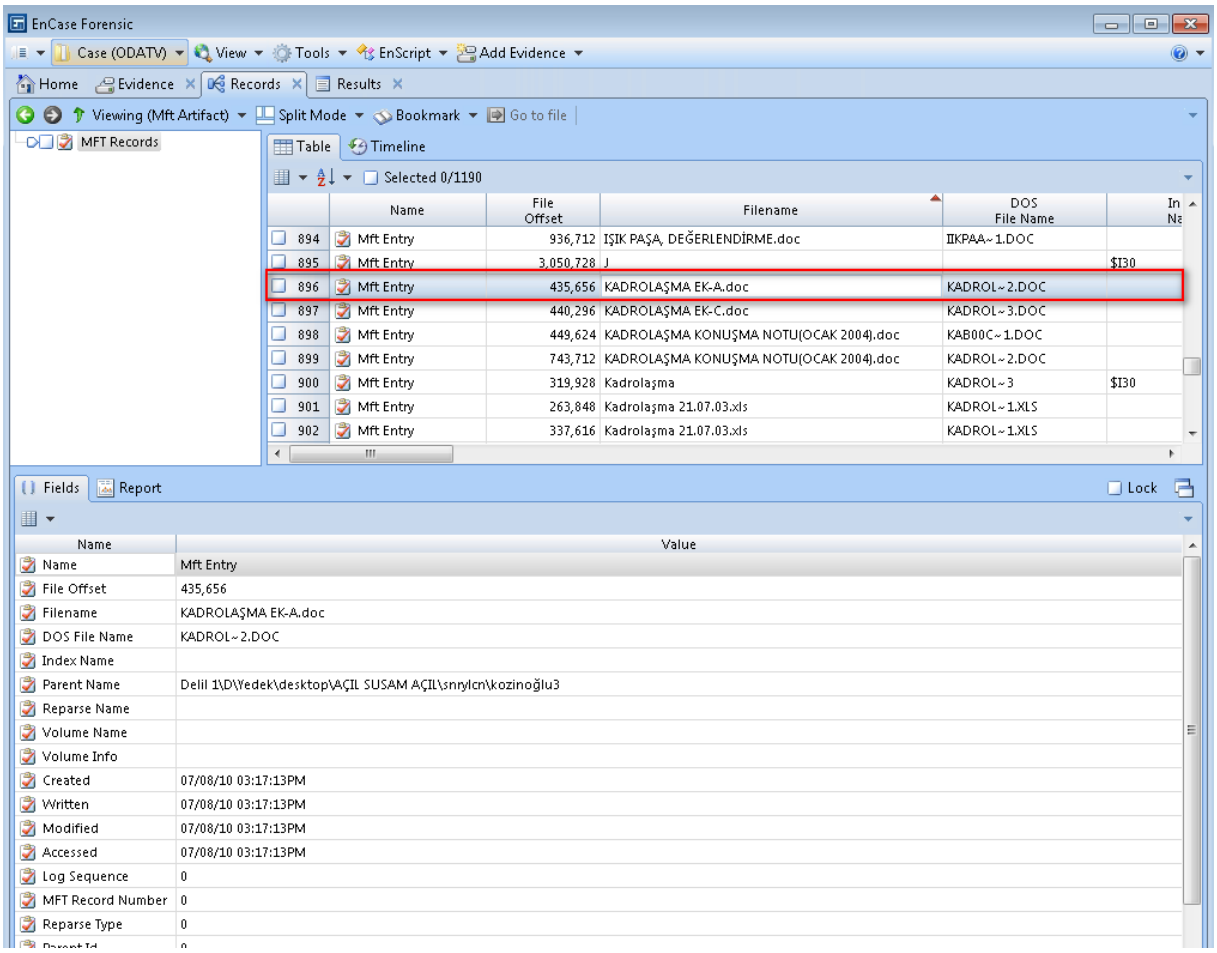
S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

20.) KADROLAŞMA EK-A.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Yapılan incelemelerde diskin Logfile alanında bu dosyaya ait kayda rastlanılmıştır. $Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.



Şekil 47 - KADROLAŞMA EK-A.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

Bununla beraber dosyanın kendisine ulaşılamamıştır. Dosyanın kendisinin bulunamayıp LogFile kayıtlarının tespit edilmesi, dosyanın silinmiş ve dosyanın bulunduğu disk alanının üzerine başka bir dosyanın verilerinin yazılmış olduğuna işaret etmektedir

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Belge Üstverileri	
Dosya Adı	KADROLAŞMA EK-A.doc
Dosya Konumu	\D\Lost Files\Kadrolasma\Kadrolasma GPP Çalismasi\KADROLASMA EK-A.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunmuyor.
Yazar	
Son Değiştiren Kullanıcı	
Yönetici	
Şirket	
Nesne Tipi	

Yazılım Tipi	
Karakter Tipi	
Karakter Sayısı	
Uygulama Versiyonu	
Dosya Boyutu	40 kB
Toplam Değiştirme Süresi	
Revizyon Numarası	
Belge Oluşturma Tarihi	
Belge Değiştirme Tarihi	
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-07-08 20:20:45.339500
FN Oluşturma Zamanı	2010-07-08 20:20:45.339500
Std Değiştirme Zamanı	2003-10-09 11:08:50
FN Değiştirme Zamanı	2010-07-08 20:20:45.339500
Std Erişim Zamanı	2010-07-08 20:20:45.339500
FN Erişim Zamanı	2010-07-08 20:20:45.339500
Std Giriş Zamanı	2010-07-08 20:20:45.339500
FN Giriş Zamanı	2010-07-08 20:20:45.339500

Bu dosyanın da daha önce bahsi geçen Tablo 3 - 08_07(2).rar Sıkıştırılmış Dosyasında Bulunan Kayıtlar isimli sıkıştırılmış dosyadan çıkarıldığı düşünülmektedir.

"KADROLAŞMA EK-A.doc" dokümanı Delil2 diskinde silinmiş ama $MFT kaydı kurtarılabilir durumda bulunmaktadır. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

21.) Kadrolaşma Bilgi Notu (Ocxak 2004).doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

İlgili dosyanın silinmiş olduğu ve $MFT kaydının bulunmadığı tespit edilmiştir. Ancak unallocated clusters alanında içeriği tespit edilen ve bu dosya olduğu düşünülen bir dosya kurtarılmıştır.

Dosya içeriği aşağıdaki gibidir.

GİZLİ

DEVLETTE KADROLAŞMA
BİLGİ NOTU
(OCAK 2004)

1. ÖNCESİ :

a. Genel :

AKP; Kasım 2002- Aralık 2003 tarihleri arasında geçen 14 aylık süre içerisinde hükümet etmeye başladığı günden itibaren sürekli ve sistemli olarak Devletin tüm kurum ve kuruluşları içerisinde, üst düzey bürokratlardan başlamak üzere en alt seviyedeki memura kadar kadrolaşma gayreti içerisindedir. Hükümet mevcut sistemi hemen yıkmak yerine, devlet yapısıyla çatışmayacak şekilde kadrolaşmak suretiyle, zaman içerisinde Devletin stratejik kurum ve kuruluşlarının içine sızmayı, bu kurum ve kuruluşları ele geçirmeyi ya da kontrol etmeyi benimsemektedir.

Hükümet arzu ettiği kadrolaşmayı gerçekleştirmek maksadıyla çeşitli yöntemler uygulamaktadır. Bu yöntemler;

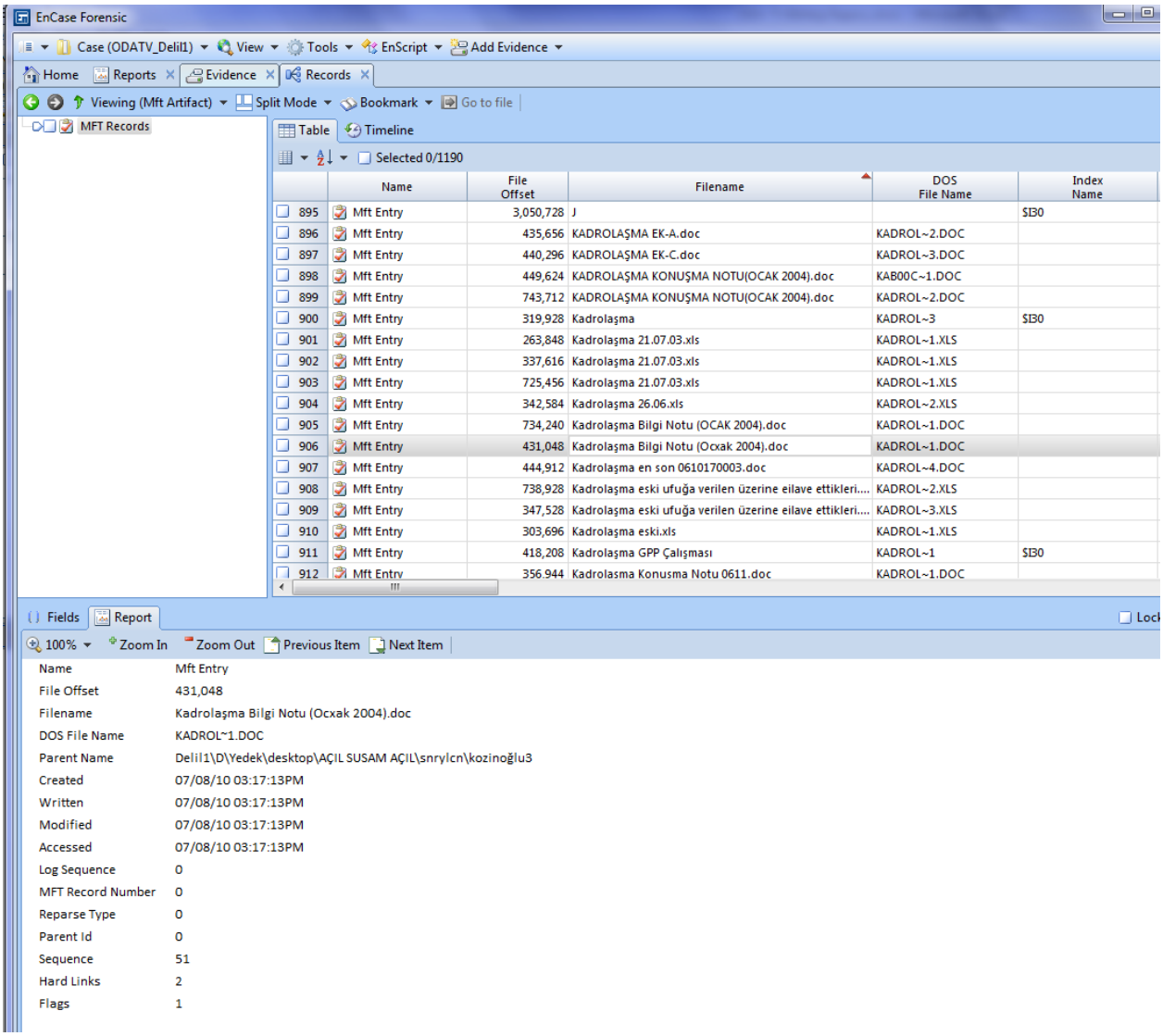
- Üst düzey bürokratları üçlü kararname ile asaleten atamak,
- Asaleten atamanın yapılamadığı durumlarda (Cumhurbaşkanının onaylamaması, atanan kişiye ait yasal engellerin bulunması, görevin gerektirdiği şartlara haiz olamama durumu vb.) vekaleten atama veya geçici görevlendirmek,
- Kurum ve kuruluşların atamaya ilişkin yönetmeliklerinde değişiklik yapmak suretiyle atamayı yapılabilir hale getirmek,
- Kurumlar arası yatay geçiş yapmak suretiyle (Diyanet işleri Başkanlığına alınan İmam Hatip mezunlarının diğer kamu kurum ve kuruluşlarına atanması) istenilen kurumda kadrolaşmak,

Şekil 48 - Kadrolaşma Bilgi Notu (Ocxak 2004).doc içerikli dosya

Tespit edilen ve görüntülenebilen Kadrolaşma Bilgi Notu (Ocxak 2004).doc dosyası tamamen kurtarılabilmiştir. Tespit edilen metaveriler için alttaki tablo incelenebilir.

Belge Üstverileri	
Dosya Adı	Kadrolaşma Bilgi Notu (Ocxak 2004).doc
Dosya Konumu	
Dosya Durumu	Silinmiş, $MFT kaydı yok,unallocated clusterda bulunuyor.
Yazar	bim
Son Değiştiren Kullanıcı	KARA KUVVETLERI KOMUTANLIGI
Yönetici	
Şirket	kkk
Nesne Tipi	Microsoft Word Belgesi
Yazılım Tipi	Microsoft Word 9.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	16674
Uygulama Versiyonu	9.4402
Dosya Boyutu	74 kB
Toplam Değiştirme Süresi	3.0 dakika
Revizyon Numarası	3
Belge Oluşturma Tarihi	2004:01:08 14:45:00
Belge Değiştirme Tarihi	2004:01:08 14:47:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	
FN Oluşturma Zamanı	
Std Değiştirme Zamanı	
FN Değiştirme Zamanı	
Std Erişim Zamanı	
FN Erişim Zamanı	
Std Giriş Zamanı	
FN Giriş Zamanı	

Kadrolaşma Bilgi Notu (Ocxak 2004).doc dosyasının bu imajda bulunduğuna dair Logfile (MFT Artifact) kaydına da rastlanmıştır.



Şekil 49 - Kadrolaşma Bilgi Notu (Ocxak 2004) .doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

Tespit edilen bu bilgilerin yanı sıra, Office Word dokümanlarının bazı versiyonlarında bulunan "Son 10 Kullanıcı Bilgisi" üstverisi incelendiğinde, dosyanın daha önce "- Kadrolaşma Bilgi Notu (Ocxak 2004) .doc" ismiyle kayıtlı olduğu tespit edilmiştir. Son 10 kullanıcıya ait bilgiler aşağıda sıralanmıştır.

Son Kullanıcı Üstveri Bilgileri		
No	**Yazar**	**Lokasyon**
1	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc

2	bim	C:\Documents and Settings\63752024\Application Data\Microsoft\Word\Otomatik Kurtarma kayd1Kadrolaşma en son 0610170003.asd
3	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc
4	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc
5	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc
6	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc
7	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc
8	bim	C:\Documents and Settings\63752024\Application Data\Microsoft\Word\Otomatik Kurtarma Kadrolaşma en son 0610170003.asd
9	bim	C:\Documents and Settings\63752024\Desktop\Kadrolaşma en son 0610170003.doc
10	KARA KUVVETLERI KOMUTANLIGI	L:\2220-ICISTIHBARATSUBE\Belgeler\3 ncü kısım\İrticai faaliyetler\Kadrolaşma GPP Çalışması\Kadrolaşma Bilgi Notu (Ocxak 2004).doc

Tespit edilen veriler ışığında, silinmiş alandan kurtarılan bu dosyanın Kadrolaşma Bilgi Notu (Ocxak 2004) .doc olduğu düşünülmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Belge Üstverileri	
Dosya Adı	Kadrolaşma Bilgi Notu (Ocxak 2004) .doc
Dosya Konumu	\D\Lost Files\Kadrolasma\Kadrolasma GPP Çalismasi\Kadrolasma Bilgi Notu (Ocxak 2004).doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunmuyor
Yazar	
Son Değiştiren Kullanıcı	
Yönetici	

Şirket	
Nesne Tipi	
Yazılım Tipi	
Karakter Tipi	
Karakter Sayısı	
Uygulama Versiyonu	
Dosya Boyutu	76 kB
Toplam Değiştirme Süresi	
Revizyon Numarası	
Belge Oluşturma Tarihi	
Belge Değiştirme Tarihi	
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-07-08 20:20:45.323875
FN Oluşturma Zamanı	2010-07-08 20:20:45.323875
Std Değiştirme Zamanı	2004-01-08 13:47:38
FN Değiştirme Zamanı	2010-07-08 20:20:45.323875
Std Erişim Zamanı	2010-07-08 20:20:45.339500
FN Erişim Zamanı	2010-07-08 20:20:45.323875
Std Giriş Zamanı	2010-07-08 20:20:45.339500
FN Giriş Zamanı	2010-07-08 20:20:45.323875

Bu dosyanın da daha önce bahsi geçen Tablo 3 - 08_07(2).rar Sıkıştırılmış Dosyasında Bulunan Kayıtlar isimli sıkıştırılmış dosyadan çıkarıldığı düşünülmektedir.

“Kadrolaşma Bilgi Notu (Ocxak 2004).doc” dokümanı Delil2 diskinde silinmiş ama $MFT kaydı kurtarılabilir durumda bulunmaktadır. Ayrıca bu dosyanın Delil1 diskinde "unallocated cluster" üzerinde bir kopyasına rastlanmış ve veri kurtarma programları yardımıyla kurtarılabilmiştir. Delil1 üzerinde bulunan dosyadan sadece belge üstverilerine, Delil2 den ise sadece dosya sistemi üstverilerine ulaşılabilmiştir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

• Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

• Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

• Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

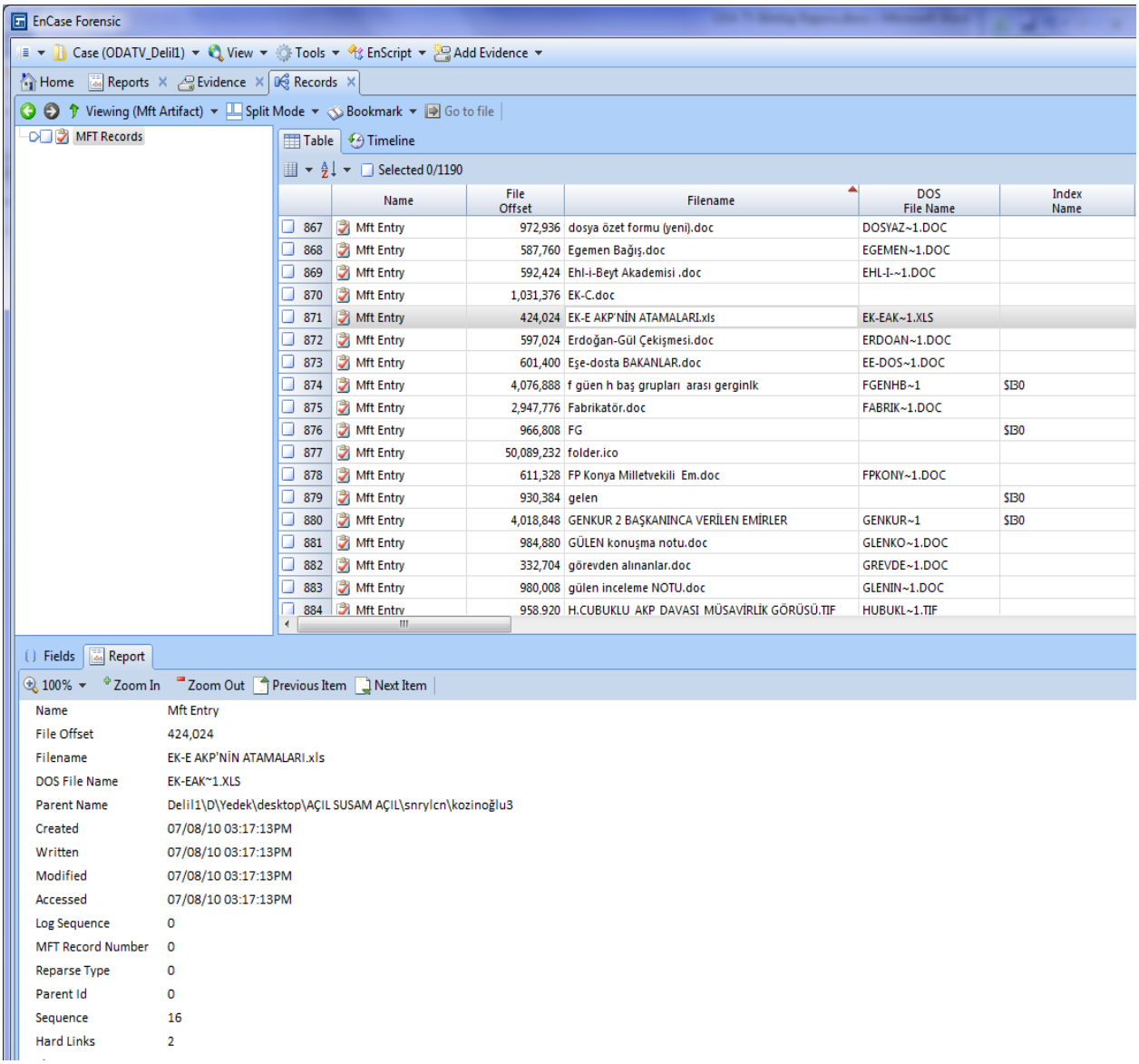
S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

22.) EK-E AKP'NİN ATAMALARI.xls

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

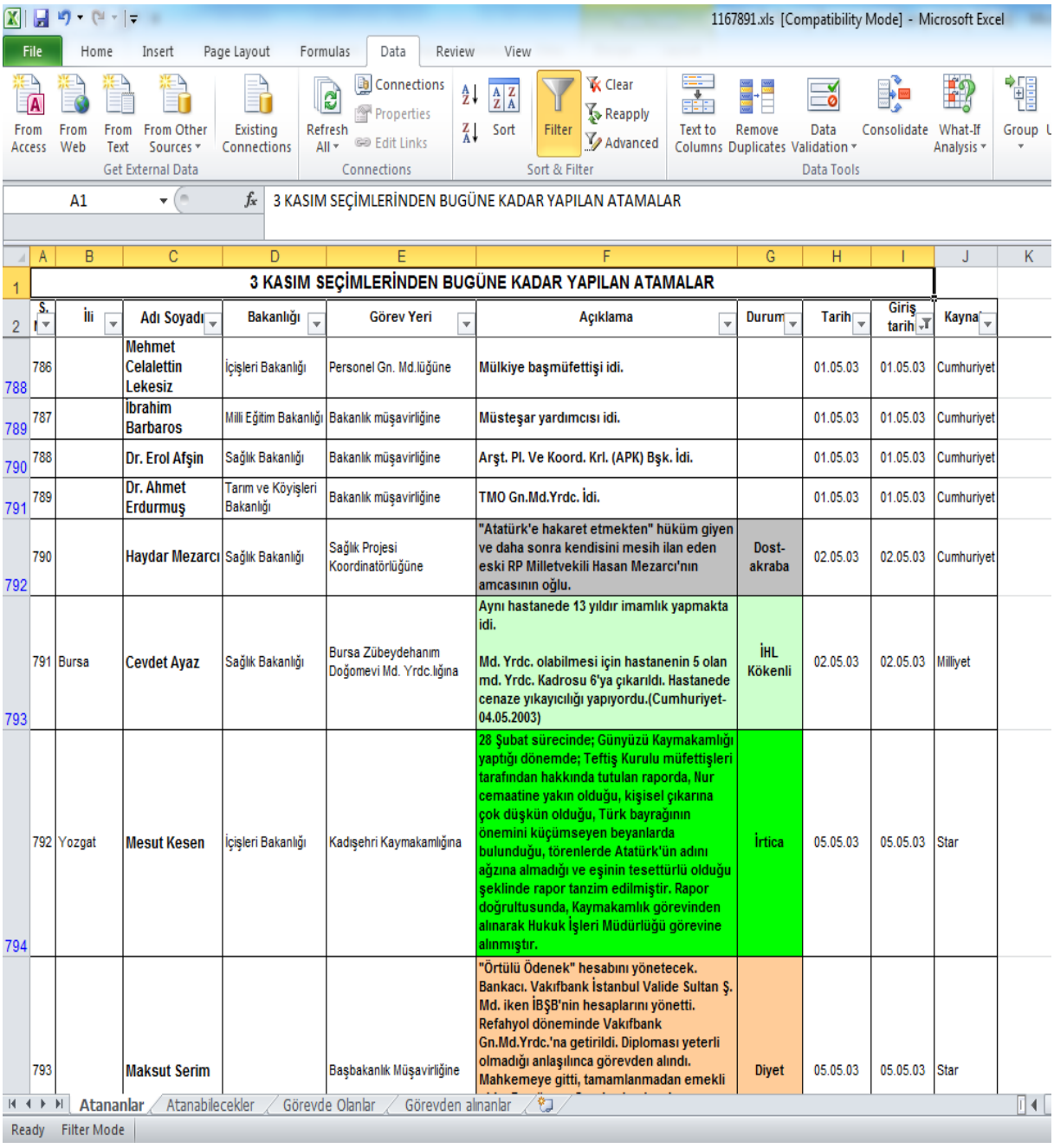
Yapılan incelemelerde diskin Logfile alanında bu dosyaya ait kayda rastlanılmıştır. $Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.



Şekil 50 - EK-E AKP'NİN ATALAMALARI.xls Dosyasına Ait Logfile (MFT Artifact) Kaydı

Gerçekleştirilen incelemeler neticesinde unallocated clusters alanında bu dosya olduğu düşünülen bir dosya bulunmuştur.

Dosyaya ait ekran kopyası aşağıda verilmiştir.



Şekil 51 - EK-E AKP'NİN ATAMALARI.xls olduğu düşünülen dosya içeriği

Kurtarılan dosyaya ait belge üstverileri aşağıdaki gibidir.

Belge Üstverileri	
Dosya Adı	EK-E AKP'NİN ATAMALARI.xls
Dosya Konumu	Unallocated clusters
Dosya Durumu	Silinmiş, $MFT kaydı yok, unallocated clusterda bulunuyor
Yazar	BIM
Son Değiştiren Kullanıcı	KARA KUVVETLERI KOMUTANLIGI

Yönetici	
Şirket	KARA KUVVETLERI KOMUTANLIGI
Nesne Tipi	Microsoft Excel
Yazılım Tipi	
Karakter Tipi	
Karakter Sayısı	
Uygulama Versiyonu	
Dosya Boyutu	
Toplam Değiştirme Süresi	
Revizyon Numarası	
Belge Oluşturma Tarihi	2003-04-11 09:31:53
Belge Değiştirme Tarihi	2003-05-09 09:39:17
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	
FN Oluşturma Zamanı	
Std Değiştirme Zamanı	
FN Değiştirme Zamanı	
Std Erişim Zamanı	
FN Erişim Zamanı	
Std Giriş Zamanı	
FN Giriş Zamanı	

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Belge Üstverileri	
Dosya Adı	EK-E AKP'NİN ATAMALARI.xls
Dosya Konumu	\D\Lost Files\Kadrolasma\Kadrolasma GPP Çalismasi\EK-E AKP'NIN ATAMALARI.xls
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunmuyor
Yazar	
Son Değiştiren Kullanıcı	
Yönetici	
Şirket	
Nesne Tipi	
Yazılım Tipi	
Karakter Tipi	
Karakter Sayısı	
Uygulama Versiyonu	
Dosya Boyutu	20 kB
Toplam Değiştirme Süresi	
Revizyon Numarası	
Belge Oluşturma Tarihi	
Belge Değiştirme Tarihi	

Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-07-08 20:20:45.323875
FN Oluşturma Zamanı	2010-07-08 20:20:45.323875
Std Değiştirme Zamanı	2003-10-31 11:58:36
FN Değiştirme Zamanı	2010-07-08 20:20:45.323875
Std Erişim Zamanı	2010-07-08 20:20:45.323875
FN Erişim Zamanı	2010-07-08 20:20:45.323875
Std Giriş Zamanı	2010-07-08 20:20:45.323875
FN Giriş Zamanı	2010-07-08 20:20:45.323875

Bu dosyanın da daha önce bahsi geçen Tablo 3 - 08_07(2).rar Sıkıştırılmış Dosyasında Bulunan Kayıtlar tablosunda belirtilen sıkıştırılmış dosyadan çıkarıldığı düşünülmektedir.

“EK-E AKP'NİN ATAMALARI.xls” dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. Delil2 diskinde dosya silinmiş ama $MFT kaydı erişilebilir durumdadır. $MFT kaydından bu dosya ile alakalı dosya sistemi üstverilerine ulaşılabilmektedir. Delil2 de silinmiş ve bulunduğu disk alanının üzerine yazılmış görünmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.

- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

• Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

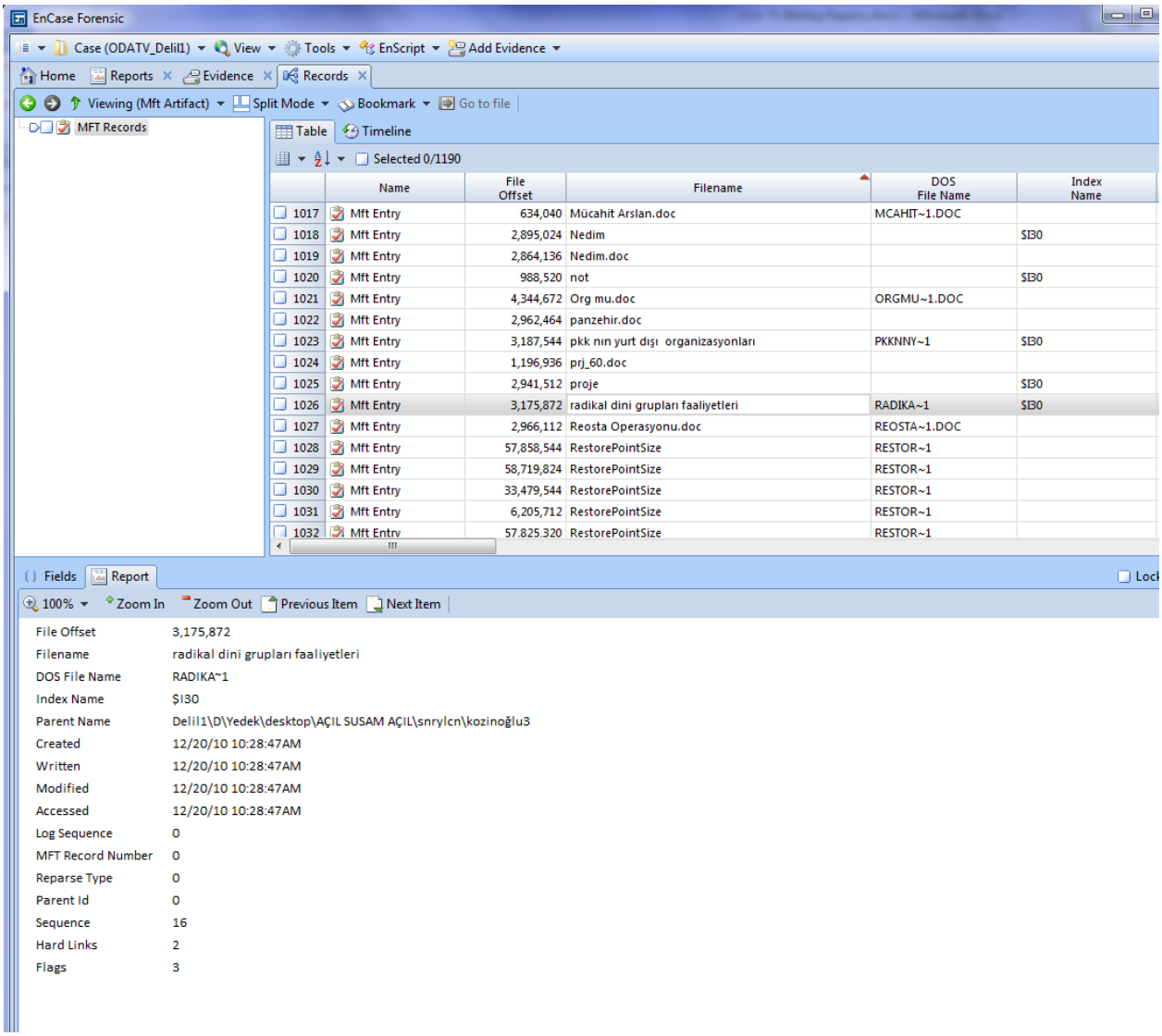
Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

23.) radikal dini grupların faaliyet alanları.pdf

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	radikal dini grupların faaliyet alanları.pdf
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\kozinoglu3\radikal dini gruplari faaliyetleri\radikal dini guruplarin faaliyet alanlari.pdf
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor
Yazar	
Son Değiştiren Kullanıcı	
Yönetici	
Şirket	
Nesne Tipi	
Yazılım Tipi	
Karakter Tipi	
Karakter Sayısı	
Uygulama Versiyonu	
Dosya Boyutu	836 kB
Toplam Değiştirme Süresi	
Revizyon Numarası	
Belge Oluşturma Tarihi	
Belge Değiştirme Tarihi	
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-12-20 08:28:47.625000
FN Oluşturma Zamanı	2010-12-20 08:28:47.625000
Std Değiştirme Zamanı	2007-12-16 22:10:50
FN Değiştirme Zamanı	2010-12-20 08:28:47.625000
Std Erişim Zamanı	2010-12-20 08:28:47.640625
FN Erişim Zamanı	2010-12-20 08:28:47.625000
Std Giriş Zamanı	2010-12-20 08:28:47.640625
FN Giriş Zamanı	2010-12-20 08:28:47.625000

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (Index Artifact) kayıtlarında da rastlanılmıştır.



Şekil 52 - radikal dini grupların faaliyetleri Dosyasına Ait Logfile (MFT Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

“radikal dini guruplarin faaliyet alanlari.pdf” dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

24.) 000KITAP.docx

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	000KITAP.docx
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\S.U\000KITAP.docx
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor
Yazar	a
Son Değiştiren Kullanıcı	sahmet
Yönetici	
Şirket	b
Nesne Tipi	
Yazılım Tipi	Microsoft Office Word
Karakter Tipi	
Karakter Sayısı	424779
Uygulama Versiyonu	
Dosya Boyutu	360 kB
Toplam Değiştirme Süresi	2.7 gün
Revizyon Numarası	
Belge Oluşturma Tarihi	2010-12-05 01:04:00
Belge Değiştirme Tarihi	2010-12-17 11:51:56
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2011-01-10 13:24:13.156248
FN Oluşturma Zamanı	2011-01-10 13:24:13.156248
Std Değiştirme Zamanı	2010-12-17 11:51:56
FN Değiştirme Zamanı	2011-01-10 13:24:13.156248
Std Erişim Zamanı	2011-01-10 13:24:13.203125
FN Erişim Zamanı	2011-01-10 13:24:13.156248
Std Giriş Zamanı	2011-01-10 13:24:13.203125
FN Giriş Zamanı	2011-01-10 13:24:13.156248

Yapılan tetkiler neticesinde dosya bu imajda silinmiş olarak tespit edilmiş ve kurtarılabilmiştir. Belge üstverilerinden hareketle, dosyanın ilk olarak **"a"** yazar bilgisine sahip bir bilgisayarda oluşturulduğu, en son olarak da **"sahmet"** isimli kullanıcı tarafından değiştirildiği görülmektedir. Elde edilen üstverilerin tamamı yukarıdaki tabloda bulunmaktadır.

"000KITAP.docx" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine

ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

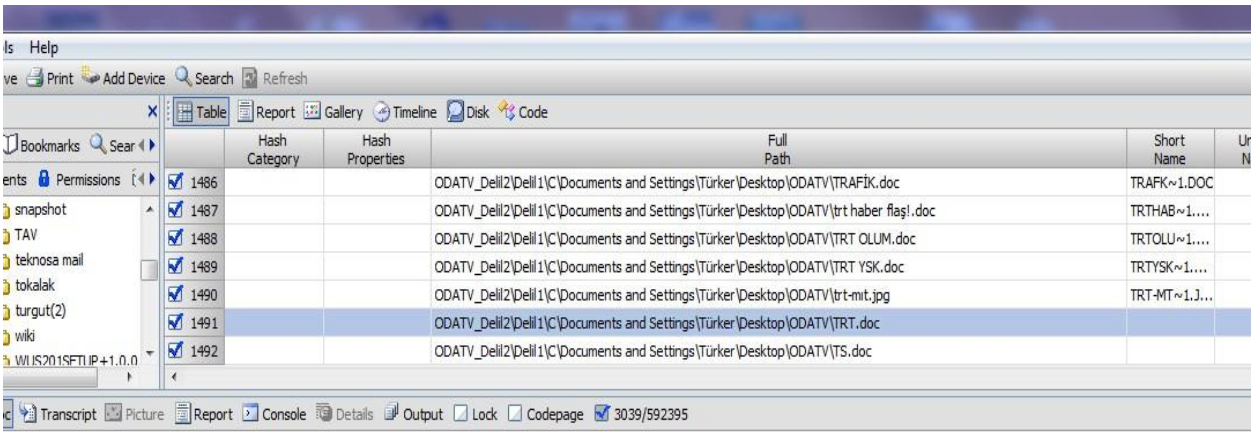
25.) trt.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

İlgili imajda 5 farklı trt.doc dosyası tespit edilmiştir. Dosyalara ait bilgiler aşağıda sıralanmış bulunmaktadır.

Belge Üstverileri	
Dosya Adı	TRT.doc
Dosya Konumu	\C\Documents and Settings\Türker\Desktop\ODATV\TRT.doc
Dosya Durumu	Aktif
Yazar	Sys
Son Değiştiren Kullanıcı	Sys
Yönetici	
Şirket	
Nesne Tipi	Microsoft Office Word Belgesi
Yazılım Tipi	Microsoft Office Word
Karakter Tipi	Windows Turkish
Karakter Sayısı	3479
Uygulama Versiyonu	11.5606
Dosya Boyutu	28 kB
Toplam Değiştirme Süresi	59.0 dakika
Revizyon Numarası	1
Belge Oluşturma Tarihi	2010:09:01 12:27:00
Belge Değiştirme Tarihi	2010:09:01 13:26:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2008-05-22 08:35:53.980000
FN Oluşturma Zamanı	2010-09-01 13:26:30.593750
Std Değiştirme Zamanı	2010-09-01 13:26:31.327999
FN Değiştirme Zamanı	2010-09-01 13:26:31.327999
Std Erişim Zamanı	2011-01-28 17:35:49.844048
FN Erişim Zamanı	2010-09-21 14:10:01.015625
Std Giriş Zamanı	2010-09-21 14:10:01.046875
FN Giriş Zamanı	2010-09-01 13:26:31.375000

Yukarıda detayı verilen TRT.doc dosyasının içeriği aşağıdaki gibidir.



TRT'DEN
SARIMSAKLI
AÇIKLAMA

TRT, yapılan barajla sular altında kalacak Allianoi üzerine hazırlattığı, **"Su Perisi Allianoi"** belgeselini 17 ve 24 Şubatta (2006) yayınlayacağını duyurdu. Ancak belgesel yayına girmedi.

DSİ'nin TRT'ye baskı yaparak belgeseli yayından kaldırttığı iddia edildi. Konu 2006 yılında Berhan Şimşek'in verdiği soru önergesine de konu oldu. Ancak TRT'den gelen cevap DSİ'nin belgesele müdahale etmediği, belgeselin yayına gireceği yönündeydi. TRT'nin 4 yıl önceki açıklamasını dönemin DSİ Genel Müdürü, bugünün Çevre ve Orman Bakanı olan Veysel Eroğlu yalanladı. Eroğlu dün sözkonusu belgeseli TRT'den kendisinin çektirdiğini söyledi.

Şekil 53 - C\Documents and Settings\Türker\Desktop\ODATV\TRT.doc dosyası

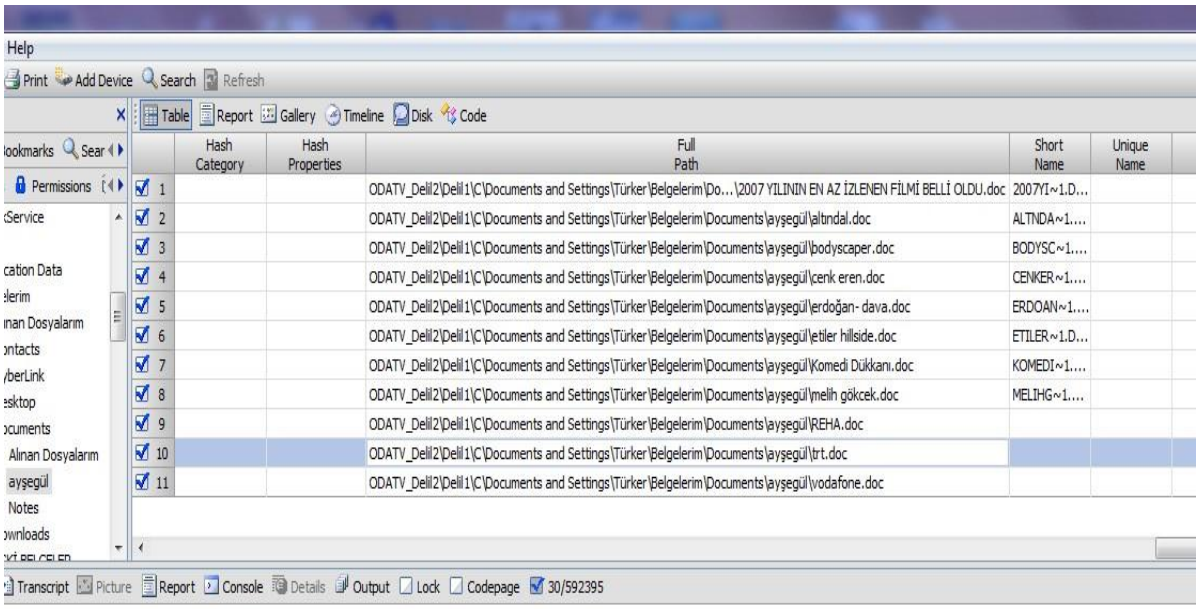
Dosya sistemi üstverilerinin ve belge üstverilerinin incelenmesi sonucu bu dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulduğu ve değiştirildiği değerlendirilmektedir. Bu sebeple bu dosyanın zararlı bir yazılım ile gelmiş olma ihtimalinin düşük olduğu düşünülmektedir.

Tespit edilen bir diğer TRT.doc dosyasına ait üstveriler aşağıdaki gibidir. Bu dosya Yıldız Teknik Üniversitesi'nde analizi yapılan TRT.doc dosyasıdır.

Belge Üstverileri	
Dosya Adı	TRT.doc
Dosya Konumu	\C\Documents and Settings\Türker\Belgelerim\Documents\aysegül\trt.doc
Dosya Durumu	Aktif
Yazar	user

Son Değiştiren Kullanıcı	user
Yönetici	
Şirket	
Nesne Tipi	Microsoft Office Word Belgesi
Yazılım Tipi	Microsoft Office Word
Karakter Tipi	Windows Turkish
Karakter Sayısı	891
Uygulama Versiyonu	11.5606
Dosya Boyutu	64 kB
Toplam Değiştirme Süresi	9.0 dakika
Revizyon Numarası	2
Belge Oluşturma Tarihi	2008:03:19 15:05:00
Belge Değiştirme Tarihi	2008:03:19 15:15:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2008-03-19 15:11:18.230000
FN Oluşturma Zamanı	2008-10-07 10:37:17.906248
Std Değiştirme Zamanı	2008-03-19 15:15:08
FN Değiştirme Zamanı	2008-10-07 10:37:17.906248
Std Erişim Zamanı	2010-10-14 14:58:03.671875
FN Erişim Zamanı	2008-10-07 10:37:17.906248
Std Giriş Zamanı	2010-07-22 09:55:46.640625
FN Giriş Zamanı	2008-10-07 10:37:17.906248

Yukarıda detayı verilen TRT.doc dosyasının içeriği aşağıdaki gibidir.



TRT sanatçısı dönemi sona eriyor, TRT 3000 çalışanını başka kurumlara gönderiyor.

Yenileşme politikası adı altında çalışma süreçlerini yavaşlatan birimleri ve unsurları ortadan kaldırmaya karar veren yeni TRT taslağı ilginç maddeler içeriyor.

TRT'deki fonksiyonu bitmiş birimlerin kaldırılmasını ve TRT sanatçılarının Kültür ve Turizm Bakanlığı'na aktarılmasını öngören taslakla, TRT bünyesinde hafiflemeye gidiyor.

3000'e yakın personelini de fazla istihdamdan kurtulmak ve bu personellerden başka alanlarda verim alabilmek adına, çeşitli kurumlara yerleştiriyor.

Şekil 54 - C\Documents and Settings\Türker\Belgelerim\Documents\aysegül\trt.doc

STD Access > STD Giriş > FN zamanları > Belge son değiştirme ~= STD son değiştirme (mikro saniye yok) > STD oluşturma (sadece salise bilgisi var) > belge son değiştirme

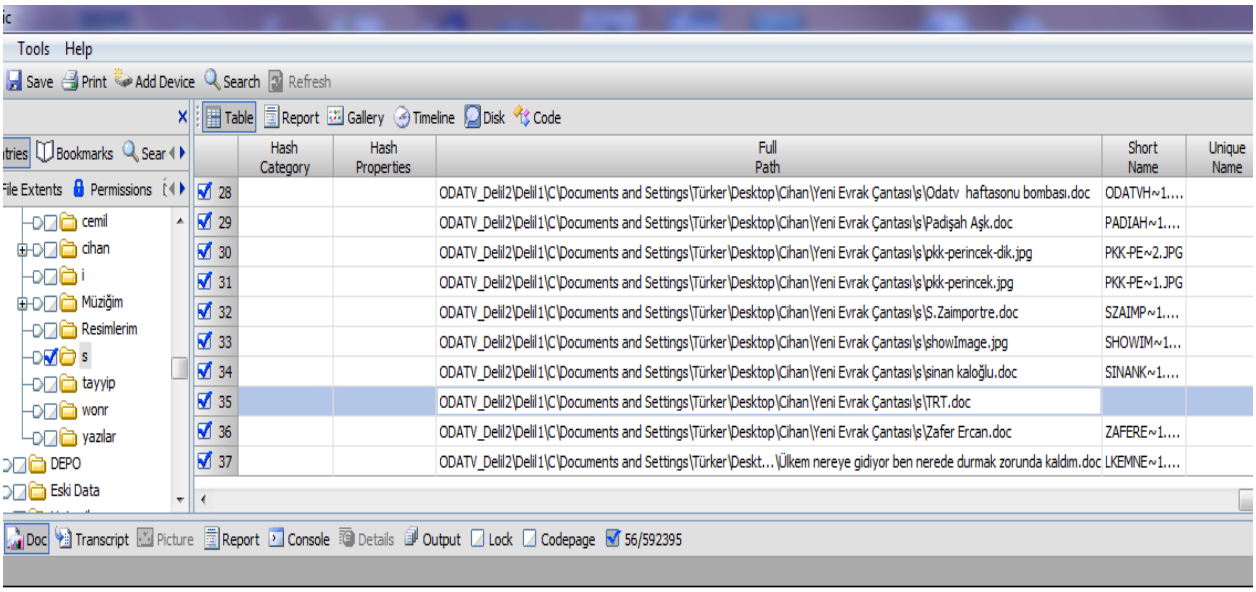
Dosya sistemi üstverilerinin ve belge üstverilerinin incelenmesi sonucu bu dosyanın farklı bir bilgisayarda oluşturulduktan sonra kopyalanmış olduğu, son olarak belge değiştirme işleminin FAT dosya sistemi olan bir sürücüde gerçekleştirildiği, daha sonra bu sürücüden şu anki konuma dosyanın taşınarak aktarıldığı değerlendirilmektedir.

Bu sebeple bu dosyanın zararlı bir yazılım ile gelmiş olma ihtimalinin düşük olduğu düşünülmektedir.

Tespit edilen üçüncü TRT.doc dosyasına ait üstveriler aşağıdaki gibidir.

Belge Üstverileri	
Dosya Adı	TRT.doc
Dosya Konumu	\C\Documents and Settings\Türker\Desktop\Cihan\Yeni Evrak Çantasi\s\TRT.doc
Dosya Durumu	Aktif
Yazar	systm
Son Değiştiren Kullanıcı	systm
Yönetici	
Şirket	
Nesne Tipi	Microsoft Office Word Belgesi
Yazılım Tipi	Microsoft Office Word
Karakter Tipi	Windows Turkish
Karakter Sayısı	3044
Uygulama Versiyonu	11.5606
Dosya Boyutu	64 kB
Toplam Değiştirme Süresi	1.7 saat
Revizyon Numarası	5
Belge Oluşturma Tarihi	2007:12:07 14:09:00
Belge Değiştirme Tarihi	2007:12:07 15:51:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2008-01-08 20:08:00.639999
FN Oluşturma Zamanı	2008-10-07 11:36:32.156248
Std Değiştirme Zamanı	2007-12-07 14:51:12
FN Değiştirme Zamanı	2008-10-07 11:36:32.156248
Std Erişim Zamanı	2011-01-28 17:27:36.640923
FN Erişim Zamanı	2008-10-07 11:36:32.156248
Std Giriş Zamanı	2008-10-07 11:36:32.156248
FN Giriş Zamanı	2008-10-07 11:36:32.156248

Yukarıda detayı verilen TRT.doc dosyasının içeriği aşağıdaki gibidir.



TRT'nin yeni genel müdürü İbrahim Şahin icraatlarıyla TRT çalışanlarını rahatlatmaya devam ediyor.

Göreve başladığında radikal kararlar alarak TRT'nin makus talihini değiştireceğini vaat eden Şahin, TRT'de sigortalı çalışan geçiçi personellerin sorunlarına el attı.

TRT'de 500'e yakın yönetmen, yapım yardımcısı, muhabir, kameraman yayıncı sigortalı olarak sözlesmeli calısıvor. Bu kisilerin 11 avda bir sözlesmeleri venilenivor fakat asla

Şekil 55 - C\Documents and Settings\Türker\Desktop\Cihan\Yeni Evrak Çantası\s\TRT.doc

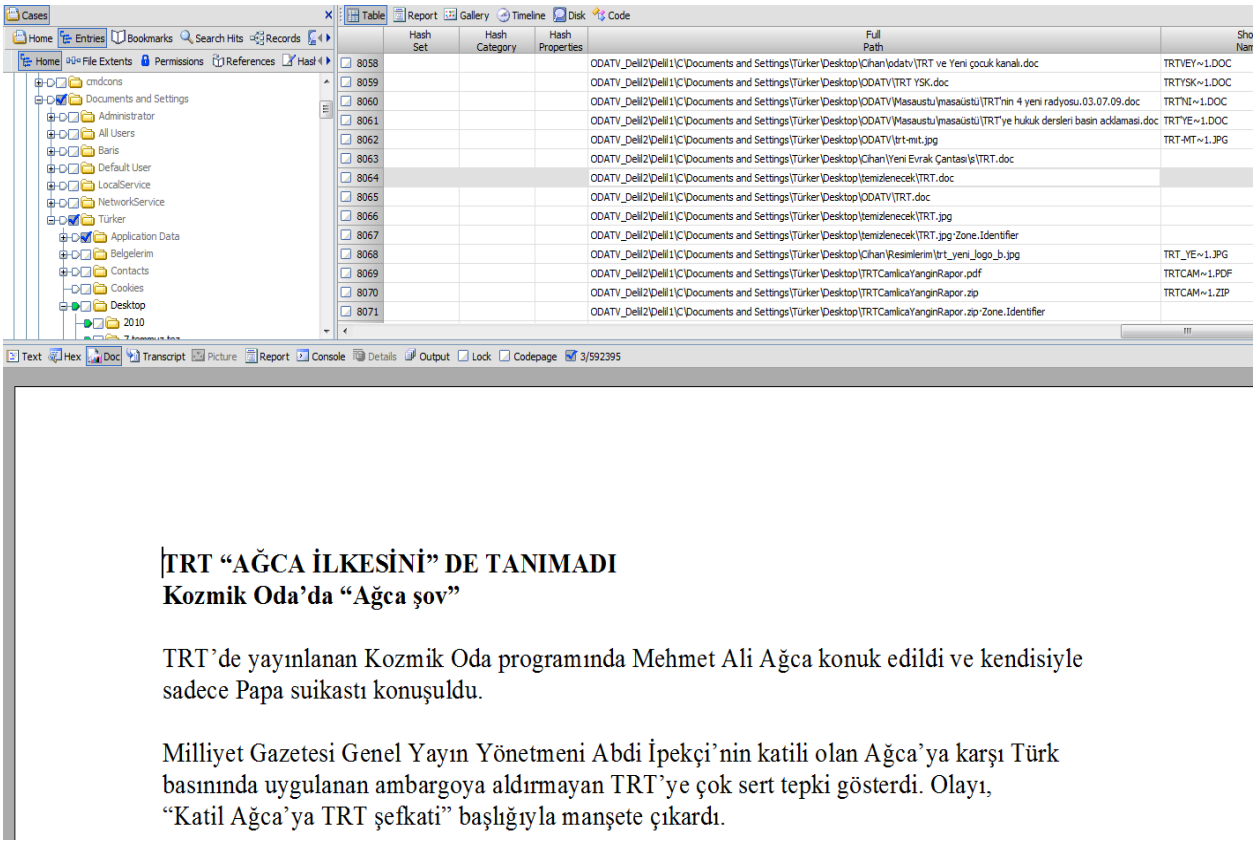
Dosya sistemi üstverilerinin ve belge üstverilerinin incelenmesi sonucu bu dosyanın farklı bir bilgisayarda oluşturuldu, bu bilgisayara FAT, RAR ve CD üzerinden (buraya klasik cevabımız verilebilir) gelmiş olabileceği değerlendirilmektedir.

Tespit edilen dördüncü TRT.doc dosyasına ait üstveriler aşağıdaki gibidir.

Belge Üstverileri	
Dosya Adı	TRT.doc
Dosya Konumu	\C\Documents and Settings\Türker\Desktop\temizlenecek\TRT.doc

Dosya Durumu	Aktif
Yazar	doğan
Son Değiştiren Kullanıcı	Sys
Yönetici	
Şirket	
Nesne Tipi	Microsoft Office Word Belgesi
Yazılım Tipi	Microsoft Office Word
Karakter Tipi	Windows Turkish
Karakter Sayısı	5550
Uygulama Versiyonu	11.5606
Dosya Boyutu	36 kB
Toplam Değiştirme Süresi	17.0 dakika
Revizyon Numarası	5
Belge Oluşturma Tarihi	2010:11:10 07:20:00
Belge Değiştirme Tarihi	2010:11:10 09:03:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-05-03 09:12:49.109373
FN Oluşturma Zamanı	2010-11-10 08:58:09.343750
Std Değiştirme Zamanı	2010-11-10 09:03:11.031000
FN Değiştirme Zamanı	2010-11-10 09:03:11.031000
Std Erişim Zamanı	2011-01-28 17:33:28.469048
FN Erişim Zamanı	2010-11-23 07:14:23.453125
Std Giriş Zamanı	2010-11-23 07:14:23.625000
FN Giriş Zamanı	2010-11-10 09:03:11.046875

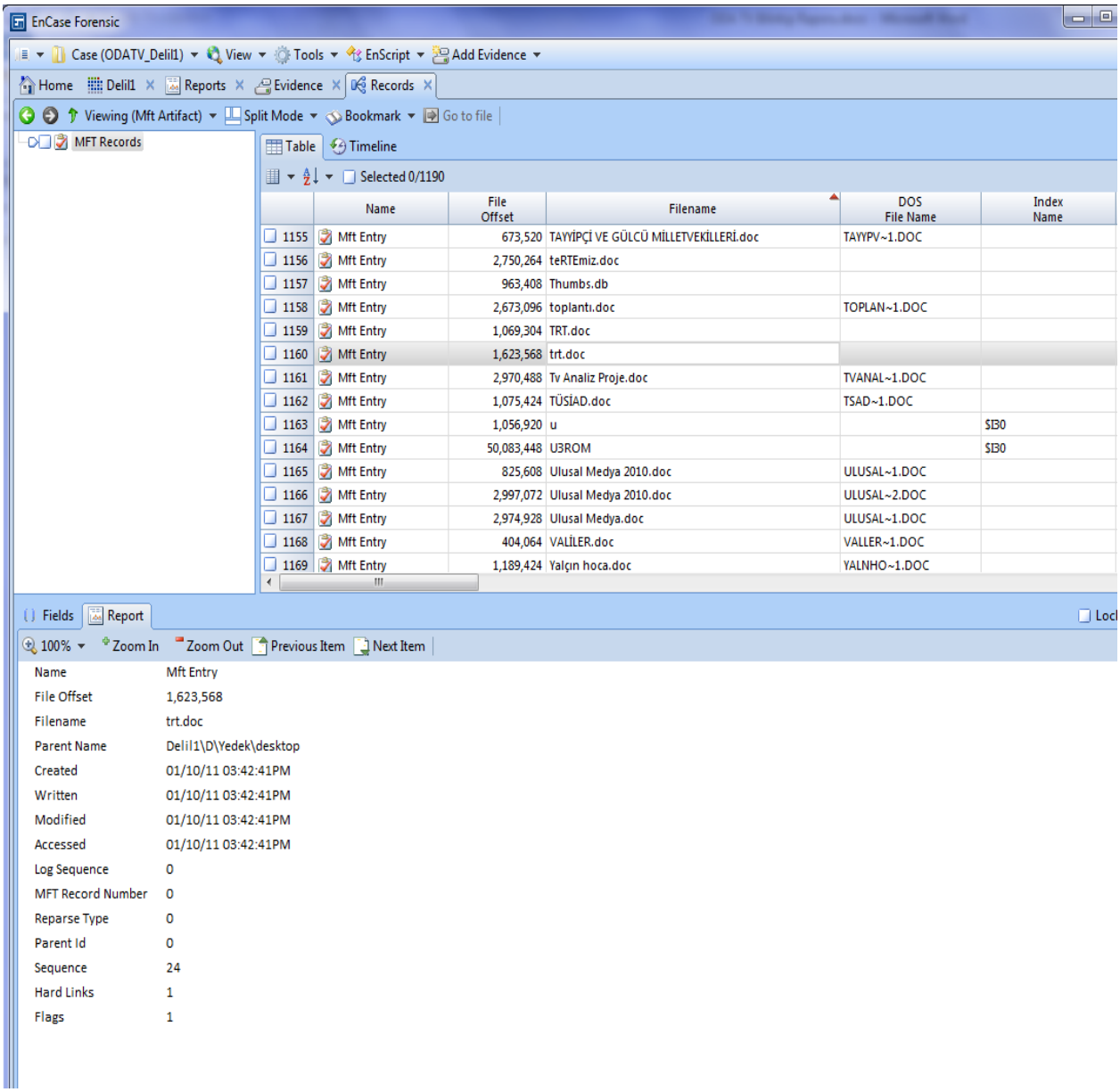
Yukarıda detayı verilen TRT.doc dosyasının içeriği aşağıdaki gibidir.



Şekil 56 - C\Documents and Settings\Türker\Desktop\temizlenecek\TRT.doc

Dosya sistemi üstverilerinin ve belge üstverilerinin incelenmesi sonucu bu dosyanın farklı bir bilgisayar kullanıcısı tarafından oluşturulduğu, daha sonra bu bilgisayara NTFS dosya formatında bir sürücü üzerinden taşındığı ve bu bilgisayar kullanıcısı tarafından değiştirildiği değerlendirilmektedir. Bu sebeple bu dosyanın zararlı bir yazılım ile gelmiş olma ihtimalinin düşük olduğu düşünülmektedir.

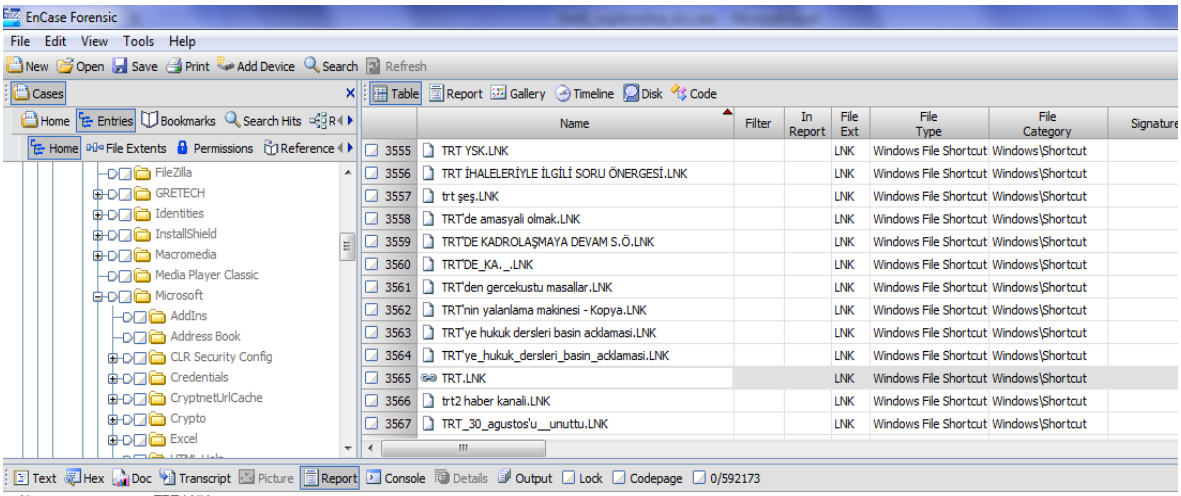
Yukarıda bahsi geçen dosyaların yanı sıra, silinmiş alan başka bir trt.doc dosyasına ait Logfile kaydı bulunmuştur.



Şekil 57 - trt.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

Bununla beraber dosyanın kendisine ulaşılamamıştır. Dosyanın kendisinin bulunamayıp LogFile kayıtlarının tespit edilmesi, dosyanın silinmiş ve dosyanın bulunduğu disk alanının üzerine başka bir dosyanın verilerinin yazılmış olduğuna işaret etmektedir.

Masaüstü klasöründe bulunan trt.doc isimli dosyanın açılmış olduğuna dair Office Son Kullanılanlar klasöründe kayda rastlanmıştır.



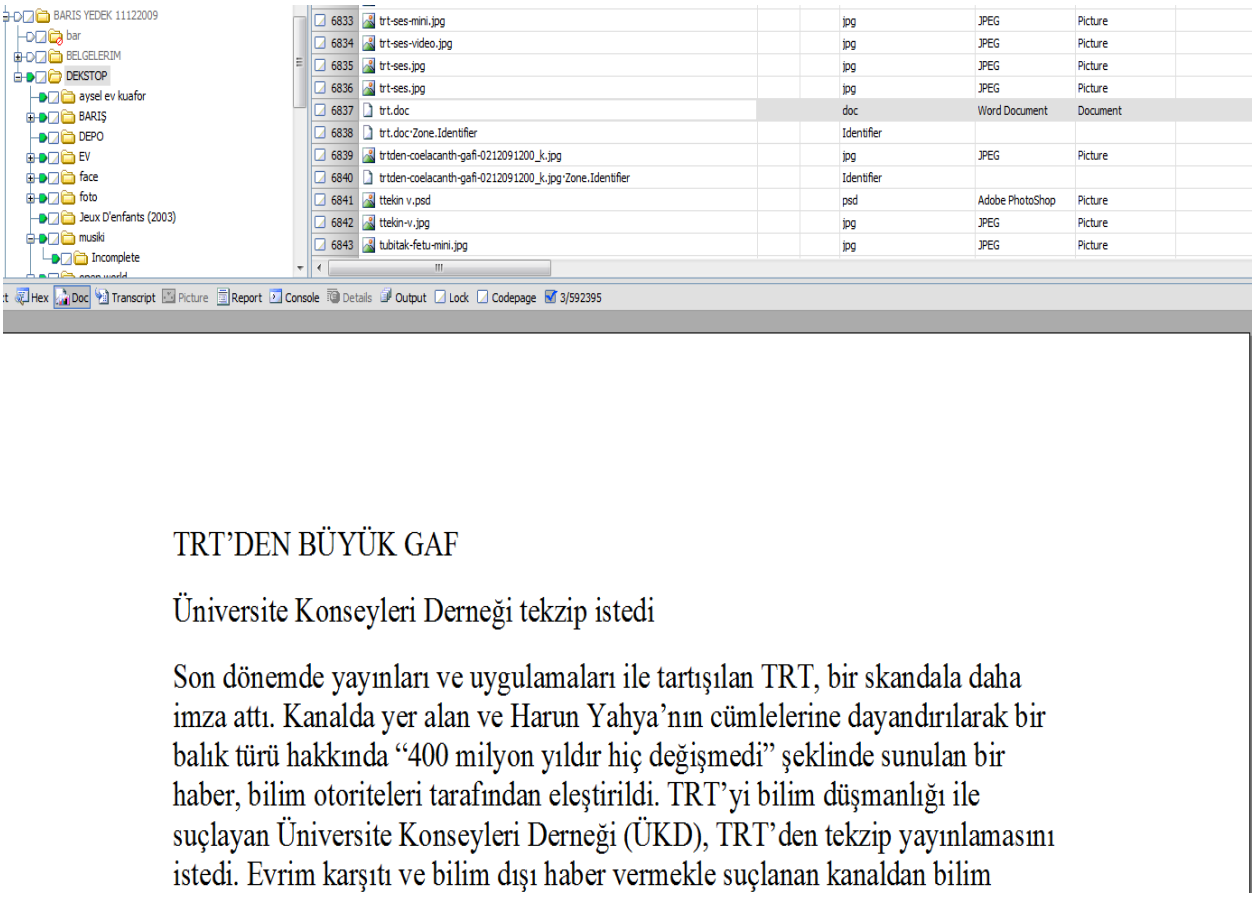
Şekil 58 - Office son kullanılan doküman kayıtları arasında trt.doc

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Belge Üstverileri	
Dosya Adı	TRT.doc
Dosya Konumu	\D\BARIS YEDEK 11122009\DEKSTOP\trt.doc
Dosya Durumu	Aktif
Yazar	X1 ff
Son Değiştiren Kullanıcı	X1 ff
Yönetici	
Şirket	gaste
Nesne Tipi	Microsoft Word 97-2004 Document
Yazılım Tipi	Microsoft Word 12.0.0

Karakter Tipi	Mac Turkish
Karakter Sayısı	2781
Uygulama Versiyonu	12
Dosya Boyutu	40 kB
Toplam Değiştirme Süresi	1.0 dakika
Revizyon Numarası	2
Belge Oluşturma Tarihi	2009:12:01 14:41:00
Belge Değiştirme Tarihi	2009:12:01 14:41:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2009-12-01 22:13:41.890625
FN Oluşturma Zamanı	2009-12-11 07:40:47.484373
Std Değiştirme Zamanı	2009-12-01 22:13:44.562498
FN Değiştirme Zamanı	2009-12-11 07:40:47.484373
Std Erişim Zamanı	2010-11-03 19:40:14.421875
FN Erişim Zamanı	2009-12-11 07:40:47.484373
Std Giriş Zamanı	2010-09-26 19:33:00.984373
FN Giriş Zamanı	2009-12-11 07:40:47.484373

İlgili dosyanın içeriği aşağıdaki gibi görüntülenmiştir.



Şekil 59 - trt.doc Dosyası İçeriği

Dosya sistemi üstverilerinin ve belge üstverilerinin incelenmesi sonucu bu dosyanın farklı bir bilgisayarda oluşturduktan sonra NTFS formatındaki bir dosya sistemine sahip bir sürücü (daha güzel bir kelime bulunabilir) ile bu bilgisayara aktarıldığı ve şu anki konumuna taşınarak konulduğu değerlendirilmektedir. Bu sebeple bu dosyanın zararlı bir yazılım ile gelmiş olma ihtimalinin düşük olduğu düşünülmektedir.

“TRT.doc” dokümanı Delil2 diskinde direk olarak bulunmaktadır ve bu yüzden hem belge üstverilerine hem de dosya sistemi üstverilerine ulaşılabilmektedir. Delil1 diskinde ise 5 farklı yerde bu isimli dosyalara rastlanmıştır. Yıldız Teknik Üniversitesi'nin raporunda "C:\Documents and Settings\Türker\Belgelerim\Documents\aysegül\trt.doc" dosyasından Emniyet Müdürlüğü' nün raporunda ise "D:\Yedek\desktop\trt.doc" bilgisi $Logfile kaydından alınarak bahsedilmiştir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.

- Delil1 deki sadece $Logfile kaydı bulunan trt.doc dosyasına (d:\yedek\desktop\trt.doc) ulaşılamamıştır. Delil1 deki diğer dosya için de bahse konu olan STD erişim zamanı ile STD giriş zamanı uyumsuzluğu iddiaları için normal kullanıcı işlemlerinden olan dosya erişim ve okuma işlemleri sırasında dosya son erişim zamanı güncellenirken, $MFT kaydı değişim zamanı işletim sistemi tarafından güncellenmek zorunda değildir.

- Delil2 deki dosya için de yukarıda yapılan yorum yapılabilir. STD erişim zamanının güncellenmesi STD giriş zamanının da güncellenmesini gerektirmez.

Bu inceleme sonucunda Delil 2 “trt.doc” dosyanın NFTS formatındaki, farklı bir sürücüden hâlihazırdaki konumuna taşınmış olabileceği düşünülmektedir. Bu farklı sürücü, harici bir veri depolama cihazı olabileceği gibi, aynı bilgisayardaki diğer sürücü de olabilir. Delil 1 üzerindeki “trt.doc” dosyasının ise FAT formatındaki bir sürücüden taşınmış olma ihtimali yüksek görülmektedir. FAT formatındaki sürücüler genellikle harici veri depolama cihazlarında bulunmaktadır, bu yüzden bu dosyanın zararlı yazılımlar vasıtasıyla uzaktan erişim yöntemiyle delil 1 bilgisayarına gelmemiş olduğu değerlendirilmektedir.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

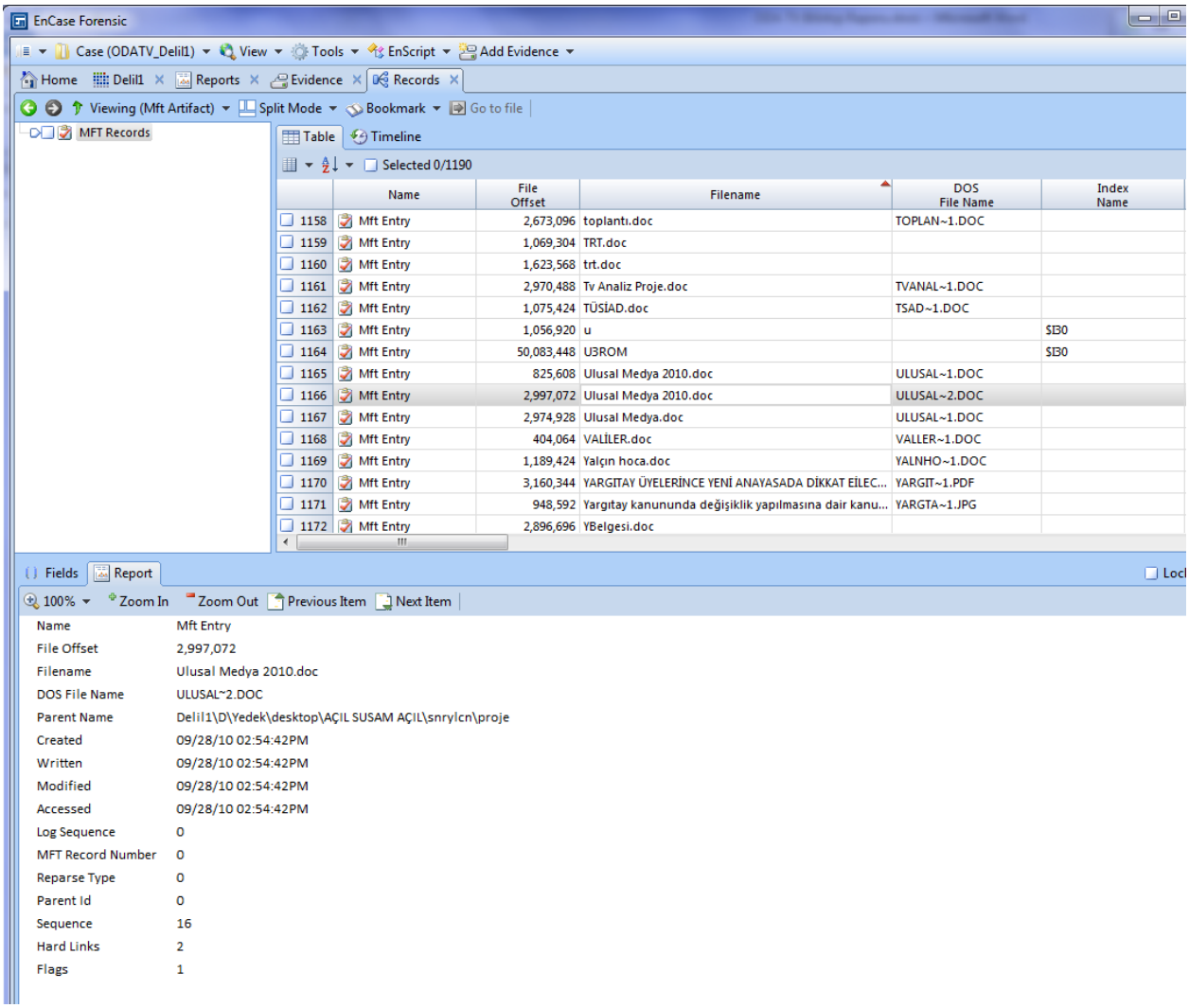
26.) Ulusal Medya 2010.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	Ulusal Medya 2010.doc
Dosya Konumu	\D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\Ulusal Medya 2010.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor.
Yazar	pc
Son Değiştiren Kullanıcı	soner
Yönetici	
Şirket	
Nesne Tipi	Microsoft Word Document
Yazılım Tipi	Microsoft Word 10.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	15368
Uygulama Versiyonu	10,2605
Dosya Boyutu	64 kB
Toplam Değiştirme Süresi	10.4 saat
Revizyon Numarası	112
Belge Oluşturma Tarihi	2010:07:21 18:03:00
Belge Değiştirme Tarihi	2010:09:27 11:33:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-09-28 11:54:42.593750
FN Oluşturma Zamanı	2010-09-28 11:54:42.593750
Std Değiştirme Zamanı	2010-09-27 12:33:10
FN Değiştirme Zamanı	2010-09-28 11:54:42.593750
Std Erişim Zamanı	2010-09-28 11:54:42.593750
FN Erişim Zamanı	2010-09-28 11:54:42.593750
Std Giriş Zamanı	2010-09-28 11:54:42.593750
FN Giriş Zamanı	2010-09-28 11:54:42.593750

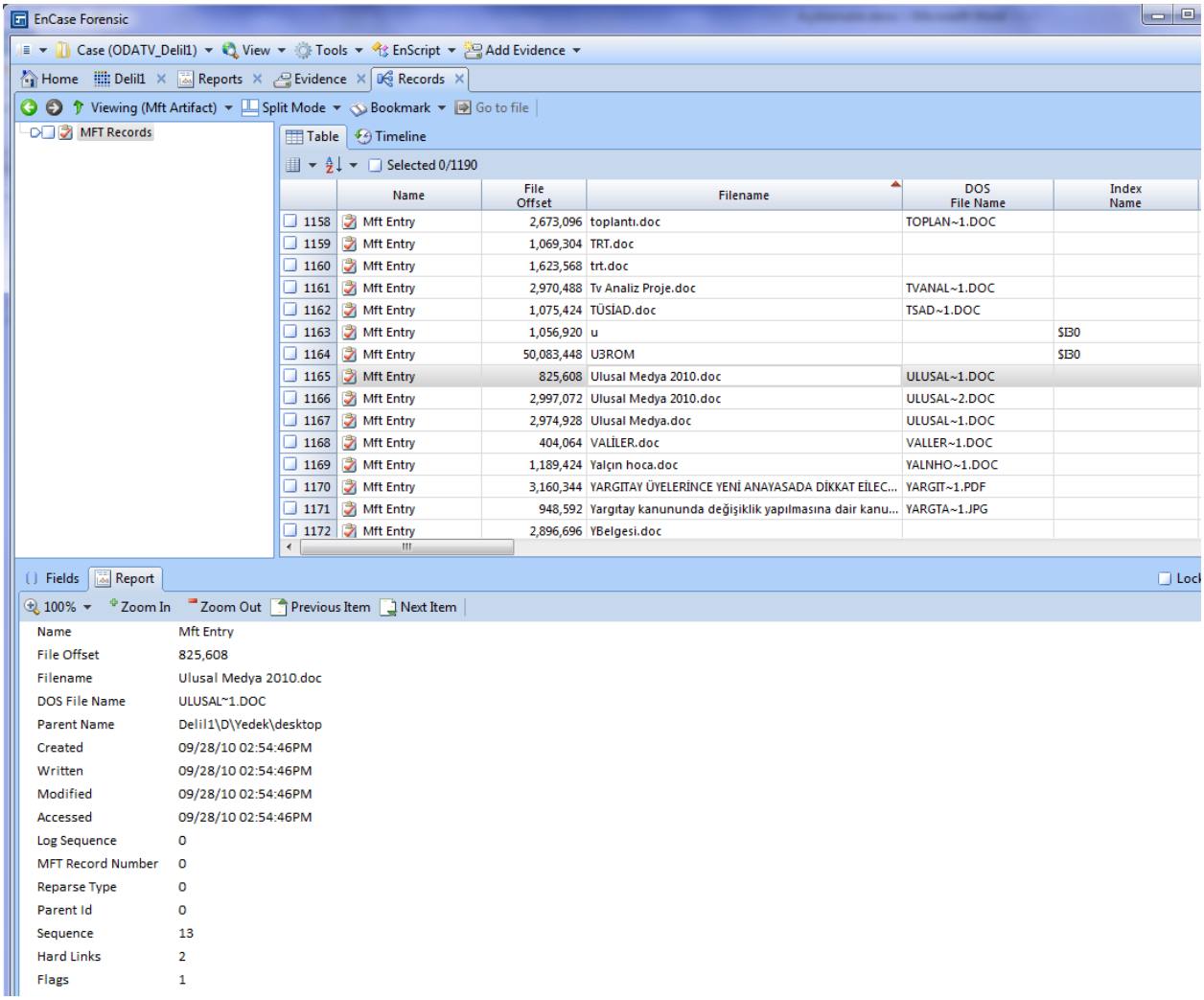
Bu imajda ilgili dosyaya ait 2 farklı kopya ve 2 farklı $LogFile (Index Artifact) kaydı görülmüştür. Dosyaların her ikisi de silinmiş olmasına rağmen, ilk dosyanın üzerine herhangi bir başka veri yazılmadığı için olduğu gibi kurtarılabilmiştir.

Bunlardan ilki **D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje** dizini altındaki dosyadır.



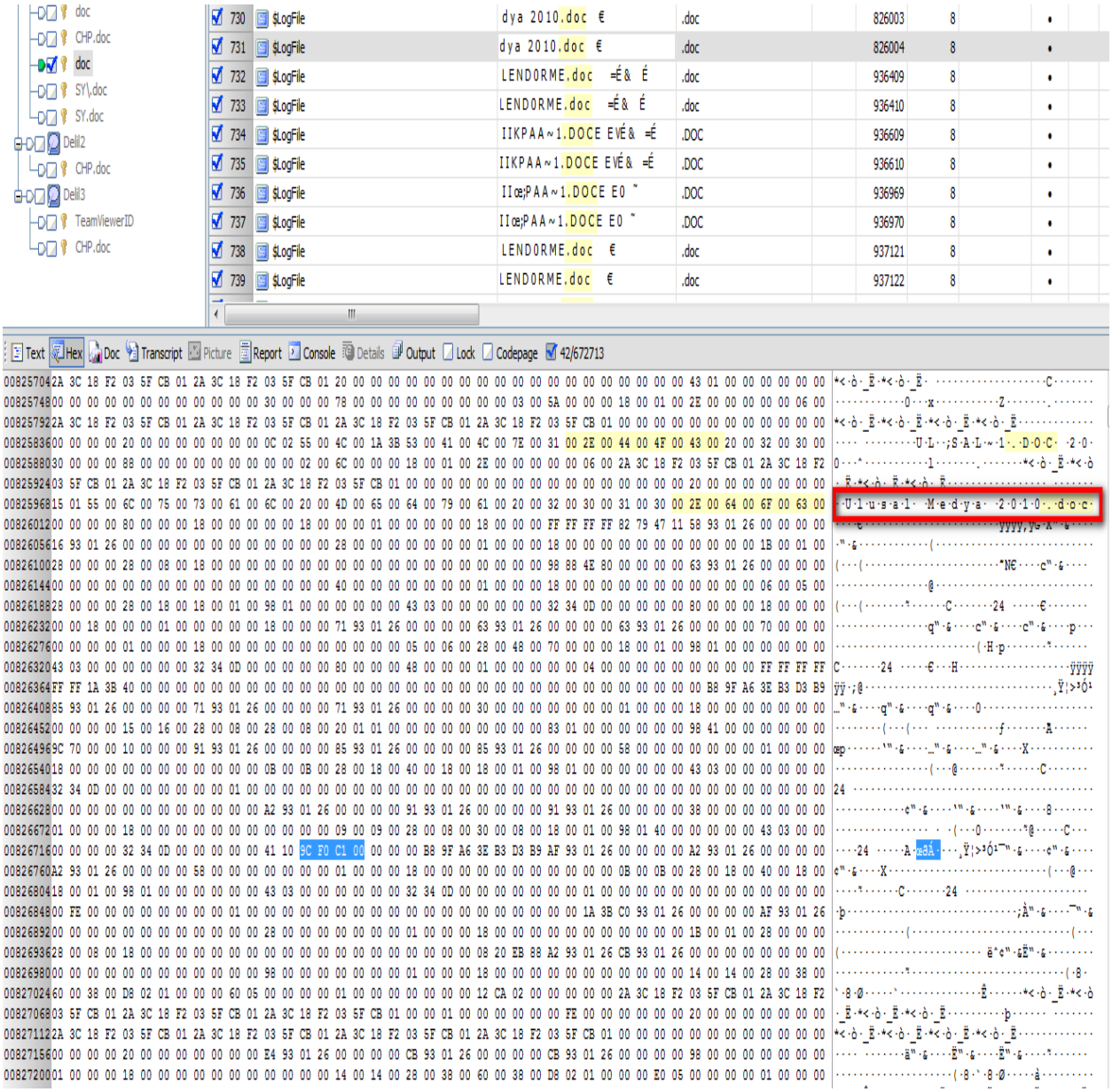
Şekil 60 - Ulusal Medya 2010.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı -1

Tespit edilen diğer kopyaya ait Logfile kaydı ise bir öncekinden 4 sn sonra oluşmuştur. İlgili kayıt bu kez **D\Yedek\desktop** dizinini göstermektedir.

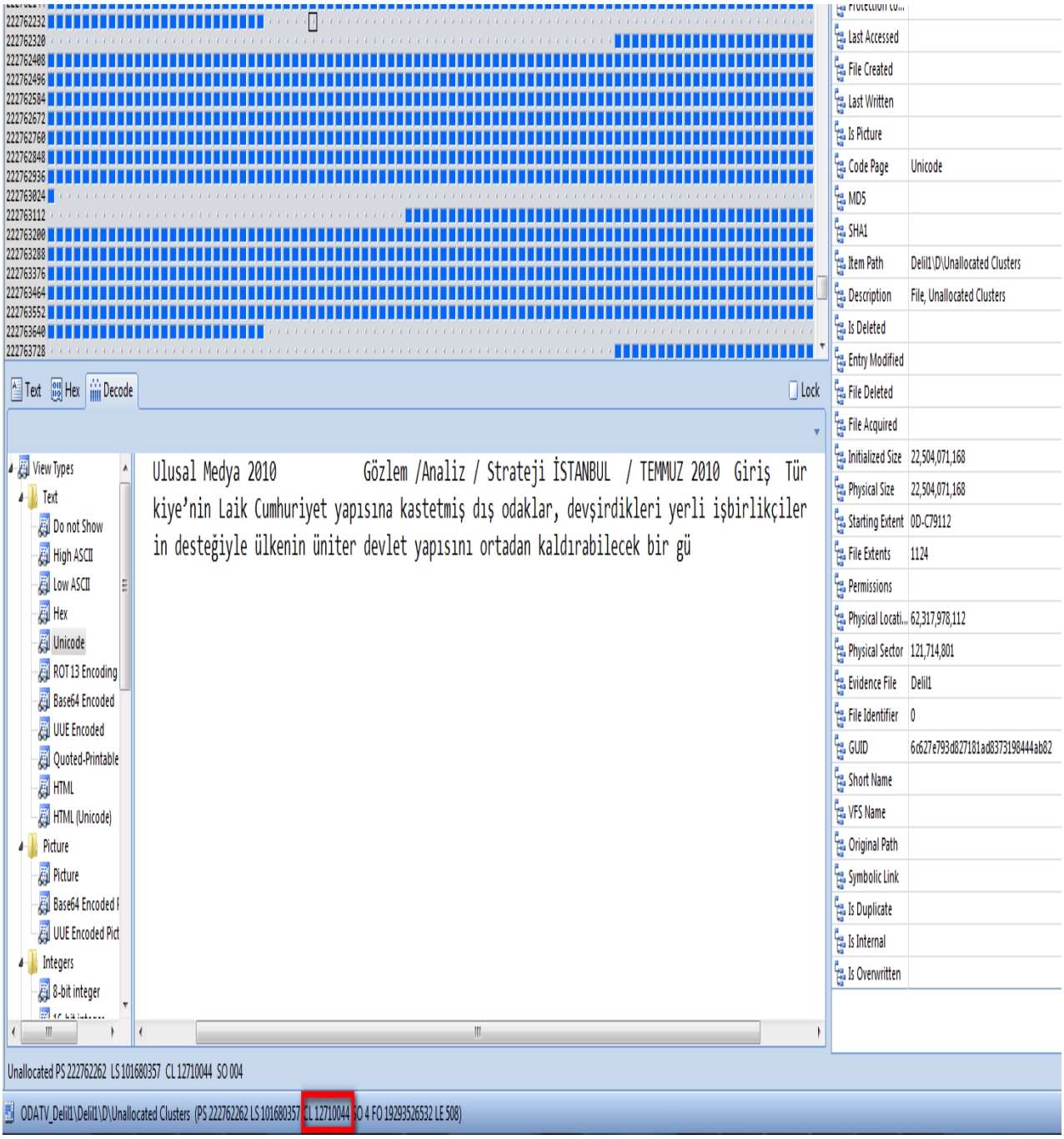


Şekil 61 - Ulusal Medya 2010.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı -2

Aynı dosya ismini taşıyan bu iki kayıt arasındaki 4 sn lik fark nedeniyle dosyanın bu dizine taşındığı veya kopyalandığı değerlendirilmektedir. Aynı dosyanın bu dizindeki kopyasının silinmiş ve üzerine yazılmış olduğu tespit edilmiştir. Dosya her ne kadar silinmiş de olsa, Logfile'dan elde edilen değerler kullanılarak dosyanın başlangıç cluster adresi tespit edilmiştir.


doc
CHP.doc
doc
SY\.doc
SY.doc
Dell2
CHP.doc
Dell3
TeamViewerID
CHP.doc
730 $LogFile dya 2010.doc € .doc 826003 8
731 $LogFile dya 2010.doc € .doc 826004 8
732 $LogFile LENDORME.doc =É& É .doc 936409 8
733 $LogFile LENDORME.doc =É& É .doc 936410 8
734 $LogFile IIKPAA~1.DOCE EVÉ& =É .DOC 936609 8
735 $LogFile IIKPAA~1.DOCE EVÉ& =É .DOC 936610 8
736 $LogFile IIœ;PAA~1.DOCE E0 ˜ .DOC 936969 8
737 $LogFile IIœ;PAA~1.DOCE E0 ˜ .DOC 936970 8
738 $LogFile LENDORME.doc € .doc 937121 8
739 $LogFile LENDORME.doc € .doc 937122 8
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 42/672713

Başlangıç adresi 9CF0C100 olan dosyanın bulunduğu cluster olan 12710044 (10'luk tabanda karşılığı) adresine gidildiğinde aşağıdaki veriler elde edilmiştir.



Şekil 62 - Ulusal Medya 2010.doc dosyasının silinmiş alanda (unallocated cluster) tespit edilen bölümü

Unallocated clusters alanında silinmiş olarak bulunan dosya da tamamen kurtarılabilmiştir. Böylece dosyanın metaverilerine de ulaşılmıştır.

Belge Üstverileri	
Dosya Adı	Ulusal Medya 2010.doc
Dosya Konumu	\D\Yedek\desktop\Ulusal Medya 2010.doc
Dosya Durumu	Silinmiş, $MFT kaydı yok, unallocated clusterda bulunuyor.
Yazar	pc
Son Değiştiren Kullanıcı	soner
Yönetici	
Şirket	
Nesne Tipi	Microsoft Word Document
Yazılım Tipi	Microsoft Word 10.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	15368
Uygulama Versiyonu	10,2605
Dosya Boyutu	64 kB
Toplam Değiştirme Süresi	10.4 saat
Revizyon Numarası	112
Belge Oluşturma Tarihi	2010:07:21 18:03:00
Belge Değiştirme Tarihi	2010:09:27 11:33:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	
FN Oluşturma Zamanı	
Std Değiştirme Zamanı	
FN Değiştirme Zamanı	
Std Erişim Zamanı	
FN Erişim Zamanı	
Std Giriş Zamanı	
FN Giriş Zamanı	

Görüldüğü üzere **\D\Yedek\desktop** ve **D\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje** dizinlerinde bulunan her 2 dosyanın üstverileri aynıdır. Dolayısıyla bu iki dosyanın birbirinin kopyası olduğu değerlendirilmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu diskte yapılan incelemelerde bu dosyaya dair LogFile kayıtlarına rastlanmıştır. İncelenen LogFile kayıtlarının zamanlarına bakarak bu dosyanın 28_09.rar adlı sıkıştırılmış dosyadan çıkartıldığı düşünülmektedir.

Dosya Adı	Bulunduğu Dizin	Oluşturma Tarihi	Giriş Tarihi	Değiştirme Tarihi	Erişim Tarihi

Ulusal Medya 2010.doc	D\BARIS YEDEK 11122009\bar	28.09.2010 00:01:14	28.09.2010 00:01:14	28.09.2010 00:01:14	28.09.2010 00:01:14

Bununla beraber dosyanın kendisine ulaşılamamıştır. Dosyanın kendisinin bulunamayıp LogFile kayıtlarının tespit edilmesi, dosyanın silinmiş ve dosyanın bulunduğu disk alanının üzerine başka bir dosyanın verilerinin yazılmış olduğuna işaret etmektedir.

"Ulusal Medya 2010.doc" dokümanı Delil2 diskinde silinmiş ama $Logfile kaydı ulaşılabilir durumda bulunmaktadır. Delil2 içindeki durumu silinmiş ve üzerine veri yazılarak dosya ulaşılamaz hale gelmiştir. Delil1 diskinde ise "unallocated cluster" alanından veri kurtarma programları yardımıyla geri döndürülebilmiştir. Bunun yanında Delil1 de $MFT kaydına da ulaşılmaktadır. Delil2 de ise sadece dosya sistemi üstverilerine ulaşılabilinmektedir. Delil3 diskinde dosya normal olarak bulunmuştur ve bu sebeple hem belge üstverilerine hem de dosya sistemi üstverilerine ulaşılabilmiştir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Delil1 ve Delil2 için dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.

- Delil3 için olan zaman anormalliklerinin sonradan bir zaman değiştirme programı kullanılması ile oluşmuş olabileceği değerlendirilmektedir.

- Her üç delil diski için dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

- Her üç delil diski için işletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

- Her üç delil diski için dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

- Delil1 için dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD

dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.

• Delil2 deki $Logfile analizi sonrası bir RAR arşiv dosyasından çıkarıldıktan sonra çıkarıldığı görülmektedir.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Belge Üstverileri	
Dosya Adı	Ulusal Medya 2010.doc
Dosya Konumu	\C\Users\user\Documents\Ulusal Medya 2010.doc
Dosya Durumu	Aktif
Yazar	pc
Son Değiştiren Kullanıcı	soner
Yönetici	
Şirket	
Nesne Tipi	Microsoft Word Document
Yazılım Tipi	Microsoft Word 10.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	15368
Uygulama Versiyonu	10,2605
Dosya Boyutu	64 kB
Toplam Değiştirme Süresi	10.4 saat
Revizyon Numarası	112
Belge Oluşturma Tarihi	2010:07:21 18:03:00
Belge Değiştirme Tarihi	2010:09:27 11:33:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-10-04 14:41:50
FN Oluşturma Zamanı	2010-10-04 14:41:50
Std Değiştirme Zamanı	2010-09-27 15:33:55
FN Değiştirme Zamanı	2010-09-27 15:33:55
Std Erişim Zamanı	2010-10-04 19:20:40
FN Erişim Zamanı	2010-10-04 19:20:40
Std Giriş Zamanı	2011-02-14 18:40:07.524328
FN Giriş Zamanı	2011-02-14 18:38:59.913929

Bu imajda tespit edilen “Ulusal Medya 2010.doc” dosyasının üstverilerinde görülen aşağıdaki özelliklerin hep birlikte gerçekleşmesinin, normal kullanıcı davranışlarıyla zor olduğu değerlendirilmektedir. Bu özellikler:

- STD oluşturma ve erişim zamanlarının, FN zamanlarından geri olması ve mikro saniye kısımlarının 0 olması ve

- STD MFT kaydı değişim zamanının mikro saniye kısmının olması ve FN zamanlarından az ileri olmasıdır.

Dosya sistemi üstverilerindeki FN zamanlarının, STD oluşturma ve erişim zamanlarından ileri olması durumu, yedekleme sistemlerinde yedekleme aşamasında STD oluşturma ve erişim zamanlarının tutulmasının istenmesi ve yedekten dönülmesi sırasında yedekleme sistemi tarafından bu değerlerin ilk tutulan değerlere geri getirilmesi gibi durumlarda oluşabilir. Bunun yanında arşivleme programlarında da bu özellik bulunabilir. Örneğin en çok kullanılan dosya arşivleme programlarından biri olan "winrar" programında bu özellik mevcuttur(Store Creation Time, Store Last Access Time)."Winrar" programı kullanılarak yapılan testlerde FN zamanlarının, STD oluşturma zamanlarından daha güncel olabileceği görülmüştür. Aynı zamanda FN zamanlarının, STD oluşturma zamanlarından daha güncel olması farklı bir sürücüden taşıma ile gelen dosyalarda normal olan durumdur. Bunun yanında Winrar programı ile yapılan testlerde, STD oluşturma ve erişim zamanlarında mikro saniye kısmı olmaması durumu ile karşılaşılmıştır.

STD oluşturma ve erişim zamanlarında mikro saniye bilgisinin olmaması (sıfır olması) aslında işletim sistemi temel dosyalarında karşılaşılabilen bir durumdur. Fakat normal kullanıcı dosyalarında olma ihtimali düşüktür.

Bu özelliklerin hepsinin birlikte olmasını açıklayan diğer bir senaryo ise şöyledir:

- Dosya bu bilgisayara "2011-02-14 18:40:07.524328" zamanından önce gelmiştir,
- Daha sonra Std MFT kaydı değişim zamanı olan "2011-02-14 18:40:07.524328" zamanında ise STD oluşturma, değiştirme ve erişim zamanları değiştirilmiştir ve sonrasında da "bölüm taşıma" yapılarak FN değerlerinin güncellenmesi gerçekleştirilmiştir.

Zaman değiştirme işlemi, yazılmış özel bir program ile ya da basit bir "visual basic script" ile olabilmektedir.

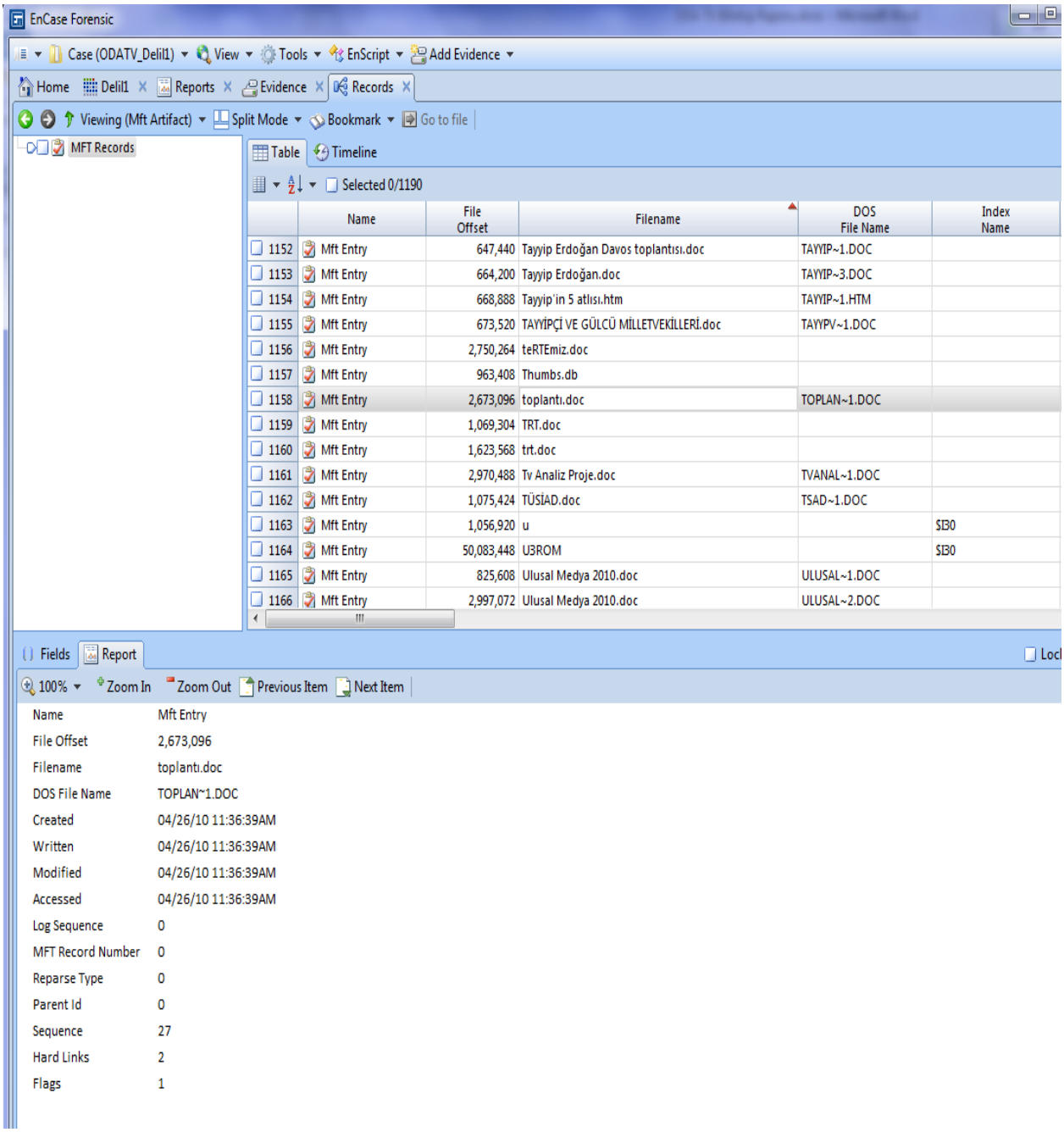
Sonuç olarak dosyadaki dosya sistemi üstverilerindeki bu uyuşmazlığın nasıl oluştuğu kesin olmamakla birlikte, yedekten dönme işlemi, RAR arşivleme ile arşiv açma işlemi ve zaman üstverilerinin sonradan değiştirilmiş olması işlemlerinden biri ile oluşmuş olabileceği değerlendirilmektedir. Bu işlemlerden gerçekleşmiş olmaya en yakın olanının, zaman üstverilerinin sonradan değiştirilmiş olması olduğu değerlendirilmektedir.

27.) toplantı.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	toplantı.doc
Dosya Konumu	\D\toplanti.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor
Yazar	Barış
Son Değiştiren Kullanıcı	Barış
Yönetici	
Şirket	
Nesne Tipi	Microsoft Office Word Belgesi
Yazılım Tipi	Microsoft Office Word
Karakter Tipi	Unicode (UTF-8)
Karakter Sayısı	1094
Uygulama Versiyonu	11,5606
Dosya Boyutu	24 kB
Toplam Değiştirme Süresi	13.0 dakika
Revizyon Numarası	8
Belge Oluşturma Tarihi	2010:04:25 10:19:00
Belge Değiştirme Tarihi	2010:04:25 10:33:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-04-26 08:36:39.140625
FN Oluşturma Zamanı	2010-04-26 08:36:39.140625
Std Değiştirme Zamanı	2010-04-25 11:33:56
FN Değiştirme Zamanı	2010-04-26 08:36:39.140625
Std Erişim Zamanı	2010-12-24 11:09:03.187500
FN Erişim Zamanı	2010-04-26 08:36:39.140625
Std Giriş Zamanı	2010-04-26 08:36:39.140625
FN Giriş Zamanı	2010-04-26 08:36:39.140625

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (Index Artifact) kayıtlarında da rastlanılmıştır.



Şekil 63 - toplantı.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

"toplantı.doc" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir.
- Dosyanın STD erişim zamanının diğer zamanlarından daha güncel olması bu dosyaya erişim sağlandığını göstermektedir. STD erişim zamanı güncellenmesi ya dosyanın üzerine fare işaretçisinin getirilmesi ile, ya tek bir kere fare ile dosyanın ikonu üzerine tıklanması ile ya da çift tıklanarak dosyanın açılması ile oluşabilmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

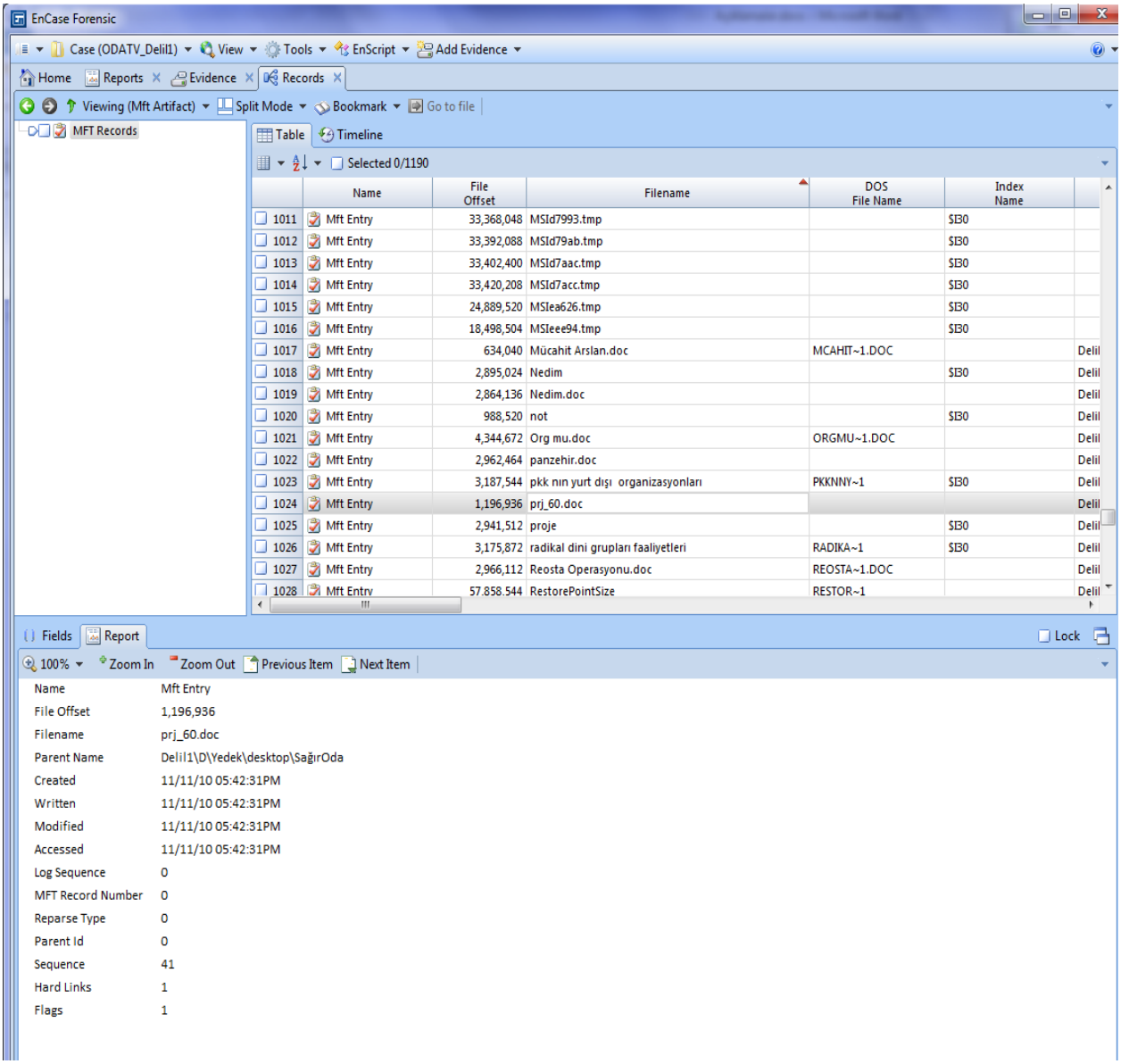
Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

28.) prj_60.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

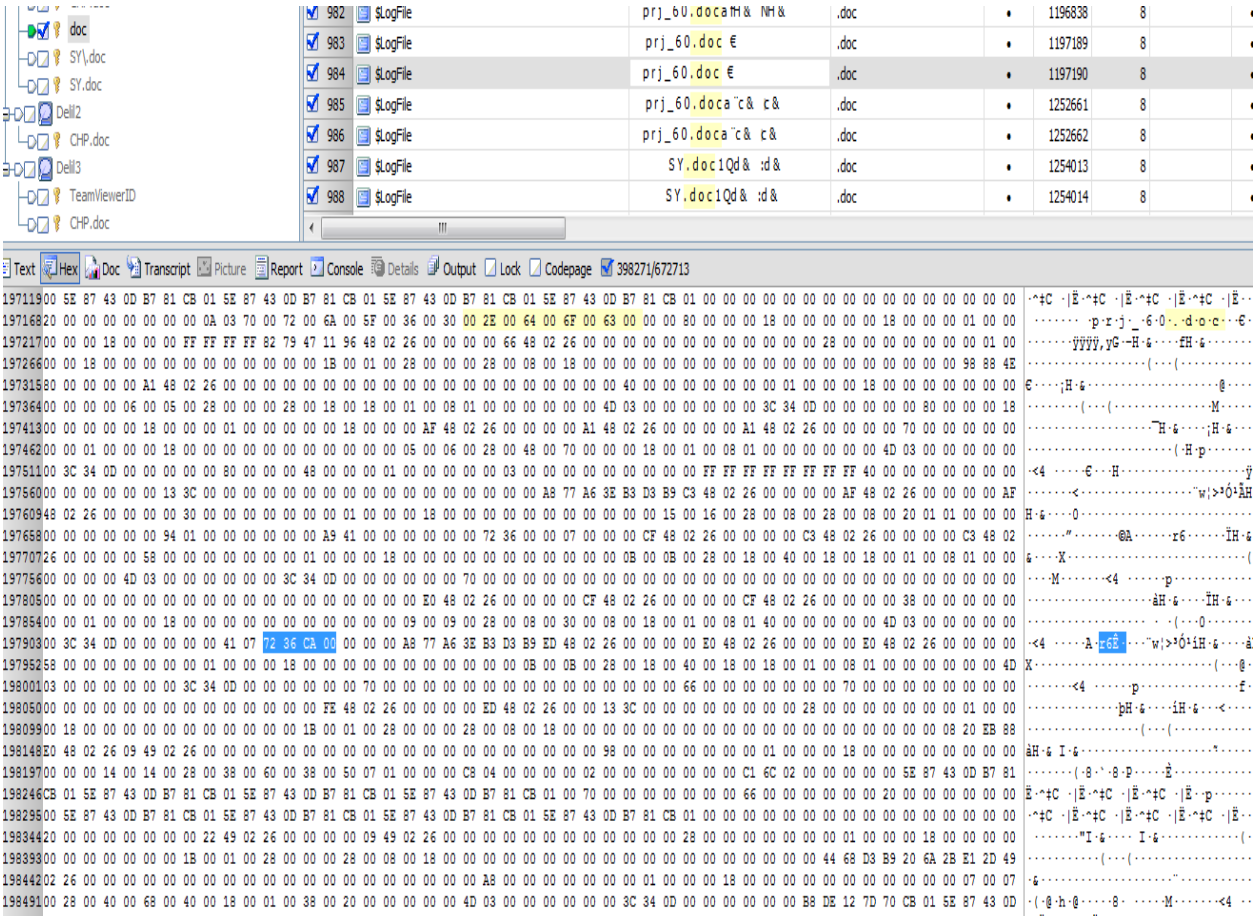
İlgili dosyanın silinmiş olduğu ve $MFT kaydının bulunmadığı tespit edilmiştir. Bununla beraber dosya unallocated clusters alanında tespit edilmiştir ve görüntülenmiştir. $Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

İlgili dosyaya ait Logfile alanında kayda rastlanılmıştır.

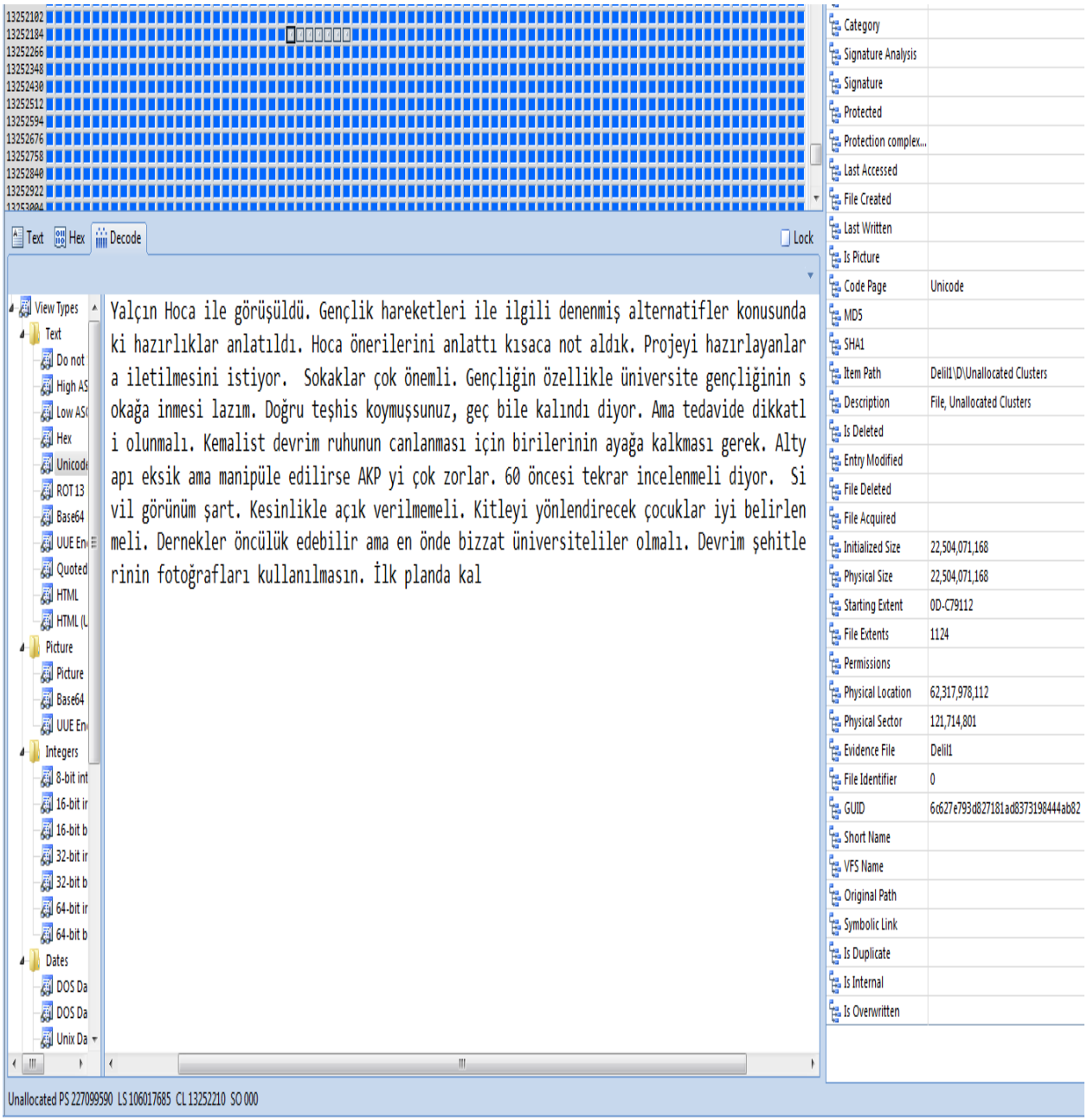


Şekil 64 - prj_60.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

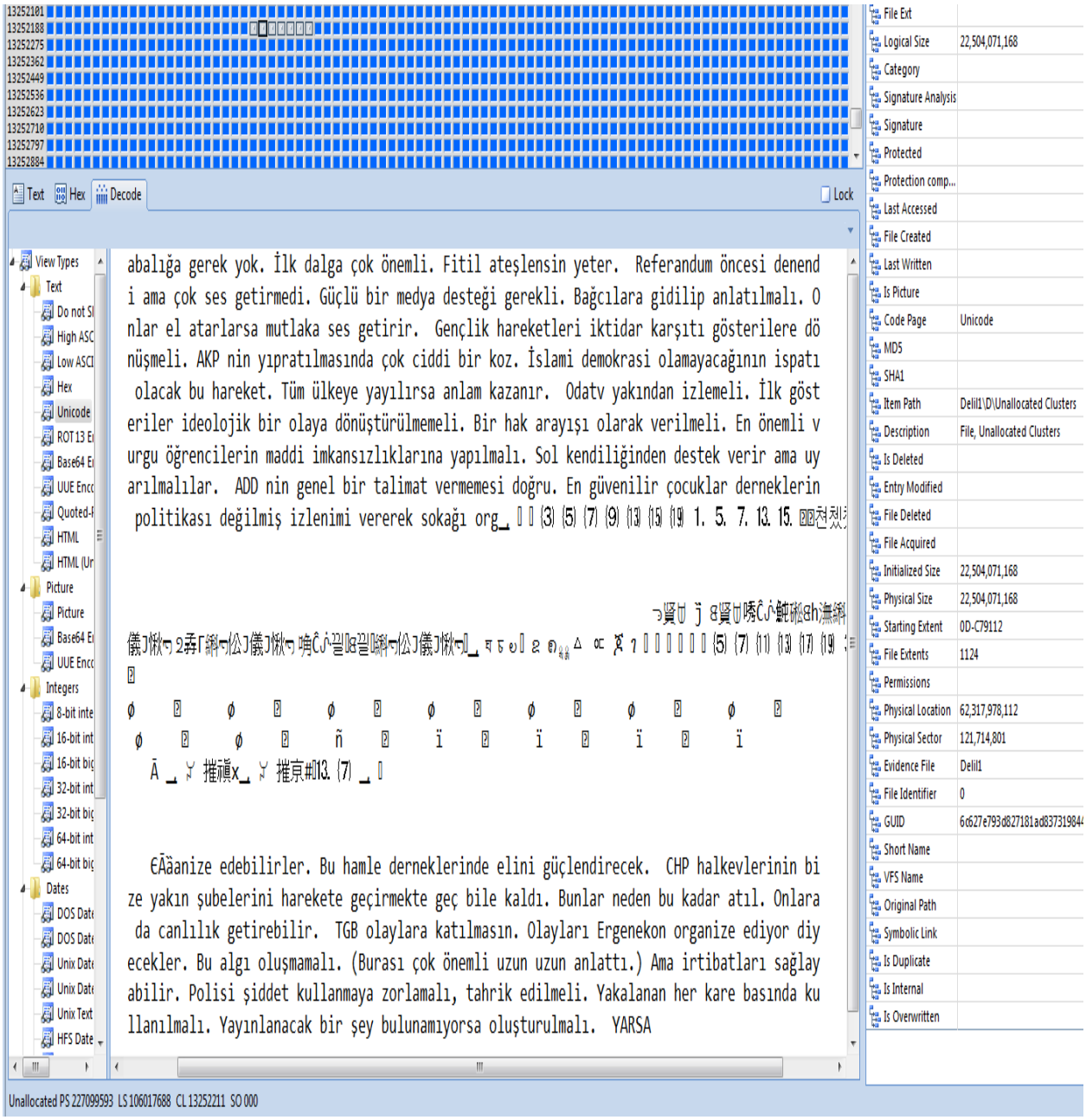
İlgili LogFile'in detaylı analizi yapıldığında ise aşağıdaki bilgiler elde edilmiştir.



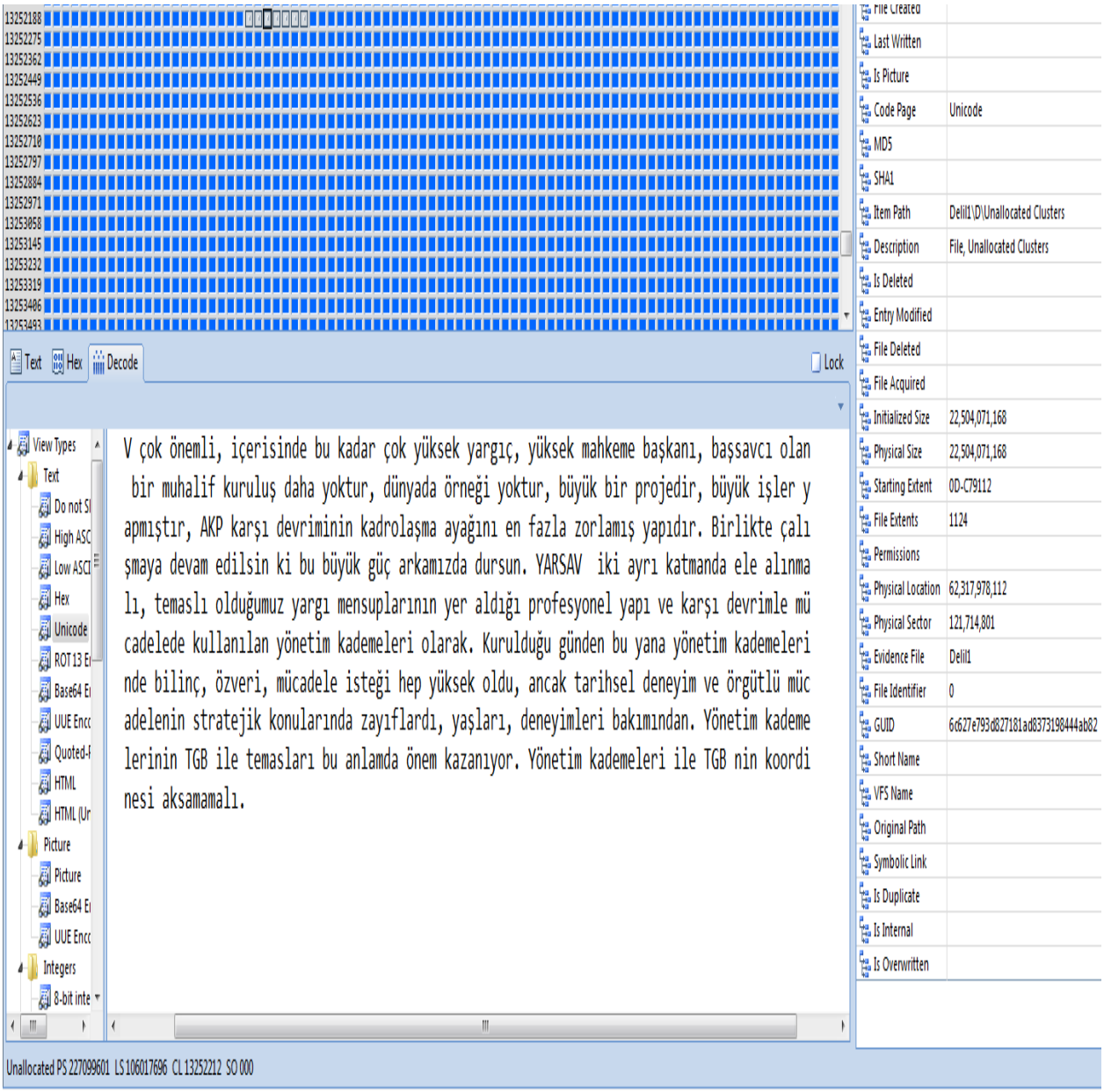
Başlangıç adresi 7236CA00 olan dosyanın bulunduğu cluster olan 13252210 (10'luk tabanda karşılığı) adresine gidildiğinde aşağıdaki veriler elde edilmiştir.



Şekil 65 - prj_60.doc dosyasının silinmiş alanda (unallocated cluster) tespit edilen bölümü -1



Şekil 66 - prj_60.doc dosyasının silinmiş alanda (unallocated cluster) tespit edilen bölümü -2



Şekil 67 - prj_60.doc dosyasının silinmiş alanda (unallocated cluster) tespit edilen bölümü -3

Tespit edilen ve görüntülenebilenprj_60.doc dosyası tamamen kurtarılabilmiştir. Kurtarılan dosyadan elde edilen metaveriler aşağıdaki gibidir.

Belge Üstverileri	
Dosya Adı	prj_60.doc
Dosya Konumu	\D\Yedek\desktop\SağırOda\prj_60.doc
Dosya Durumu	Silinmiş, $MFT kaydı yok,unallocated clusterda bulunuyor

Yazar	Barış
Son Değiştiren Kullanıcı	TOSHIBA
Yönetici	
Şirket	
Nesne Tipi	Microsoft Office Word Belgesi
Yazılım Tipi	Microsoft Office Word
Karakter Tipi	Unicode (UTF-8)
Karakter Sayısı	2448
Uygulama Versiyonu	11.5606
Dosya Boyutu	26 kB
Toplam Değiştirme Süresi	30.0 dakika
Revizyon Numarası	20
Belge Oluşturma Tarihi	2010:10:19 07:21:00
Belge Değiştirme Tarihi	2010:10:20 16:34:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	
FN Oluşturma Zamanı	
Std Değiştirme Zamanı	
FN Değiştirme Zamanı	
Std Erişim Zamanı	
FN Erişim Zamanı	
Std Giriş Zamanı	
FN Giriş Zamanı	

Dosya metaverilerinden elde edilen tarih bilgisinden hareketle, PRJ_60.doc dosyasının 19 Ekim 2010 tarihinde Barış isimli kullanıcının bilgisayarında kaydedildiği ve bir gün sonra değiştirildiği tespit edilmiştir. Aynı dosyanın 11 Kasım 2010 tarihinde ODATV bilgisayarına geldiği görülmüştür. Bu tarih, ilk kısımda bulunan Logfile (Index Artifact) kaydında görüntülenebilmektedir.

Dosyayı oluşturan kullanıcının adı **Barış** ve dosyayı en son değiştiren kullanıcı **TOSHIBA** (MHV2060BH_NW18T6229459 Seri Numaralı imajın kullanıcısı Barış PEHLİVAN'ın bilgisayardaki kullanıcı adı) değerlendirildiğinde, dosyanın son olarak Barış PEHLİVAN'ın bilgisayarında değiştirilmiş olma ihtimali mevcuttur.

Bu imajdan elde edilen prj_60.doc dosyasının en son 20 Ekim 2010'da işlem görmüş olduğu yukarıda tespit edilmiştir. İlgili tarihte MHV2060BH_NW18T6229459 seri numaralı Barış PEHLİVAN'ın bilgisayarında da yine prj_60.doc dosyasının işlem gördüğüne dair bulgular aşağıda belirtilmiştir. Bu durum, prj_60.doc dosyasının ilk olarak MHV2060BH_NW18T6229459 seri numaralı Barış PEHLİVAN'ın bilgisayarında işlem

gördüğünü, daha sonra ST3120927AS_4MS1TF89 seri numaraları ODATV bilgisayarına geldiğine işaret etmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu diskte yapılan incelemelerde bu dosyaya dair LogFile kayıtlarına rastlanmıştır. İncelenen LogFile kayıtlarının zamanlarına bakarak bu dosyanın 20_10.rar adlı sıkıştırılmış dosyadan çıkartıldığı düşünülmektedir.

Dosya Adı	Bulunduğu Dizin	Oluşturma Tarihi	Giriş Tarihi	Değiştirme Tarihi	Erişim Tarihi
20_10.rar	Disk Image\D\BARIS YEDEK 11122009\DEKSTOP\DEPO	20.10.2010 22:56:47	20.10.2010 22:56:47	20.10.2010 22:56:47	20.10.2010 22:56:47
prj_60.doc	Disk Image\D\BARIS YEDEK 11122009\DEKSTOP\DEPO	20.10.2010 22:59:41	20.10.2010 22:59:41	20.10.2010 22:59:41	20.10.2010 22:59:41

Bununla beraber dosyanın kendisine ulaşılamamıştır. Dosyanın kendisinin bulunamayıp LogFile kayıtlarının tespit edilmesi, dosyanın silinmiş ve dosyanın bulunduğu disk alanının üzerine başka bir dosyanın verilerinin yazılmış olduğuna işaret etmektedir.

"prj_60.doc" dokümanı Delil2 diskinde silinmiş ama $MFT kaydı kurtarılabilir durumda bulunmaktadır. Ayrıca bu dosyanın Delil1 diskinde "unallocated cluster" üzerinde bir kopyasına rastlanmış ve veri kurtarma programları yardımıyla kurtarılabilmiştir. Delil1 üzerinde bulunan dosyadan sadece belge üstverilerine, Delil2 den ise sadece dosya sistemi üstverilerine ulaşılabilmiştir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.

- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

- Delil1 de bulunan son kaydedeici belge üstverisinin TOSHIBA olması ve bu ismin de Delil2 deki ofis kullanıcı ismi olması sebebiyle son olarak Delil2 diskinin takılı olduğu bilgisayarda dosyanın kaydedilmiş olma ihtimali yüksektir.

- Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

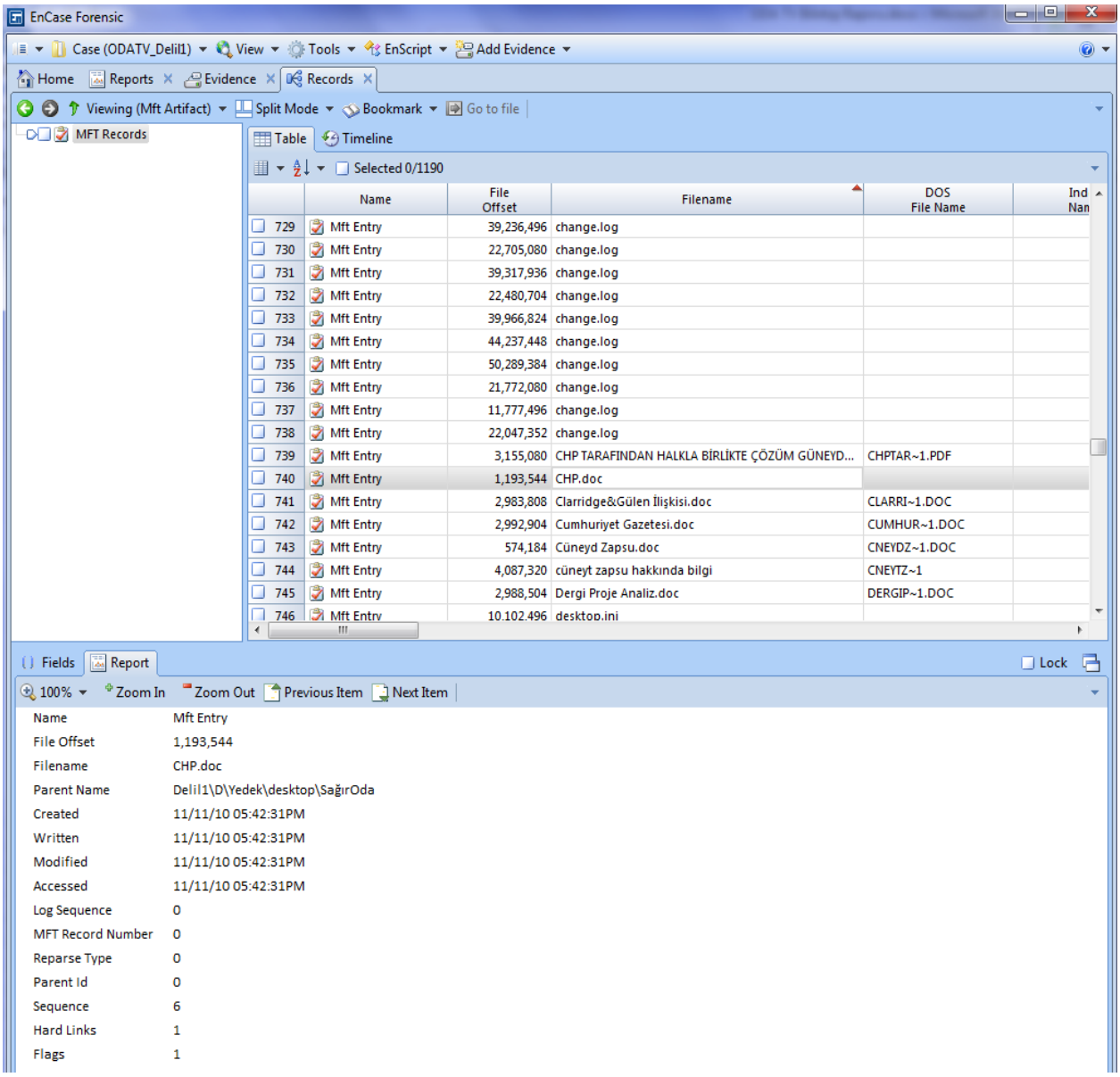
29.) CHP.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Bu imajda CHP.doc isimli 3 adet dosyaya rastlanmıştır. Bunlardan ilki *"Kılıçdaroğluna destek zorunlu.."* içeriğiyle başlayan dosyadır. Bu dosyayla ilişkili bulgular aşağıdaki gibidir.

İlgili dosyanın silinmiş olduğu ve $MFT kaydının bulunmadığı tespit edilmiştir. Ancak dosya unallocated clusters alanında tespit edilmiştir ve görüntülenmiştir.

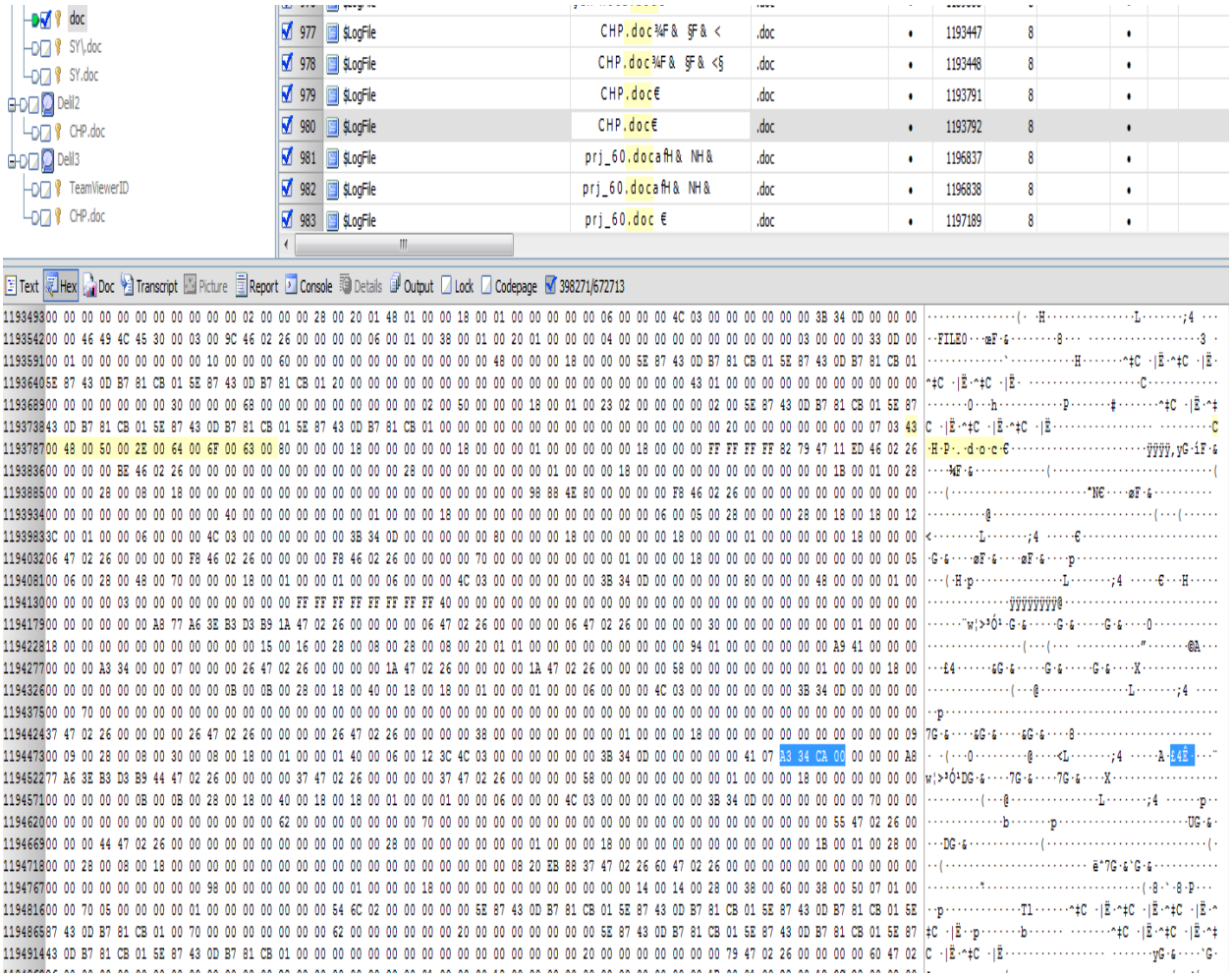
İlgili dosyaya ait Logfile alanında kayda rastlanılmıştır. $Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.



Şekil 68 - CHP.doc Dosyasına Ait Logfile (Index Artifact) Kaydı

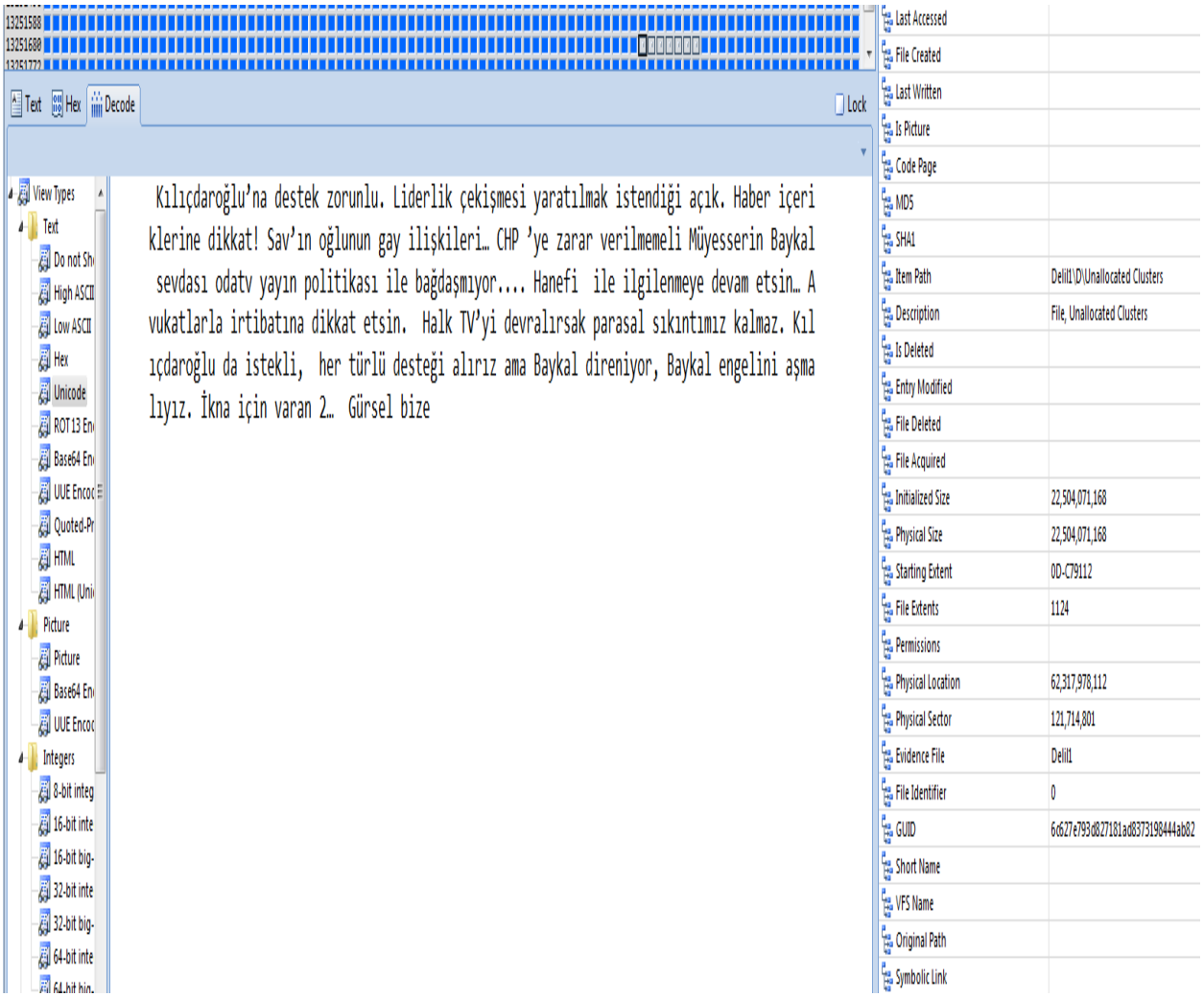
$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

İlgili LogFile'in detaylı analizi yapıldığında ise aşağıdaki bilgiler elde edilmiştir.

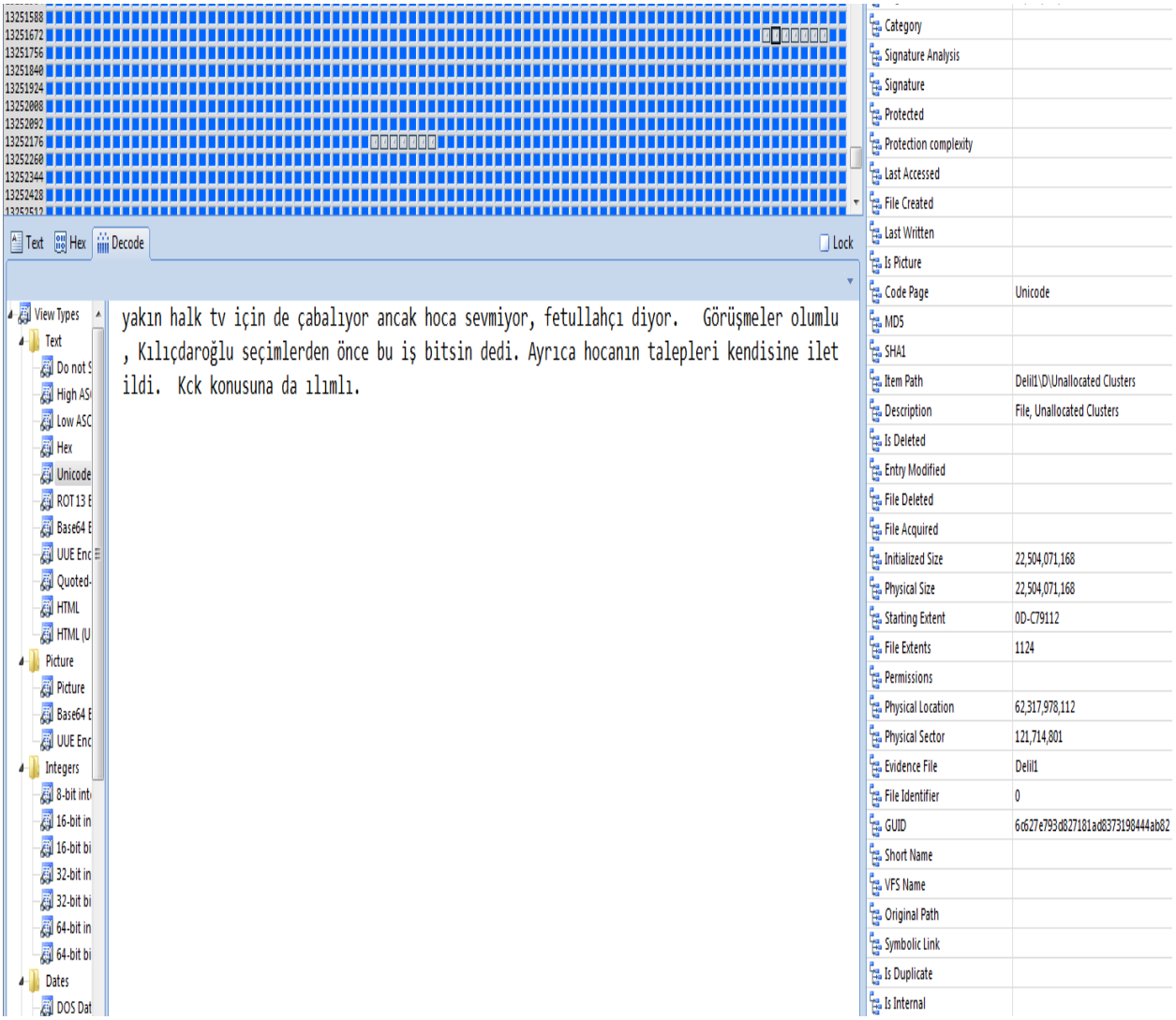


Şekil 69 - CHP.doc dosyasının başlangıç cluster değeri

Başlangıç adresi A334CA00 olan dosyanın bulunduğu cluster olan 13251747 (10'luk tabanda karşılığı) adresine gidildiğinde aşağıdaki veriler elde edilmiştir.



Şekil 70 - CHP.doc dosyasının silinmiş alanda (unallocated cluster) tespit edilen bölümü -1



Şekil 71 - CHP.doc dosyasının silinmiş alanda (unallocated cluster) tespit edilen bölümü -2

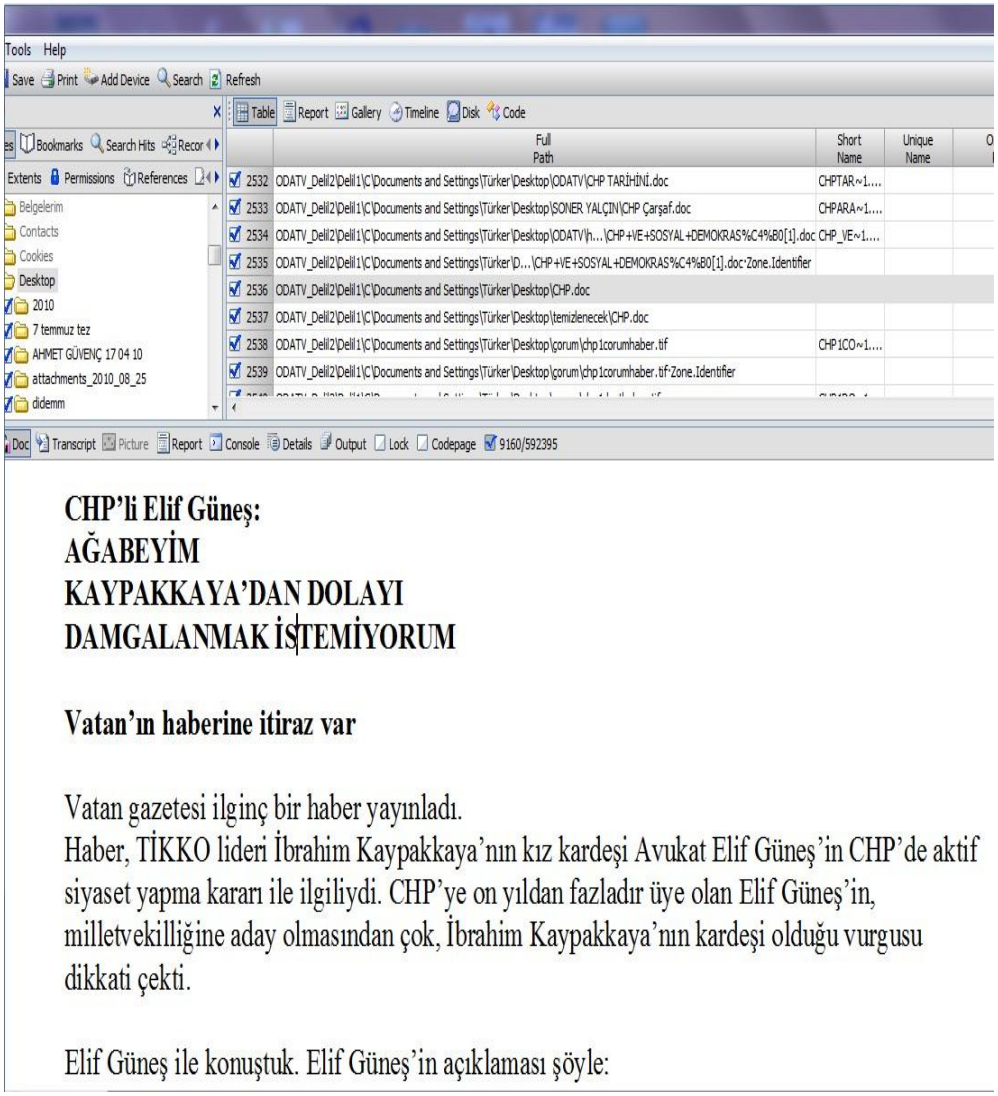
Tespit edilen ve görüntülenebilen CHP.doc dosyası tamamen kurtarılabilmiştir. Kurtarılan dosyadan elde edilen metaveriler aşağıdaki gibidir.

Belge Üstverileri	
Dosya Adı	CHP.doc
Dosya Konumu	\D\Yedek\desktop\SağırOda\chp.doc
Dosya Durumu	Silinmiş, $MFT kaydı yok,unallocated clusterda bulunuyor

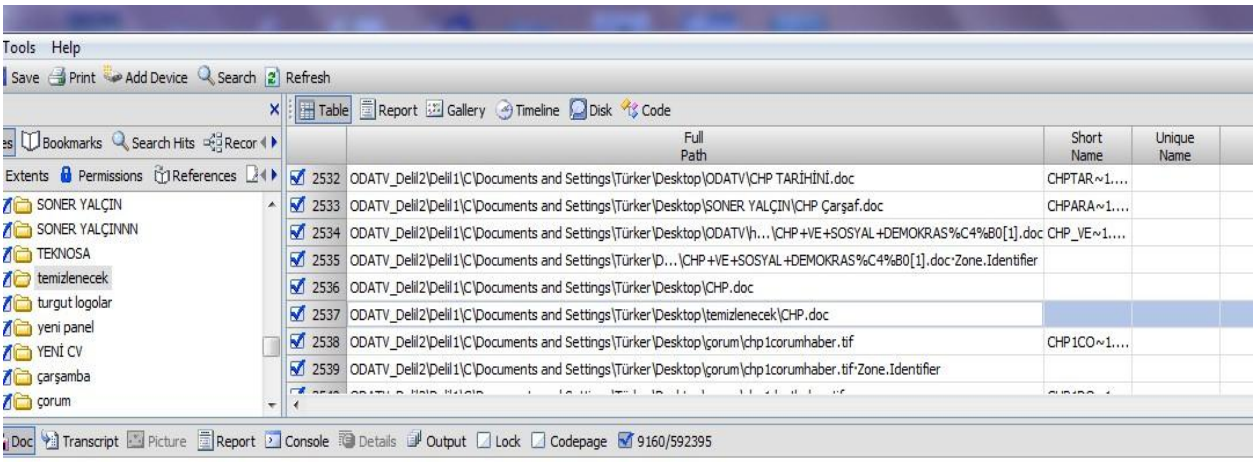
Yazar	soner
Son Değiştiren Kullanıcı	soner
Yönetici	
Şirket	
Nesne Tipi	Microsoft Office Word Belgesi
Yazılım Tipi	Microsoft Word 10.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	596
Uygulama Versiyonu	10.2605
Dosya Boyutu	24 kB
Toplam Değiştirme Süresi	21.0 dakika
Revizyon Numarası	20
Belge Oluşturma Tarihi	2010:10:30 19:22:00
Belge Değiştirme Tarihi	2010:10:30 19:44:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	
FN Oluşturma Zamanı	
Std Değiştirme Zamanı	
FN Değiştirme Zamanı	
Std Erişim Zamanı	
FN Erişim Zamanı	
Std Giriş Zamanı	
FN Giriş Zamanı	

Dosya metaverilerinden elde edilen tarih bilgisinden hareketle, CHP.doc dosyasının 30 Ekim 2010 tarihinde soner isimli kullanıcının bilgisayarında kaydedildiği ve aynı gün değiştirildiği tespit edilmiştir. Aynı dosyanın bu tarihten 11 gün sonra, 11 Kasım 2010 tarihinde ODATV bilgisayarına geldiği görülmüştür. Bu tarih, ilk kısımda bulunan Logfile (Index Artifact) kaydında görüntülenebilmektedir.

Tespit edilen diğer CHP.doc dosyalarının içeriği aşağıdaki gibidir. Bu dosyalar Yıldız Teknik Üniversitesi'nin hazırladığı bilirkişi raporunda belirtilen dosyalardır. Bu iki dosyaya ait **yazar** ve **son değiştiren kullanıcı** gibi üstveri bilgilerinden hareketle bu dosyaların ilgili bilgisayarda oluşturulduğu ve değiştirildiği düşünülmektedir. Bu dosyalarla ilgili Yıldız Teknik Üniversitesi'nin hazırladığı rapora ilişkin yorumlar 13. Sorunun cevabında verilmiştir.



Şekil 72 - C:\Documents and Settings\Türker\Desktop\CHP.doc dosyası



CHP'deki durumun özeti, bence şu: Kemal Kılıçdaroğlu, partisinin içindeki kriz günlerini aştı ve daha da güçlendi.

Bugün, attığı adımın hukukî dayanağına bakalım. Bu, sağlam bir dayanak. CHP, 2008'deki olağanüstü kurultayında bir tüzük değişikliği kabul etmiş, Kılıçdaroğlu onu uyguluyor.

'Ama o değişiklik demokratik değildir, genel başkana aşırı yetkiler veriyor' derseniz, faydası yok... Çünkü, o değişiklik, o tarihte Genel Başkan Deniz Baykal tarafından ısrarla istenilmiş, Genel Sekreter Önder Sav'ın da olurunu almış ve olağanüstü kurultayda çok büyük bir çoğunlukla kabul edilmiş...

Değişiklik şu: Partinin 20 kişilik Merkez Yönetim Kurulu, 80 kişilik Parti Meclisi'nde seçim yapılarak belirleniyordu. Artık o seçim yapılmayacak... Genel Başkan, kendine 13 'genel başkan yardımcısı' ile bir genel sekreter atayacak... Merkez Yönetim Kurulu onlardan oluşacak. (Ayrıca genel başkanın onları istediği zaman görevinden uzaklaştırıp, yerlerine yenilerini atama yetkisi de olacak.)

Şekil 73 - C:\Documents and Settings\Türker\Desktop\temizlenecek\CHP.doc dosyası

"chp.doc" dokümanı Delil1 diskinde $Logfile kayıtlarında bulunmuştur. 3 farklı yerde bu isimli dosya bulunsa da sadece bir tanesi Ek–1 deki dosyadır. Bu dosya da $Logfile da kayıtlı bulunmasına rağmen silinmiş durumdadır ve veri kurtarma programları yardımıyla kurtarılabilmiştir. $MFT kayıtları olmadığından dosya sistemi üstverilerine ulaşılamamaktadır. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Belge üstverileri uyumludur.
- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

Ancak bununla beraber silinmiş durumunda olan ve bu sebeple ne dosyası olduğu anlaşılamayan, açılmış bir internet sitesi ya da okunmuş bir dokümanda bu dosyanın ismi geçmektedir. Dosya isminin disk üzerindeki aramalarda bu şekilde bir doküman ya da internet geçmişinde çıkmış olması, bu dosyanın bu disk üzerinde bulunduğuna dair net bir bilgi vermemektedir.

Dosya isminin geçtiği cluster ve sektör adresleri aşağıdaki gibidir:

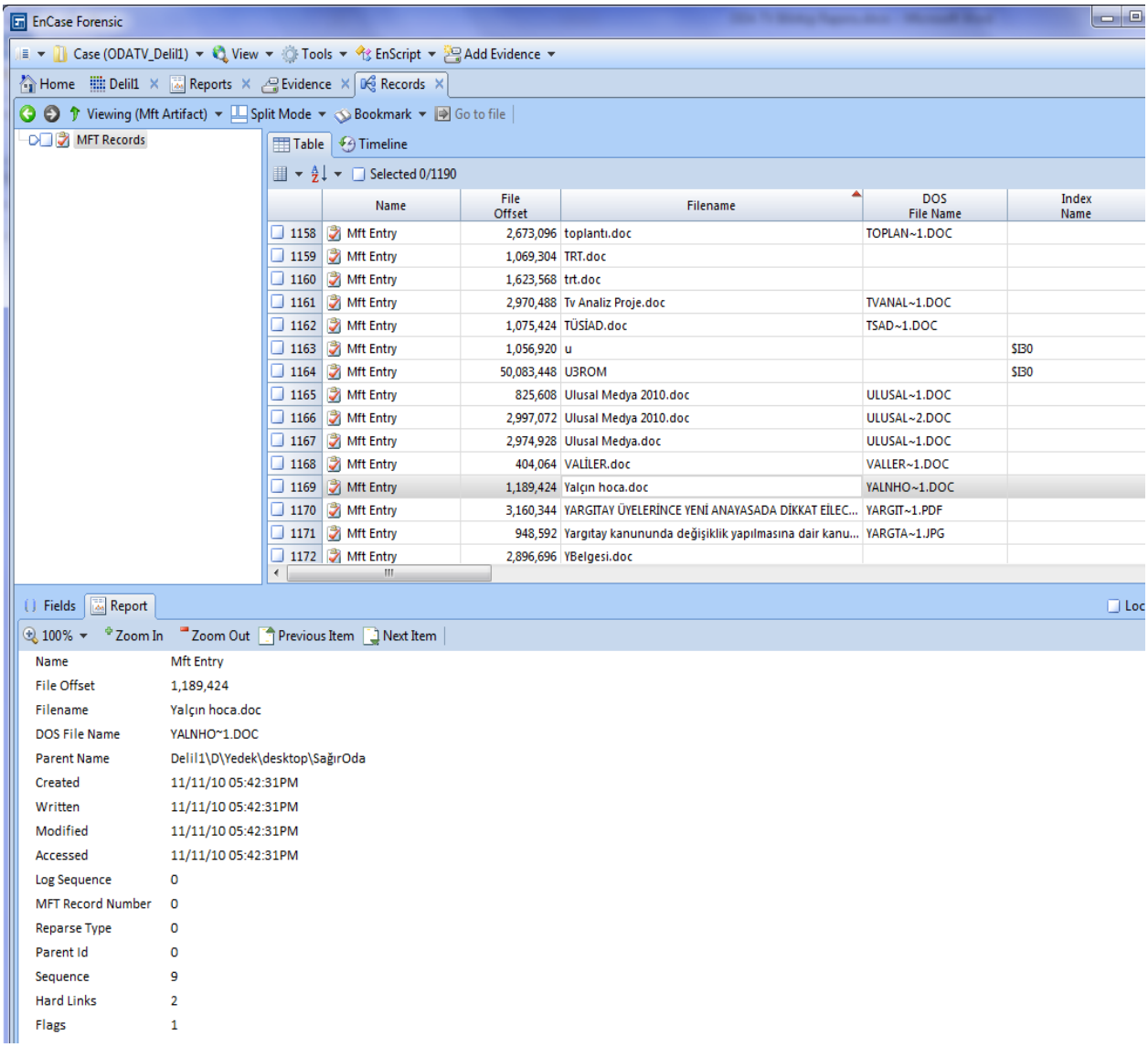
CL 14539568 SO 196 ,CL 14538994 SO 186 ,CL 14538751 SO 444 ,CL 14538501 SO 118 ,CL 14539239 SO 228 ,CL 526260 SO 196 ,CL 525931 SO 228 ,CL 525193 SO 118 ,CL 525443 SO 444 ,CL 525686 SO 186 ,CL 13247888 SO 196 ,CL 13247559 SO 228 ,CL 13247314 SO 186 ,CL 105976571 SO 444

30.) Yalçın hoca.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

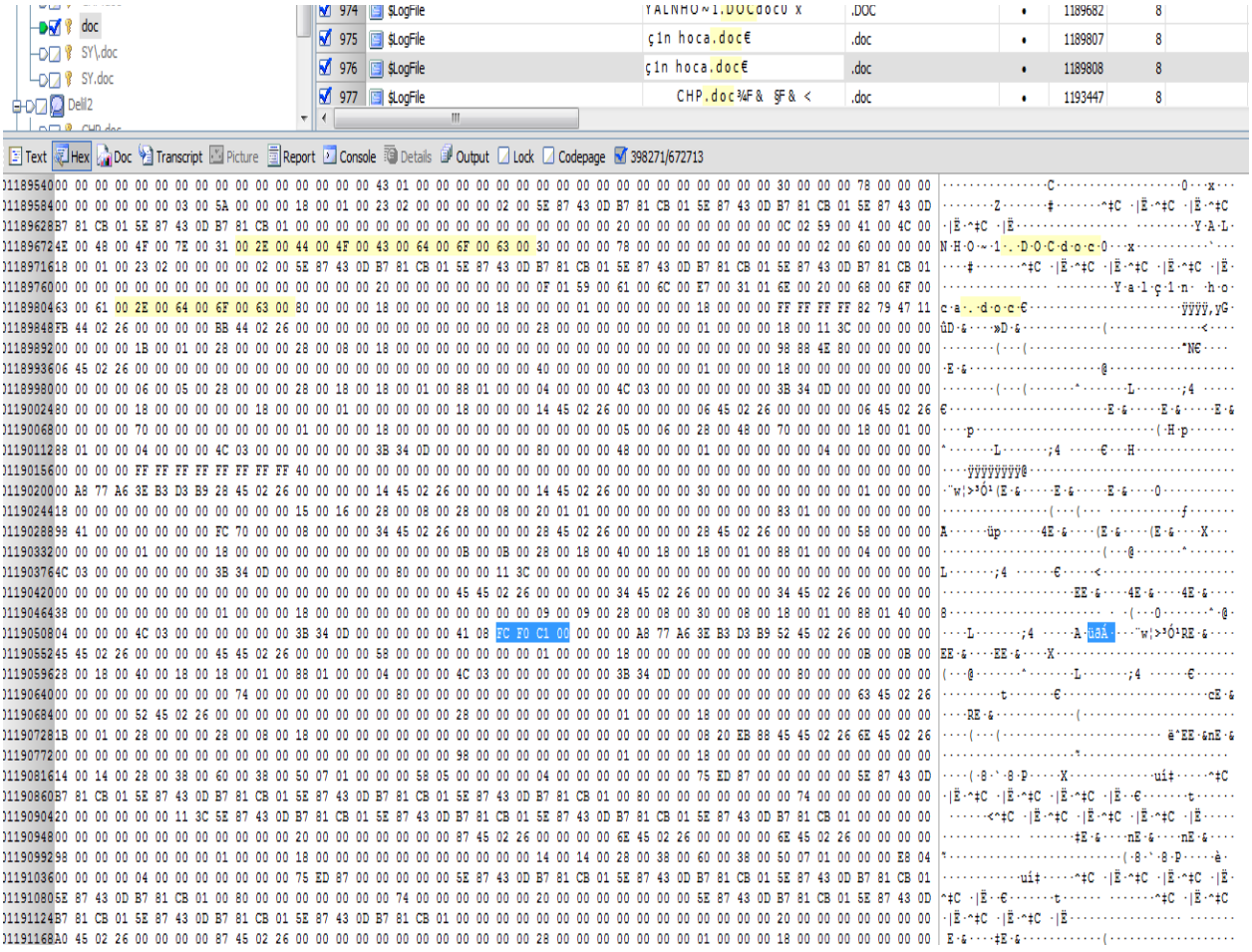
İlgili dosyanın silinmiş olduğu ve $MFT kaydının bulunmadığı tespit edilmiştir. Bununla beraber dosya unallocated clusters alanında tespit edilmiştir ve görüntülenmiştir.

İlgili dosyaya ait Logfile kaydı aşağıda görülmektedir.



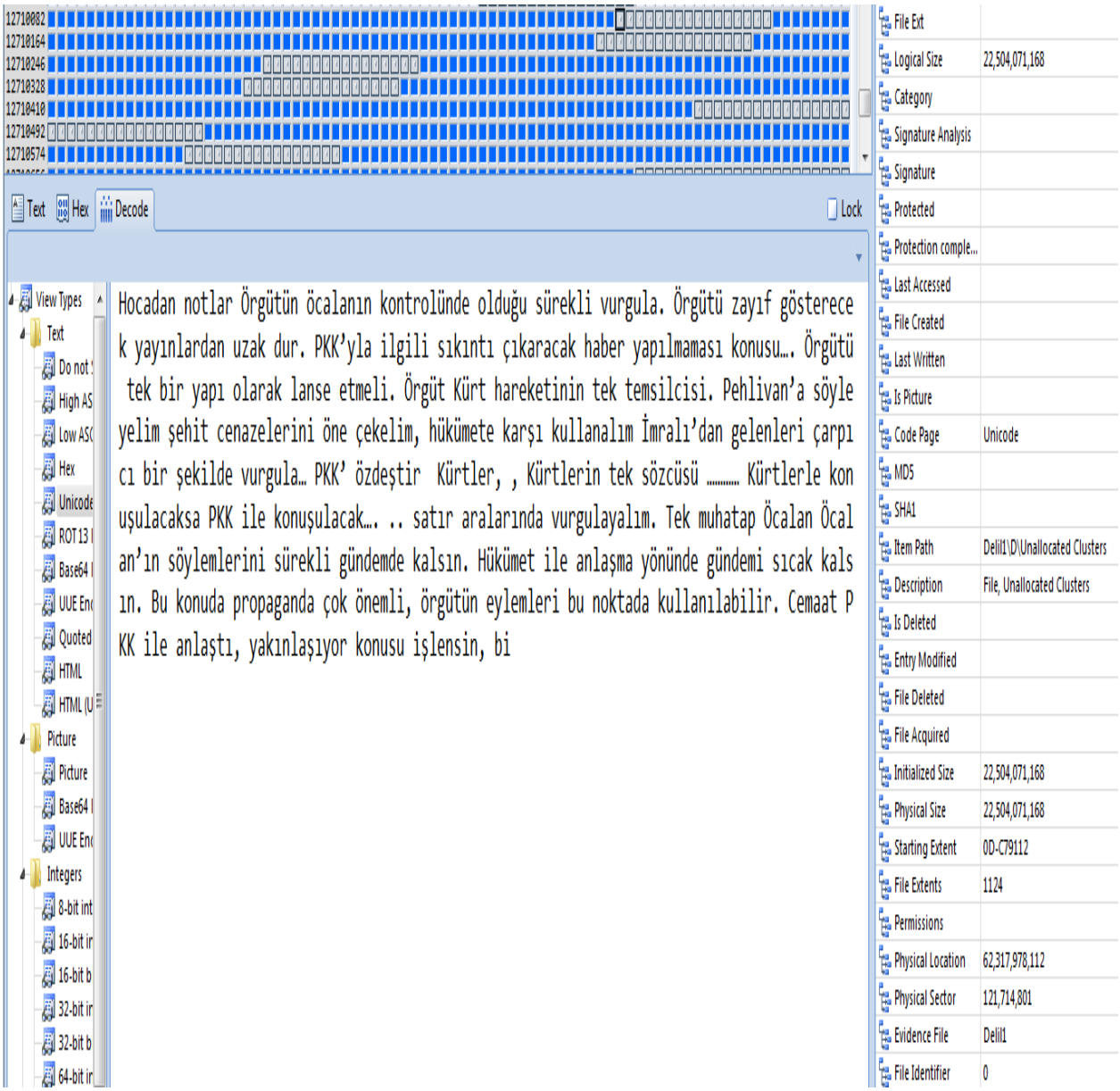
Şekil 74 - Yalçın hoca.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

Logfile'dan elde edilen değerler kullanılarak dosyanın başlangıç cluster adresi tespit edilmiştir.

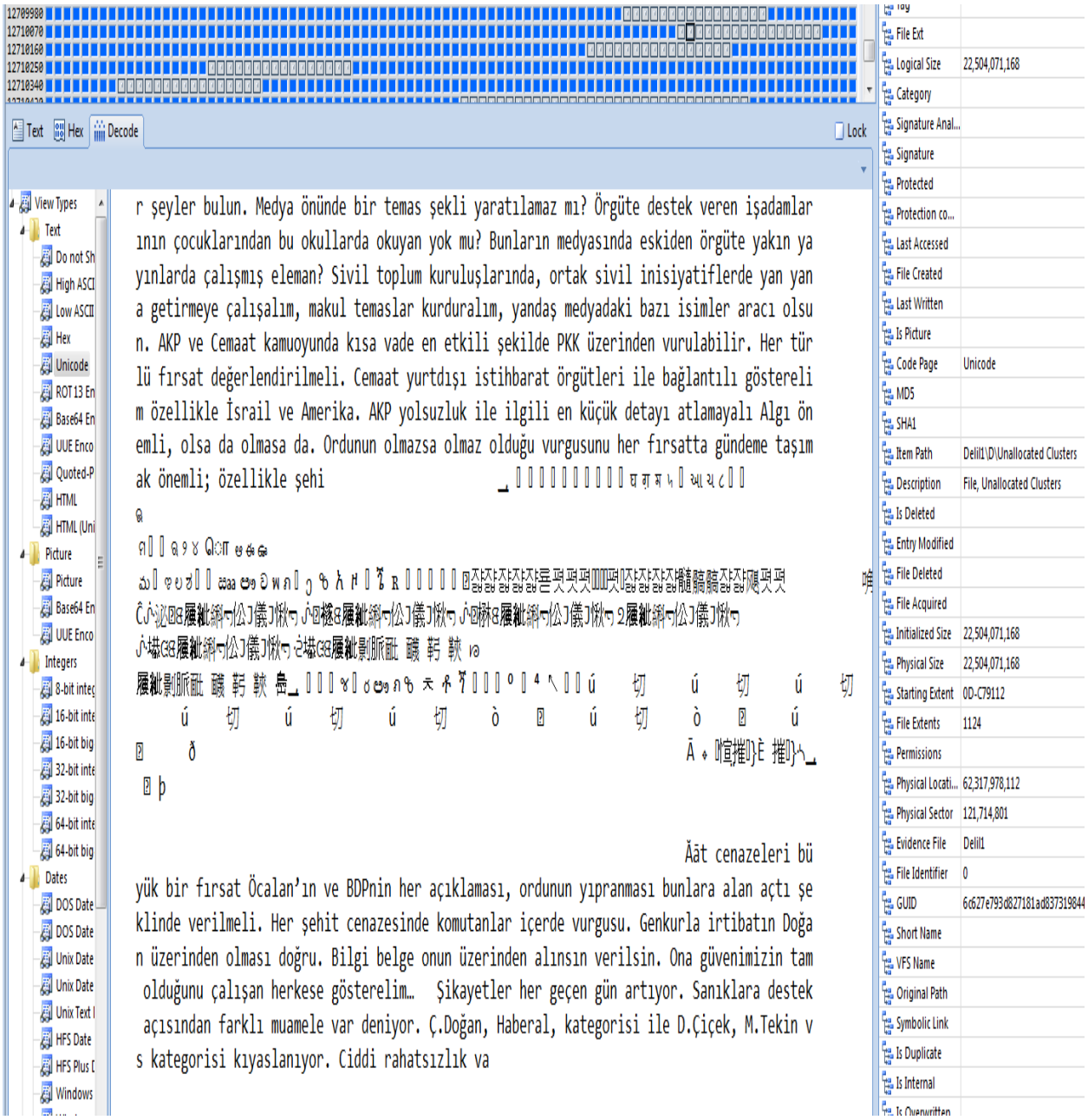


Şekil 75 - Yalçın hoca.doc dosyasının başlangıç cluster değeri

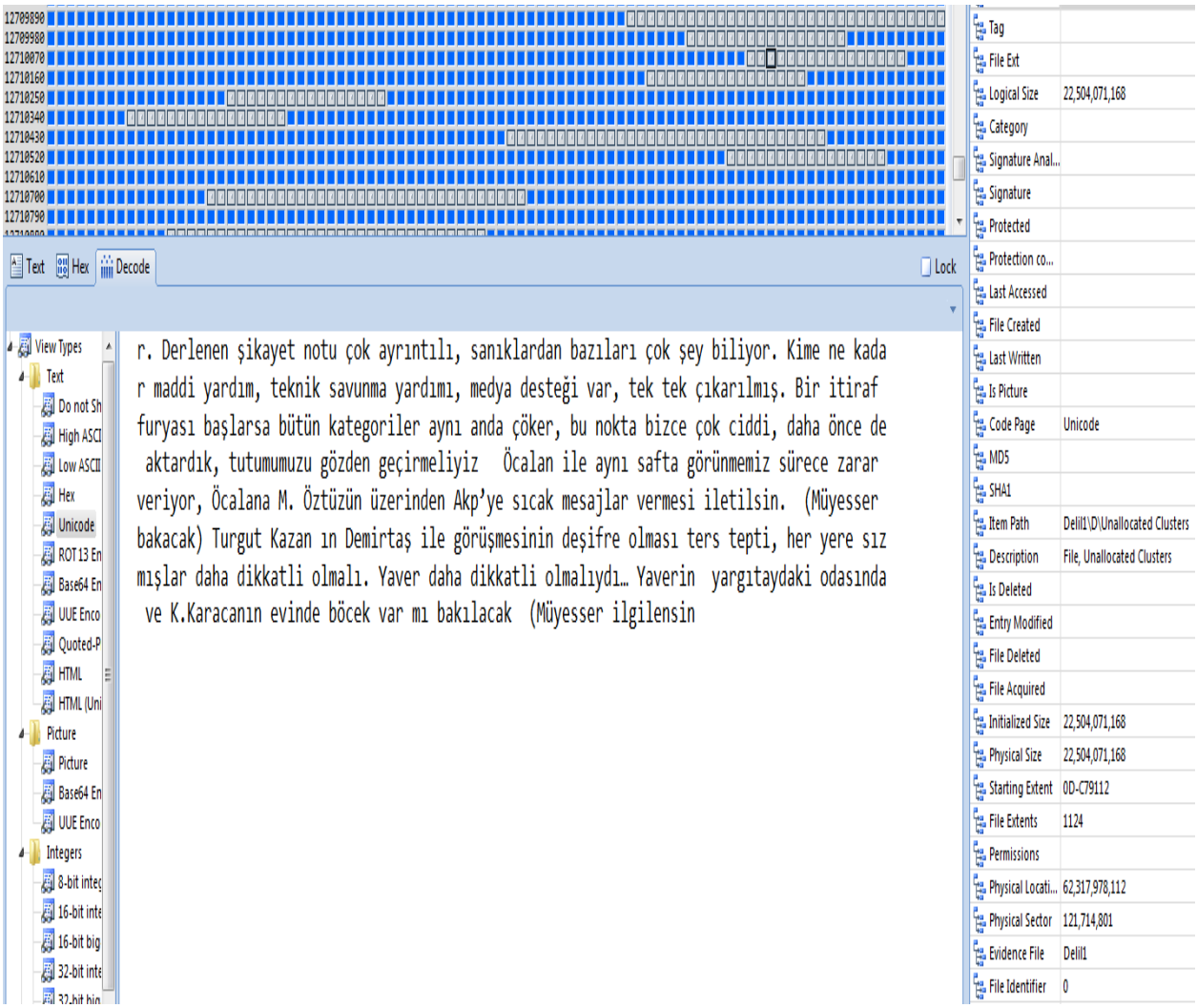
Başlangıç adresi FCF0C100 olan dosyanın bulunduğu cluster olan 12710140 (10'luk tabanda karşılığı) adresine gidildiğinde aşağıdaki veriler elde edilmiştir.



Şekil 76 - Yalçın hoca.doc dosyasının silinmiş alanda (unallocated cluster)tespit edilen bölümü-1



Şekil 77 - Yalçın hoca.doc dosyasının silinmiş alanda (unallocated cluster)tespit edilen bölümü-2



Şekil 78 - Yalçın hoca.doc dosyasının silinmiş alanda (unallocated cluster)tespit edilen bölümü-3

Tespit edilen bu dosya tamamen kurtarılabilmiştir. Böylece metaverileri elde edilmiştir.

Belge Üstverileri	
Dosya Adı	Yalçın hoca.doc
Dosya Konumu	\D\Yedek\desktop\SağırOda\yalçin hoca.doc
Dosya Durumu	Silinmiş, $MFT kaydı yok,unallocated clusterda bulunuyor.
Yazar	soner
Son Değiştiren Kullanıcı	soner
Yönetici	
Şirket	Conqueror
Nesne Tipi	Microsoft Office Word Belgesi
Yazılım Tipi	Microsoft Word 10.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	2719
Uygulama Versiyonu	10.2605
Dosya Boyutu	29 kB

Toplam Değiştirme Süresi	22.0 dakika
Revizyon Numarası	16
Belge Oluşturma Tarihi	2010:06:18 08:23:00
Belge Değiştirme Tarihi	2010:09:08 06:31:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	
FN Oluşturma Zamanı	
Std Değiştirme Zamanı	
FN Değiştirme Zamanı	
Std Erişim Zamanı	
FN Erişim Zamanı	
Std Giriş Zamanı	
FN Giriş Zamanı	

"Yalçın hoca.doc" dokümanı Delil2 diskinde silinmiş ama $Logfile kaydı ulaşılabilir durumda bulunmaktadır. Delil2 içindeki son durumu dosyanın silinmiş ve üzerine veri yazılarak ulaşılamaz hale gelmiştir. Delil1 diskinde ise "unallocated cluster" alanından veri kurtarma programları yardımıyla geri döndürülebilmiştir. Delil1 de sadece belge üstverisi bulunmakta, Delil2 de ise sadece dosya sistemi üstverilerine ulaşılabilinmektedir. Delil3 diskinde ise dosya normal olarak bulunmuştur ve bu sebeple hem belge üstverilerine hem de dosya sistemi üstverilerine ulaşılabilmiştir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Delil1 ve Delil2 için dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.

- Delil3 için olan zaman anormalliklerinin sonradan bir zaman değiştirme programı kullanılması ile oluşmuş olabileceği değerlendirilmektedir.

- Her üç delil diski için dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

- Her üç delil diski için işletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

- Her üç delil diski için dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu

dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

• Delil2 için dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu diskte yapılan incelemelerde bu dosyaya dair LogFile kayıtlarına rastlanmıştır. İncelenen LogFile kayıtlarının zamanlarına bakarak bu dosyanın 28_09.rar adlı sıkıştırılmış dosyadan çıkartıldığı düşünülmektedir.

Dosya Adı	Bulunduğu Dizin	Oluşturma Tarihi	Giriş Tarihi	Değiştirme Tarihi	Erişim Tarihi
28_09.rar	D\BARIS YEDEK 11122009\DEKSTOP\DEPO	28.09.2010 23:08:25	28.09.2010 23:08:25	28.09.2010 23:08:25	28.09.2010 23:08:25
Yalçın hoca.doc	D\BARIS YEDEK 11122009\DEKSTOP\DEPO	28.09.2010 23:08:41	28.09.2010 23:08:41	28.09.2010 23:08:41	28.09.2010 23:08:41

Bununla beraber dosyanın kendisine ulaşılamamıştır. Dosyanın kendisinin bulunamayıp LogFile kayıtlarının tespit edilmesi, dosyanın silinmiş ve dosyanın bulunduğu disk alanının üzerine başka bir dosyanın verilerinin yazılmış olduğuna işaret etmektedir.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Belge Üstverileri	
Dosya Adı	Yalçın hoca.doc
Dosya Konumu	\C\Users\user\Documents\Yalçin hoca.doc
Dosya Durumu	Aktif
Yazar	soner
Son Değiştiren Kullanıcı	user
Yönetici	
Şirket	Conqueror
Nesne Tipi	Microsoft Word Document
Yazılım Tipi	Microsoft Word 10.0

Karakter Tipi	Windows Turkish
Karakter Sayısı	2699
Uygulama Versiyonu	10,2605
Dosya Boyutu	28 kB
Toplam Değiştirme Süresi	22.0 dakika
Revizyon Numarası	17
Belge Oluşturma Tarihi	2010:06:18 08:23:00
Belge Değiştirme Tarihi	2010:09:09 11:18:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-09-09 15:21:22
FN Oluşturma Zamanı	2011-02-14 07:30:42.564129
Std Değiştirme Zamanı	2010-09-09 15:18:25
FN Değiştirme Zamanı	2011-02-14 07:30:42.564129
Std Erişim Zamanı	2010-09-09 17:38:55
FN Erişim Zamanı	2011-02-14 07:30:42.564129
Std Giriş Zamanı	2011-02-14 18:44:51.553530
FN Giriş Zamanı	2011-02-14 07:30:42.564129

Bu imajda tespit edilen "Yalçın hoca.doc" dosyasının üstverilerinde görülen aşağıdaki özelliklerin hep birlikte gerçekleşmesinin, normal kullanıcı davranışlarıyla zor olduğu değerlendirilmektedir. Bu özellikler:

- STD oluşturma ve erişim zamanlarının, FN zamanlarından geri olması ve mikro saniye kısımlarının 0 olması ve
- STD MFT kaydı değişim zamanının mikro saniye kısmının olması ve FN zamanlarından az ileri olmasıdır.

Dosya sistemi üstverilerindeki FN zamanlarının, STD oluşturma ve erişim zamanlarından ileri olması durumu, yedekleme sistemlerinde yedekleme aşamasında STD oluşturma ve erişim zamanlarının tutulmasının istenmesi ve yedekten dönülmesi sırasında yedekleme sistemi tarafından bu değerlerin ilk tutulan değerlere geri getirilmesi gibi durumlarda oluşabilir. Bunun yanında arşivleme programlarında da bu özellik bulunabilir. Örneğin en çok kullanılan dosya arşivleme programlarından biri olan "winrar" programında bu özellik mevcuttur(Store Creation Time, Store Last Access Time)."Winrar" programı kullanılarak yapılan testlerde FN zamanlarının, STD oluşturma zamanlarından daha güncel olabileceği görülmüştür. Aynı zamanda FN zamanlarının, STD oluşturma zamanlarından daha güncel olması farklı bir sürücüden taşıma ile gelen dosyalarda normal olan durumdur. Bunun yanında Winrar programı ile yapılan testlerde, STD oluşturma ve erişim zamanlarında mikro saniye kısmı olmaması durumu ile karşılaşılmıştır.

STD oluşturma ve erişim zamanlarında mikro saniye bilgisinin olmaması (sıfır olması) aslında işletim sistemi temel dosyalarında karşılaşılabilen bir durumdur. Fakat normal kullanıcı dosyalarında olma ihtimali düşüktür.

Bu özelliklerin hepsinin birlikte olmasını açıklayan diğer bir senaryo ise şöyledir:

- Dosya bu bilgisayara FN zamanlarında belirtilen "2011-02-14 07:30:42.564129" zamanında gelmiştir,
- Dosya daha sonra Std MFT kaydı değişim zamanı olan "2011-02-14 18:44:51.553530" zamanında ise STD oluşturma, değiştirme ve erişim zamanları değiştirilmiştir.

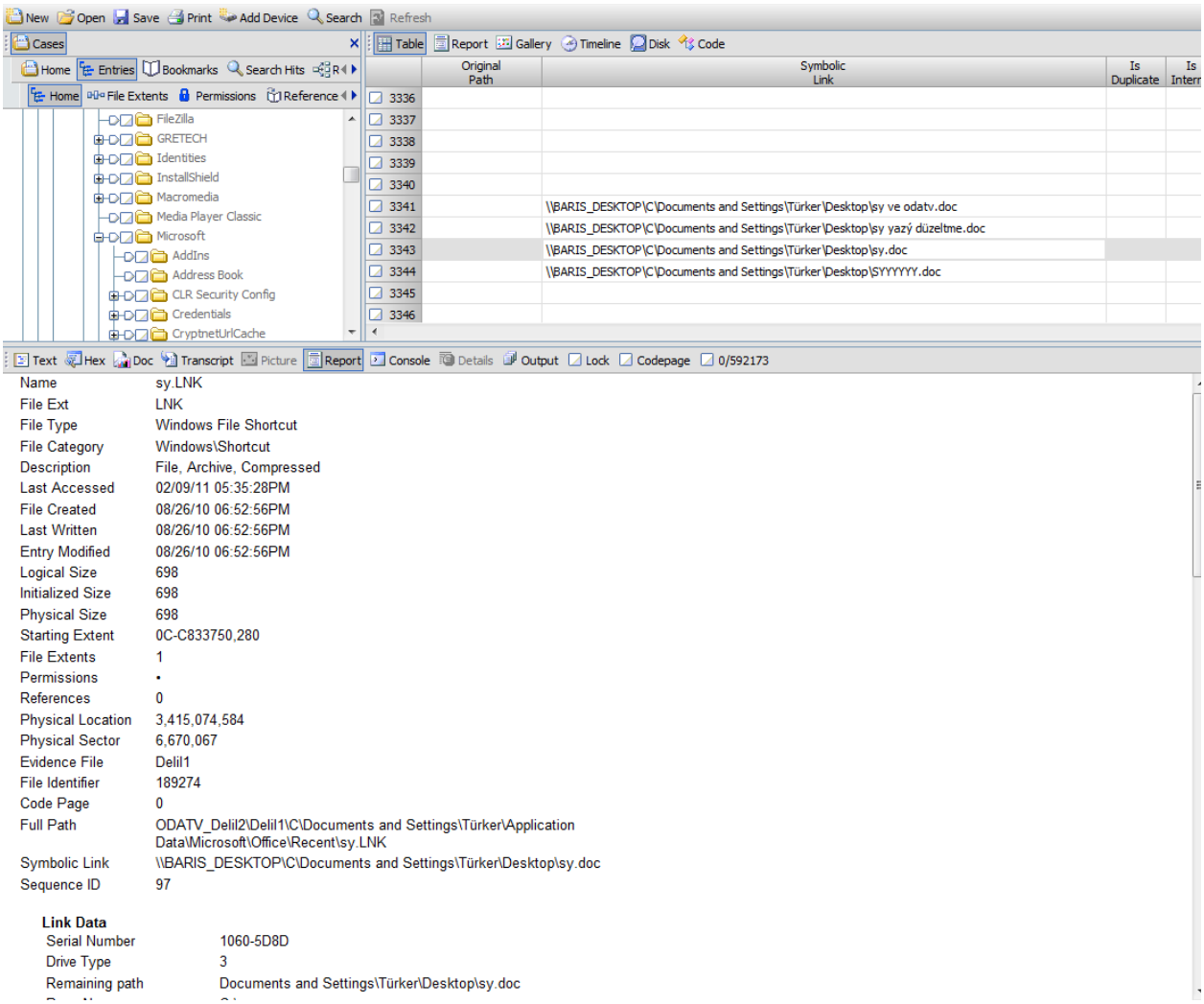
Zaman değiştirme işlemi, yazılmış özel bir program ile ya da basit bir "visual basic script" ile olabilmektedir.

Sonuç olarak dosyadaki dosya sistemi üstverilerindeki bu uyuşmazlığın nasıl oluştuğu kesin olmamakla birlikte, yedekten dönme işlemi, RAR arşivleme ile arşiv açma işlemi ve zaman üstverilerinin sonradan değiştirilmiş olması işlemlerinden biri ile oluşmuş olabileceği değerlendirilmektedir. Bu işlemlerden gerçekleşmiş olmaya en yakın olanının, zaman üstverilerinin sonradan değiştirilmiş olması olduğu değerlendirilmektedir.

31.) SY.doc

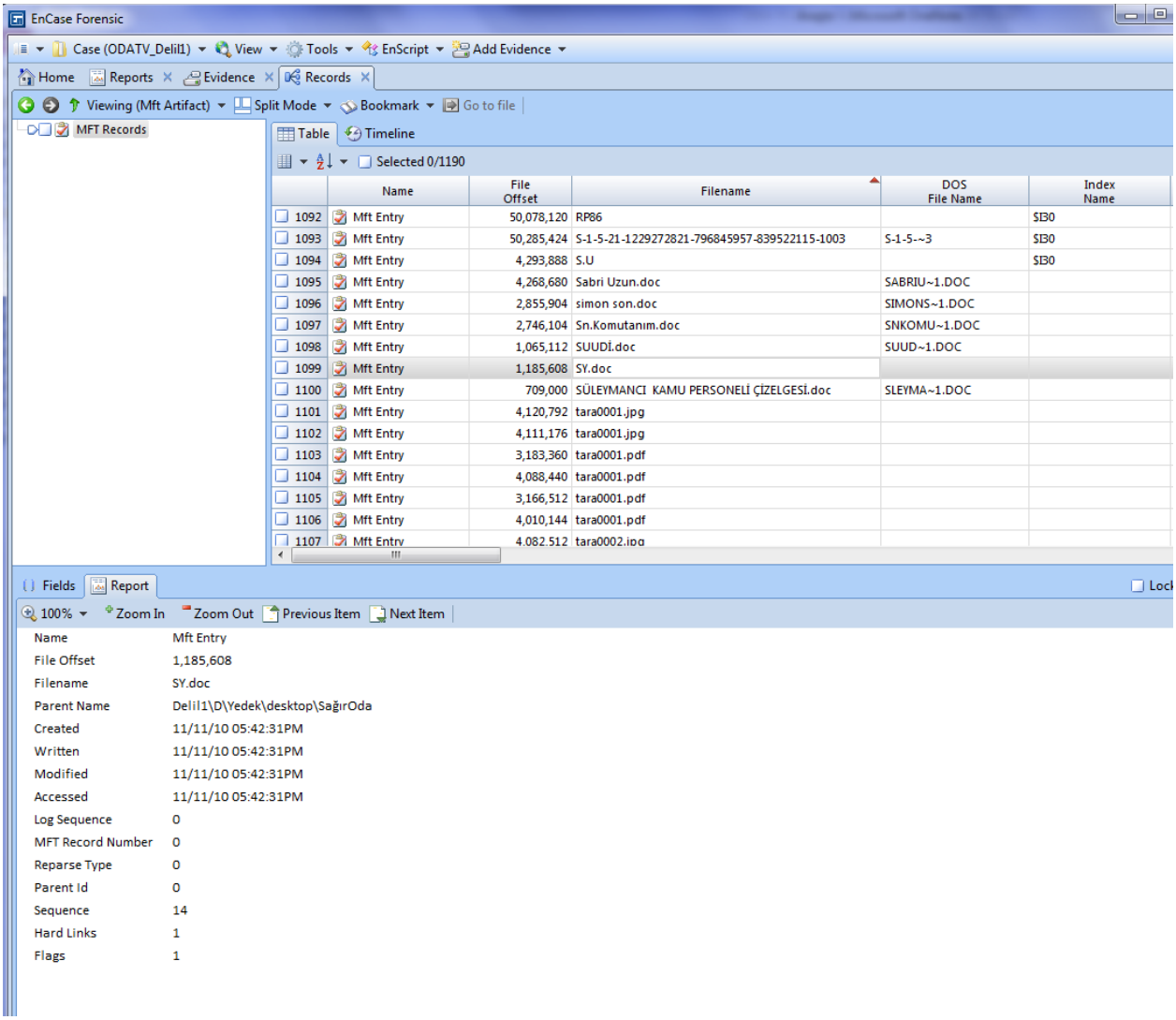
ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

İlgili imajda 2 adet SY.doc dosyası bulunmuştur. İlki, bilgisayarın masaüstü klasöründe silinmiş halde olan sy.doc dosyasıdır. Office son kullanılanlar klasöründe bu dosyanın açıldığına dair bir bağlantı bulunmuştur.



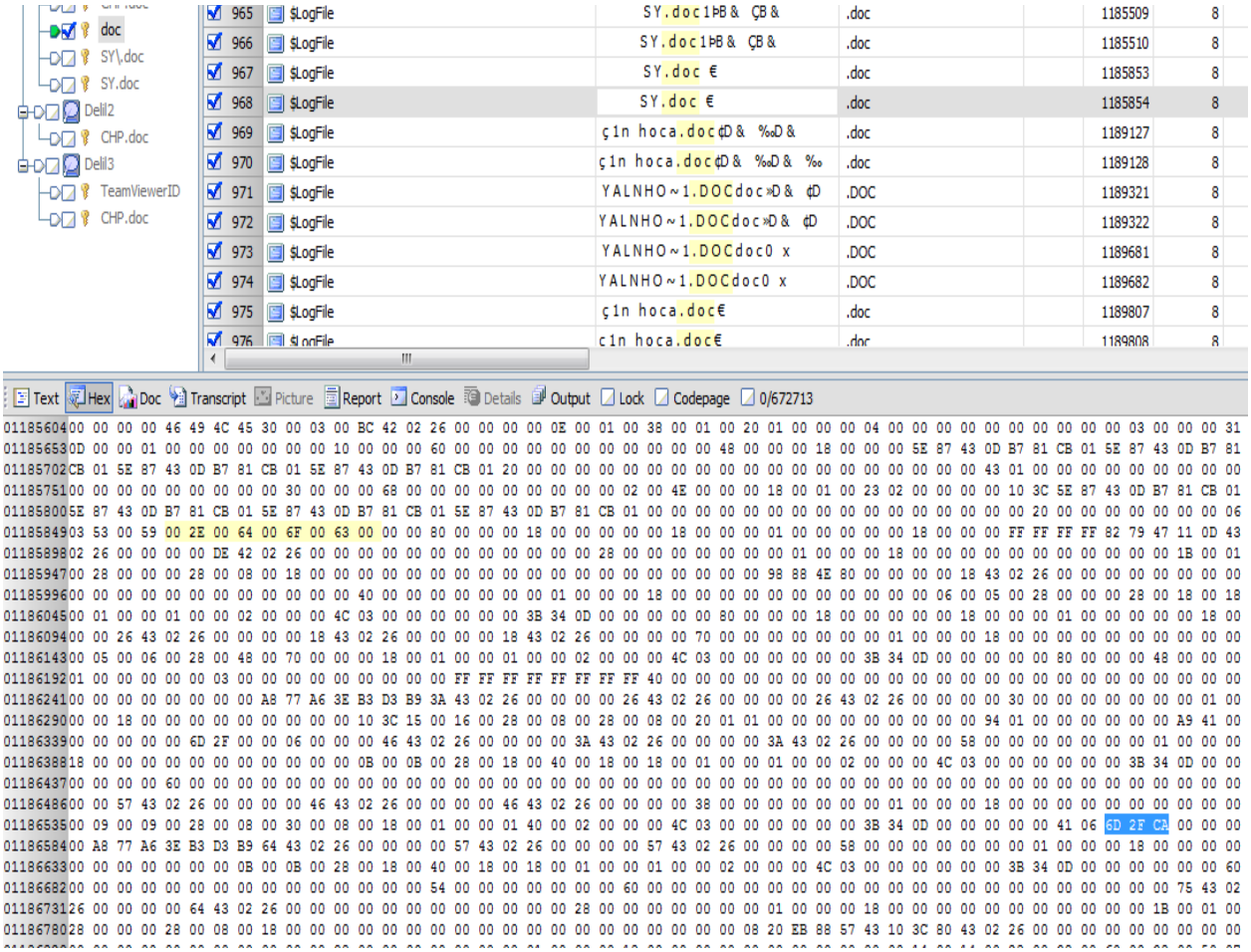
Şekil 79 - sy.doc isimli dosya ve Office Son Kullanılanlar bağlantısı

Tespit edilen bir diğer dosya ise, **D\Yedek\desktop\SağırOda** klasöründe tespit edilen silinmiş SY.doc dosyasıdır.Bu dosya için Logfile (MFT Artifact) alanına kayıt düştüğü gözlenmektedir. $Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.



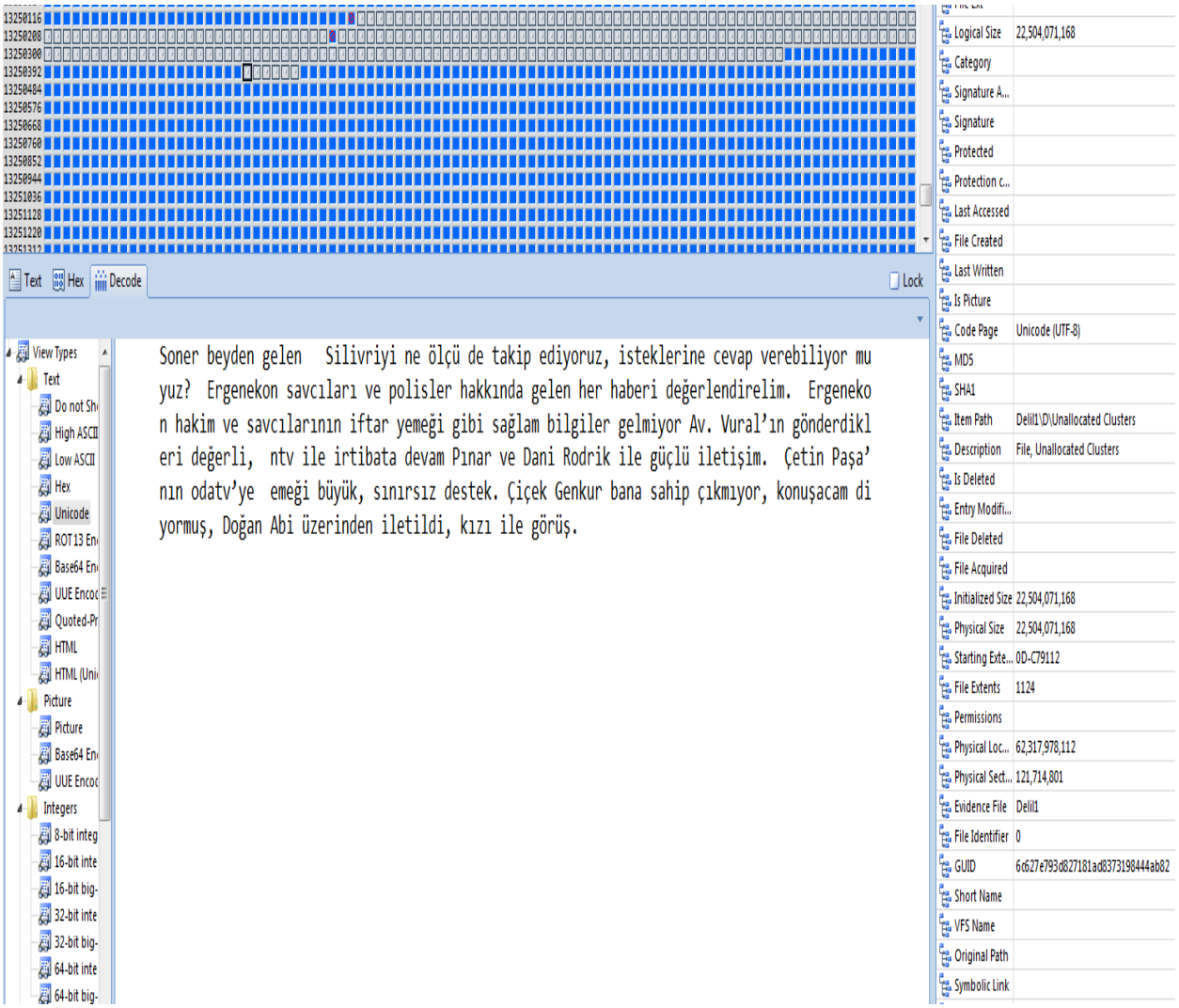
Şekil 80 - SY.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

Logfile'dan elde edilen değerler kullanılarak dosyanın başlangıç cluster adresi tespit edilmiştir.

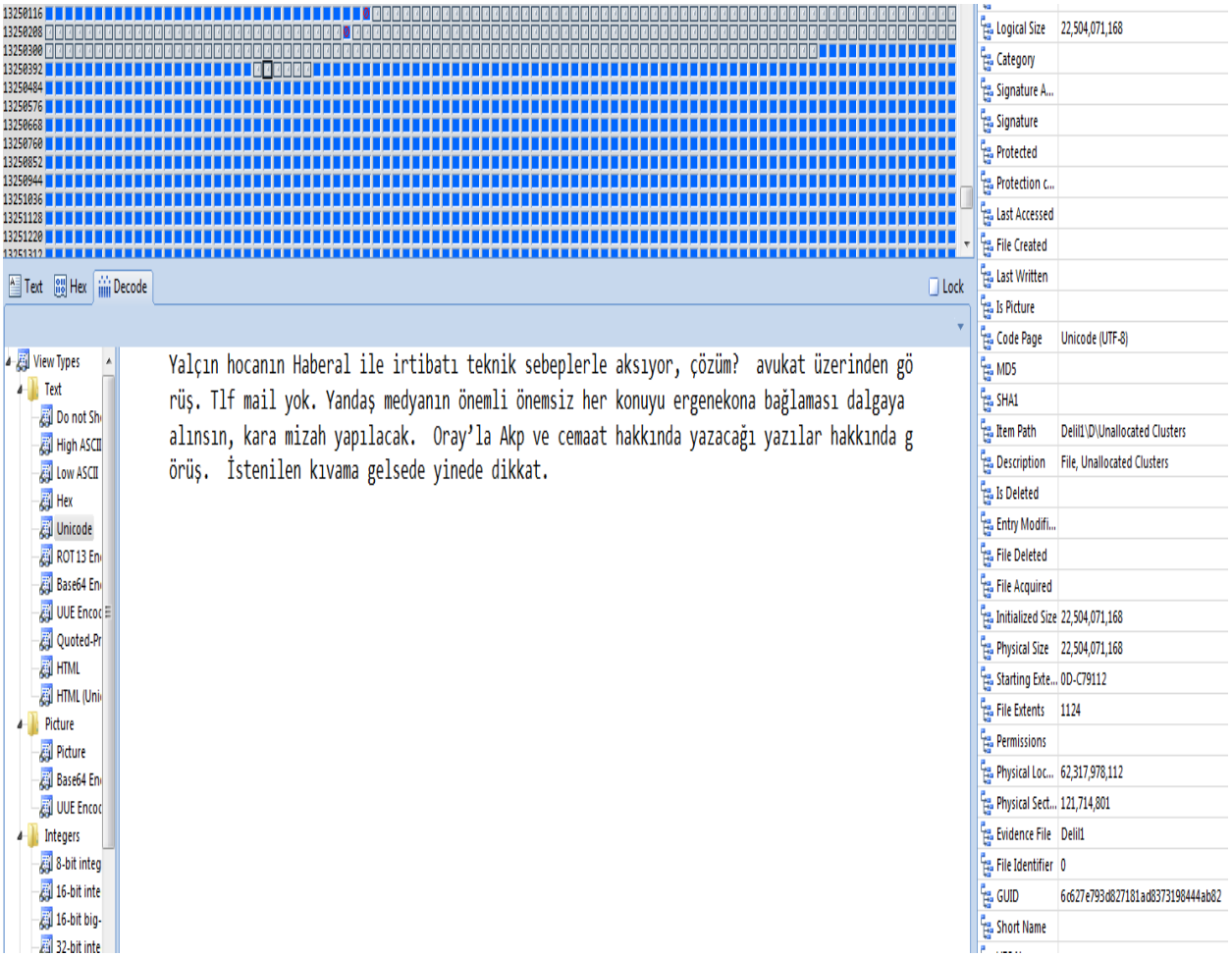


Şekil 81 - SY.doc dosyasının başlangıç cluster değeri

Başlangıç adresi 6D2FCA00 olan dosyanın bulunduğu cluster olan 13250413 (10'luk tabanda karşılığı) adresine gidildiğinde aşağıdaki veriler elde edilmiştir.



Şekil 82 - SY.doc dosyasının silinmiş alanda (unallocated cluster) tespit edilen bölümü -1



Şekil 83 - SY.doc dosyasının silinmiş alanda (unallocated cluster) tespit edilen bölümü -2

Tespit edilen ve görüntülenebilen SY.doc dosyası tamamen kurtarılabilmiştir. Kurtarılan dosyadan elde edilen metaveriler aşağıdaki gibidir.

Belge Üstverileri	
Dosya Adı	SY.doc
Dosya Konumu	\D\Yedek\desktop\SağırOda\SY.doc
Dosya Durumu	Silinmiş, $MFT kaydı yok,unallocated clusterda bulunuyor
Yazar	soner
Son Değiştiren Kullanıcı	TOSHIBA
Yönetici	
Şirket	Conqueror
Nesne Tipi	Microsoft Office Word Belgesi

Yazılım Tipi	Microsoft Office Word
Karakter Tipi	Unicode (UTF-8)
Karakter Sayısı	701
Uygulama Versiyonu	11.5606
Dosya Boyutu	21 kB
Toplam Değiştirme Süresi	18.0 dakika
Revizyon Numarası	12
Belge Oluşturma Tarihi	2010:07:23 12:20:00
Belge Değiştirme Tarihi	2010:07:26 06:05:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	
FN Oluşturma Zamanı	
Std Değiştirme Zamanı	
FN Değiştirme Zamanı	
Std Erişim Zamanı	
FN Erişim Zamanı	
Std Giriş Zamanı	
FN Giriş Zamanı	

Dosya üstverilerinden elde edilen tarih bilgisinden hareketle; "SY.doc" dosyasının 23 Temmuz 2010 tarihinde "soner" isimli kullanıcının bilgisayarında oluşturulduğu ve 3 gün sonra 26 Temmuz 2010 tarihinde "TOSHIBA" isimli kullanıcının bilgisayarında değiştirildiği anlaşılmaktadır. Aynı dosyanın 11 Kasım 2010 tarihinde ODATV bilgisayarında işlem gördüğü tespit edilmiştir.

Dosyayı en son değiştiren kullanıcı adının "**TOSHIBA"** yani MHV2060BH_NW18T6229459 Seri Numaralı imajın kullanıcısı Barış PEHLİVAN'ın bilgisayardaki kullanıcı adı olduğu görülmektedir. Bu bulgu "SY.doc" dosyasının en son olarak o bilgisayarda değiştirilmiş olabileceği ihtimalini doğurmaktadır. Fakat "SY.doc" dosya üstverisinde belge son değiştirilme zamanı olarak geçen 26 Temmuz 2010 tarihi "06:05:00" saatinde delil 2 bilgisayarının açıldığına ve çalışır durumda olduğuna dair bir bulgu mevcut değildir. Bunun yanında ilgili tarihte MHV2060BH_NW18T6229459 seri numaralı Barış PEHLİVAN'ın bilgisayarında da yine "SY.doc" dosyasının işlem gördüğüne dair aşağıda belirtilen bulgular 26 Temmuz 2010 tarihi 23:05:31 saati gibi ileri bir saatte "SY.doc" dosyasının "SY.rar" dosyasından gelmiş olabileceğine işaret etmektedir. Bu sebeple "SY.doc" dosyasının son olarak MHV2060BH_NW18T6229459 seri numaraları Barış PEHLİVAN'ın bilgisayarında değiştirildiği şüphelidir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu diskte yapılan incelemelerde bu dosyaya dair LogFile kayıtlarına rastlanmıştır. İncelenen LogFile kayıtlarının zamanlarına bakarak bu dosyanın SY.rar adlı sıkıştırılmış dosyadan çıkartıldığı düşünülmektedir. Hatta daha sonra dosyanın farklı bir lokasyona kopyalandığı bu sebeple ikinci bir LogFile kaydının düştüğü düşünülmektedir.

Dosya Adı	Bulunduğu Dizin	Oluşturma Tarihi	Giriş Tarihi	Değiştirme Tarihi	Erişim Tarihi
SY.rar	D\BARIS YEDEK 11122009\DEKSTOP\DEPO	26.07.2010 23:05:31	26.07.2010 23:05:31	26.07.2010 23:05:31	26.07.2010 23:05:31
SY.doc	D\BARIS YEDEK 11122009\DEKSTOP\DEPO	26.07.2010 23:05:53	26.07.2010 23:05:53	26.07.2010 23:05:53	26.07.2010 23:05:53
SY.doc	D\BARIS YEDEK 11122009	26.07.2010 23:52:58	26.07.2010 23:52:58	26.07.2010 23:52:58	26.07.2010 23:52:58

Tablo 5 - SY.rar ve SY.doc Dosyasıyla İlgili Logfile Kayıtları

Bununla beraber dosyanın kendisine ulaşılamamıştır. Dosyanın kendisinin bulunamayıp LogFile kayıtlarının tespit edilmesi, dosyanın silinmiş ve dosyanın bulunduğu disk alanının üzerine başka bir dosyanın verilerinin yazılmış olduğuna işaret etmektedir.

"SY.doc" dokümanı Delil2 diskinde silinmiş ama $Logfile kaydı ulaşılabilir durumda bulunmaktadır. Ayrıca Delil2 diskindeki $Logfile kayıtlarına göre bu dosya disk üzerinde iki farklı dizinde bulunmuştur. Delil2 içindeki son durumu ise bu iki dizindeki dosyalar silinmiş ve üzerlerine veri yazılarak dosyalar ulaşılamaz hale gelmişlerdir. Delil1 diskinde ise "unallocated cluster" alanından veri kurtarma programları yardımıyla geri döndürülebilmiştir. Delil1 de sadece belge üstverisi bulunmakta, Delil2 de ise sadece dosya sistemi üstverilerine ulaşıla bilinmektedir. Delil3 diskinde ise dosya normal olarak bulunmuştur ve bu sebeple hem belge üstverilerine hem de dosya sistemi üstverilerine ulaşılabilinmiştir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Delil1 ve Delil2 için dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Delil3 için olan zaman anormalliklerinin sonradan bir zaman değiştirme programı kullanılması ile oluşmuş olabileceği değerlendirilmektedir.
- Her üç delil diski için dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

- Her üç delil diski için işletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Her üç delil diski için dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Delil2 için dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.
- Delil2 deki $Logfile analizi sonrası bir RAR arşiv dosyasından çıkarıldıktan sonra çıkarıldığı dizinden başka bir dizine kopyalandığı görülmektedir.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Belge Üstverileri	
Dosya Adı	SY.doc
Dosya Konumu	\C\Users\user\Documents\SY.doc
Dosya Durumu	Aktif
Yazar	soner
Son Değiştiren Kullanıcı	TOSHIBA
Yönetici	
Şirket	Conqueror
Nesne Tipi	Microsoft Office Word Belgesi
Yazılım Tipi	Microsoft Office Word
Karakter Tipi	Unicode (UTF-8)
Karakter Sayısı	822
Uygulama Versiyonu	11,5606
Dosya Boyutu	24 kB
Toplam Değiştirme Süresi	18.0 dakika
Revizyon Numarası	12
Belge Oluşturma Tarihi	2010:07:23 12:20:00
Belge Değiştirme Tarihi	2010:07:26 06:05:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-08-01 20:35:12
FN Oluşturma Zamanı	2011-02-14 07:30:19.242128
Std Değiştirme Zamanı	2010-07-26 10:05:55
FN Değiştirme Zamanı	2011-02-14 07:30:19.242128

Std Erişim Zamanı	2010-08-01 21:34:50
FN Erişim Zamanı	2011-02-14 07:30:19.242128
Std Giriş Zamanı	2011-02-14 07:33:43.984529
FN Giriş Zamanı	2011-02-14 07:30:19.242128

Bu imajda tespit edilen “SY.doc” dosyasının üstverilerinde görülen aşağıdaki özelliklerin hep birlikte gerçekleşmesinin, normal kullanıcı davranışlarıyla zor olduğu değerlendirilmektedir. Bu özellikler:

- STD oluşturma ve erişim zamanlarının, FN zamanlarından geri olması ve mikro saniye kısımlarının 0 olması ve
- STD MFT kaydı değişim zamanının mikro saniye kısmının olması ve FN zamanlarından az ileri olmasıdır.

Dosya sistemi üstverilerindeki FN zamanlarının, STD oluşturma ve erişim zamanlarından ileri olması durumu, yedekleme sistemlerinde yedekleme aşamasında STD oluşturma ve erişim zamanlarının tutulmasının istenmesi ve yedekten dönülmesi sırasında yedekleme sistemi tarafından bu değerlerin ilk tutulan değerlere geri getirilmesi gibi durumlarda oluşabilir. Bunun yanında arşivleme programlarında da bu özellik bulunabilir. Örneğin en çok kullanılan dosya arşivleme programlarından biri olan “winrar” programında bu özellik mevcuttur(Store Creation Time, Store Last Access Time).“Winrar” programı kullanılarak yapılan testlerde FN zamanlarının, STD oluşturma zamanlarından daha güncel olabileceği görülmüştür. Aynı zamanda FN zamanlarının, STD oluşturma zamanlarından daha güncel olması farklı bir sürücüden taşıma ile gelen dosyalarda normal olan durumdur. Bunun yanında Winrar programı ile yapılan testlerde, STD oluşturma ve erişim zamanlarında mikro saniye kısmı olmaması durumu ile karşılaşılmıştır.

STD oluşturma ve erişim zamanlarında mikro saniye bilgisinin olmaması (sıfır olması) aslında işletim sistemi temel dosyalarında karşılaşılabilen bir durumdur. Fakat normal kullanıcı dosyalarında olma ihtimali düşüktür.

Bu özelliklerin hepsinin birlikte olmasını açıklayan diğer bir senaryo ise şöyledir:

- Dosya bu bilgisayara FN zamanlarında belirtilen “2011-02-14 07:30:19.242128” zamanında gelmiştir,
- Daha sonra Std MFT kaydı değişim zamanı olan “2011-02-14 07:33:43.984529” zamanında ise STD oluşturma, değiştirme ve erişim zamanları değiştirilmiştir.

Zaman değiştirme işlemi, yazılmış özel bir program ile ya da basit bir “visual basic script” ile olabilmektedir.

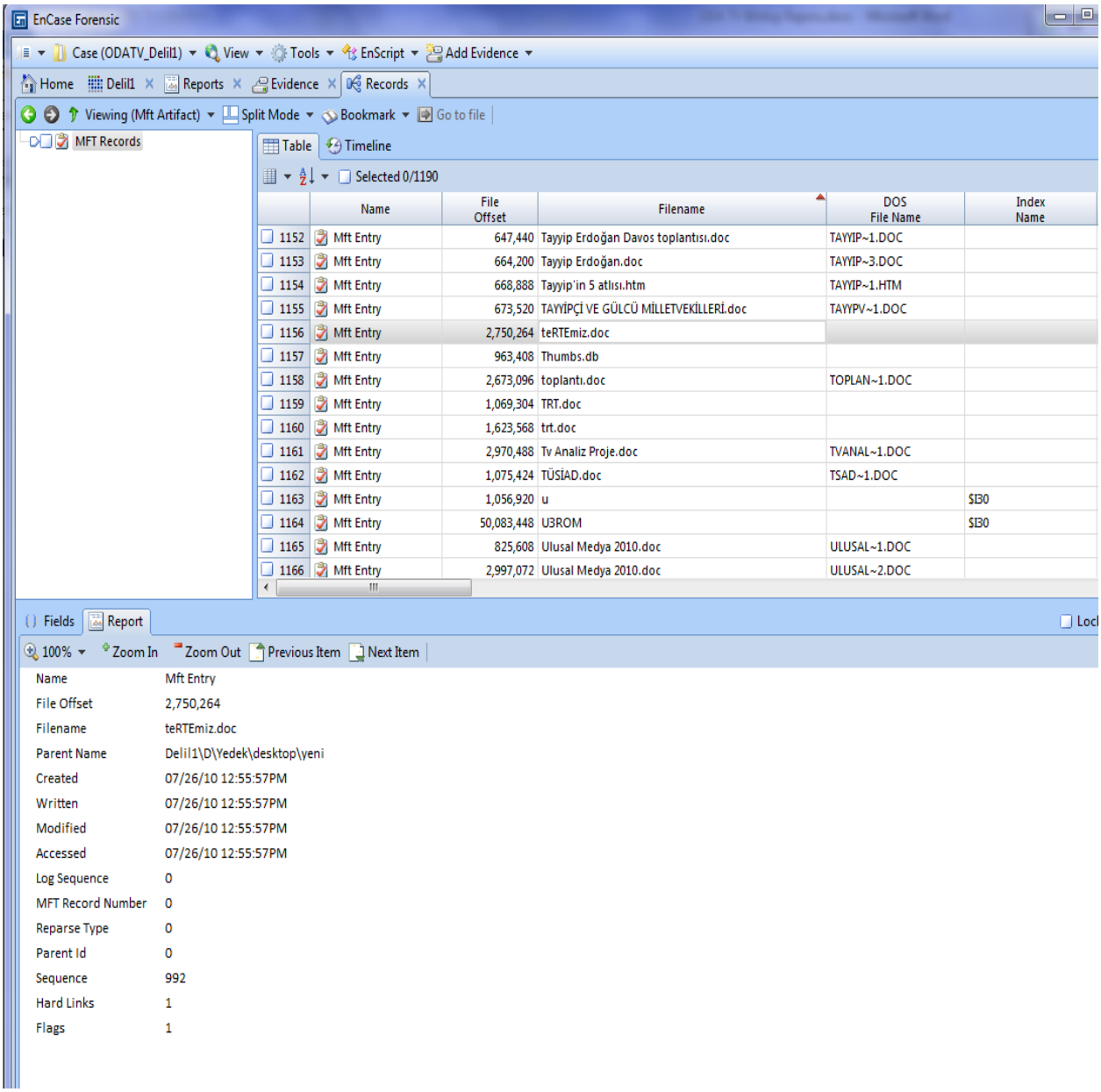
Sonuç olarak dosyadaki dosya sistemi üstverilerindeki bu uyuşmazlığın nasıl oluştuğu kesin olmamakla birlikte, yedekten dönme işlemi, RAR arşivleme ile arşiv açma işlemi ve zaman üstverilerinin sonradan değiştirilmiş olması işlemlerinden biri ile oluşmuş olabileceği değerlendirilmektedir. Bu işlemlerden gerçekleşmiş olmaya en yakın olanının, zaman üstverilerinin sonradan değiştirilmiş olması olduğu değerlendirilmektedir.

32.) teRTEemiz.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	teRTEemiz.doc
Dosya Konumu	\D\Yedek\desktop\yeni\teRTEmiz.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor
Yazar	Your User Name
Son Değiştiren Kullanıcı	soner
Yönetici	
Şirket	
Nesne Tipi	Microsoft Word Document
Yazılım Tipi	Microsoft Word 10.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	3438
Uygulama Versiyonu	10,2605
Dosya Boyutu	32 kB
Toplam Değiştirme Süresi	48.0 dakika
Revizyon Numarası	27
Belge Oluşturma Tarihi	2008:10:02 09:47:00
Belge Değiştirme Tarihi	2008:10:09 10:12:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-07-26 09:55:57.500000
FN Oluşturma Zamanı	2010-07-26 09:55:57.500000
Std Değiştirme Zamanı	2008-10-09 11:12:18
FN Değiştirme Zamanı	2010-07-26 09:55:57.500000
Std Erişim Zamanı	2010-07-26 09:55:57.546875
FN Erişim Zamanı	2010-07-26 09:55:57.500000
Std Giriş Zamanı	2010-07-26 09:55:57.546875
FN Giriş Zamanı	2010-07-26 09:55:57.500000

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (Index Artifact) kayıtlarında da rastlanılmıştır.



Şekil 84 - teRTEtemiz.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu diskte yapılan incelemelerde bu dosyaya dair LogFile kayıtlarına rastlanmıştır. İncelenen LogFile kayıtlarının zamanlarına bakarak bu dosyanın 23_08.rar adlı sıkıştırılmış dosyadan çıkartıldığı düşünülmektedir. Bu sıkıştırılmış dosyadan çıkarıldığı düşünülen 3 dosya

aşağıda görülmektedir. 23_08.rar dosyasından çıkarılan bu dosyalar yaklaşık 45 dk sonra 2 üst klasöre kopyalandığından ötürü ikinci defa LogFile kayıtlarının düştüğü düşünülmektedir.

Dosya Adı	Bulunduğu Dizin	Oluşturma Tarihi	Giriş Tarihi	Değiştirme Tarihi	Erişim Tarihi
23_08.rar	\D\BARIS YEDEK 11122009\DEKSTOP\DEPO	23.08.2010 23:06:51	23.08.2010 23:06:51	23.08.2010 23:06:51	23.08.2010 23:06:51
Bilinçlendirme.doc	\D\BARIS YEDEK 11122009\DEKSTOP\DEPO	23.08.2010 23:07:13	23.08.2010 23:07:13	23.08.2010 23:07:13	23.08.2010 23:07:13
Sn.Komutanım.doc	\D\BARIS YEDEK 11122009\DEKSTOP\DEPO	23.08.2010 23:07:14	23.08.2010 23:07:14	23.08.2010 23:07:14	23.08.2010 23:07:14
teRTEmiz.doc	**\D\BARIS YEDEK 11122009\DEKSTOP\DEPO**	**23.08.2010 23:07:14**	**23.08.2010 23:07:14**	**23.08.2010 23:07:14**	**23.08.2010 23:07:14**
Bilinçlendirme.doc	\D\BARIS YEDEK 11122009	23.08.2010 23:54:26	23.08.2010 23:54:26	23.08.2010 23:54:26	23.08.2010 23:54:26
Sn.Komutanim.doc	\D\BARIS YEDEK 11122009	23.08.2010 23:54:31	23.08.2010 23:54:31	23.08.2010 23:54:31	23.08.2010 23:54:31
teRTEmiz.doc	**\D\BARIS YEDEK 11122009**	**23.08.2010 23:54:37**	**23.08.2010 23:54:37**	**23.08.2010 23:54:37**	**23.08.2010 23:54:37**
Sn.Komutanim.doc	\D\BARIS YEDEK 11122009	23.08.2010 23:58:58	23.08.2010 23:58:58	23.08.2010 23:58:58	23.08.2010 23:58:58

Tablo 6 - 23_08.rar ve teRTEmiz.doc Dosyasının Logfile Kayıtları

Bununla beraber dosyanın kendisine ulaşılamamıştır. Dosyanın kendisinin bulunamayıp LogFile kayıtlarının tespit edilmesi, dosyanın silinmiş ve dosyanın bulunduğu disk alanının üzerine başka bir dosyanın verilerinin yazılmış olduğuna işaret etmektedir.

"teRTEemiz.doc" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Delil2 diskinde silinmiş ama $Logfile kaydı erişilebilir durumdadır. Delil2 de silinmiş ve bulunduğu disk alanının üzerine yazılmış görünmektedir. Delil2 de dosyanın kendisine ulaşılamadığından sadece dosya sistemi üstverilerine ulaşılmaktadır. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

• İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

• Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

• Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

• Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

• Delil2 deki $Logfile analizi sonrası bir RAR arşiv dosyasından çıkarıldıktan sonra çıkarıldığı dizinden başka bir dizine kopyalandığı görülmektedir.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

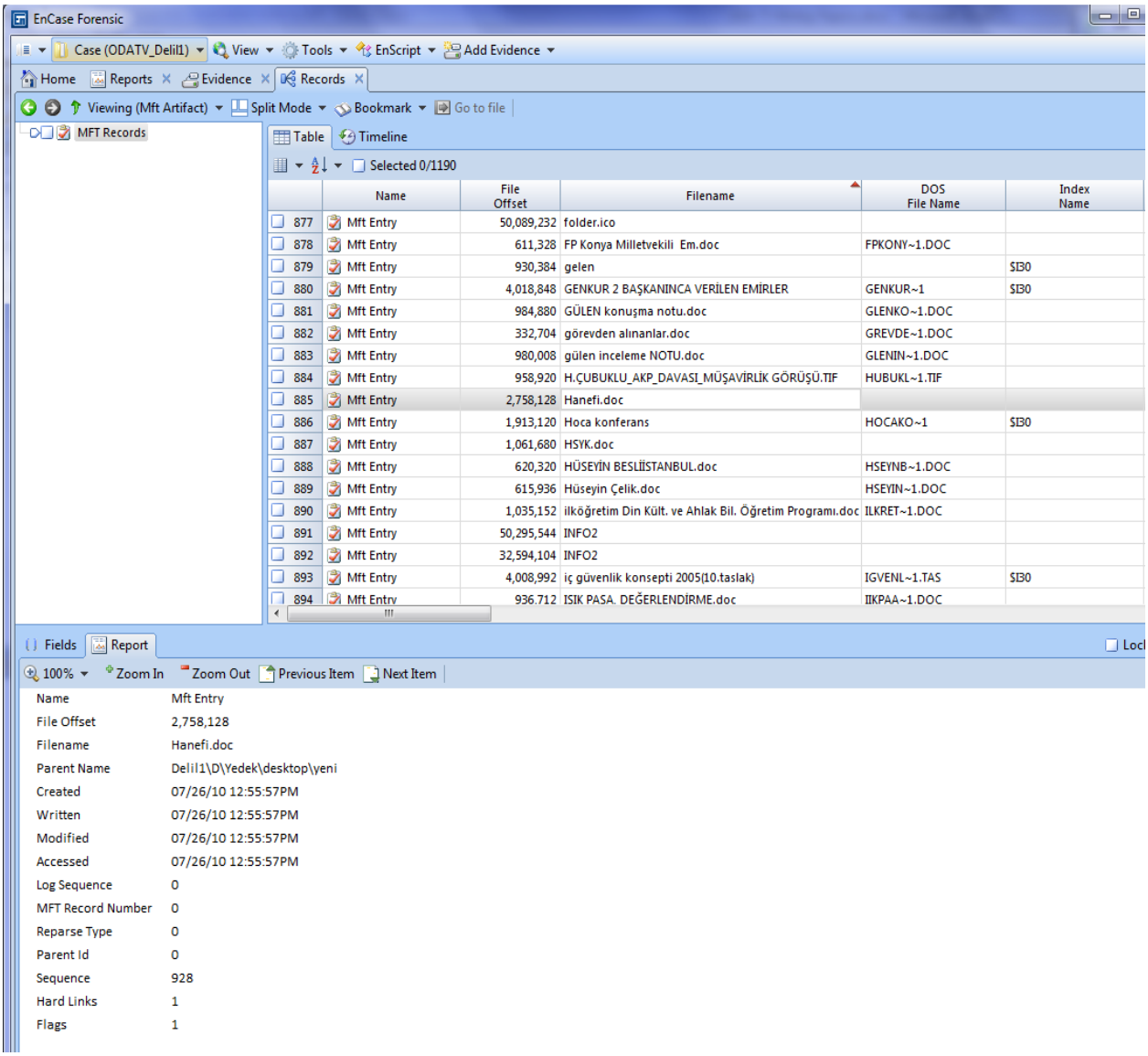
Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

33.) Hanefi.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	Hanefi.doc
Dosya Konumu	\D\Yedek\desktop\yeni\Hanefi.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor
Yazar	soner
Son Değiştiren Kullanıcı	soner
Yönetici	
Şirket	Conqueror
Nesne Tipi	Microsoft Word Document
Yazılım Tipi	Microsoft Word 10.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	1648
Uygulama Versiyonu	10,2605
Dosya Boyutu	28 kB
Toplam Değiştirme Süresi	11.0 dakika
Revizyon Numarası	10
Belge Oluşturma Tarihi	2010:07:12 07:06:00
Belge Değiştirme Tarihi	2010:07:12 07:17:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-07-26 09:55:57.546875
FN Oluşturma Zamanı	2010-07-26 09:55:57.546875
Std Değiştirme Zamanı	2010-07-12 09:17:48
FN Değiştirme Zamanı	2010-07-26 09:55:57.546875
Std Erişim Zamanı	2011-01-26 12:07:37.390625
FN Erişim Zamanı	2010-07-26 09:55:57.546875
Std Giriş Zamanı	2010-07-26 09:55:57.562498
FN Giriş Zamanı	2010-07-26 09:55:57.546875

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (MFT Artifact) kayıtlarında da rastlanılmıştır.



Şekil 85 - Hanefi.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

"Hanefi.doc" dokümanı Delil1 ve Delil3 disklerinde bulunmuştur ve her iki diskteki durumları da belge ve dosya sistemi üstverilerinin elde edilebilmesine sebep olmuştur. Delil1 diskinde dosya silinmiş olsa da gerş döndürülmüş ve $MFT kaydına ulaşılmış, Delil3 te de dosyanın aktif olduğu gözlenmiştir. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Delil1 için dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır. Sy.doc dosyası için yapılan açıklamada olduğu gibi burada da STD erişim

zamanı STD giriş zamanından daha ileridir ki bu her dosya erişimi sırasında STD giriş zamanının güncellenme zorunluluğu olmaması ilkesiyle anlatılmıştı.

• Delil3 için olan zaman anormalliklerinin sonradan bir zaman değiştirme programı kullanılması ile oluşmuş olabileceği değerlendirilmektedir.

• Her iki delil diski için dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

• Her iki delil diski için işletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

• Her iki delil diski için dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

• Delil1 için dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Belge Üstverileri	
Dosya Adı	Hanefi.doc
Dosya Konumu	\C\Users\user\Documents\Hanefi.doc
Dosya Durumu	Aktif
Yazar	Soner
Son Değiştiren Kullanıcı	Soner
Yönetici	
Şirket	Conqueror
Nesne Tipi	Microsoft Word Document
Yazılım Tipi	Microsoft Word 10.0
Karakter Tipi	Windows Turkish

Karakter Sayısı	1648
Uygulama Versiyonu	10,2605
Dosya Boyutu	28 kB
Toplam Değiştirme Süresi	11.0 dakika
Revizyon Numarası	10
Belge Oluşturma Tarihi	2010:07:12 07:06:00
Belge Değiştirme Tarihi	2010:07:12 07:17:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-08-17 12:51:12
FN Oluşturma Zamanı	2011-02-14 07:30:27.790930
Std Değiştirme Zamanı	2010-07-12 11:17:55
FN Değiştirme Zamanı	2011-02-14 07:30:27.790930
Std Erişim Zamanı	2010-08-17 14:22:55
FN Erişim Zamanı	2011-02-14 07:30:27.790930
Std Giriş Zamanı	2011-02-14 18:36:29.888729
FN Giriş Zamanı	2011-02-14 07:30:27.790930

Bu imajda tespit edilen “Hanefi.doc” dosyasının üstverilerinde görülen aşağıdaki özelliklerin hep birlikte gerçekleşmesinin, normal kullanıcı davranışlarıyla zor olduğu değerlendirilmektedir. Bu özellikler:

- STD oluşturma ve erişim zamanlarının, FN zamanlarından geri olması ve mikro saniye kısımlarının 0 olması ve
- STD MFT kaydı değişim zamanının mikro saniye kısmının olması ve FN zamanlarından az ileri olmasıdır.

Dosya sistemi üstverilerindeki FN zamanlarının, STD oluşturma ve erişim zamanlarından ileri olması durumu, yedekleme sistemlerinde yedekleme aşamasında STD oluşturma ve erişim zamanlarının tutulmasının istenmesi ve yedekten dönülmesi sırasında yedekleme sistemi tarafından bu değerlerin ilk tutulan değerlere geri getirilmesi gibi durumlarda oluşabilir. Bunun yanında arşivleme programlarında da bu özellik bulunabilir. Örneğin en çok kullanılan dosya arşivleme programlarından biri olan “winrar” programında bu özellik mevcuttur(Store Creation Time, Store Last Access Time).“Winrar” programı kullanılarak yapılan testlerde FN zamanlarının, STD oluşturma zamanlarından daha güncel olabileceği görülmüştür. Aynı zamanda FN zamanlarının, STD oluşturma zamanlarından daha güncel olması farklı bir sürücüden taşıma ile gelen dosyalarda normal olan durumdur. Bunun yanında Winrar programı ile yapılan testlerde, STD oluşturma ve erişim zamanlarında mikro saniye kısmı olmaması durumu ile karşılaşılmıştır.

STD oluşturma ve erişim zamanlarında mikro saniye bilgisinin olmaması (sıfır olması) aslında işletim sistemi temel dosyalarında karşılaşılabilen bir durumdur. Fakat normal kullanıcı dosyalarında olma ihtimali düşüktür.

Bu özelliklerin hepsinin birlikte olmasını açıklayan diğer bir senaryo ise şöyledir:

- Dosya bu bilgisayara FN zamanlarında belirtilen "2011-02-14 07:30:27.790930" zamanında gelmiştir,
- Daha sonra Std MFT kaydı değişim zamanı olan "2011-02-14 18:36:29.888729" zamanında ise STD oluşturma, değiştirme ve erişim zamanları değiştirilmiştir.

Zaman değiştirme işlemi, yazılmış özel bir program ile ya da basit bir "visual basic script" ile olabilmektedir.

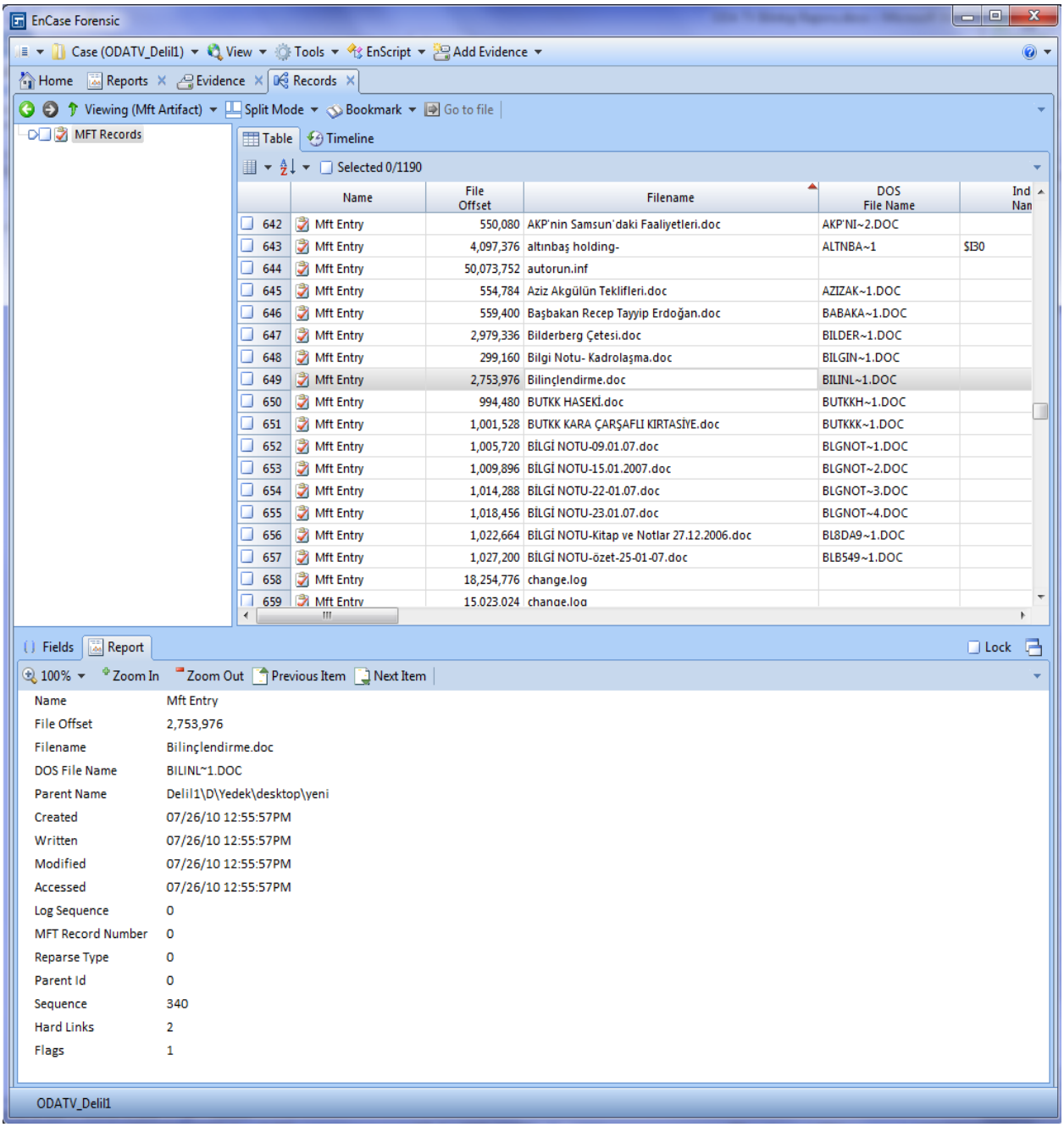
Sonuç olarak dosyadaki dosya sistemi üstverilerindeki bu uyuşmazlığın nasıl oluştuğu kesin olmamakla birlikte, yedekten dönme işlemi, RAR arşivleme ile arşiv açma işlemi ve zaman üstverilerinin sonradan değiştirilmiş olması işlemlerinden biri ile oluşmuş olabileceği değerlendirilmektedir. Bu işlemlerden gerçekleşmiş olmaya en yakın olanının, zaman üstverilerinin sonradan değiştirilmiş olması olduğu değerlendirilmektedir.

34.) Bilinçlendirme.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	Bilinçlendirme.doc
Dosya Konumu	\D\Yedek\desktop\yeni\Bilinçlendirme.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor
Yazar	USER
Son Değiştiren Kullanıcı	soner
Yönetici	
Şirket	
Nesne Tipi	Microsoft Word Document
Yazılım Tipi	Microsoft Word 10.0
Karakter Tipi	Windows Turkish
Karakter Sayısı	6912
Uygulama Versiyonu	10,2605
Dosya Boyutu	40 kB
Toplam Değiştirme Süresi	1.4 saat
Revizyon Numarası	16
Belge Oluşturma Tarihi	2010:03:03 17:56:00
Belge Değiştirme Tarihi	2010:03:24 23:15:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-07-26 09:55:57.546875
FN Oluşturma Zamanı	2010-07-26 09:55:57.546875
Std Değiştirme Zamanı	2010-03-24 23:15:04
FN Değiştirme Zamanı	2010-07-26 09:55:57.546875
Std Erişim Zamanı	2010-07-26 09:55:57.546875
FN Erişim Zamanı	2010-07-26 09:55:57.546875
Std Giriş Zamanı	2010-07-26 09:55:57.546875
FN Giriş Zamanı	2010-07-26 09:55:57.546875

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (MFT Artifact) kayıtlarında da rastlanılmıştır.



Şekil 86 - Bilinçlendirme.doc Dosyasının Logfile Kayıtları

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu diskte yapılan incelemelerde bu dosyaya dair LogFile kayıtlarına rastlanmıştır. İncelenen LogFile kayıtlarının zamanlarına bakarak bu dosyanın 23_08.rar adlı sıkıştırılmış dosyadan

çıkartıldığı düşünülmektedir. Bu sıkıştırılmış dosyadan çıkarıldığını düşünülen 3 dosya aşağıda görülmektedir. 23_08.rar dosyasından çıkarılan bu dosyalar yaklaşık 45 dk sonra 2 üst klasöre kopyalandığından ötürü ikinci defa LogFile kayıtlarının düştüğü düşünülmektedir.

Dosya Adı	Bulunduğu Dizin	Oluşturma Tarihi	Giriş Tarihi	Değiştirme Tarihi	Erişim Tarihi
23_08.rar	\D\BARIS YEDEK 11122009\DEKSTOP\DEPO	23.08.2010 23:06:51	23.08.2010 23:06:51	23.08.2010 23:06:51	23.08.2010 23:06:51
Bilinçlendirme.doc	**\D\BARIS YEDEK 11122009\DEKSTOP\DEPO**	**23.08.2010 23:07:13**	**23.08.2010 23:07:13**	**23.08.2010 23:07:13**	**23.08.2010 23:07:13**
Sn.Komutanım.doc	\D\BARIS YEDEK 11122009\DEKSTOP\DEPO	23.08.2010 23:07:14	23.08.2010 23:07:14	23.08.2010 23:07:14	23.08.2010 23:07:14
teRTEmiz.doc	\D\BARIS YEDEK 11122009\DEKSTOP\DEPO	23.08.2010 23:07:14	23.08.2010 23:07:14	23.08.2010 23:07:14	23.08.2010 23:07:14
Bilinçlendirme.doc	**\D\BARIS YEDEK 11122009**	**23.08.2010 23:54:26**	**23.08.2010 23:54:26**	**23.08.2010 23:54:26**	**23.08.2010 23:54:26**
Sn.Komutanim.doc	\D\BARIS YEDEK 11122009	23.08.2010 23:54:31	23.08.2010 23:54:31	23.08.2010 23:54:31	23.08.2010 23:54:31
teRTEmiz.doc	\D\BARIS YEDEK 11122009	23.08.2010 23:54:37	23.08.2010 23:54:37	23.08.2010 23:54:37	23.08.2010 23:54:37
Sn.Komutanim.doc	\D\BARIS YEDEK 11122009	23.08.2010 23:58:58	23.08.2010 23:58:58	23.08.2010 23:58:58	23.08.2010 23:58:58

Tablo 7 - 23_08.rar ve Bilinçlendirme.doc Dosyasına ait Logfile Kaydı

Bununla beraber dosyanın kendisine ulaşılamamıştır. Dosyanın kendisinin bulunamayıp LogFile kayıtlarının tespit edilmesi, dosyanın silinmiş ve dosyanın bulunduğu disk alanının üzerine başka bir dosyanın verilerinin yazılmış olduğuna işaret etmektedir.

- "Bilinçlendirme.doc" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Delil2 diskinde silinmiş ama $Logfile kaydı erişilebilir durumdadır. Delil2 de silinmiş ve bulunduğu disk alanının üzerine yazılmış görünmektedir. Delil2 de dosyanın kendisine ulaşılamadığından sadece dosya sistemi üstverilerine ulaşılmaktadır. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:
- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

- İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.
- Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.
- Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.
- Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.
- Delil2 deki $Logfile analizi sonrası bir RAR arşiv dosyasından çıkarıldıktan sonra çıkarıldığı dizinden başka bir dizine kopyalandığı görülmektedir.
- Delil1 deki zaman verileri incelendiğinde de dosya üzerindeki son işlemin bir kopyalama işlemi olabileceği değerlendirilmektedir (dosyanın STD değiştirme hariç bütün zamanlarının aynı olmasından dolayı).

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

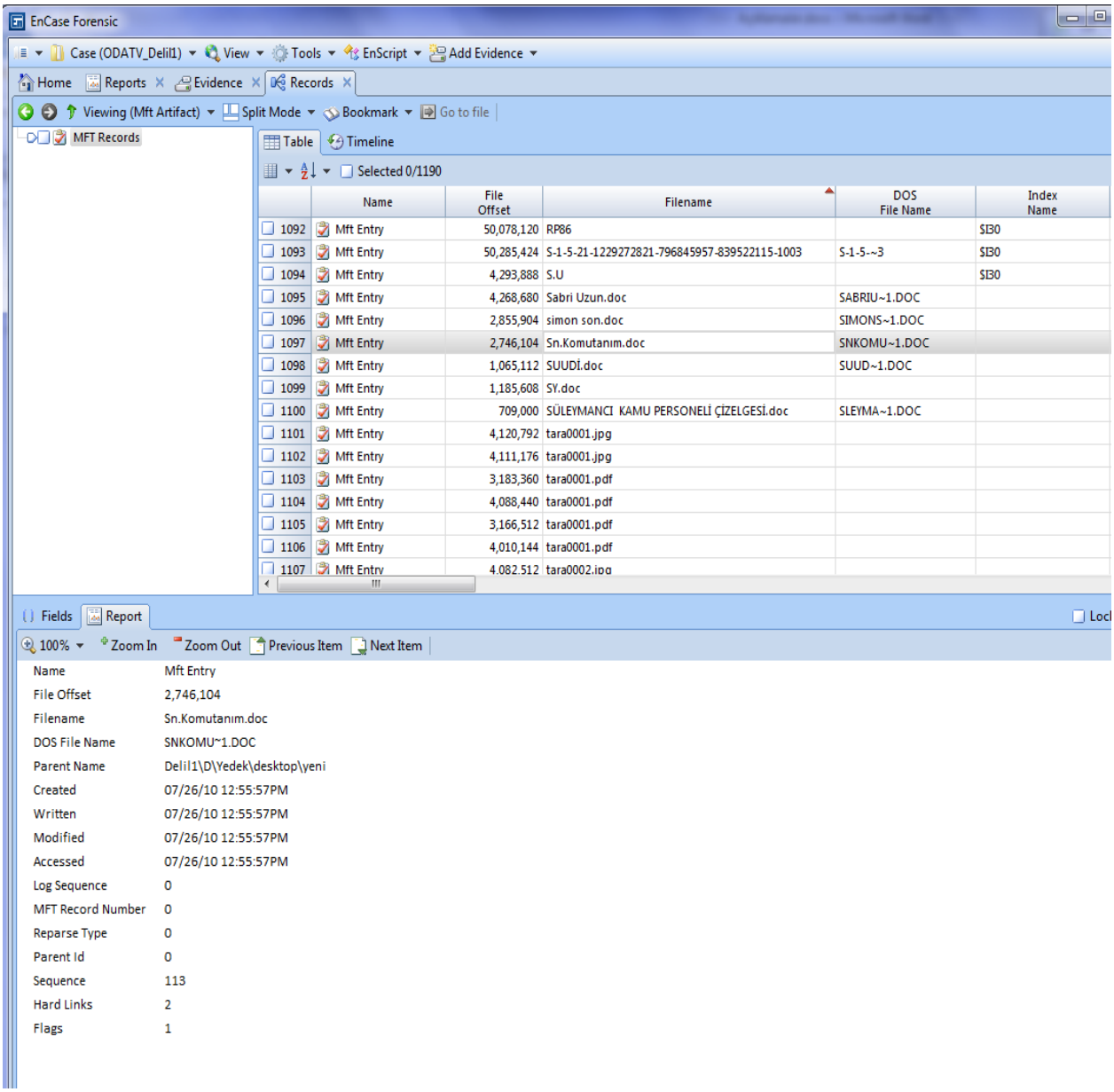
Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

35.) Sn. Komutanım.doc

ST3120927AS_4MS1TF89 Seri Numaralı ODATV imajı verileri

Belge Üstverileri	
Dosya Adı	Sn. Komutanım.doc
Dosya Konumu	\D\Yedek\desktop\yeni\Sn.Komutanim.doc
Dosya Durumu	Silinmiş, $MFT kaydı var, unallocated clusterda bulunuyor
Yazar	pc
Son Değiştiren Kullanıcı	pc
Yönetici	
Şirket	
Nesne Tipi	Microsoft Office Word Belgesi
Yazılım Tipi	Microsoft Office Word
Karakter Tipi	Unicode (UTF-8)
Karakter Sayısı	4796
Uygulama Versiyonu	11,5606
Dosya Boyutu	32 kB
Toplam Değiştirme Süresi	1.3 saat
Revizyon Numarası	44
Belge Oluşturma Tarihi	2010:07:01 12:03:00
Belge Değiştirme Tarihi	2010:07:01 13:19:00
Dosya Sistemi Tarih Üstverileri	
Std Oluşturma Zamanı	2010-07-26 09:55:57.500000
FN Oluşturma Zamanı	2010-07-26 09:55:57.500000
Std Değiştirme Zamanı	2010-07-01 14:19:34
FN Değiştirme Zamanı	2010-07-26 09:55:57.500000
Std Erişim Zamanı	2010-12-24 11:08:23.281248
FN Erişim Zamanı	2010-07-26 09:55:57.500000
Std Giriş Zamanı	2010-07-26 09:55:57.500000
FN Giriş Zamanı	2010-07-26 09:55:57.500000

Dosyanın kendisi tespit edildiği gibi, bu dosyaya $LogFile (Index Artifact) kayıtlarında da rastlanılmıştır.



Şekil 87 - Sn.Komutanım.doc Dosyasına Ait Logfile (MFT Artifact) Kaydı

$Logfile'da kaydının olması bu dosya ismine ait bir dosyanın $MFT kaydının oluşturulduğuna veya var olan MFT kaydının değiştirildiğine işaret eder.

MHV2060BH_NW18T6229459 Seri Numaralı Barış PEHLİVAN imajı verileri

Bu diskte yapılan incelemelerde bu dosyaya dair LogFile kayıtlarına rastlanmıştır. İncelenen LogFile kayıtlarının zamanlarına bakarak bu dosyanın 23_08.rar adlı sıkıştırılmış dosyadan çıkartıldığı düşünülmektedir. Bu sıkıştırılmış dosyadan çıkarıldığını düşünülen 3 dosya

aşağıda görülmektedir. 23_08.rar dosyasından çıkarılan bu dosyalar yaklaşık 45 dk sonra 2 üst klasöre kopyalandığından ötürü ikinci defa LogFile kayıtlarının düştüğü düşünülmektedir.

Dosya Adı	Bulunduğu Dizin	Oluşturma Tarihi	Giriş Tarihi	Değiştirme Tarihi	Erişim Tarihi
23_08.rar	\D\BARIS YEDEK 11122009\DEKSTOP\DEPO	23.08.2010 23:06:51	23.08.2010 23:06:51	23.08.2010 23:06:51	23.08.2010 23:06:51
Bilinçlendirme.doc	\D\BARIS YEDEK 11122009\DEKSTOP\DEPO	23.08.2010 23:07:13	23.08.2010 23:07:13	23.08.2010 23:07:13	23.08.2010 23:07:13
Sn.Komutanım.doc	**\D\BARIS YEDEK 11122009\DEKSTOP\DEPO**	**23.08.2010 23:07:14**	**23.08.2010 23:07:14**	**23.08.2010 23:07:14**	**23.08.2010 23:07:14**
teRTEmiz.doc	\D\BARIS YEDEK 11122009\DEKSTOP\DEPO	23.08.2010 23:07:14	23.08.2010 23:07:14	23.08.2010 23:07:14	23.08.2010 23:07:14
Bilinçlendirme.doc	\D\BARIS YEDEK 11122009	23.08.2010 23:54:26	23.08.2010 23:54:26	23.08.2010 23:54:26	23.08.2010 23:54:26
Sn.Komutanım.doc	**\D\BARIS YEDEK 11122009**	**23.08.2010 23:54:31**	**23.08.2010 23:54:31**	**23.08.2010 23:54:31**	**23.08.2010 23:54:31**
teRTEmiz.doc	\D\BARIS YEDEK 11122009	23.08.2010 23:54:37	23.08.2010 23:54:37	23.08.2010 23:54:37	23.08.2010 23:54:37
Sn.Komutanim.doc	**\D\BARIS YEDEK 11122009**	**23.08.2010 23:58:58**	**23.08.2010 23:58:58**	**23.08.2010 23:58:58**	**23.08.2010 23:58:58**

Şekil 88 - 23_08.rar ve Sn. Komutanım.doc Dosyasına ait Logfile Kaydı

Bununla beraber dosyanın kendisine ulaşılamamıştır. Dosyanın kendisinin bulunamayıp LogFile kayıtlarının tespit edilmesi, dosyanın silinmiş ve dosyanın bulunduğu disk alanının üzerine başka bir dosyanın verilerinin yazılmış olduğuna işaret etmektedir.

"Sn. Komutanım.doc" dokümanı Delil1 diskinde silinmiş ama kurtarılabilir durumda bulunmaktadır. $MFT kaydından bu dosya ile alakalı dosya sistemi bilgilerine ulaşılabilmektedir. Delil2 diskinde silinmiş ama $Logfile kaydı erişilebilir durumdadır. Delil2 de silinmiş ve bulunduğu disk alanının üzerine yazılmış görünmektedir. Delil2 de dosyanın kendisine ulaşılamadığından sadece dosya sistemi üstverilerine ulaşılmaktadır. Bu dosya ile ilgili üstveriler üzerinde incelemelerde bulunulmuş ve şu sonuçlara ulaşılmıştır:

- Dosya sistemi ve belge üstverilerinde herhangi bir uyumsuzluğa rastlanmamıştır.
- Dosyanın belge üstverilerinin incelenmesi sonucu, dosyanın ilgili bilgisayar kullanıcısı tarafından oluşturulmadığı veya değiştirilmediği değerlendirilmektedir.

• İşletim sistemi izlerinin incelenmesi sonucunda dosyanın kullanıcı tarafından açıldığına dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın kullanıcı tarafından kesin olarak açılmadığı anlamına gelmemektedir.

• Dosyanın zararlı bir yazılım tarafından gönderildiğine veya değiştirildiğine dair bir bulguya rastlanmamıştır. Bu tür bir bulgunun bulunmamış olması bu dosyanın zararlı bir yazılım tarafından kesin olarak gönderilmemiş veya değiştirilmemiş olduğu anlamına gelmemektedir.

• Dosyanın dosya sistemi üstverilerine bakıldığında STD değiştirme zamanının milisaniye değerinin sıfır olduğu görülmüştür. Bu sebeple dosyanın, dosya sistemi zaman bilgilerinde milisaniyeleri tutmayan bir bölüm ya da diskten (FAT ya da ISO9660 -CD dosya sistemi- gibi) buraya aktarıldığı veya bu tür bir dosya sisteminde oluşturulmuş bir arşiv dosyasından (RAR, ZIP, …) çıkarılmış olduğu düşünülmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

• Dosya için dosya sistemi üstverilerinden olan STD değiştirme zamanının STD oluşturma zamanından eski olması ve FN alanındaki bütün zamanların da STD dosya oluşturma zamanı ile aynı olması, bu dosyanın başka bir bölüm ya da diskten buraya kopyalandığına ya da bir arşivden (RAR, ZIP, ...) çıkarıldığına işaret etmektedir. Delil2 için yapılan $Logfile analizinden bu dosyanın RAR arşivinden çıkarılmış olduğu düşünülmektedir.

• Delil2 deki $Logfile analizi sonrası bir RAR arşiv dosyasından çıkarıldıktan sonra çıkarıldığı dizinden başka bir dizine kopyalandığı görülmektedir.

• Delil1 deki zaman verileri incelendiğinde de dosya üzerindeki son işlemin bir kopyalama sonrası erişim işlemi olabileceği değerlendirilmektedir (dosyanın STD değiştirme ve STD erişim hariç bütün zamanlarının aynı olması ve STD erişim tarihinin en yeni olmasından dolayı).

S17HJ90Q816726 Seri Numaralı Müyesser Yıldız Uğur imajı verileri

Bu dosyanın bu disk imajında bulunduğuna dair bir delile rastlanmamıştır.

Soru 6.)

Ek-1 listede belirtilen hard disk imajının kullanıcı bilgileri, sistem bilgileri ve güvenlik önlemlerinin neler olduğunun açıklanması?

Cevap 6.)

Müzekkere ekinde teslim edilen imajlara ait kullanıcı ve sistem bilgileri alttaki gibidir.

ST3120927AS_4MS1TF89 Seri Numaralı Disk

Genel Bilgiler

İmajın Bulunduğu Hard Diskin Adı	ODATV
İmaj Seri No	ST3120927AS_4MS1TF89
İmaj Hash Değeri (MD5)	5d533c43c70eccd368539c5107c63439
İşletim Sistemi	Microsoft Windows XP
İşlemci Mimarisi	x86
Kayıtlı Kullanıcı (Registered User)	Sys
Bilgisayar Adı	BARIS_DESKTOP
Çalışma Grubu Adı	INFOR
Kullanıcı Hesapları (User Accounts)	Administrator,Guest,Türker
Aynı Ağda Bulunan Diğer Bilgisayarların İsimleri	CAN,ENGIN,INGEST,ODA1,PLAYBOXU,SALİH,CİHAN,EXPER,PRINT,SEKRETERYA,SONERYALCIN,DIDEM,GRAFİK,HUSEYİN,MUNİRE,ODATV5,NEWYORK,DUYGU,HAKAN-PC
Kablolu İnternet Arayüzü	Marvell Yukon 88E8053 PCI-E Gigabit Ethernet Controller
Saat Dilimi	GTB (Yunanistan, Türkiye, Belarus)

Tablo 8 - ST3120927AS_4MS1TF89 İmajına Ait Genel Bilgiler

Güvenlik Önlemleri

ST3120827AS_4MS1TF89 seri nolu hard disk imajında Windows XP işletim sisteminin en son 10.02.2011 tarihinde güncelleştirme işlemini gerçekleştirdiği tespit edilmiştir. Tüm güncelleme dosyalarının listesi Ek-1'de mevcuttur.

ST3120827AS_4MS1TF89 seri nolu hard disk imajında "ESET NOD32 Antivirüs 4" isimli antivirüs uygulamasının çalıştığı ve Windows güvenlik duvarının aktif olduğu, Antivirüs programının en son 03.12.2010 tarihinde güncellendiği tespit edilmiştir.

MHV2060BH_NW18T6229459 Seri Numaralı Disk

Genel Bilgiler

İmajın Bulunduğu Hard Diskin Adı	Barış PEHLİVAN
İmaj Seri No	MHV2060BH_NW18T6229459
İmaj Hash Değeri (MD5)	58F0C95FF0C794B1BEBA41D5930C3C
İşletim Sistemi	Microsoft Windows XP
İşlemci Mimarisi	x86
Kayıtlı Kullanıcı (Registered User)	TOSHIBA
Bilgisayar Adı	satellit-9bb883
Çalışma Grubu Adı	WORKGROUP
Kullanıcı Hesapları (User Accounts)	Administrator,Guest,Barış
Aynı Ağda Bulunan Diğer Bilgisayarların İsimleri	SALİH
Kablolu İnternet Arayüzü	Realtek RTL8139 Family PCI Fast Ethernet NIC
Kablosuz İnternet Arayüzü	Atheros AR5005G Wireless Network Adapter
Saat Dilimi	GTB (Yunanistan, Türkiye, Belarus)

Tablo 9 - MHV2060BH_NW18T6229459 İmajına Ait Genel Bilgiler

Güvenlik Önlemleri

FUJITSU_MHV2060BH_NW18T6229459 seri nolu hard disk imajında Windows XP işletim sisteminin hiç güncelleştirme işlemi gerçekleştirmediği tespit edilmiştir. İşletim sistemine "service pack" yüklenmesi işlemi kurulum sırasında yani 11.12.2009 tarihinde gerçekleştirildiği görülmüş olup tüm güncelleme listesi Ek-2'de mevcuttur.

FUJITSU_MHV2060BH_NW18T6229459 seri nolu hard disk imajında "ESET NOD32 Antivirüs Xpista Edition" isimli antivirüs uygulamasının çalıştığı fakat Windows güvenlik duvarının aktif olmadığı tespit edilmiştir. Antivirüs programında otomatik güncellemenin en son 20.10.2010 tarihinde başarılı olmasına karşın kullanıcı tarafından virüs veritabanı bilgisinin 12.02.2011 tarihli versiyonuna güncellendiği tespit edilmiştir.

S17HJ90Q816726 Seri Numaralı Disk

Genel Bilgiler

İmajın Bulunduğu Hard Diskin Adı	Müyesser Yıldız Uğur
İmaj Seri No	S17HJ90Q816726
İmaj Hash Değeri (MD5)	a71117720107bb18cef5f3f0d7c8cd97
İşletim Sistemi	Windows Vista (TM) Home Premium
İşlemci Mimarisi	x86
Bilgisayar Adı	user-PC
Çalışma Grubu Adı	WORKGROUP
Kayıtlı Kullanıcı (Registered User)	user
Kullanıcı Hesapları (User Accounts)	Administrator,Guest,admin,user
Kablolu İnternet Arayüzü	Realtek RTL8168B/8111B Family PCI-E Gigabit Ethernet NIC
Kablosuz İnternet Arayüzü	-
Saat Dilimi	GTB (Yunanistan, Türkiye, Belarus)

Tablo 10 - S17HJ90Q816726 İmajına Ait Genel Bilgiler

Bu imajda yapılan incelemelerde, ilgili bilgisayarda **İlim** isimli yetkili bir kullanıcının da işlem yaptığı tespit edilmiştir. ilimugur@gmail.com e-posta adresiyle işlem yapan bu kullanıcının, bilgisayarlar ve zararlı yazılımlar konusunda bilgi sahibi olduğu düşünülmektedir. Aynı kullanıcının bu imajda bir takım zararlı yazılımlar oluşturduğu tespit edilmiştir.

EK-8'de ayrıntısı bulunan *C:\Users\user\yedek 04.01.2006.rar » RAR » yedek 04.01.2006\masa □st□ yedek\ilimin yeri\ilim nasıl biri.exe* kaydı konuyla ilgili örnek olarak incelenebilir.

Güvenlik Önlemleri

SAMSUNG_HD252HJ_S17HJ90Q816726 seri nolu hard disk imajında Windows Vista işletim sisteminin en son 01.03.2011 tarihinde güncelleştirme işlemini gerçekleştirdiği tespit edilmiştir. Tüm güncelleme dosyalarının listesi Ek-3'de mevcuttur.

SAMSUNG_HD252HJ_S17HJ90Q816726 seri nolu hard disk imajında "ESET Smart Security 4" isimli antivirüs uygulamasının çalıştığı, Windows güvenlik duvarının aktif olduğu, kötücül yazılımlara karşı "Malwarebytes Anti-Malware" uygulamasının çalıştığı, Ayrıca Windows işletim sistemi içerisinde gelen "Windows Defender" ve "Windows Kötü amaçlı yazılımları temizleme aracı" uygulamalarının aktif olarak çalıştığı tespit edilmiştir. Antivirüs programının en son 28.08.2010 tarihinde, Anti-Malware uygulamasının en son 30.12.2009

tarihinde, Windows Defender Uygulamasının en son 01.03.2011 tarihinde ve Windows kötü amaçlı yazılımları temizleme aracı uygulamasının en son 11.02.2011 tarihinde güncellendiği tespit edilmiştir.

Ortak kullanılan taşınabilir cihazlar

Gerçekleştirilen analiz ve incelemeler sonucunda ortaya çıkarılan taşınabilir bellek verileri yorumlandığında, ST3120927AS_4MS1TF89 seri numaralı *ODATV* imajı ile MHV2060BH_NW18T6229459 seri numaralı *Barış PEHLİVAN* imajı arasında ortak kullanılan USB taşınabilir bellekler olduğu anlaşılmaktadır.

Delil Seri No	Üretici	USB Seri Numarası	Ürün Açıklaması	USB Son Yazım Tarihi
ST3120927AS_4MS1TF89	Seagate	2GH2080R____&0	Seagate Portable USB Device	10/12/10 09:56:27AM
MHV2060BH_NW18T6229459	Seagate	2GH2080R____&0	Seagate Portable USB Device	01/30/11 09:34:10PM
ST3120927AS_4MS1TF89	ZTE	P673A4AVED010000&0	ZTE USB SCSI CD-ROM USB Device	10/12/10 09:56:27AM
MHV2060BH_NW18T6229459	ZTE	P673A4AVED010000&0	ZTE USB SCSI CD-ROM USB Device	08/01/10 12:59:24AM

Tablo 11 - Ortak USB Cihazları

Yukardaki tabloda seri numaraları aynı olan 2 farklı USB aygıtı için, ST3120927AS_4MS1TF89 ve MHV2060BH_NW18T6229459 imajlarına ait kayıtlar görünmektedir.

Soru 7.)

Hard disk imajının hangi bilgisayara veya kullanıcıya ait olduğu konusunda değerlendirmede bulunulup bulunulamayacağı?

Cevap 7.)

Bir hard disk imajının hangi bilgisayara ait olduğu konusunda değerlendirme yapmak için çeşitli yöntemler kullanılabilir. Bunlardan bir tanesi, imajı alınan hard diskin incelenmesiyle elde edilecek olan işletim sistemi, ana kart, ekran kartı vb. donanımsal aygıtların seri numaları gibi ayırt edici verilerle, bilgisayarda bulunan bu donanımsal aygıtların seri numaralarının karşılaştırılması olabilir. Hard disklerin hangi bilgisayardan elde edildiğinin tespiti için farklı yöntemler de kullanılabilir. Hard disklerde saklanan çeşitli metadata (üstveri) verileri arasında, o bilgisayarda bulunan her türlü donanımsal aygıt için çeşitli sürücüler ve ayırt edici bilgiler bulunmaktadır.

Örnek vermek gerekirse; hard disk imajından elde edilecek registry kayıtları arasında hardware (donanım) başlığı altında çeşitli bilgiler bulunmaktadır. *DeviceArtifactClass* sınıfı içindeki verilerde bu gibi çok sayıda donanım verisi bulunmaktadır.

Dava kapsamında teslim edilen imajlarda, ST3120927AS_4MS1TF89 seri numaralı disk için 1238, MHV2060BH_NW18T6229459 seri numaralı disk için 775**,** S17HJ90Q816726 seri numaralı disk için 706 farklı, yukarıda açıklanan şekilde donanımsal kayıt bulunmuştur. Bu verilerin içinde seri numaraları da bulunmaktadır. Bu verilerin imajı alınan bilgisayardaki donanımlarla tutarlılığı bu bağlamda fikir verebilir.

Hard disk imajlarının hangi kullanıcıya ait olduğu konusunda ise farklı verilerden faydanılabilir. Bu yöntemlerle ilgili detaylı açıklamalar, müzekkeredeki 3. ve 4. soruların cevaplarında bulunmaktadır. Kısaca özetlemek gerekirse; hard diskin elde edildiği bilgisayarın kullanıcısı olduğu düşünülen kişiler için, hard diskten elde edilen her türlü veri, internet ve e-posta kayıtları, çeşitli notlar, adres ve telefonlar vb. kişisel verilerin analizi yöntemi kullanılabilir.

Delillere el konulması ve bize iletilmesi sırasında dijital adli analiz imajı alma kurallarına uyulduğu için imajların tutanaklarda bahsi geçen bilgisayarlara ait olduğu konusunda herhangi bir şüphe bulunmamaktadır. İnceleme sonucu elde edilen ve incelenen dijital delillerde tespit edilen bilgiler aşağıda sıralanmıştır.

ST3120927AS_4MS1TF89 Seri Numaralı Disk

Odatv kullanıcı ismiyle açılan bilgisayarda, barisp@odatv.com, sonery@odatv.com, barist@odatv.com e-posta hesaplarıyla işlem yapıldığı, aynı bilgisayarda kaydı görülen Türker ile Barış isimli 2 farklı hesap daha olduğu ve 153692070 kullanıcı numarasıyla Teamviewer uzaktan bağlantı ve yönetim programının kullanıldığı tespit edilmiştir.

İlgili imaja ait diğer sistemsel bilgiler 6. Sorunun cevabında verilmiştir.

MHV2060BH_NW18T6229459 Seri Numaralı Disk

Barış kullanıcı ismiyle açılan bilgisayarda sabiumicya@yahoo.com ve barisalim@hotmail.com e-posta hesaplarıyla işlem yapıldığı, **Barislifeline** kullanıcı adıyla Skype anlık mesajlaşma programı kullanıldığı ve 717570224 kullanıcı numarasıyla Teamviewer uzaktan bağlantı ve yönetim programının kullanıldığı tespit edilmiştir.

İlgili imaja ait diğer sistemsel bilgiler 6. Sorunun cevabında verilmiştir.

S17HJ90Q816726 Seri Numaralı Disk

User kullanıcı ismiyle açılan bilgisayarda muyesseryildiz@yahoo.com, ilimugur@gmail.com, naciugur@hotmail.com e-posta hesaplarıyla işlem yapıldığı, **ilimtherummer** kullanıcı adıyla Skype anlık mesajlaşma programı kullanıldığı ve 476374846 kullanıcı numarasıyla Teamviewer uzaktan bağlantı ve yönetim programının kullanıldığı tespit edilmiştir.

İlgili imaja ait diğer sistemsel bilgiler 6. Sorunun cevabında verilmiştir.

Soru 8.)

Ek-1 Listede belirtilen dosyalara son yazım tarihinin, dosyaların disk üzerindeki yaratılma tarihlerinden önce olması durumunun söz konusu olup olmadığı, bu durum söz konusu ise anılan dosyaların sadece incelenen bilgisayarda oluşturulup oluşturulmadığı konusunda nasıl bir değerlendirme yapılmasının gerektiği?

Cevap 8.)

Ek-1 listede belirtilen dosyalarda son yazım tarihinin, dosyaların disk üzerinde yaratılma tarihlerinden önce olması durumu söz konusudur ve bu dosyalar cevap 5 de belirtilmiştir. Bu durum tek başına ilgili dosyaların sadece incelenen bilgisayarda oluşturulup oluşturulmadığı konusunda kesin bir bilgi vermemekle birlikte, dosyaların son yazım tarihinin disk üzerindeki yaratılma tarihinden önce olması, bilgisayarın olağan çalışma süreci esnasında sıklıkla oluşabilen bir durumdur.

Örnek vermek gerekirse, NTFS dosya sistemi bulunan bir bilgisayarda oluşturduğumuz bir dosyayı, başka bir klasöre kopyaladığımızda oluşturma tarihi, kopyalama işlemini yaptığımız tarih olacaktır. Ancak değiştirme tarihi, dosyayı ilk değiştirdiğimiz tarih olarak kalır. Bu işlem dizisine göre değiştirme tarihi, oluşturma tarihinden önce görünecektir.

NTFS dosya sisteminde bulunan her bir dosya için en az iki farklı tip (Standart Information, Filename Information) tarih bilgisi tutulmaktadır. Bu tarih bilgilerinin içeriği ve nasıl değiştiği; işletim sisteminin tipine göre, dosyanın hangi dosya sistemine sahip bir veri depolama cihazında kopyalanıp kopyalanmadığına veya taşınıp taşınmadığına göre, dosyanın ZIP/RAR vb. programlarla sıkıştırılmış arşivlerden çıkarılıp çıkarılmadığına göre, vb faktörlere göre değişebilmektedir.

Bu bilgilerden hareketle, dosyaların değiştirilme tarihinin oluşturma tarihinden önce olması, tek başına bir anlam **ifade etmez**. EK-1 listesinde bulunan dosyalar hakkındaki detaylı inceleme ve açıklamalar 5. soru'nun cevabında verilmiştir.

Soru 9.)

Ek-1 Listede belirtilen dosyaların hard disk üzerindeki konumlarının belirtilmesi, olağana uygun olup olmadığı, dosyaların silinmiş veya silinmemiş alanda bulunup bulunmadığının belirtilerek açıklanması?

Cevap 9.)

Ek-1 listede belirtilen her bir dosya için hard disk konumları, silinmiş veya silinmemiş durumda oldukları ve varsa olağan dışı bir durum görülüp görülmediği, 5. Soruda ayrıntılı şekilde cevaplanmıştır.

Soru 10.)

Bilirkişilerin inceleme ve değerlendirme raporlarında belirttikleri Unallocated Cluster bölümün ne olduğu, nasıl oluşturulacağı?

Cevap 10.)

Hard diskler, veri adreslenebilen çok sayıda birime ayrılmışlardır. Bu birimlerine her birine cluster (yığın) adı verilmektedir. Cluster'lar, 1-2-4-8-16 gibi 2'nin üstleri şeklinde katlanan çeşitli sayıda sektörlerin birleşmesiyle oluşurlar. [17]

Windows işletim sistemi, bilgisayarda bulunan dosyaları bu clusterlar içine belirli bir algoritmaya göre yerleştirmektedir. Bu algoritma, dosyaların en uygun (best-fit) yere yerleştirmesini ve hard diskin olabildiğince verimli kullanılmasını amaçlamaktadır. Söz gelimi, bilgisayarda yeni bir dosya oluşturulduğunda veya başka bir ortamdan yeni bir dosya kopyalandığında, işletim sistemi o dosya için hard disk üzerinde en uygun yeri bulur ve dosyayı oraya yerleştirir. Büyük dosyalar için farklı clusterlar kullanılabileceği gibi, küçük dosyalar için art arda gelen clusterlar da kullanılabilmektedir. Bu tamamen clusterların uygunluğuna ve işletim sisteminin o anda vereceği karara bağlıdır. Bir dosyanın hangi clusterlarda bulunduğu, dosyanın oluşumu esnasında $MFT (Master File Table) denilen ve bir anlamda indeks mekanizması olarak çalışan bir dosyada tutulur. İlgili dosyaya erişilmesi gerektiğinde, işletim sistemi $MFT dosyasını okuyarak dosyanın hangi clusterlarda tutulduğu bulur ve veriye erişir.

Herhangi bir hard disk satın alındığında veya yeni formatlandığında, üzerinde bulunan clusterların çok büyük bir bölümü kullanıma hazır haldedir. Yeni satın alınmış ve daha önce hiç kullanılmamış bir hard disktte, clusterlarda hiçbir veri bulunmamaktadır. Ancak daha önce kullanılan bir hard diskte, ilgili hard diskteki veriler silinse veya formatlansa bile eskiye dair veriler clusterlarda bulunmaya devam eder.

Örnek vermek gerekirse; NTFS dosya sistemi kullanılan ve Windows işletim sistemi üzerinde çalışan bilgisayarda bulunan bir dosya silindiği zaman, dosyanın $MFT kaydına o dosyanın silindiğine dair bir işaret konur. Bunun dışında $Bitmap dosyasında saklanan ve o dosyaya ait verilerin hangi clusterlarda tutulduğunu gösteren veriler güncellenir. Kullanılmakta olan (allocated) clusterlar, kullanıma hazır (unallocated) clusterlar olarak işaratlenir. Sonuç olarak o dosyaya ait hem $MFT kaydında hem de dosyanın clusterlarında veri bulunmaya devam eder, ta ki dosyanın üzerine başkaca veri yazılana kadar. Bu nedenle bilgisayarlarda bulunan bir dosya silinse bile geri getirilme ihtimali bulunmaktadır. Soru 5'e verilen cevaplarda da

[17] Carrier,Brian, File System Analysis, Sayfa 224

görüleceği üzere, EK-1 listesindeki silinmiş bir çok veri bu sayede geri döndürülebilmiştir. Silindiği tespit edilen dosyaların bazılarının tamamen, bazılarının ise kısmen geri döndürülebilmesinin altında yatan neden budur. Silinen bir dosya, $MFT kaydının veya cluster bölümünün üzerinde başka bir veri yazılmadığı zaman büyük olasılıkla tamamen kurtarılabilir. Ancak dosyanın $MFT kaydı hasar gördüğünde, yani üzerine başka bir veri yazıldığında, dosyanın indeksi kaybolmuş olur. Burada devreye **unallocated cluster** kavramı girer. Çünkü dosya hard diskte gerçekten bulunuyor olmasına rağmen, indeks verisi kaybolduğu için geri döndürmek zorlaşır. Ancak buna rağmen çeşitli tekniklerle veriye ulaşılabilir. Dosya verisinin bulunduğu o alan, artık unallocated cluster adını almaktadır.

Sonuç olarak, unallocated cluster alanı, işletim sistemi tarafından kullanılmaya hazır halde bekleyen alanı ifade eder. Bu alan boş olabileceği gibi, daha önceden kullanılmış da olabilir. Dolayısıyla unallocated cluster alanında herhangi bir veriye ait kalıntı bulunması, ilgili verinin daha önceden bilgisayarda bulunduğunu ancak silindiğini göstermektedir.

Soru 11.)

Ek-1 Listede belirtilen dosyaların SMFT ve $LogFile kayıtları hakkında ayrıntılı bilgi ve açıklamalarda bulunulması?

Cevap 11.)

$MFT (Master File Table), veri depolama ünitelerinde kullanılan dosya sistemlerinden NTFS'in (New Technology File System) bütün dosyaların ve klasörlerin kayıtlarını tuttuğu ve verilerine erişim için referans aldığı tabloyu içeren dosya sistemi metaveri dosyasıdır, NTFS'in merkezidir.

$MFT tablosu, NTFS ile formatlanmış bir diskteki dosyalar için; dosya isimleri, dosya tarih-zaman bilgileri, dosyaların bulunduğu cluster numaraları, dosya değişken bilgileri (sıkıştırılmış dosya, sadece okunabilir dosya, şifreli dosya vb.) gibi bilgileri ihtiva eder.

$LogFile, NTFS dosya sisteminde dosya veya klasör oluşturma, içeriğini veya ismini değiştirme ve MFT kaydındaki herhangi bir veriyi değiştirme vb işlemlerin kayıtlarını tutmak için kullanılan dosya sistemi metaveri dosyasıdır. $MFT kaydının değişmesine sebep olacak bir işlemden önce halihazırdaki kaydın bilgileri ve yeni oluşacak kaydın bilgileri, işlemden sonra ise işlemin başarıyla tamamlandığına dair bir bilgi $Logfile dosyasına kaydedilir. Buradaki amaç $MFT kayıtlarını değiştirecek olan işlemlerin gerçekleşmesi yarıda kalır veya bir şekilde tamamlanamazsa, $LogFile dosyasındaki bilgiler doğrultusunda bozulan $MFT kayıtlarının eski haline getirilebilmesidir. Bu şekilde dosya sisteminin bütünlüğünün korunması amaçlanmaktadır. Fakat $LogFile dosyasıını boyutu sabittir. İncelenen üç imaj için de $logFile boyutu 67.108.864 btye olarak tespit edilmiştir. Bu yüzden dosyada yeni kayıtlar için yeterli yer kalmadığı takdirde bu kayıtlar sırayla en eski kayıtların üzerine yazılacaktır.

Yukarıda açıklanan bilgilerden ışığında, bir diskteki her bir dosya için $MFT kaydının olması gerekir. Ancak dosya silindiğinde $MFT kaydında o dosyanın silindiğine dair bir işaret konur. Kullanılan adli analiz araçlarıyla o işaret görmezden gelinerek silinmiş dosyalara ulaşılabilir. Ancak ilgili dosyanın $MFT kaydının üzerine veya dosyanın kendi veri kısmının üzerine başka bir veri yazıldığında tahribat olur. Bu nedenle o dosyanın geri dönüşümü, üzerine yazılan sektörler için imkansız hale gelecektir. Bununla beraber, silinmiş dosyanın yalnızca bir kısmının üzerine başka bir veri yazılırsa, üzerine veri yazılmamış alan kurtarılabilir.

$LogFile ise $MFT kaydı tamamen silinmiş olan ve üzerine yazılmış dosyalar için bilgi verebilir niteliktedir. Bir dosyanın $MFT kaydının bulunmamasına rağmen $LogFile kaydının olması, o dosyanın daha önce o diskte bulunduğu ancak silindiği ve daha sonra $MFT kaydı

üzerine başka bir veri yazıldığı anlamına gelmektedir. Bununla beraber $LogFile'dan elde edilecek veriler kullanılarak o dosyanın veri kısmına ulaşmak ve tamamını ya da bir kısmını geri döndürebilmek mümkün olabilmektedir.

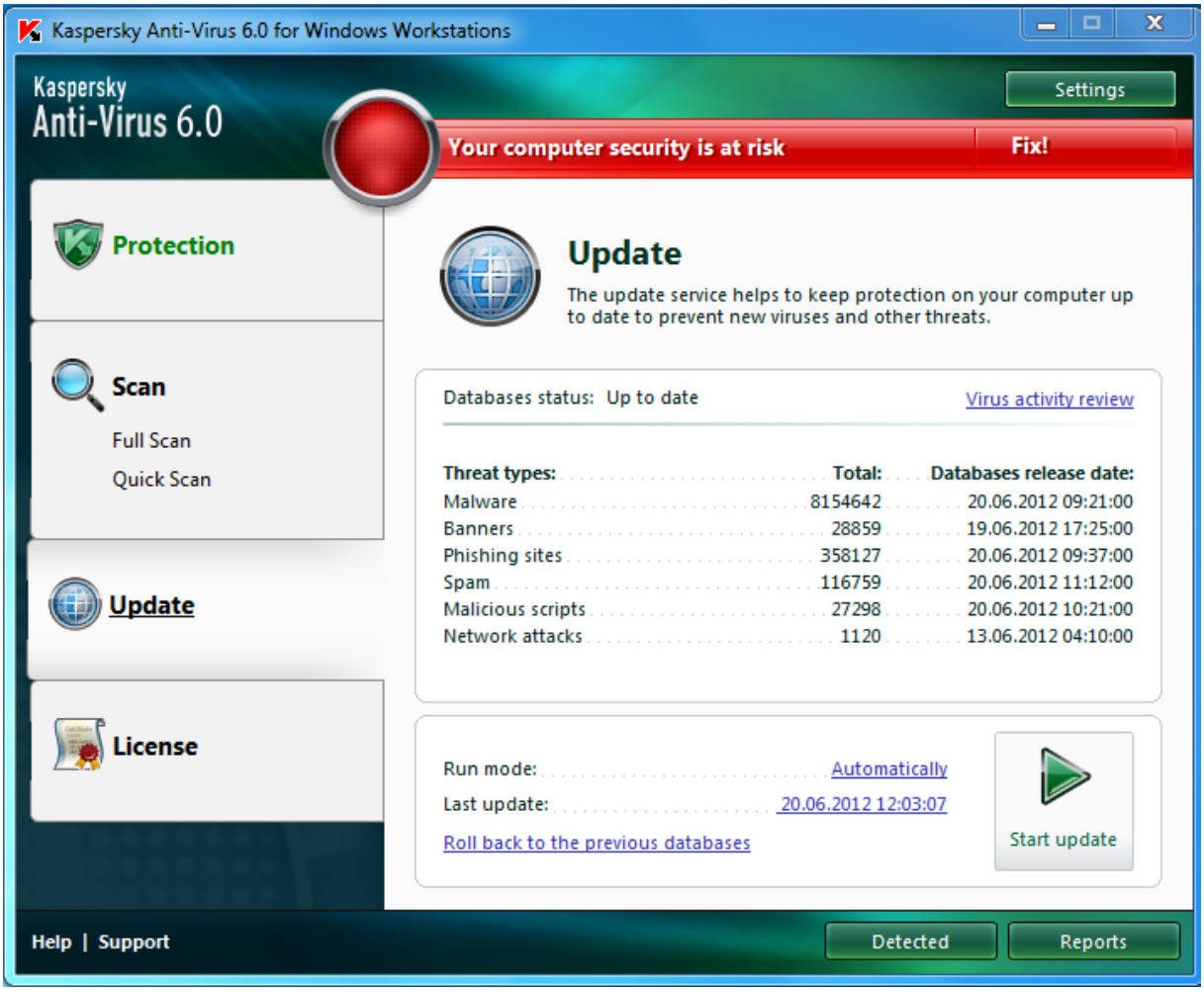
EK-1 listesindeki dosyalar için detaylı $MFT ve $LogFile verileri Soru 5'te cevaplanmıştır. İlgili cevap incelenebilir.

Soru 12.)

Belirtilen bilgisayarlarda her türlü virus, trojen v.b gibi zararlı yazılım bulunup bulunmadığı, bulunuyor ise Ek-1 Listede belirtilen dosyaların bu zararlı yazılımlarla oluşturulup oluşturulmadığı, teknik olarak oluşturulup oluşturulamayacağı, e-mail, spam vb. aracılığı ile bilgisayara korsan olarak gönderilip gönderilmediği, gönderilmiş ise nasıl ve ne şekilde gönderildiğinin ayrıntılı bir şekilde her bir dosya için ayrı ayrı belirtilmesi sureti ile açıklanması?

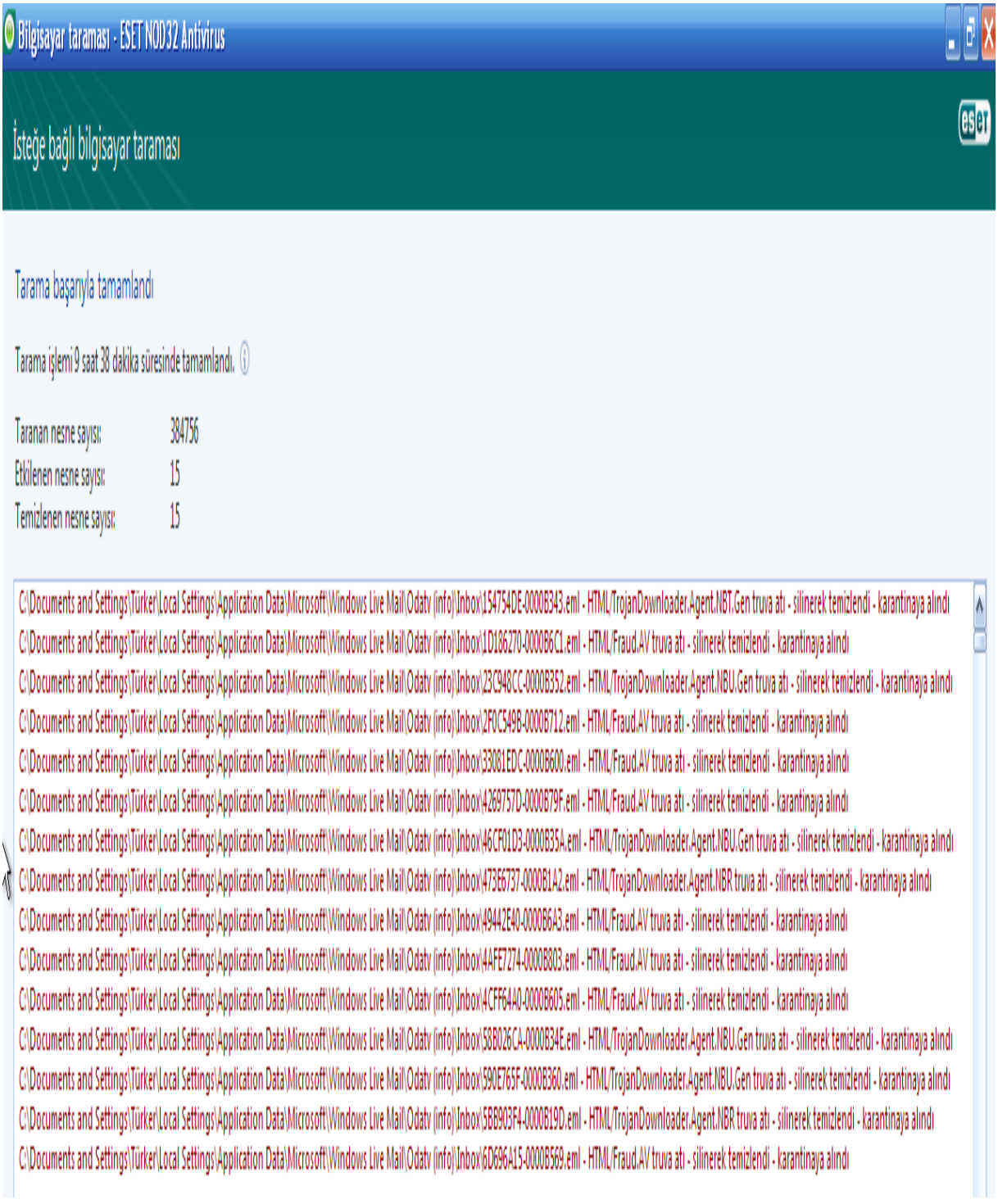
Cevap 12.)

Bilgisayarlar üzerinde virüs, trojan gibi zararlı yazılımların tespiti için öncelikle bilgisayarlar üzerindeki antivirüs uygulamaları ile tarama gerçekleştirilmiştir. Daha sonra 20.06.2012 tarihinde en son güncellemeleri (20.06.2012 tarihli veritabanı güncellemesi) yüklü "Kaspersky Anti-virus 6.0" uygulaması ile tarama yapılmıştır. Sonuçlar aşağıda görülmektedir.

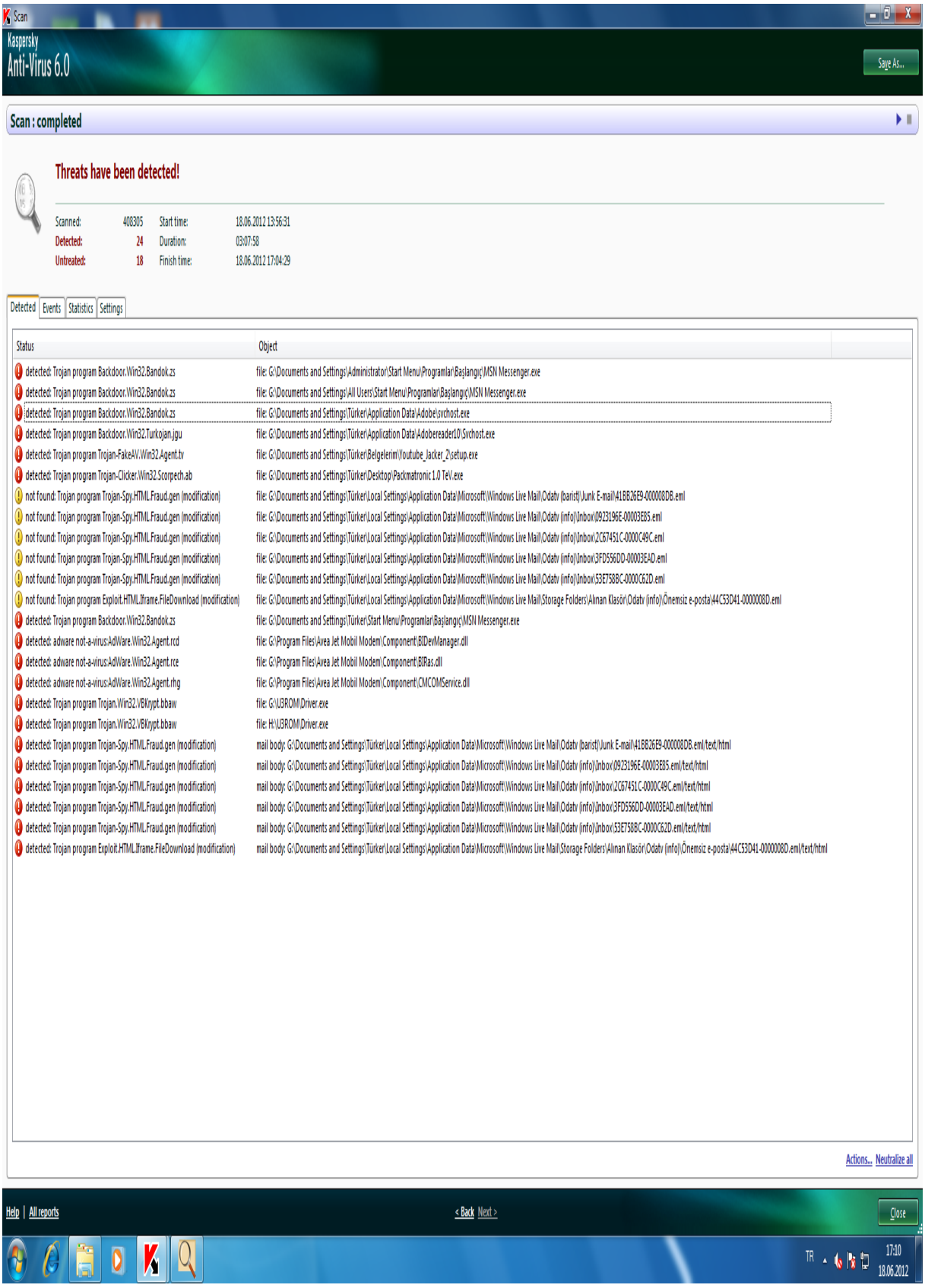


Şekil 89 - Tarama yapılan antivirüs uygulaması bilgileri

ST3120827AS_4MS1TF89 seri nolu hard disk imajı üzerinde yapılan tarama sonuçlarına ait ekran görüntüsü Şekil 90 ve Şekil 91'da gösterilmiş olup ayrıntılı tarama sonucu EK-4 ve EK-5'te sunulmuştur.

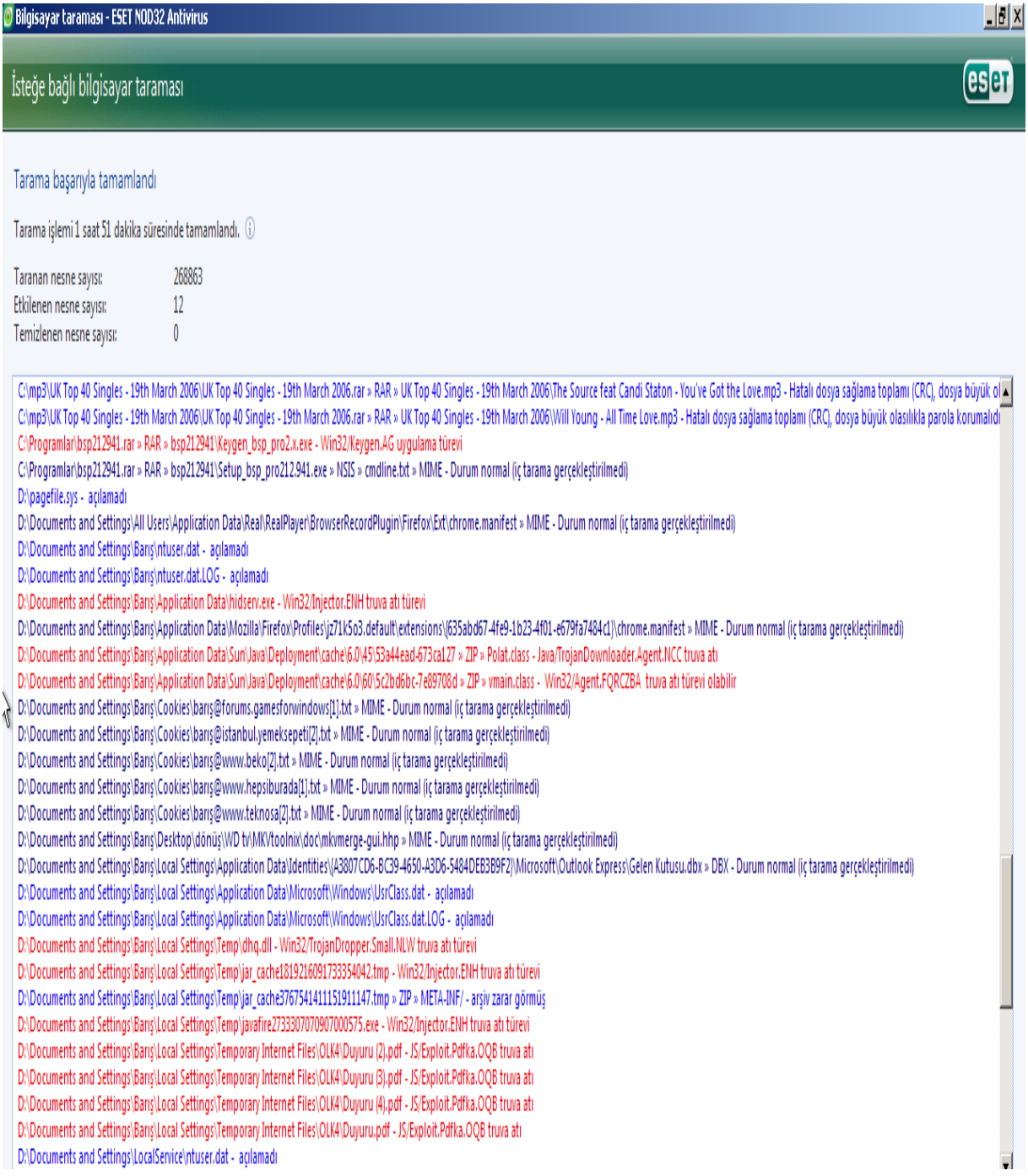


Şekil 90 - ST3120827AS_4MS1TF89 imajı üzerindeki antivirüs ile tarama sonucu

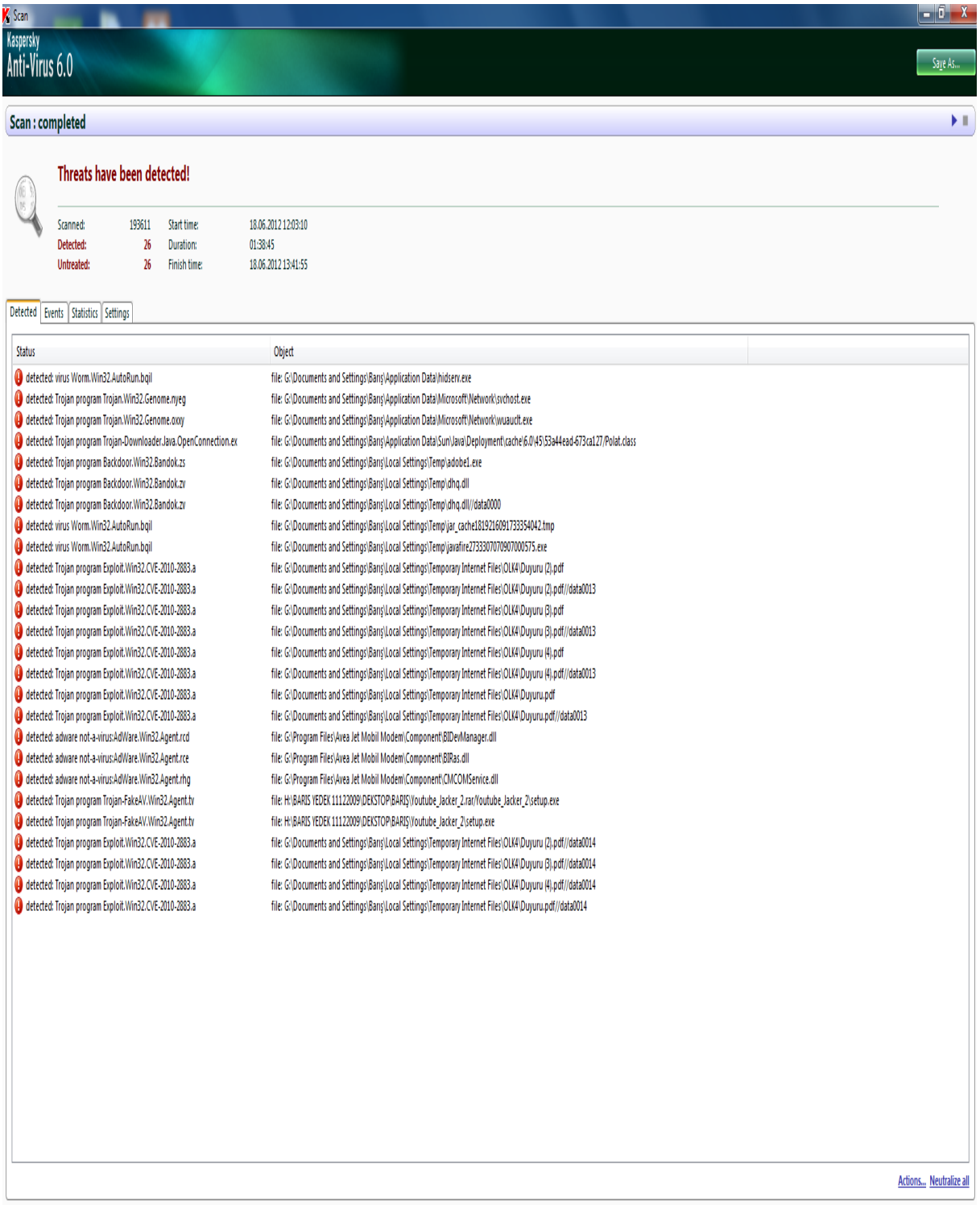


Şekil 91 - ST3120827AS_4MS1TF89 İmajının Güncel Antivirüs ile Taranması Sonucu

MHV2060BH_NW18T6229459 seri nolu hard disk imajı üzerinde yapılan tarama sonuçlarına ait ekran görüntüsü Şekil 92ve Şekil 93'te gösterilmiş olup ayrıntılı rapor sunucu EK-6 ve EK-7'de sunulmuştur.

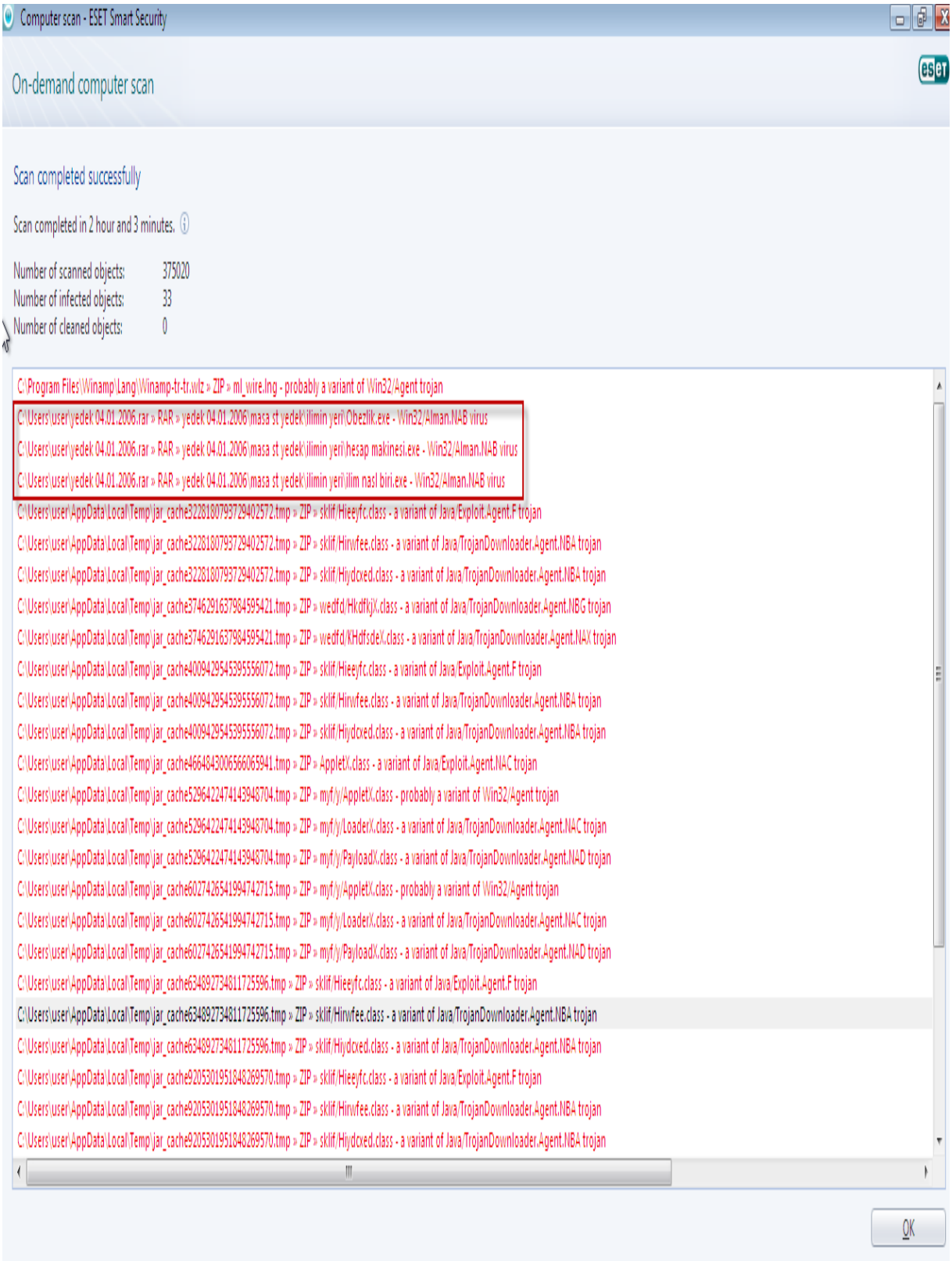


Şekil 92 - MHV2060BH_NW18T6229459 imajı üzerindeki antivirüs ile tarama sonucu

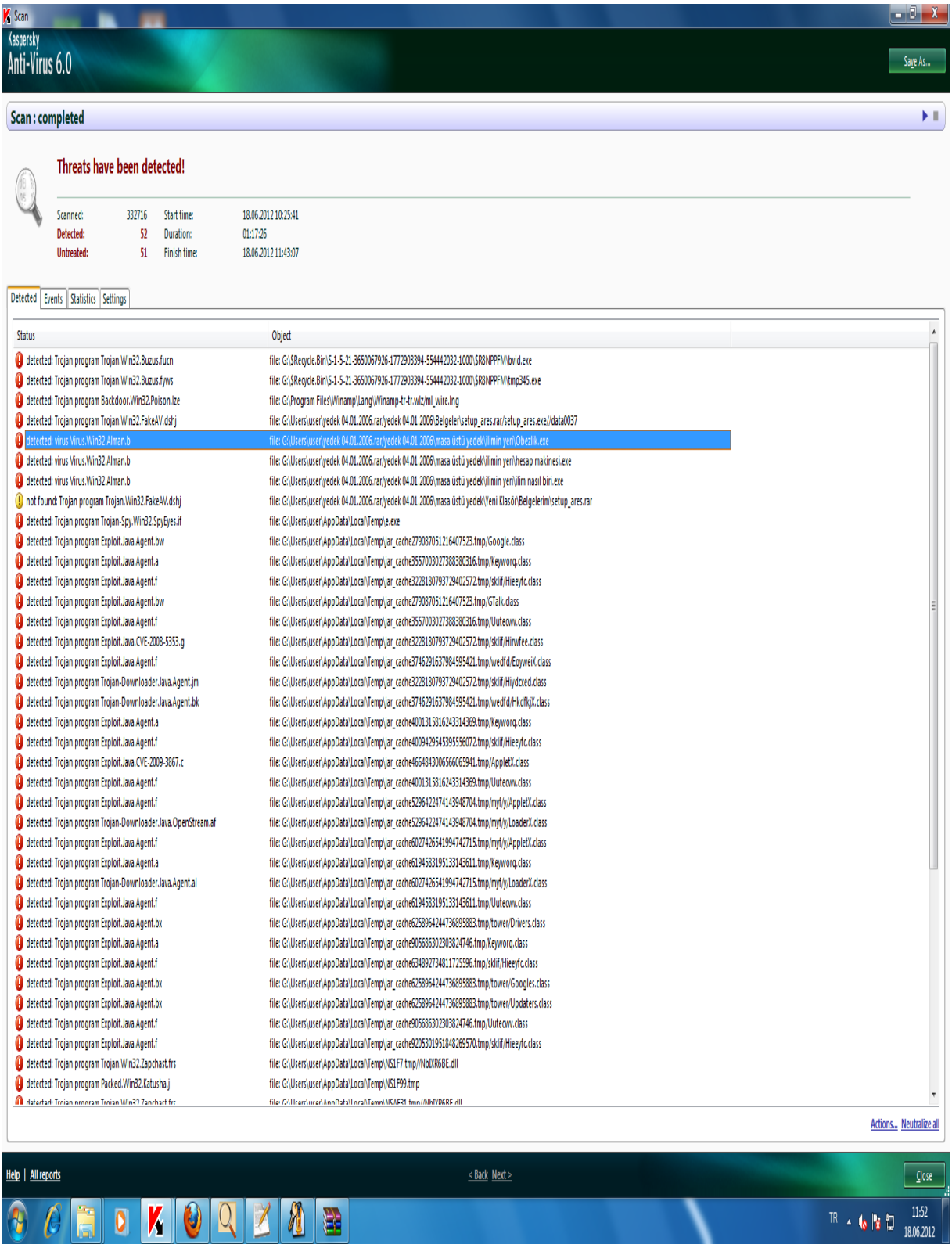


Şekil 93 - MHV2060BH_NW18T6229459 İmajının Güncel Antivirüs ile Taranması Sonucu

S17HJ90Q816726 seri nolu hard disk imajı üzerinde yapılan tarama sonuçlarına ait ekran görüntüsü Şekil 16 ve Şekil 17 de gösterilmiş olup ayrıntılı rapor sunucu EK-8 ve EK-9 da sunulmuştur.



Şekil 94 - S17HJ90Q816726 imajı üzerindeki antivirüs ile tarama sonucu



Şekil 95 - S17HJ90Q816726 İmajının Güncel Antivirüs ile Taranması Sonucu

İncelemeler sonucunda gerek güncel antivirüs uygulamalarının, gerekse hard disk imajlarında hali hazırda kurulu bulunan antivirüs uygulamalarının çeşitli zararlı yazılımlar tespit ettiği görülmektedir. Detaylı bilgiler için alt bölümler incelenebilir.

Teslim edilen bilgisayarlar imajlarında, 20 Haziran 2012 tarihinde güncellenmiş Kaspersky Anti-Virus 6.0 antivirüs yazılımı ile virüs taraması yapılmıştır. Yapılan virüs taraması sonucu; delil 1 bilgisayarında 24 adet, delil 2 bilgisayarında 24 adet ve delil 3 bilgisayarında 52 adet zararlı yazılım tespit edilmiştir. Bu zararlı yazılımların listesi EK-4, EK-5, EK-6, EK-7, EK-8 ve EK-9 da verilmiştir. Tespit edilen bu zararlı yazılımların birçoğu ya aktif konumda değil, ya da aynı zararlı yazılımın uzantısı olan farklı dosyaları göstermektedir. Bunun yanında tespit edilen zararlı yazılımların büyük çoğunluğu genel amaçlı olup, birçok kullanıcı bilgisayarında bulunabilmektedir. Genel amaçlı zararlı yazılımlardan kasıt; spam e-posta gönderimi, internet bankacılık bilgilerinin çalınması, hizmet dışı bırakma saldırılarında (DDOS) bulunulması, reklam yayınlanması gibi çeşitli faaliyetler yoluyla maddi çıkar sağlama amacıyla kullanılan zararlı yazılımlardır. Bu zararlı yazılımların teknik olarak uzaktan yönetim ve dosya atma kabiliyetleri olsa dahi sadece zombi (bot) bilgisayar sayısını arttırmak için kullanılan bu yazılımların kurban bilgisayarlara özel olarak dosya atma amaçlı kullanılma ihtimali düşüktür. Bahse konu olan dosyaları ilgili bilgisayarlara uzaktan koyabilmek için:

ilgili bilgisayar kullanıcısını özel olarak hedef almış olan bir sosyal mühendislik saldırısının düzenlenmesinin,

bu saldırı ile uzaktan kontrol ve dosya atma özelliği olan bir zararlı yazılım gönderilmesinin,

gönderilen bu zararlı yazılımın kurban bilgisayarda başarılı bir şekilde çalışmasının

gerekli olduğu değerlendirilmektedir. Bu sebeple ilgili dosyaların üçüncü şahıslar tarafından, bilgisayar kullanıcısının iradesi dışında zararlı yazılımlar ile gönderilmiş olma ihtimali anlamak amacıyla, sosyal mühendislik saldırıları ile özel olarak ilgili bilgisayar kullanıcılarını hedef alan saldırılar ile gönderilen zararlı yazılımlar ayrıntılı bir şekilde incelenmiş, bu zararlı yazılımların uzaktan dosya atma kabiliyetinin olup olmadığı, bilgisayarda aktif olarak çalışıp çalışmadığı tespit edilmeye çalışılmıştır.

Hedefli saldırı sonucu gönderilen zararlı yazılımların analizi, her bir delil için iki aşamada yapılmıştır. İlk aşamada, zararlı yazılım delil bilgisayarına eş konfigürasyondaki bir analiz ortamında çalıştırılıp gerçekleştirdiği işlemler ve bilgisayar üzerinde bıraktığı izler tespit edilip listelenmiştir. İkinci aşamada ise, her bir kötücül yazılımın bıraktığı izler ilgili delil bilgisayarında aranarak, gönderilen kötücül yazılımın bu bilgisayarda çalıştırılıp çalıştırılmadığı konusunda bir kanaate varılmaya çalışılmıştır.

Delil 1 bilgisayarından erişilen e-posta hesaplarına ait kayıtlı e-postalar araştırılarak, benzer kaynaktan hedefli bir saldırı sonucu gönderildiği tespit edilen e-postalar ve bu e-postalar ile ilgili ayrıntılı bilgiler Tablo 12 - Delil 1'e Jangomail kullanılarak gönderilmiş e-postalar

'de gösterilmiştir. Bu e-postalarda yer alan eklenti dosyaları ve bu dosyaların "Virustotal" adındaki websitesi üzerinde birden çok antivirüs yazılımına taratılması sonucunda belirlenen zararlı yazılım türleri de Tablo 12'de ayrıca gösterilmiştir. Bu tabloda "barisp@odatv.com" hesabına gelen e-postalar, aynı zamanda Delil 2 bilgisayar kullanıcısına gelen e-postalardır. Delil 3 bilgisayar kullanıcısına gelen hedefli saldırıları incelemek için sanık avukatı tarafından teslim edilen e-posta örnekleri kullanılmıştır.

E-posta Adı	Gözüken Gönderici	Alıcı	Geldiği Tarih	Eklenti	Eklenti Türü	Jangomail Dönüş Adresi
187E16C5-000056A4.eml	kemalizm1919@yahoo.com	barisp@odatv.com, sonery@hurriyet.com.tr	31 Ocak 2011 7:34	AKP_oncesi-sonrasi.pdf	Turkojan-RAT	winnerr5@jangomail.com
5A9C4EFE-0000E9F3.eml	kemalizm1919@yahoo.com	info@odatv.com	3 Şubat 2011 13:59	Ataturk_Ekrankoruma.scr	Turkojan-RAT	winnerr5@jangomail.com
66B46747-000042CF.eml	kemalizm1919@yahoo.com	barist@odatv.com, sonery@odatv.com	3 Şubat 2011 14:08	Ataturk_Ekrankoruma.scr	Turkojan-RAT	winnerr5@jangomail.com
37EA0857-00004396.eml	dhayurt@dha.com.tr	barisp@odatv.com	5 Şubat 2011 4:32	RssReader 2.1.zip	Turkojan-RAT	winnerr5@jangomail.com
1609770D-000058F0.eml	dhayurt@dha.com.tr	barist@odatv.com	5 Şubat 2011 4:32	RssReader 2.1.zip	Turkojan-RAT	winnerr5@jangomail.com
56825A91-00004377.eml	basinbirimi@chp.org.tr	barist@odatv.com	5 Şubat 2011 23:51	Duyuru.pdf	Bandook-RAT	winnerr51@jangomail.com
56AF62F7-000058C2.eml	basinbirimi@chp.org.tr	barisp@odatv.com	5 Şubat 2011 23:51	Duyuru.pdf	Bandook-RAT	winnerr51@jangomail.com
29C64C6C-	disk@disk.org.tr	barisp@odatv.com	5 Şubat 2011 23:58	Duyuru.pdf	Bandook-	winnerr51@jangomail.com

000058C1.eml					RAT	
72010E0A-00004376.eml	disk@disk.org.tr	barist@odatv.com	5 Şubat 2011 23:59	Duyuru.pdf	Bandook-RAT	winnerr51@jangomail.com
21974EA4-00004375.eml	info@lemaan.com.tr	barist@odatv.com	6 Şubat 2011 0:35	AKPkarikaturleri.zip	Bandook-RAT	winnerr7@jangomail.com

Tablo 12 - Delil 1'e Jangomail kullanılarak gönderilmiş e-postalar

Tablo 12'den de anlaşılabileceği üzere hedefli saldırılar sonucu gönderilmeye çalışılan zararlı yazılım türleri "Turkojan" ve "Bandook" zararlı yazılımlarıdır. Bu zararlı yazılımların uzaktan yönetim ve dosya atma kabiliyetleri mevcuttur. Bu yazılımların ilgili bilgisayarda çalışıp çalışmadıklarını tespit edebilmek amacıyla hedefli saldırılarla gelen ve aynı türden sadece birini içeren "Ataturk_Ekrankoruma.scr" ve "Duyuru.pdf" dosyaları seçilmiş ve analiz edilmiştir.

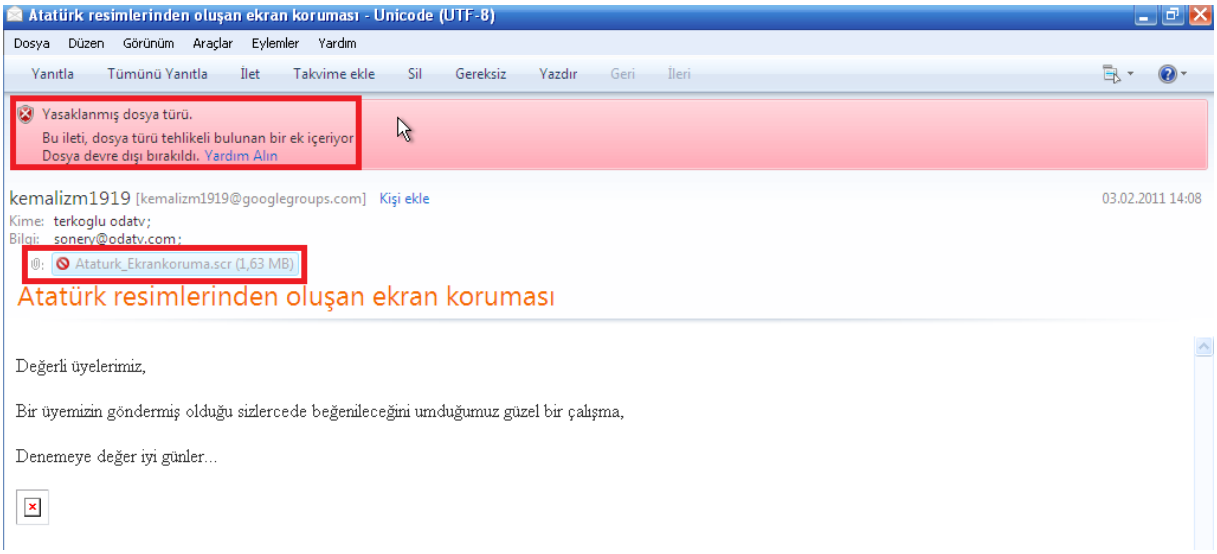
Aşağıdaki yorumlarda; ODATV'den elde edilen ST3120827AS_4MS1TF89 seri numaralı imaj için **Delil 1,** Barış PEHLİVAN'dan elde edilen MHV2060BHNW18T6229459 seri numaralı imaj için **Delil 2**, Müyesser Uğur YILDIZ'dan elde edilen imaj için **Delil 3** numaralandırması yapılmıştır.

Delil 1 Bilgisayarındaki Hedefli Saldırı Olabilecek Kötücül Yazılımların Analizi

Delil 1 bilgisayarından erişildiği tespit edilen Barist@odatv.com e-posta hesabına, e-posta yolu ile gönderilen "Ataturk_Ekrankoruma.scr" ve "Duyuru.pdf" zararlı yazılımların analizi aşağıdaki şekildedir:

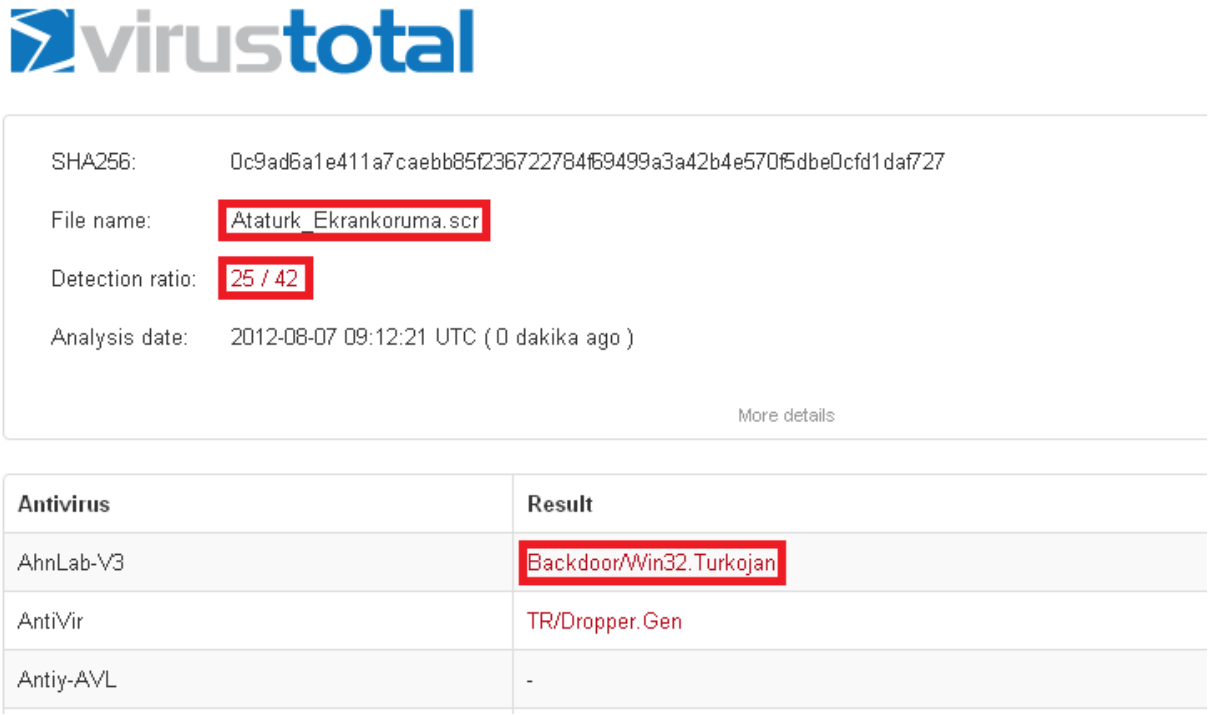
"Ataturk_Ekrankoruma.scr" Analizi

Delil 1 bilgisayarında yapılan incelemede, Barist@odatv.com e-posta hesabının gelen kutusunda, 03.02.2011 14:08 tarihinde kemalizm1919@googlegroups.com adresinden geliyor gözüken e-postanın ekinde "Ataturk_Ekrankoruma.scr" dosyası bulunmuştur. Fakat e-posta hizmet sağlayıcısı tarafından, ekte gönderilen dosyanın tehlikeli olduğu kanaatine varılarak devre dışı bırakıldığı ve "Ataturk_Ekrankoruma.scr" dosyasının e-posta üzerinden erişimine izin verilmediği görülmüştür.



Şekil 96 - Delil 1 Ataturk_Ekrankoruma.scr e-postası

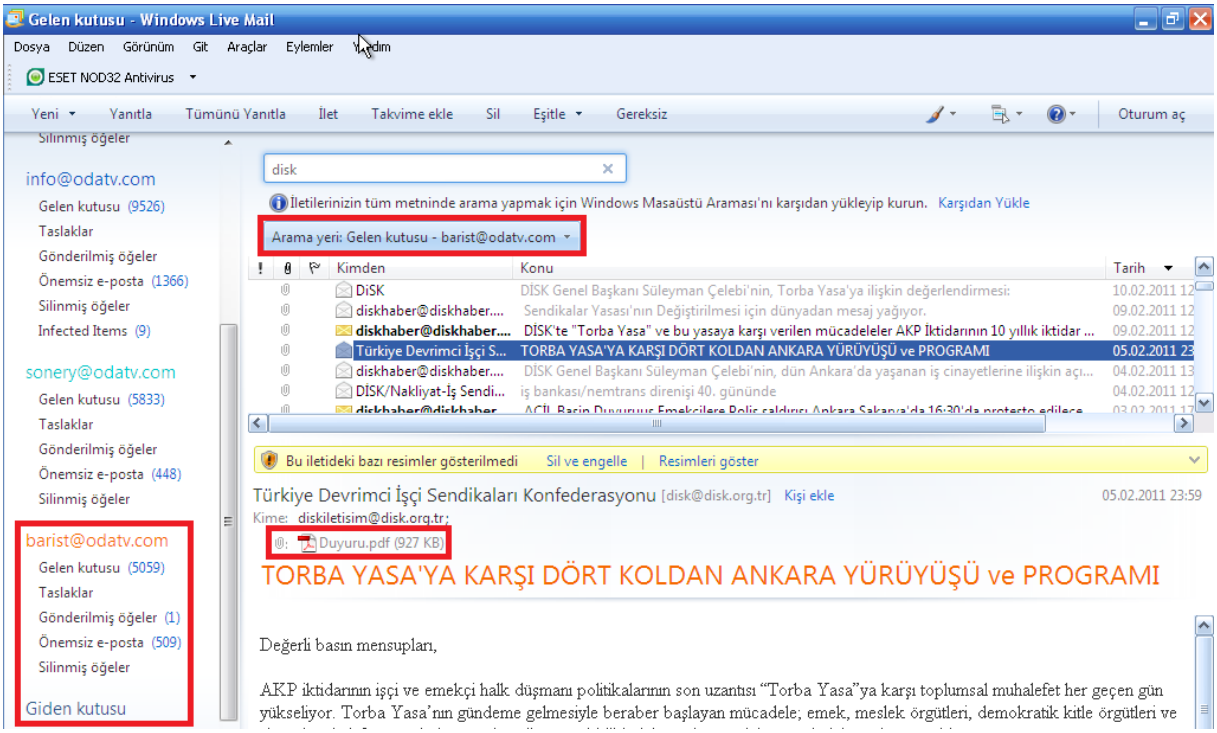
E-postanın ekinde yer alan "Ataturk_Ekrankoruma.scr" eklentisinin erişimine izin verilmediği için dosyanın çalıştırılmamış olduğu değerlendirilmektedir ve bu sebeple detaylı analizi yapılmamıştır. Fakat eklentinin zararlı bir yazılım olup olmadığının ve zararlı yazılım ise türünün öğrenilebilmesi için eklenti özel bir yolla elde edilmiştir. Bu dosyanın "Virustotal" üzerinde birden çok antivirüs yazılımına taratılması sonucu, "Turkojan RAT" türü bir truva atı (trojan) olduğu görülmüştür.



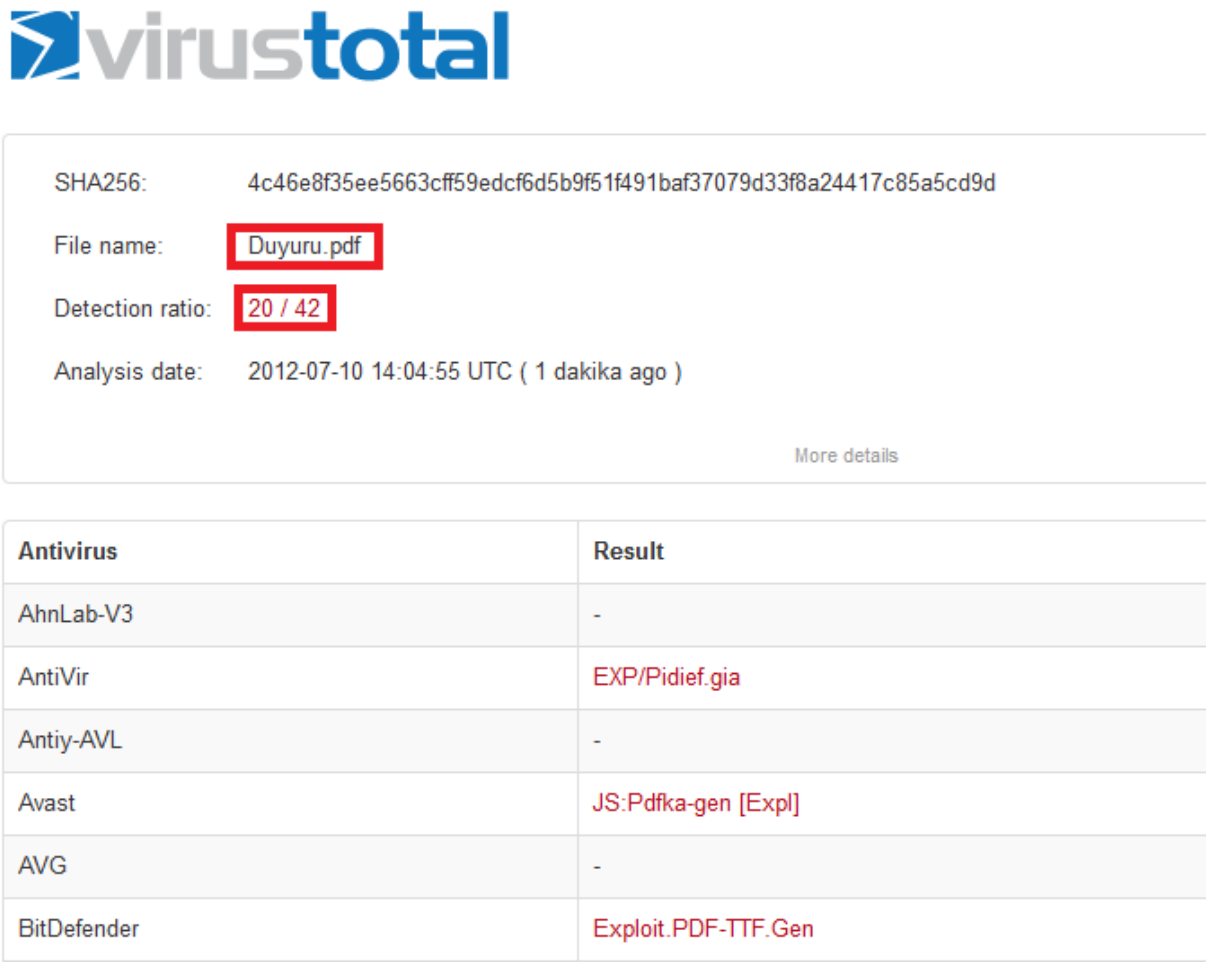
Şekil 97. Ataturk_Ekrankoruma.scr Virustotal tarama sonucu

"Duyuru.pdf" Analizi

Delil 1 bilgisayarında yapılan incelemede, "Duyuru.pdf" dosyasının 05.02.2011 23:59'da diskiletişim@disk.org.tr adresinden geliyor gözüken e-posta, Barist@odatv.com e-posta hesabının gelen kutusunda bulunmuştur. E-posta içeriğinin ekran görüntüleri Şekil 98'de gösterilmiştir.



Şekil 98. Delil1 Duyuru.pdf e-postası



virustotal

SHA256: 4c46e8f35ee5663cff59edcf6d5b9f51f491baf37079d33f8a24417c85a5cd9d

File name: Duyuru.pdf

Detection ratio: 20 / 42

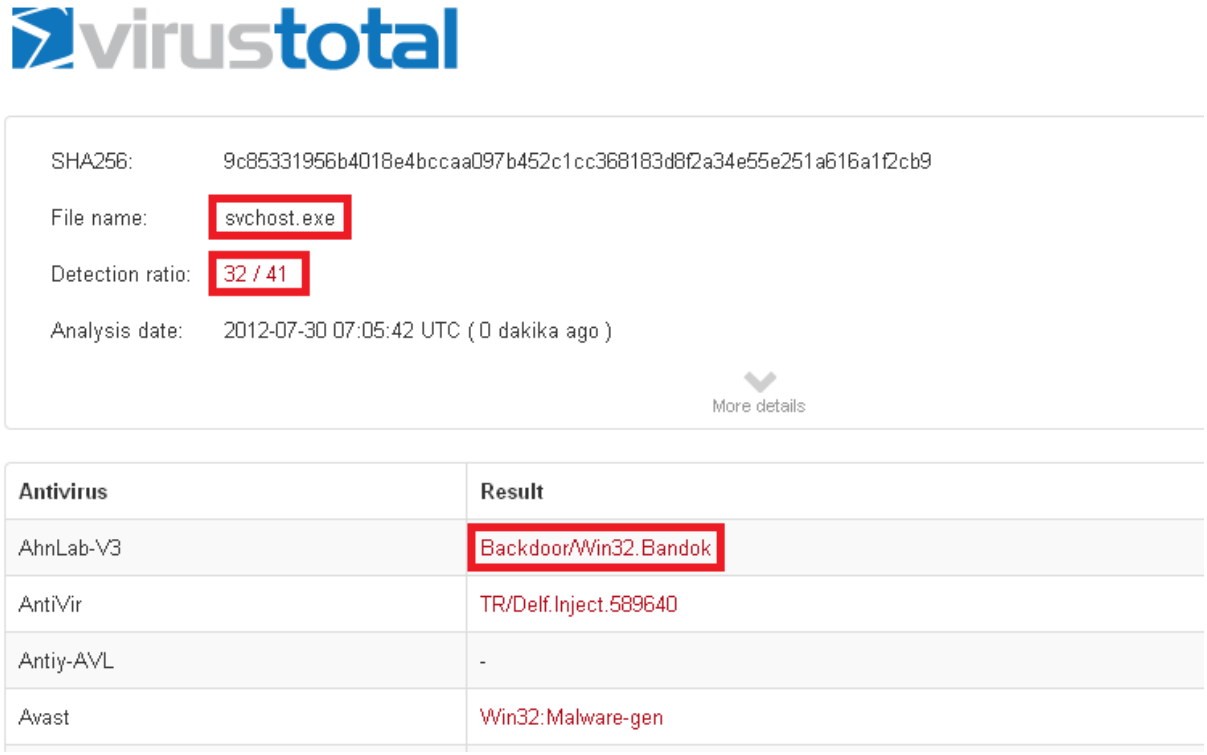
Analysis date: 2012-07-10 14:04:55 UTC (1 dakika ago)

More details

Antivirus	Result
AhnLab-V3	-
AntiVir	EXP/Pidief.gia
Antiy-AVL	-
Avast	JS:Pdfka-gen [Expl]
AVG	-
BitDefender	Exploit.PDF-TTF.Gen

Şekil 99. Duyuru.pdf Virustotal tarama sonucu

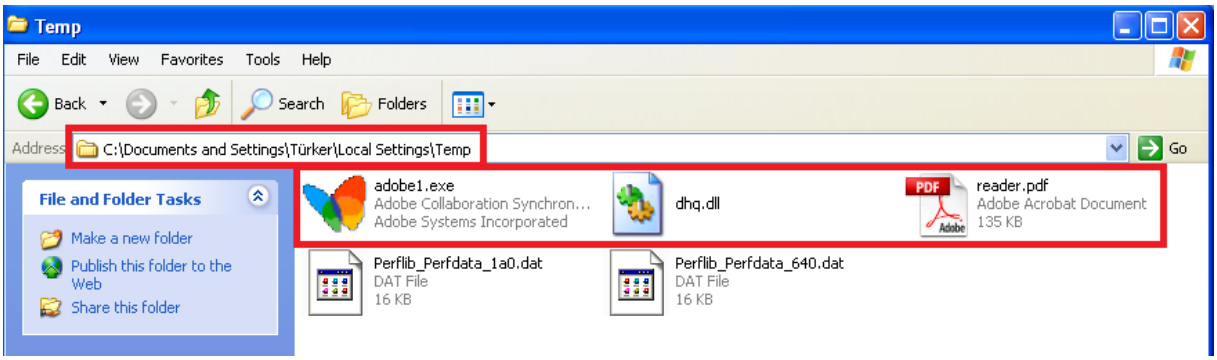
"Duyuru.pdf" kötücül yazılımının dinamik analizinde, "Duyuru.pdf" dosyası tarafından oluşturulan ve analiz adımları sırasında gösterilen asıl virüs dosyası "svchost.exe" dosyasının, "Virustotal" adındaki websitesi üzerinde birden çok antivirüs yazılımına taratılması sonucunda bu dosyanın "Bandook RAT" türü bir truva atı (trojan) olduğu görülmüştür.



Şekil 100. Duyuru.pdf svchost.exe Virustotal tarama sonucu

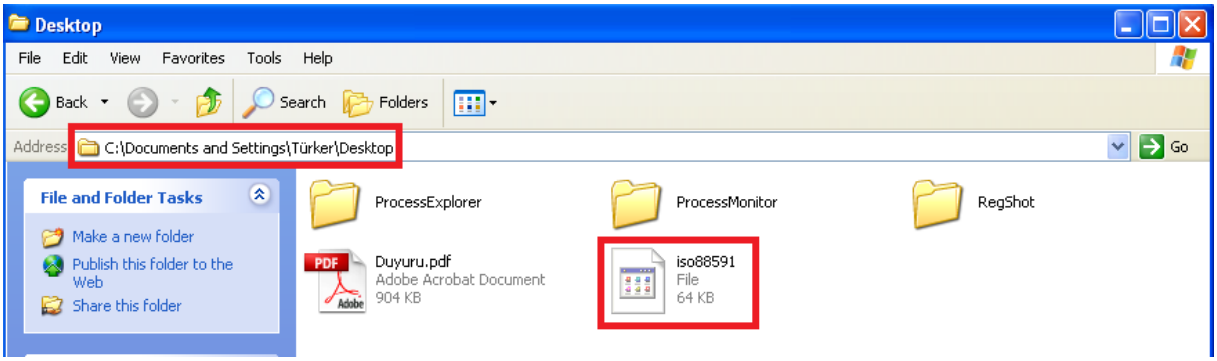
"Duyuru.pdf" dosyası ayrıntılı olarak incelenerek, bilgisayar üzerinde yaptığı değişiklikler ve gerçekleştirdiği işlemler tespit edilmeye çalışılmıştır. Analiz sırasında takip edilen yöntem ve zararlı yazılımın gerçekleştirdiği tespit edilen işlemler aşağıda sıralanmıştır:

1. E-posta'nın gönderildiği kişiye ait delil imajında Microsoft Windows XP işletim sisteminin kurulu olduğu görülmüştür. Analiz işlemi için, aynı işletim sistemine sahip bir analiz bilgisayarı hazırlanmıştır. Delil imajına uygun olarak,
    a. Kullanıcı adı "Türker" ve tam adı "Odatv" olan bir kullanıcı oluşturulmuştur.
2. Delil imajında PDF dosya okuyucu yazılımı olarak, Adobe Reader 9 (Version 9.0.0) yazılımının kullanıldığı görülmüş ve analiz bilgisayarına kurulumu gerçekleştirilmiştir.
3. İşletim sisteminde analiz için gerekli sistem ayarları yapılmış ve analiz işleminde kullanılacak yardımcı araçlar kurulmuştur.
4. İnceleme için gerekli araçlar çalıştırıldıktan sonra, "Duyuru.pdf" dosyası açılmıştır.
5. "Duyuru.pdf" dosyası açıldıktan sonra bilgisayar üzerinde gerçekleştirdiği işlemler genel olarak aşağıda sıralanmıştır.
    a. "C:\Documents and Settings\Türker\Local Settings\Temp" klasörü altında "adobe1.exe", "reader.pdf" ve "dhq.dll" adında dosyalar oluşturur.



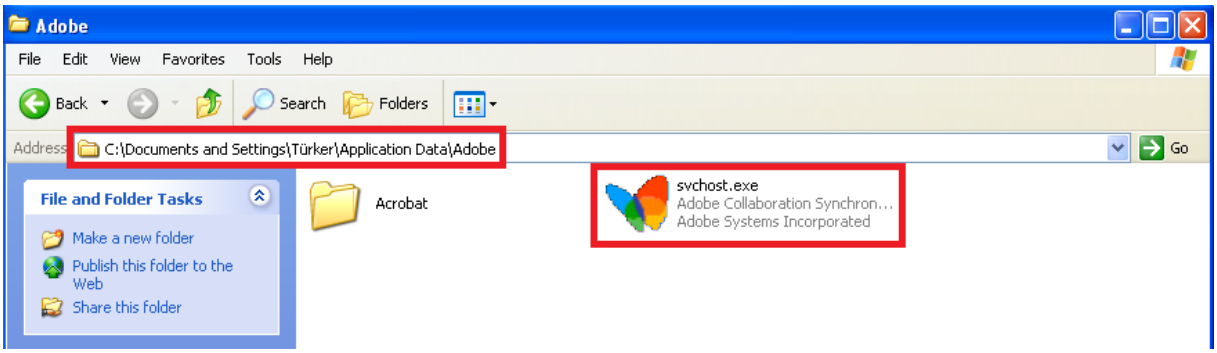
Şekil 101. Duyuru.pdf Temp klasöründe oluşturduğu dosyalar

b. "C:\Documents and Settings\Türker\Desktop" klasörü altında "iso88591" adında bir dosya oluşturur.



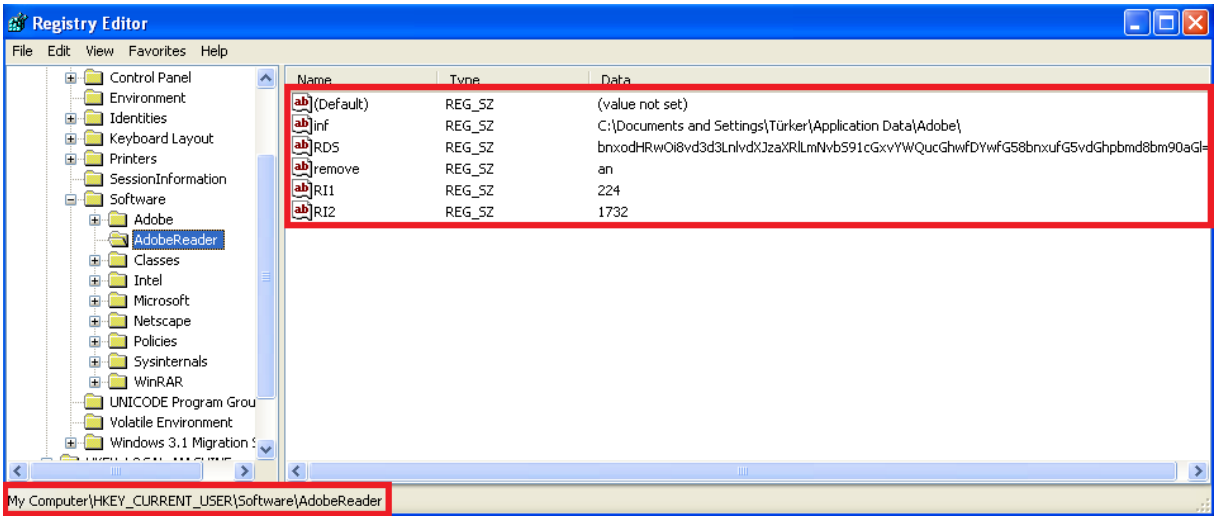
Şekil 102. Duyuru.pdf masaüstünde oluşturduğu dosya

c. Adobe1.exe prosesini çalıştırır.
d. "Reader.pdf" dosyası PDF görüntüleyici yazılım tarafından görüntülenir.
e. "C:\Documents and Settings\Türker\Application Data" klasörü altında "xxx.html" adında bir dosya oluşturur.
f. Firefox.exe prosesini çalıştırır.
g. Notepad.exe prosesini çalıştırır.
h. "C:\Documents and Settings\Türker\Application Data\Adobe\" klasörü altında "svchost.exe" adında çalıştırılabilir bir dosya oluşturur.



Şekil 103. Duyuru.pdf Adobe klasörü altında oluşturduğu svchost.exe dosyası

i. Registry kayıtlarında “HKCU\Software\AdobeReader” anahtarı ve altında “inf”, “RDS”, “remove”, “RI1” ve “RI2” değerleri oluşturur.

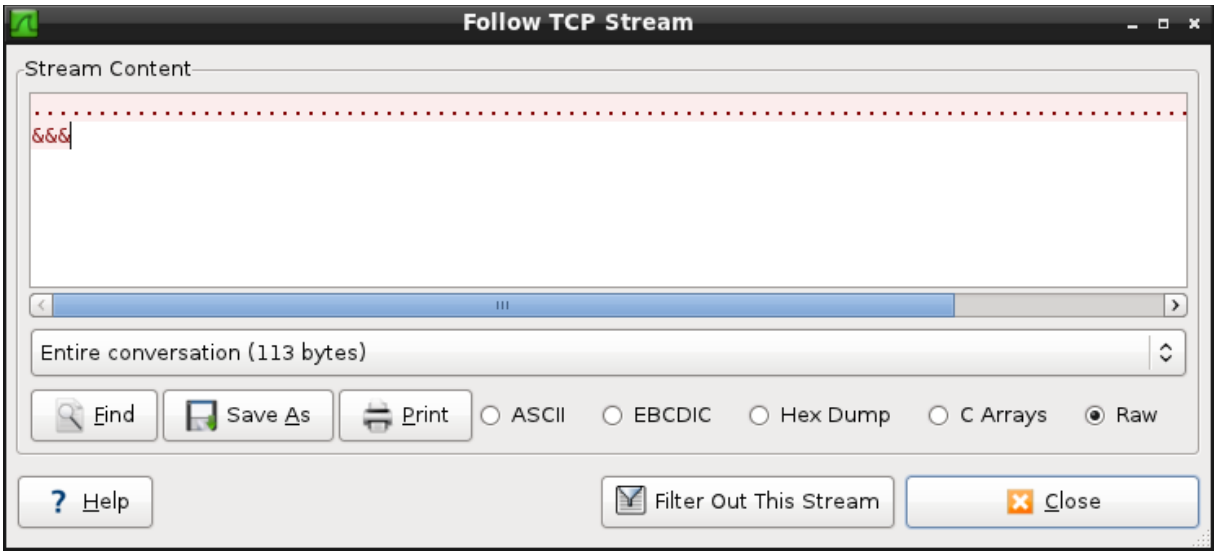


Şekil 104. Duyuru.pdf AdobeReader registry anahtarı

i. inf değeri, oluşturulan “svchost.exe” dosyasının yolunu tutmaktadır. (C:\Documents and Settings\Türker\Application Data\Adobe\)
ii. RDS değeri, birçok parametre ve bir web adresi içeren Base64 yöntemi kullanılarak kodlanmış bir sözcük tutmaktadır.
iii. RI1 ve RI2 değerleri, başlatılan iki farklı “notepad.exe” prosesinin proses numarasını tutmaktadır.

j. Bilgisayarın her açılışında, oluşturulan “svchost.exe” dosyasının otomatik olarak çalıştırılması için registry üzerinde kayıt oluşturur.
i. Registry anahtarı: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
ii. Registry değer adı: {B6A807N6-42DF-4W02-93E5-B156B3FA8AL1}
iii. Registry değeri: C:\Documents and Settings\Türker\Application Data\Adobe\

6. “Duyuru.pdf” dosyası çalıştırılması sonrasında ağ ve internet üzerinde gerçekleştirdiği işlemler aşağıda sıralanmıştır.
a. “adobupdate.serveftp.com” ve “adobupdate.servehttp.com” web adreslerine bağlanabilmek için, bu adreslerin IP adreslerini çözmeye yönelik DNS sorgusu göndermektedir.
b. Başarılı DNS çözümlemesi sonrası, “adobupdate.serveftp.com” ve “adobupdate.servehttp.com” web adreslerine 443 portu üzerinden bağlantı kurmaya çalışmaktadır.
c. Bağlantı sırasındaki iletişimi görebilmek için, yukarıdaki adresler bir analiz bilgisayarına yönlendirilmiş ve üzerinde 443 portundan dinleyen bir uygulama çalıştırılmıştır. Bu işlem sonrası, zararlı yazılım analiz bilgisayarına 443 portundan bağlantı kurmuş ve SSL ile şifreli bir iletişime geçmiştir.



Şekil 105. Duyuru.pdf SSL iletişimi

7. "Duyuru.pdf" dosyası çalıştırılması sonrasında bilgisayar üzerinde işletim sistemi tarafından oluşturulan, doğrudan veya adli analiz yapılarak elde edilen kayıtlar aşağıda listelenmiştir.
    a. $MFT dosyasında, çalıştırılan "Duyuru.pdf" dosyasına ait kaydın oluşturulduğu görülmüştür.

Dosya Tipi	Dosya Adı
Dosya	/<Duyuru.pdf dosyasının çalıştırıldığı yer>/Duyuru.pdf

    b. $MFT dosyasında, "Duyuru.pdf" dosyası çalıştırılması sonrasında oluşan "adobe1.exe", "reader.pdf" ve "dhq.dll" dosyalarına ait kayıtların bulunduğu görülmüştür.

Dosya Tipi	Dosya Adı
Dosya	/Documents and Settings/Türker/Local Settings/Temp/adobe1.exe
Dosya	/Documents and Settings/Türker/Local Settings/Temp/reader.pdf
Dosya	/Documents and Settings/Türker/Local Settings/Temp/dhq.dll

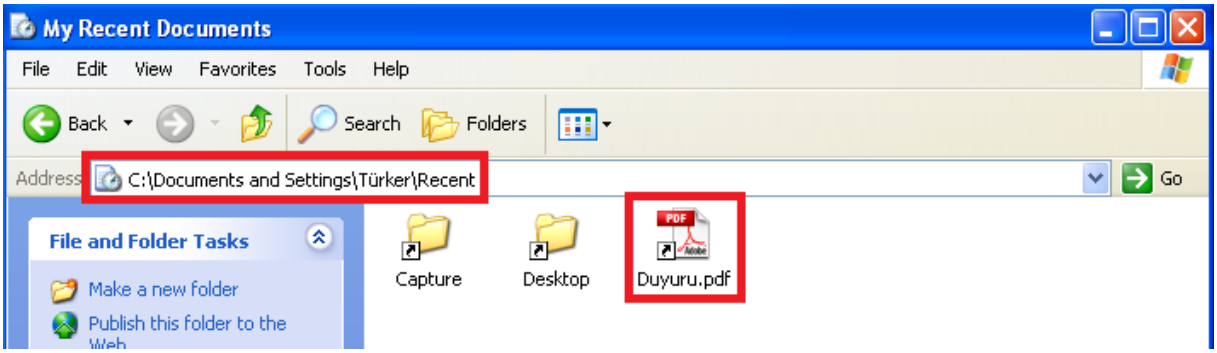
    c. $MFT dosyasında, "Duyuru.pdf" dosyası çalıştırılması sonrası oluşturulan "iso88591" adlı dosyanın kaydının bulunduğu görülmüştür.

Dosya Tipi	Dosya Adı
Dosya	/Documents and Settings/Türker/Desktop/iso88591

d. $MFT dosyasında, "Duyuru.pdf" dosyası çalıştırılması sonrası oluşturulan "svchost.exe" adlı dosyanın kaydının bulunduğu görülmüştür.

Dosya Tipi	Dosya Adı
Dosya	/Documents and Settings/Türker/Application Data/Adobe/svchost.exe

e. Açılan "Duyuru.pdf" dosyası için işletim sistemi tarafından, "C:\Documents and Settings\Türker\Recent" klasörü altında "Duyuru.pdf.lnk" adında bir bağlantı dosyasının oluşturulduğu görülmüştür.



Şekil 106. Duyuru.pdf.lnk dosyası

f. $MFT dosyasında, yukarıda gösterilen .lnk uzantılı bağlantı dosyasının kaydının oluşturulduğu görülmüştür.

Dosya Tipi	Dosya Adı
Dosya	/Documents and Settings/Türker/Recent/Duyuru.pdf.lnk

g. Recent klasöründe oluşan ".lnk" uzantılı dosyanın ve oluşan diğer dosyaların $LogFile dosyasında kayıtlarının bulunduğu görülmüştür.

"Duyuru.pdf" Analiz Sonuçlarının Delil 1'de Aranması

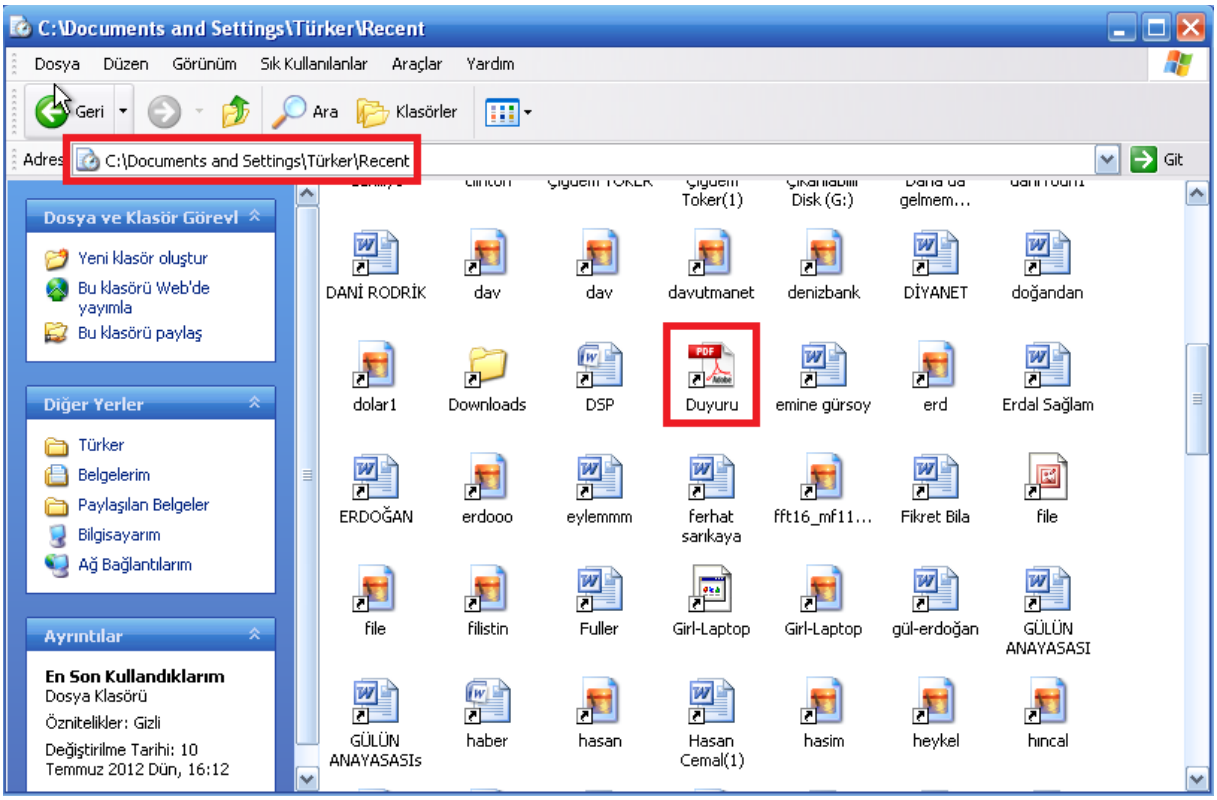
Yapılan analiz sonrası, e-posta yoluyla gönderilen "Duyuru.pdf" dosyasının bilgisayar üzerinde oluşturduğu dosyalar ve kayıtlar ile kullanılan işletim sistemi tarafından oluşturulan ve adli analiz yöntemleriyle elde edilen kayıtların tümü Tablo 13'de listelenmiştir.

No	Kayıt	Türü	Kaydın Yeri
1	Xxx.html	Dosya	C:\Documents and Settings\Türker\Application Data
2	Adobe1.exe	Dosya	C:\Documents and Settings\Türker\Local Settings\Temp

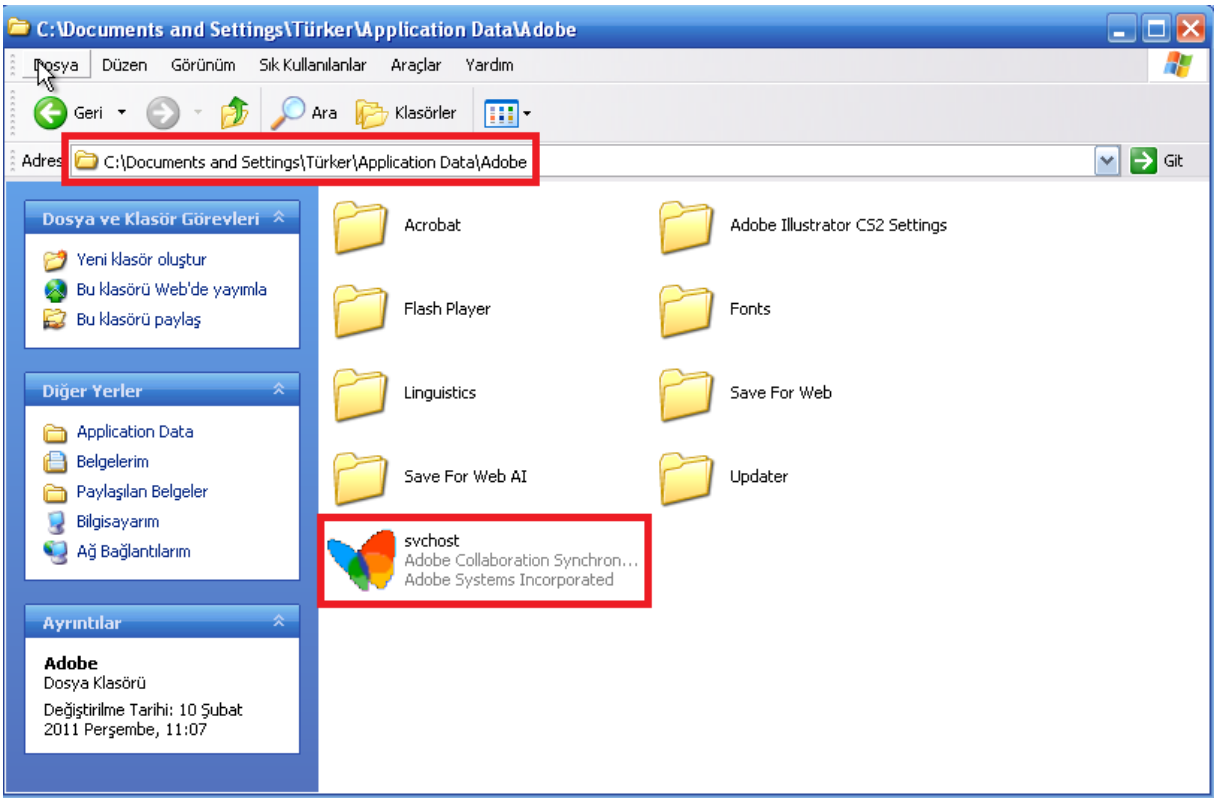
3	Adobe1.exe	MFT	C:\$MFT
4	Adobe1.exe	LogFile	C:\$LogFile
5	Reader.pdf	Dosya	C:\Documents and Settings\Türker\Local Settings\Temp
6	Reader.pdf	MFT	C:\$MFT
7	Reader.pdf	LogFile	C:\$LogFile
8	Dhq.dll	Dosya	C:\Documents and Settings\Türker\Local Settings\Temp
9	Dhq.dll	MFT	C:\$MFT
10	Dhq.dll	LogFile	C:\$LogFile
11	iso88591	Dosya	C:\Documents and Settings\Türker\Desktop
12	iso88591	MFT	C:\$MFT
13	iso88591	LogFile	C:\$LogFile
14	Duyuru.pdf	Dosya	C:\<Duyuru.pdf dosyasının çalıştırıldığı yer>\Duyuru.pdf
15	Duyuru.pdf	MFT	C:\$MFT
16	Duyuru.pdf	LogFile	C:\$LogFile
17	Duyuru.pdf.lnk	Dosya	C:\Documents and Settings\Türker\Recent
18	Duyuru.pdf.lnk	MFT	C:\$MFT
19	Duyuru.pdf.lnk	LogFile	C:\$LogFile
20	Svchost.exe	Dosya	C:\Documents and Settings\Türker\Application Data\Adobe\
21	Svchost.exe	MFT	C:\$MFT
22	Svchost.exe	LogFile	C:\$LogFile
23	AdobeReader	Registry	HKCU\Software\AdobeReader
24	{B6A807N6-42DF-4W02-93E5-B156B3FA8AL1}	Registry	HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Tablo 13. Duyuru.pdf kötücül yazılımı çalıştırıldığında ortaya çıkan izler

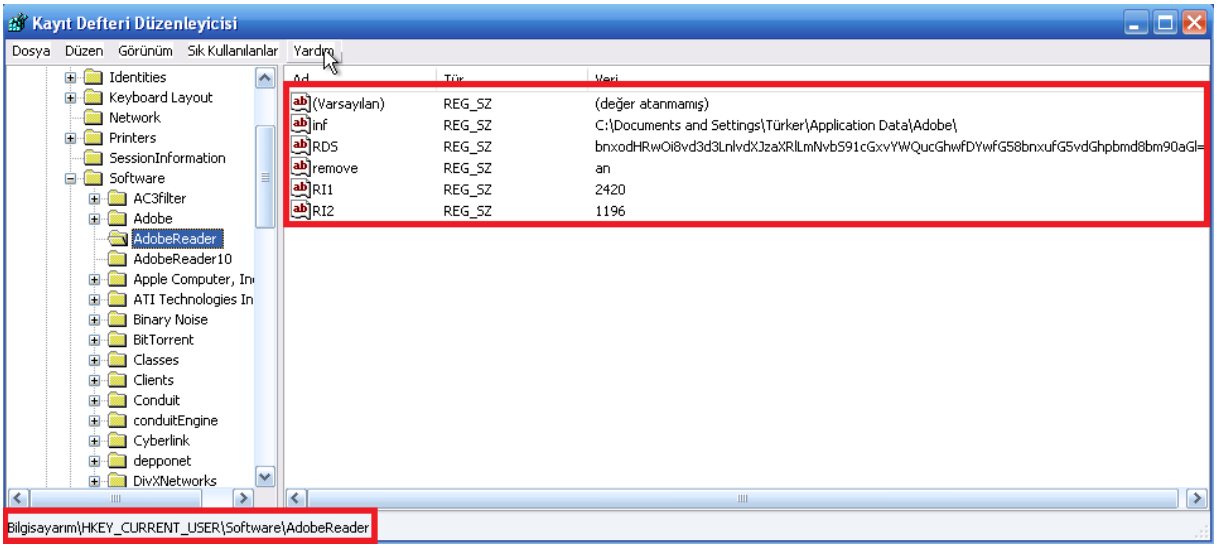
Aşağıdaki ekran görüntülerinden de görülebileceği gibi yukarıdaki listede yer alan izlerden en önemlilerinin Delil 1 bilgisayarı üzerinde bulunduğu ve zararlı yazılım prosesinin çalıştığı görülmüştür. Bu sebeplerle “Duyuru.pdf” dosyasının açılmış olduğu ve bu dosyadan bulaşan kötücül yazılımın bilgisayar üzerinde etkin olduğu kanaatine varılmıştır.



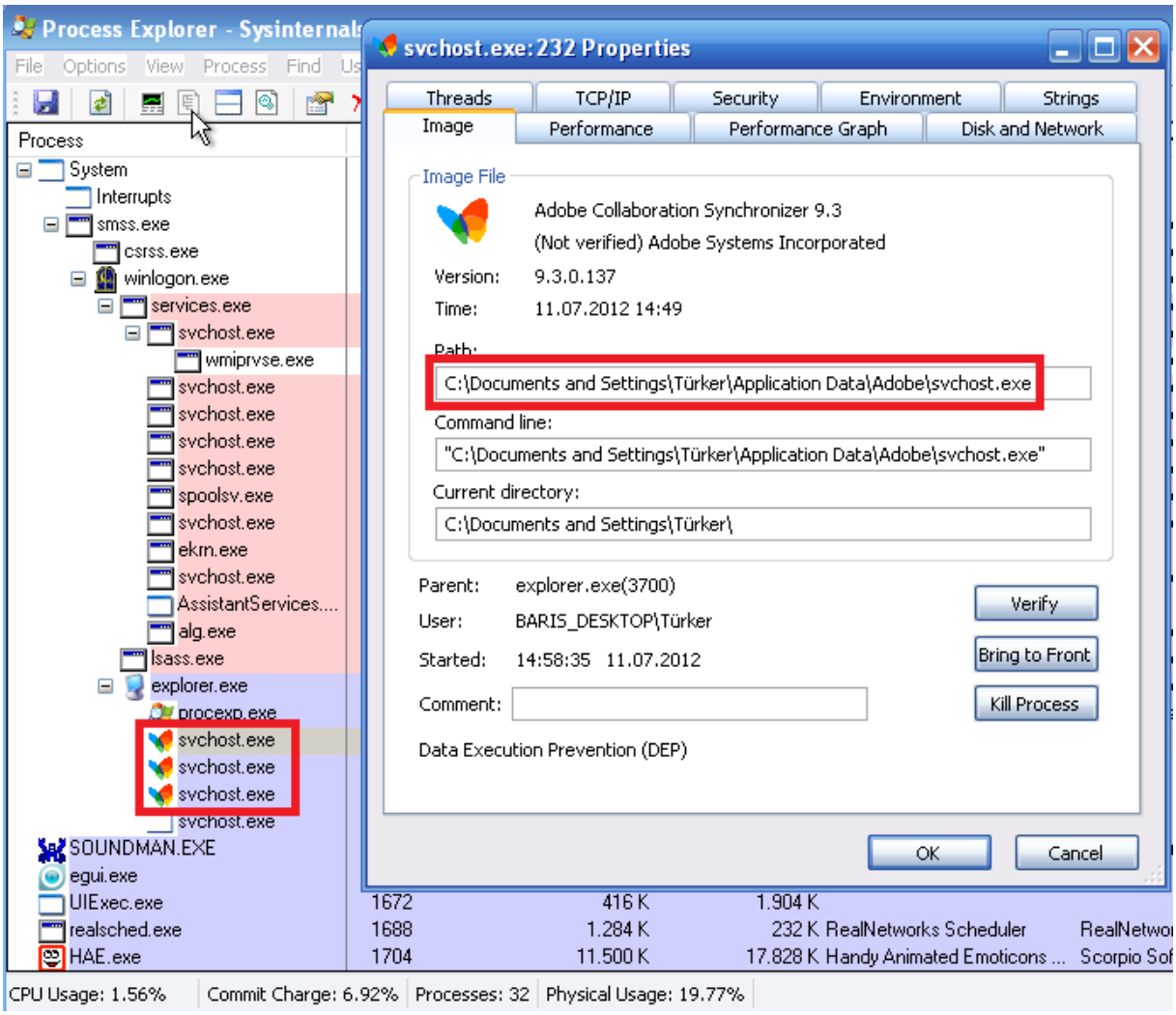
Şekil 107. Delil 1 duyuru.pdf.lnk dosyası



Şekil 108. Delil 1 svchost.exe dosyası



Şekil 109. Delil 1 AdobeReader registry dosyası



Şekil 110. Delil 1 çalışan svchost.exe prosesleri

Oluşturulan ek dosyalar dışında, “Duyuru.pdf” dosyasının çalıştırılması sonrası “svchost.exe” dosyasının oluşturulması ve bulunduğu yer, oluşturulan registry anahtarı ve içerisindeki değerler, oluşturulan otomatik çalıştırma anahtarı ve değeri, xxx.html dosyasının oluşturulması gibi işlemler, Delil 3 bilgisayar kullanıcısına gönderilen “AKPkarikatürleri.zip” dosyasında bulunan kötücül yazılımların gerçekleştirdiği işlemlere benzemektedir. Ayrıca, Virustotal web sitesinden yapılan tarama sonucunda hem “AKPkarikatürleri.zip” dosyasında bulunan kötücül yazılımlar hem de “Duyuru.pdf” dosyasının çalıştırılması sonrası oluşan “svchost.exe” dosyası “Bandook RAT” türü bir trojan olarak tespit edilmiştir. “Bandook RAT” birçok bilgisayarda yaygın olarak bulunabilen ve saldırgana göre konfigürasyon ayarları değişebilen bir zararlı yazılımdır. İki farklı bilgisayardaki “Bandook RAT” türü zararlı yazılımlar tarafından bağlanılmaya çalışılan adreslerin her ikisinde de

"adobupdate.serveftp.com" ve "adobupdate.servehttp.com" olması, bu dosyaların aynı saldırgan tarafından gönderilmiş olma ihtimalini oldukça arttırmaktadır.

Delil 2 Bilgisayarındaki Hedefli Saldırı Olabilecek Kötücül Yazılımların Analizi

Delil 1 bilgisayarından erişilen Barist@odatv.com e-posta hesabına e-posta yolu ile gönderilen "Ataturk_Ekrankoruma.scr" ve "Duyuru.pdf" dosyalarının, aynı şekilde Delil 2 bilgisayarından erişilen, Barış Pehlivan'a ait Barisp@odatv.com e-posta hesabına da e-posta yoluyla gönderildiği tespit edilmiştir.

Hedefli bir saldırı olduğundan şüphelenilen e-postanın ekinde yer alan "Ataturk_Ekrankoruması.scr" dosyasının hem Delil 1 hem de Delil 2'de zararlı olarak tespit edilip otomatik olarak engellenmesinden dolayı bu dosyanın detaylı analizi yapılmamış fakat "Virustotal" üzerinde çoklu virüs tarama sonucu Delil 1'de ile ilgili bölümde verilmiştir.

"Duyuru.pdf" Analiz Sonuçlarının Delil 2'de Aranması

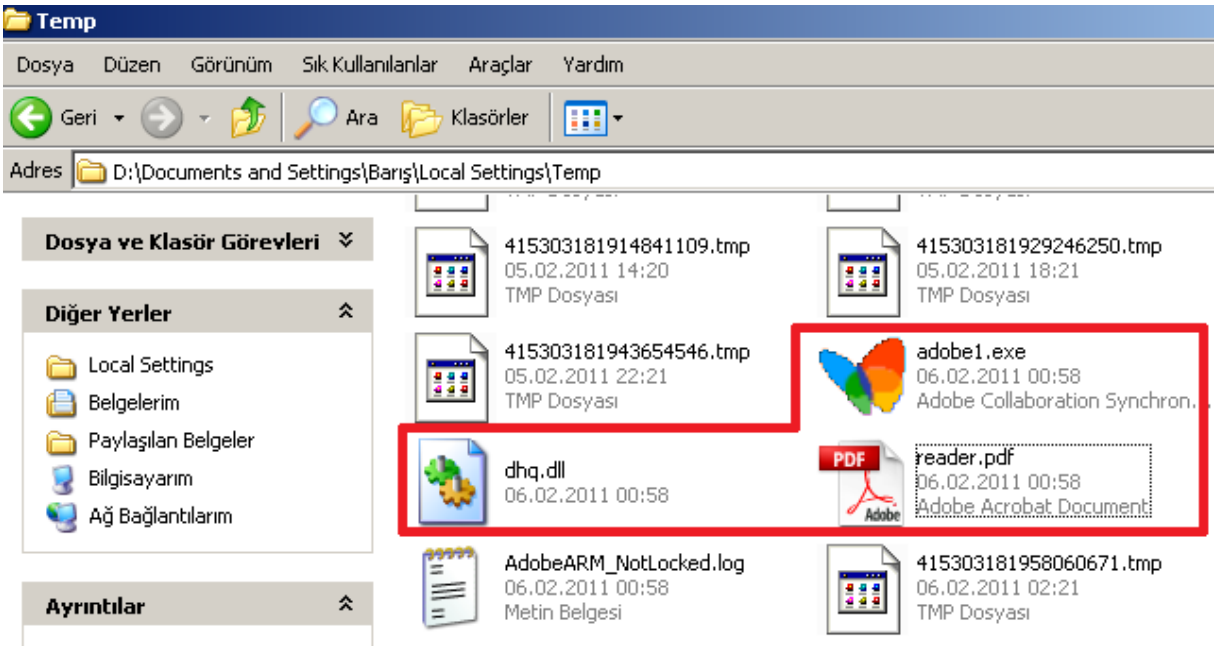
"Duyuru.pdf" dosyasının analizi Delil 1 bilgisayarı için gerçekleştirilmiş ve bu dosyanın bilgisayar üzerinde oluşturduğu dosyalar ve kayıtlar ile kullanılan işletim sistemi tarafından oluşturulan ve adli analiz yöntemleriyle elde edilen kayıtların tümü Tablo 13'de listelenmiştir. Bu izler ve bu izlerden Delil 2'de tespit edilenler 'de gösterilmiştir.

No	Kayıt	Türü	Kaydın Yeri	Delil 2 üzerinde tespiti
1	Xxx.html	Dosya	D:\Documents and Settings\Barış\Application Data	Yok
2	Adobe1.exe	Dosya	D:\Documents and Settings\Barış\Local Settings\Temp	Var
3	Adobe1.exe	MFT	D:\$MFT	Var
4	Adobe1.exe	LogFile	D:\$LogFile	-
5	Reader.pdf	Dosya	D:\Documents and Settings\Barış\Local Settings\Temp	Var
6	Reader.pdf	MFT	D:\$MFT	Var
7	Reader.pdf	LogFile	D:\$LogFile	-
8	Dhq.dll	Dosya	D:\Documents and Settings\Barış\Local Settings\Temp	Var
9	Dhq.dll	MFT	D:\$MFT	Var
10	Dhq.dll	LogFile	D:\$LogFile	-

11	iso88591	Dosya	D:\Program Files\Common Files\System\MSMAPI\1055	Var
12	iso88591	MFT	D:\$MFT	Var
13	iso88591	LogFile	D:\$LogFile	-
14	Duyuru.pdf	Dosya	D:\Documents and Settings\Barış\Local Settings\Temporary Internet Files\OLK4\Duyuru.pdf	Var
15	Duyuru.pdf	MFT	D:\$MFT	Var
16	Duyuru.pdf	LogFile	D:\$LogFile	-
17	Duyuru.pdf.lnk	Dosya	D:\Documents and Settings\Barış\Recent	Yok
18	Duyuru.pdf.lnk	MFT	D:\$MFT	Yok
19	Duyuru.pdf.lnk	LogFile	D:\$LogFile	-
20	Svchost.exe	Dosya	D:\Documents and Settings\Barış\Application Data\Adobe\	Yok
21	Svchost.exe	MFT	D:\$MFT	Yok
22	Svchost.exe	LogFile	D:\$LogFile	-
23	AdobeReader	Registry	HKCU\Software\AdobeReader	Yok
24	{B6A807N6-42DF-4W02-93E5-B156B3FA8AL1}	Registry	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	Yok

Tablo 14. Duyuru.pdf izleri ve Delil 2'de tespiti

Tablo 14'de listelenen 24 izden net olarak 10 iz tespit edilmiştir. Aşağıdaki ekran görüntülerinden de görülebileceği gibi, Delil 2 imajı sanal makinaya dönüştürülüp çalıştırılması sonucu, Tablo 13'de yer alan izlerden "Duyuru.pdf" dosyası çalıştırılması sonrası oluşan dosyaların oluştuğu görülmektedir. Bunun yanında "C:\Windows\Prefetch" klasörü altındaki "SVCHOST.EXE-14EE9BB2.pf" dosyasının incelenmesi sonucu iz 20 de belirtilen "Svchost.exe" dosyasının bilgisayarda oluşturulduğu ve ilk olarak "02/06/11 01:26:34" tarihinde, son olarak da "02/13/11 02:07:08" tarihinde çalıştırıldığı tespit edilmiştir. İmajın son halinde iz 20, 23 ve 24'ün bulunmaması, bu zararlı yazılımın el konulmadan önce kendi kendini sildiğine veya bir virüs koruma tarafında silindiğine işaret etmektedir.



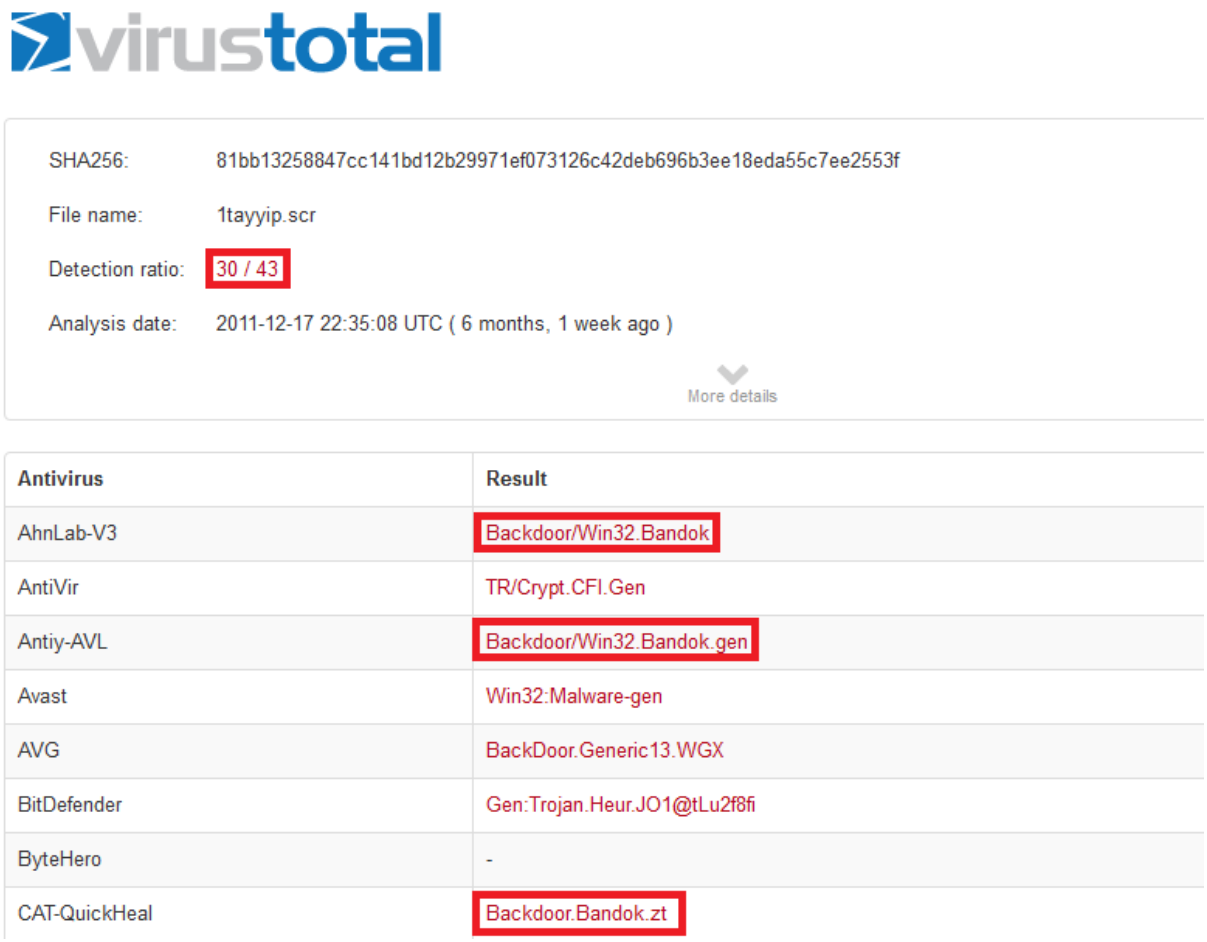
Şekil 111. Delil 2 Temp klasörü altındaki dosyalar

Delil 3 Bilgisayarındaki Hedefli Saldırı Olabilecek Kötücül Yazılımların Analizi

Delil 3 bilgisayarı kullanıcısı Müyesser Yıldız'a e-posta yoluyla gönderildiği belirtilen ve incelenmek üzere CD ile teslim edilen "AKPkarikatürleri.zip" ve "kayseri.rar" arşiv dosyalarında bulunan kötücül yazılımlar incelenmiştir.

"AKPkarikatürleri.zip" Analizi

"05.02.2011 23:34" tarihinde gönderilen e-posta ile gelen, "AKPkarikatürleri.zip" arşiv dosyası açılmış ve içinde "0tayyip2it2.scr" ve "1tayyip.scr" adında iki dosya olduğu görülmüştür. Bu dosyaların özet (hash) değerleri kontrol edildiğinde, aynı özet değerine sahip oldukları yani bu iki dosyanın aynı içeriğe sahip dosyalar oldukları tespit edilmiştir. Bu dosyaların "Virustotal" adındaki websitesi üzerinde birden çok antivirüs yazılımına taratılması sonucu, "Bandook RAT" türü bir truva atı (trojan) olduğu görülmüştür.



SHA256: 81bb13258847cc141bd12b29971ef073126c42deb696b3ee18eda55c7ee2553f

File name: 1tayyip.scr

Detection ratio: 30 / 43

Analysis date: 2011-12-17 22:35:08 UTC (6 months, 1 week ago)

More details

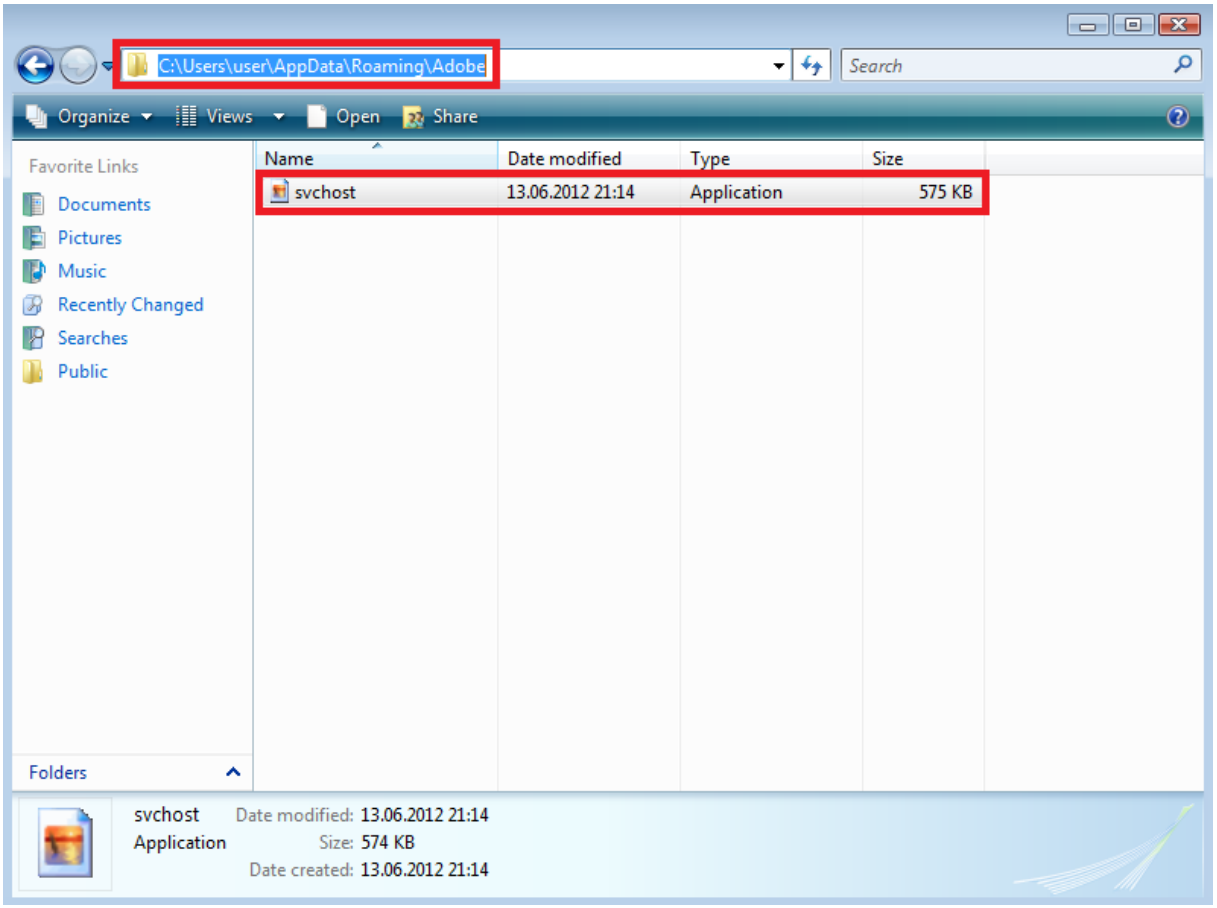
Antivirus	Result
AhnLab-V3	Backdoor/Win32.Bandok
AntiVir	TR/Crypt.CFI.Gen
Antiy-AVL	Backdoor/Win32.Bandok.gen
Avast	Win32:Malware-gen
AVG	BackDoor.Generic13.WGX
BitDefender	Gen:Trojan.Heur.JO1@tLu2f8fi
ByteHero	-
CAT-QuickHeal	Backdoor.Bandok.zt

Şekil 112. 1tayyip.scr Virustotal tarama sonucu

Analiz sırasında yapılan adımlar ve kötücül yazılımın gerçekleştirdiği tespit edilen işlemler aşağıda sıralanmıştır.

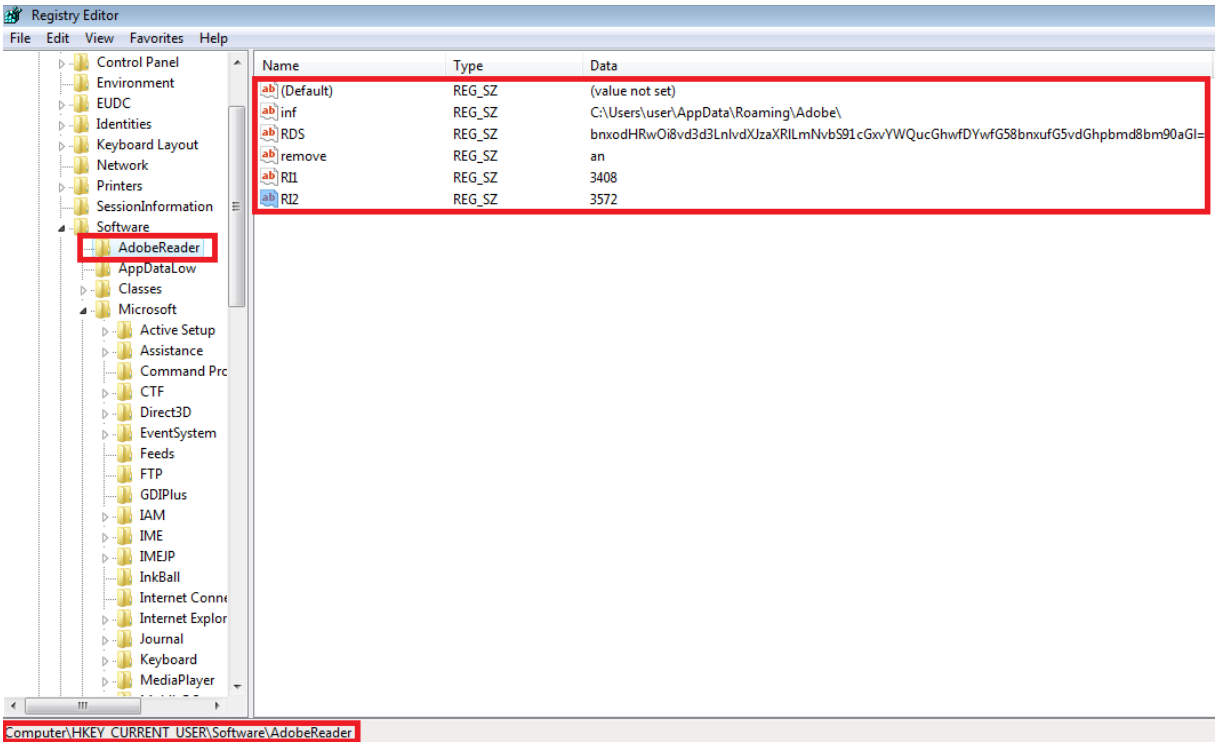
a. E-posta'nın gönderildiği kişiye ait delil imajında Microsoft Windows Vista işletim sisteminin kurulu olduğu görülmüştür. Bu işletim sistemine ait kurulum dosyası, Microsoft Technet web sitesinden indirilmiştir.
    a. İşletim Sistemi Adı: Windows Vista (x86) - DVD (English)
    b. Dosya adı: en_windows_vista_x86_dvd_x12-34293.iso
    c. Bağlantı adresi: http://technet.microsoft.com/en-us/subscriptions/downloads/#searchTerm=&ProductFamilyId=146&Languages=en&PageSize=10&PageIndex=5&FileId=0
b. İndirilen işletim sistemi kurulum dosyası kullanılarak, analizin yapılacağı bilgisayara ilgili işletim sistemi kurulmuştur. Kurulum sırasında ilgili delil imajına uygun olarak;
    a. İşletim sistemi versiyonu "Vista Home Premium" seçilmiştir.
    b. Kullanıcı oluşturma ekranında "user" adında şifresi boş olan bir kullanıcı oluşturulmuştur.
c. İşletim sistemi kurulması sonrasında, gerekli sistem ayarları yapılmış ve analiz işleminde kullanılacak yardımcı araçlar kurulmuştur.

d. İnceleme için gerekli araçlar çalıştırıldıktan sonra, "AKPkarikatürleri.zip" dosyası içinde bulunan "0tayyip2it2.scr" adındaki kötücül yazılım çalıştırılmıştır. Aynı dosya olduklarından ve aynı işlemleri gerçekleştirdiklerinden dolayı "1tayyip.scr" dosyası ayrıca belirtilmemiştir
e. "0tayyip2it2.scr" kötücül yazılımı tarafından bilgisayar üzerinde gerçekleştirilen işlemler genel olarak aşağıda sıralanmıştır:
    a. "C:\Users\user\AppData\Roaming" klasörü altında "xxx.html" adında kısa süreli oluşup silinen bir dosya oluşturur.
    b. İexplore.exe prosesini, registry kayıtlarından .html uzantılı dosyaları çalıştıracak olan yazılım nedir tespit ederek çalıştırır.
    c. Notepad.exe prosesini çalıştırır.
    d. "C:\Users\user\AppData\Roaming\Adobe" klasörü altında "svchost.exe" adında çalıştırılabilir bir dosya oluşturur.



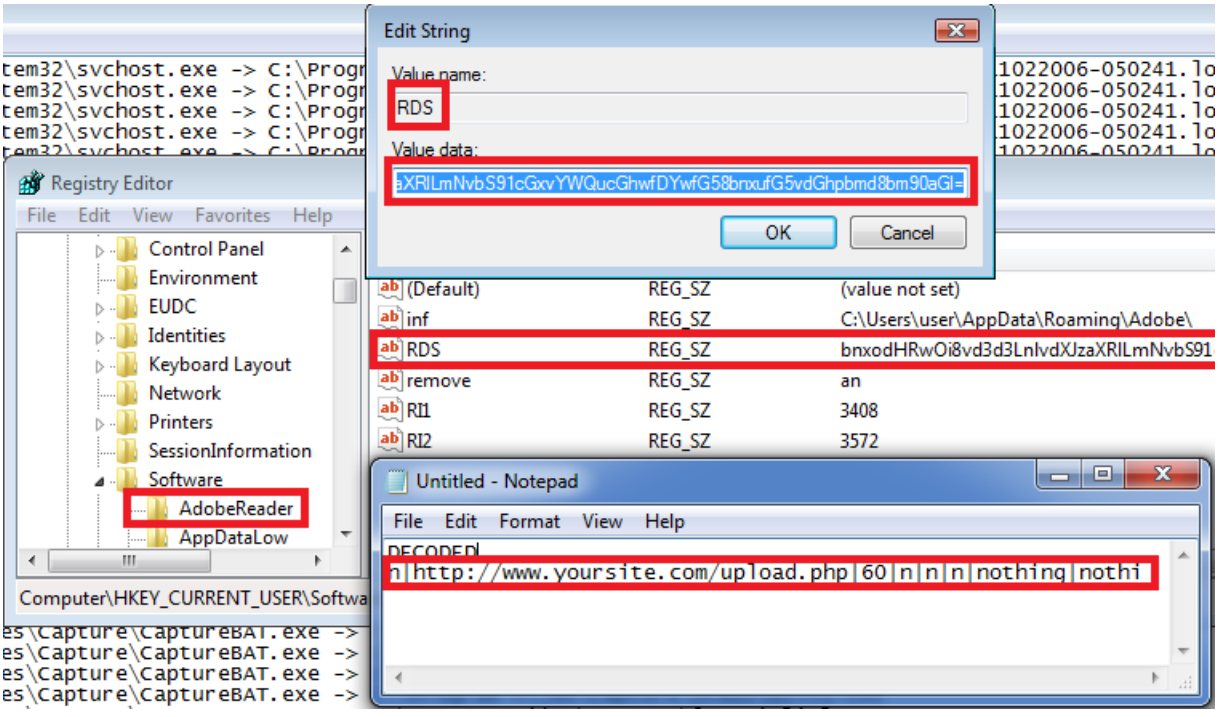
Şekil 113. 0tayyip2it2.scr svchost dosyasının yeri

e. Registry kayıtlarında "HKCU\Software\AdobeReader" anahtarı ve altında "inf", "RDS", "remove", "RI1" ve "RI2" değerleri oluşturur.



Şekil 114. 0tayyip2it2.scr oluşturulan registry anahtarı

i. İnf değeri, oluşturulan "svchost.exe" dosyasının yolunu tutmaktadır. (C:\Users\user\AppData\Roaming\Adobe\svchost.exe)
ii. RDS değeri, birçok parametre ile birlikte bir web sitesi adresi içeren, Base64 yöntemi kullanılarak kodlanmış bir veri tutmaktadır.



Şekil 115. 0tayyip2it2.scr registry RDS değeri

iii. RI1 ve RI2 değerleri, başlatılan iki farklı “notepad.exe” prosesinin proses numaralarını tutmaktadır.

f. Bilgisayarın her açılışında, oluşturulan “svchost.exe” dosyasının otomatik olarak çalıştırılması için registry üzerinde kayıt oluşturur.

i. Registry anahtarı: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

ii. Registry değer adı: {B6A807N6-42DF-4W02-93E5-B156B3FA8AL1}

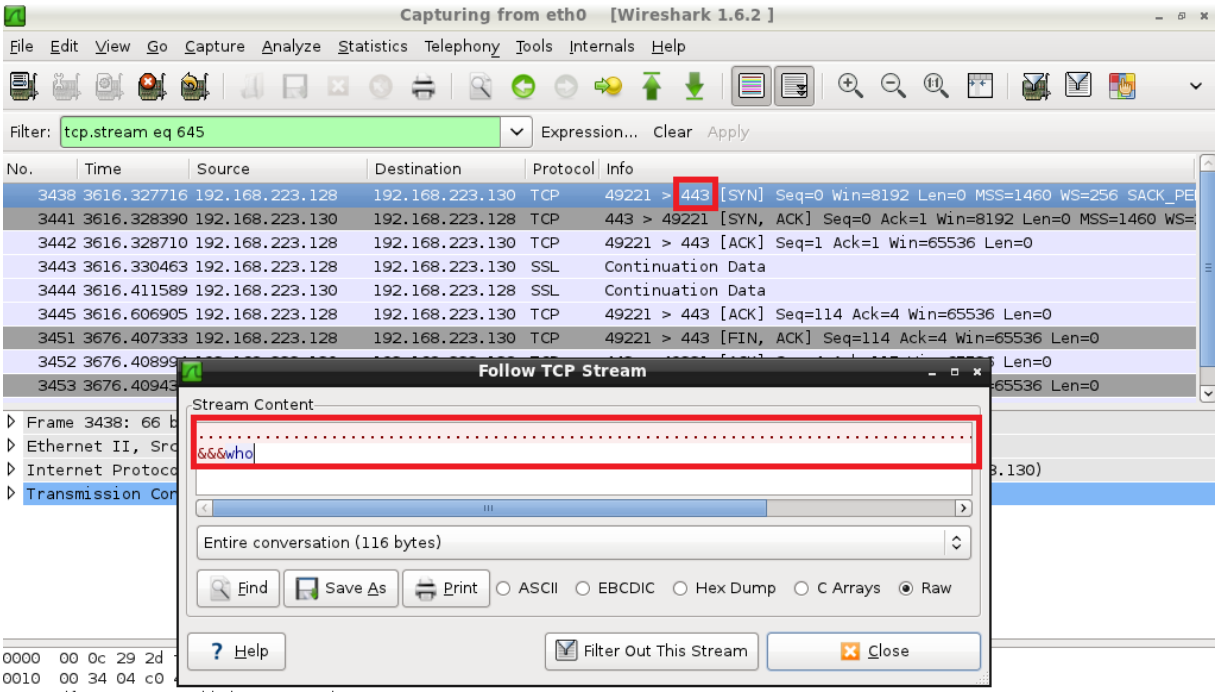
iii. Registry değeri: C:\Users\user\AppData\Roaming\Adobe\svchost.exe

f. “0tayyip2it2.scr” kötücül yazılımının ağ ve internet üzerinde gerçekleştirdiği işlemler aşağıda sıralanmıştır:

a. “adobupdate.serveftp.com” ve “adobupdate.servehttp.com” web adreslerine bağlanabilmek için, bu adreslerin IP adreslerini çözmeye yönelik DNS sorgusu göndermektedir.

b. Başarılı DNS çözümlemesi sonrası, “adobupdate.serveftp.com” ve “adobupdate.servehttp.com” web adreslerine 443 portu üzerinden bağlantı kurmaya çalışmaktadır.

c. Bağlantı sırasındaki iletişimi görebilmek için, bağlantı bir analiz bilgisayarına yönlendirilmiş ve üzerinde 443 portunu dinleyen bir uygulama çalıştırılmıştır. Bu işlem sonrası, zararlı yazılım analiz bilgisayarına 443 portundan bağlantı kurmuş ve SSL ile şifreli bir iletişime geçmiştir. Bu iletişimin, zararlı yazılımın bağlantı için parola istemesinden dolayı, devam etmeyip kesildiği düşünülmektedir.



Şekil 116. 0tayyip2it2.scr SSL iletişimi

g. “0tayyip2it2.scr” kötücül yazılımının çalıştırılması sonrasında bilgisayar üzerinde işletim sistemi tarafından oluşturulan ve doğrudan veya adli analiz yapılarak elde edilen kayıtlar aşağıda listelenmiştir. Aynı dosya olmalarına rağmen isim farklılığı

sebebiyle farklı kayıtların oluşmasından dolayı, “1tayyip.scr” dosyası ayrıca belirtilmiştir.

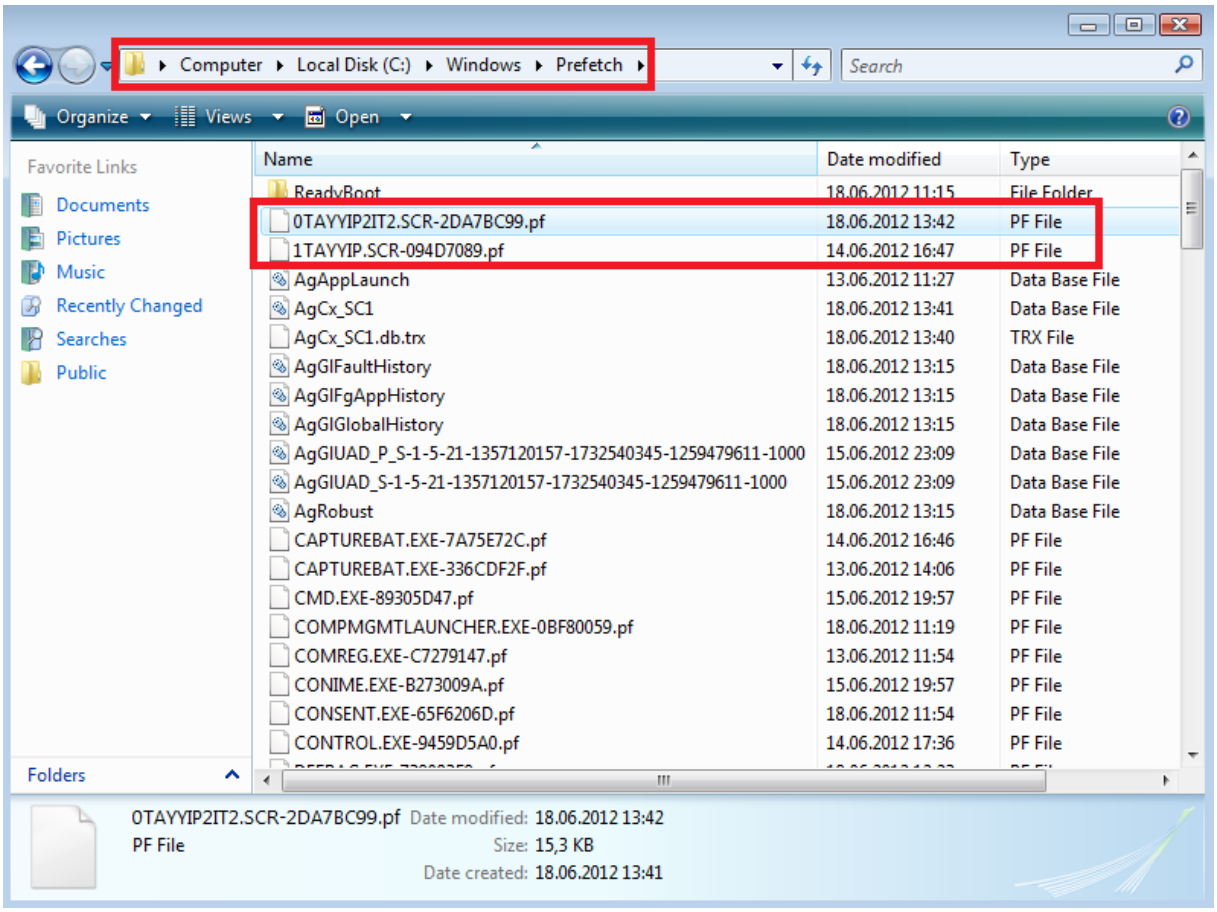
a. $MFT dosyasında, çalıştırılan “0tayyip2it2.scr” ve “1tayyip.scr” dosyalarına ait kayıtların oluşturulduğu görülmüştür.

Dosya Tipi	**Dosya Adı**
Dosya	/Users/user/Desktop/karikaturler/0tayyip2it2.scr
Dosya	/Users/user/Desktop/karikaturler/1tayyip.scr

b. $MFT dosyasında, “0tayyip2it2.scr” veya “1tayyip.scr” dosyaları çalıştırılması sonrası oluşturulan “svchost.exe” adlı dosya kaydının oluşturulduğu görülmüştür.

Dosya Tipi	**Dosya Adı**
Dosya	/Users/user/AppData/Roaming/Adobe/svchost.exe

c. C:\Windows\Prefetch klasörü altında, başlangıç sırasında dosyaların daha hızlı yüklenmesi ve uygulamaların daha hızlı çalıştırılması için, “0tayyip2it2.scr” ve “1tayyip.scr” dosyaları için ayrı ayrı .pf uzantılı dosyaların oluşturulduğu görülmüştür.

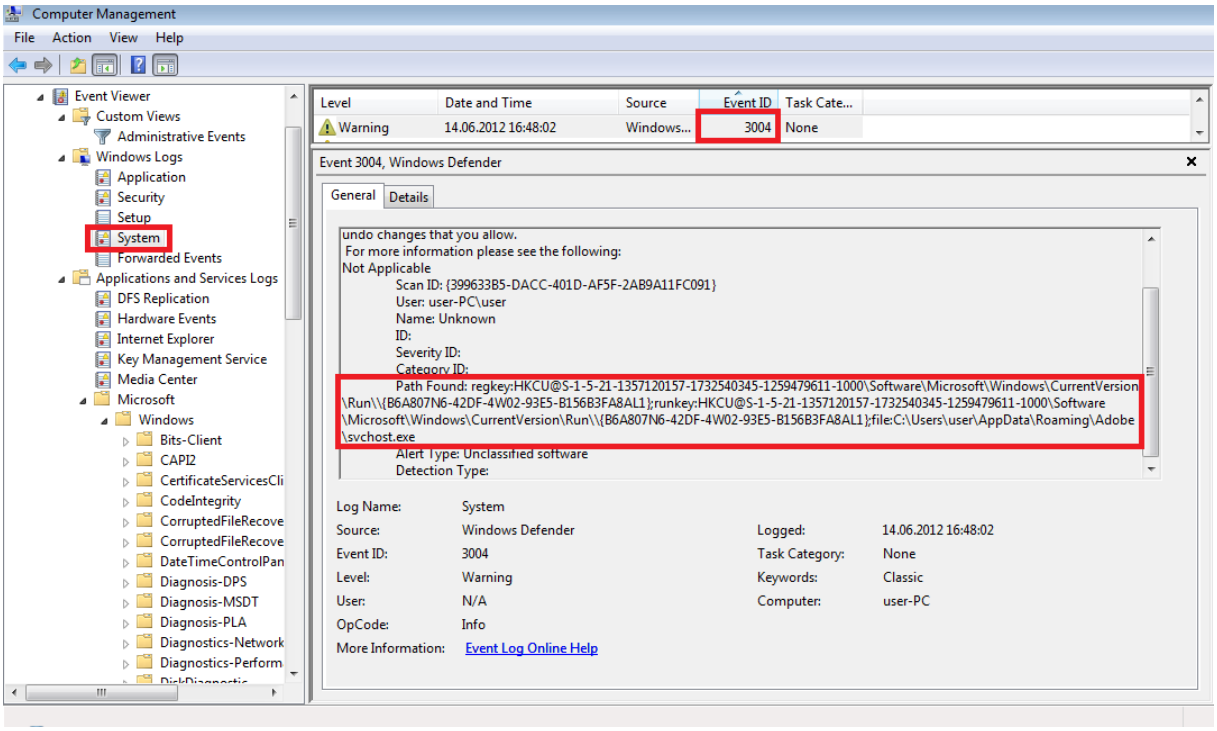


Şekil 117. 0tayyip2it2.scr ve 1tayyip.scr prefetch dosyaları

d. $MFT dosyasında, yukarıda gösterilen .pf uzantılı prefetch dosyalarının kayıtlarının oluşturulduğu görülmüştür.

Dosya Tipi	Dosya Adı
Dosya	/Windows/Prefetch/0TAYYIP2IT2.SCR-2DA7BC99.pf
Dosya	/Windows/Prefetch/1TAYYIP.SCR-094D7089.pf

e. Prefetch klasöründe oluşan .pf uzantılı dosyaların, $LogFile dosyasında kayıtlarının bulunduğu görülmüştür.
f. Otomatik çalıştırılma için registry kaydı oluşturulması sırasında, Windows Olay Görüntüleyicisinin Sistem bölümünde bir olay kaydı oluştuğu görülmüştür.



Şekil 118. 0tayyip2it2.scr sistem olay kaydı

"AKPkarikatürleri.zip" Analiz Sonuçlarının Delil 3'te Aranması

Yapılan analiz sonrası, e-posta yoluyla gönderilen "0tayyip2it2.scr" ve "1tayyip.scr" dosyalarının bilgisayar üzerinde oluşturduğu dosyalar ve kayıtlar ile kullanılan işletim sistemi tarafından oluşturulan ve adli analiz yöntemleriyle elde edilen kayıtların tümü Tablo 15'de listelenmiştir. Ayrıca her bir kayıt için, bu kaydın Delil 3 bilgisayarında bulunup bulunmadığı da gösterilmiştir.

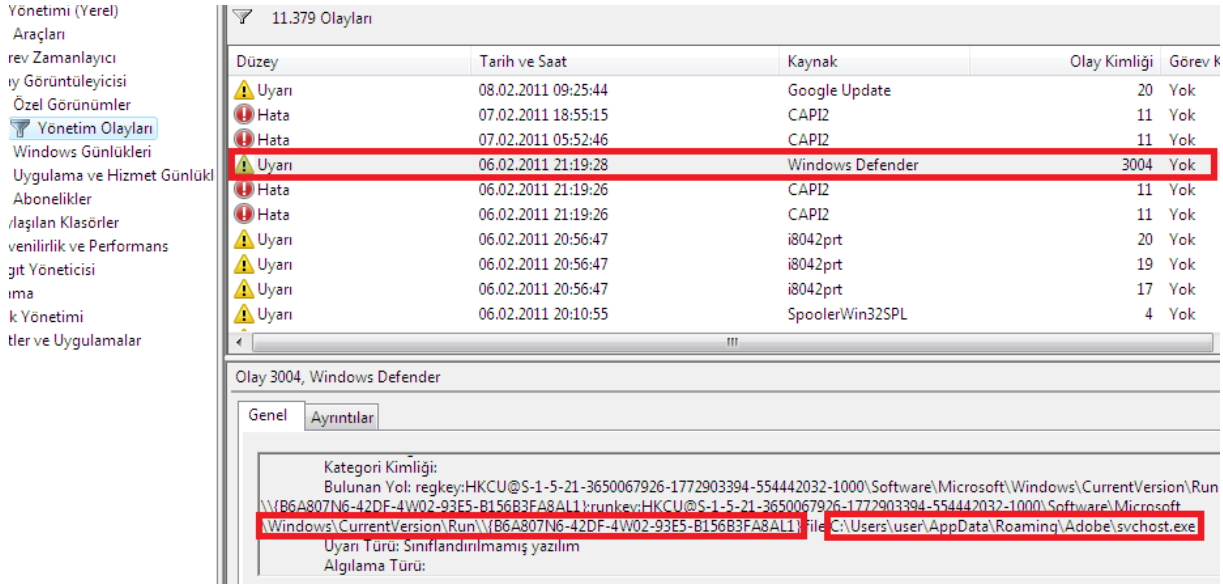
No	Kayıt	Türü	Kaydın Yeri	Delil 3 üzerinde tespiti
1	Xxx.html	Dosya	C:\Users\user\AppData\Roaming	Yok
2	Svchost.exe	Dosya	C:\Users\user\AppData\Roaming\Adobe	Yok
3	AdobeReader	Registry	HKCU\Software\AdobeReader	Yok
4	{B6A807N6-42DF-4W02-93E5-B156B3FA8AL1}	Registry	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	Yok
5	0tayyip2it2.scr	MFT	C:\$MFT	Yok

6	1tayyip.scr	MFT	C:\$MFT	Yok
7	0tayyip2it2.scr	LogFile	C:\$LogFile	Yok
8	1tayyip.scr	LogFile	C:\$LogFile	Yok
9	Svchost.exe	MFT	C:\$MFT	Yok
10	Svchost.exe	LogFile	C:\$LogFile	Yok
11	0TAYYIP2IT2.SCR-2DA7BC99.pf	Prefetch	C:\Windows\Prefetch	Yok
12	1TAYYIP.SCR-094D7089.pf	Prefetch	C:\Windows\Prefetch	Yok
13	0TAYYIP2IT2.SCR-2DA7BC99.pf	MFT	C:\$MFT	Yok
14	1TAYYIP.SCR-094D7089.pf	MFT	C:\$MFT	Yok
15	0TAYYIP2IT2.SCR-2DA7BC99.pf	LogFile	C:\$LogFile	Yok
16	1TAYYIP.SCR-094D7089.pf	LogFile	C:\$LogFile	Yok
17	Windows Defender – 3004	Event	C:\Windows\System32\winevt\Logs\System.evtx	Var

Tablo 15. Akpkarikatürleri.zip izleri ve Delil 3'te tespiti

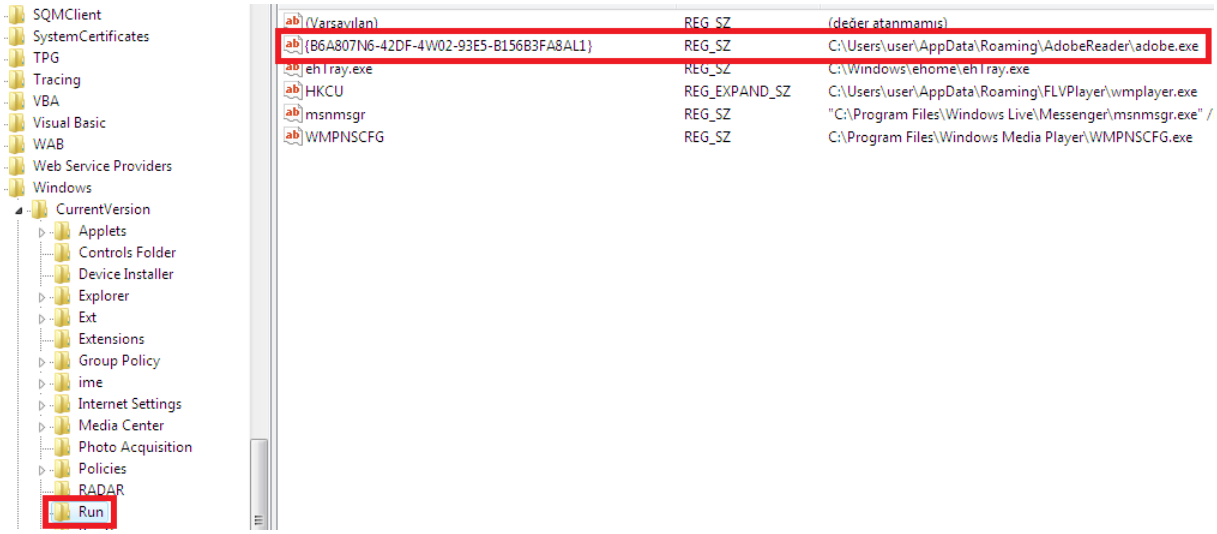
Tablo 15'de listelenen 17 izden, net olarak sadece bir iz ve kısmi olarak iki iz bulunabilmiştir. Delil 3 bilgisayarında tespit edilebilen bu izler şu şekildedir:

a. 17 numaralı iz aşağıdaki ekran görüntüsünde görüldüğü gibi tespit edilebilmiştir.



Şekil 119. Akpkarikatürleri.zip delil 3 olay kaydı

b. 1 numaralı izin kendisi tespit edilememiş fakat sadece dosya ismi disk üzerindeki unallocated cluster alanında tespit edilmiştir.
c. 4 numaralı iz ile ilgili olarak, otomatik çalıştırma registry değer adı tespit edilmiş fakat registry değerinin farklı olduğu görülmüştür. Registry değeri olarak, kötücül yazılımın çalışması sonrası oluşturulan asıl virüs dosyası olan "svchost.exe" olması gerekirken, bunun yerine "adobe.exe" adında farklı bir dosyanın bulunduğu görülmüştür.



Şekil 120. Akpkaritakurleri.zip delil 3 otomatik çalıştırma kaydı

Bu izlerin yanında "C:\Windows\prefetch\NOTEPAD.EXE-3D2AFDB4.pf" dosyasının incelenmesi sonucu:

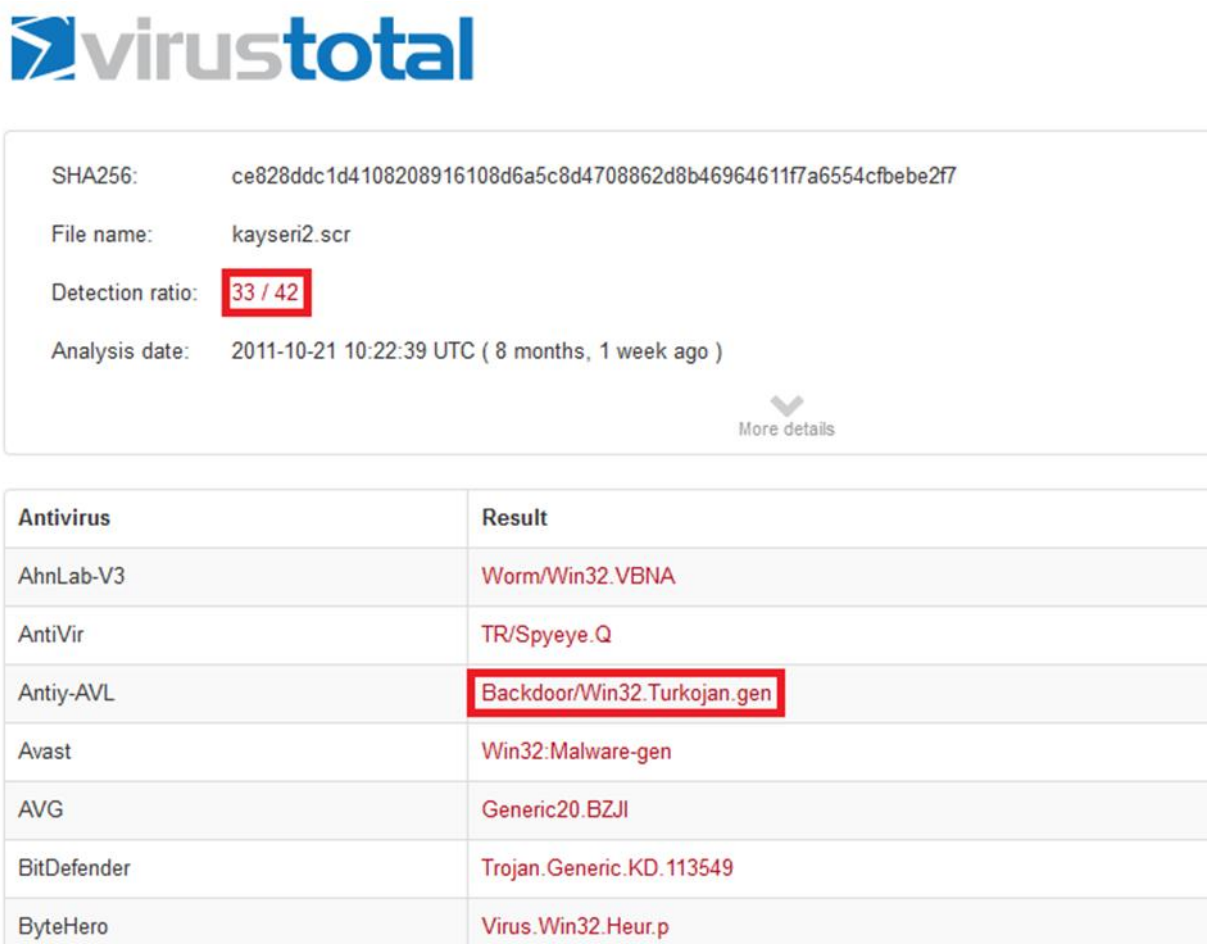
- "Notepad.exe" programının ilk çalıştırılma tarihinin "02/06/11 21:19:03" olduğu tespit edilmiştir. Bu tarih Windows olay kaydının oluşturulduğu zamana gayet yakındır ve yukarıdaki analiz de belirtildiği gibi, ilgili zararlı yazılım ilk çalışması sırasında "Notepad.exe" prosesini çalıştırması senaryosuna uygundur.
- "Notepad.exe" prosesinin en son çalışması sırasında "WSOCK32.DLL" ve "WININET.DLL" gibi internet üzerinde haberleşmeye yarayan ve normal şartlarda "notepad.exe" uygulaması tarafından kullanılmayan kütüphaneleri de yüklediği görülmektedir. Bu durum, ilgili prosesin içinde "dll injection" tarzı yöntemlerle saklı olarak çalışan zararlı yazılımlara işaret etmektedir.

Üstte belirtilen bulgular sonucunda, e-posta yoluyla gönderilen "0tayyip2it2.scr" ve "1tayyip.scr" dosyalarının bilgisayar üzerinde çalıştırıldığı, daha sonrada ya kendisi kendisini sildiği veyahut bir virüs yazılımı tarafından silindiği düşünülmektedir.

Bu inceleme sırasında göze çarpan diğer bir zararlı yazılım ise bilgisayarın imajının alınması sırasında yukarıdaki bilgiler ışığında aktif olduğu görülen "C:\Users\user\AppData\Roaming\AdobeReader\adobe.exe" dosyasıdır. Bu yazılımın "VirüsTotal" internet sayfasında incelenmesi sonucunda "Bandok.Rat" türü bir zararlı yazılım olduğu tespit edilmiştir. Bu sebeple yukarıda analiz edilen zararlı yazılım ile aynı tür olduğu anlaşılan bu zararlı yazılımın bilgisayara geliş zamanı, Windows olay kayıtları oluşturduğu kayıt sayesinde "27.02.2011 19:55:56" olarak tespit edilmiştir.

"Kayseri.rar" Analizi

"24.01.2011 20:59" tarihinde gönderilen e-posta ile gelen "Kayseri.rar" arşiv dosyası açılmış ve içinde "kayseri2.scr" adında bir dosya olduğu görülmüştür. Bu dosya "Virustotal" adındaki websitesi üzerinden birden çok antivirüs yazılımına taratılması sonucu, bu dosyanın "Turkojan RAT" türü bir truva atı (trojan) olduğu görülmüştür.



Şekil 121. Kayseri2.scr Virustotal tarama sonucu

Yukarıda "AKPkarikatürleri.zip" dosyası içindeki zararlı yazılımlar için yapılan ve adım adım anlatılan analiz "kayseri.rar" dosyası içinde bulunan "kayseri2.scr" zararlı yazılımı için de yapılmıştır.

"Kayseri.rar" Analiz Sonuçlarının Delil 3'te Aranması

Yapılan analiz sonrası, e-posta yoluyla gönderilen "kayseri2.scr" dosyalarının bilgisayar üzerinde oluşturduğu dosya ve kayıtlar ile kullanılan işletim sistemi tarafından oluşturulan ve adli analiz yöntemiyle elde edilen kayıtların tümü birden aşağıdaki tabloda listelenmiştir. Ayrıca her bir kayıt için, bu kaydın Delil 3 bilgisayarında bulunup bulunmadığı da gösterilmiştir.

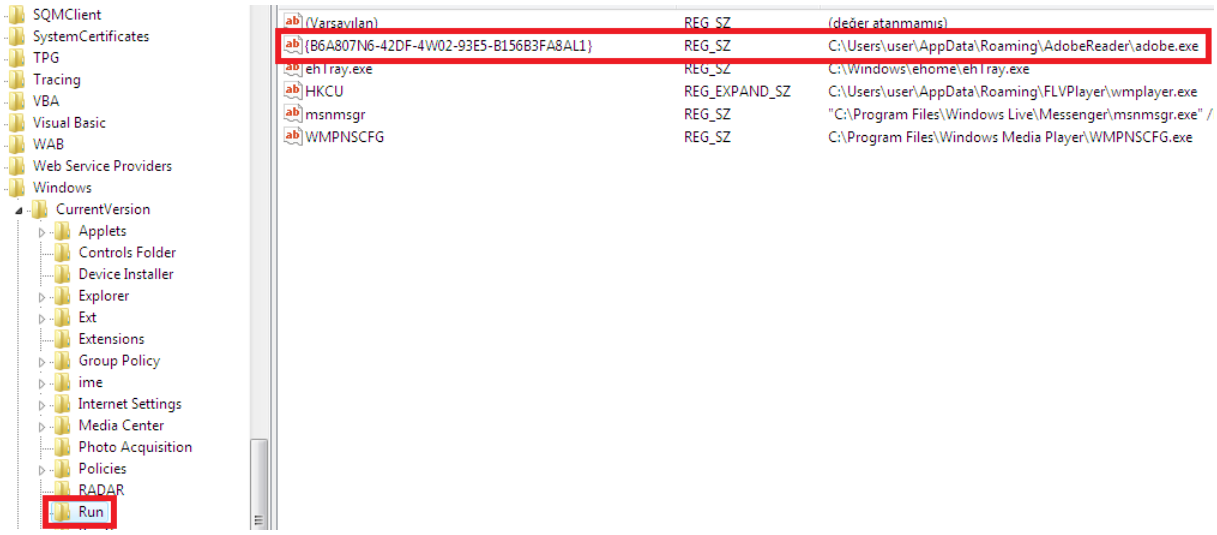
No	Kayıt	Türü	Kaydın Yeri	Delil 3 üzerinde tespiti
1	Xxx.html	Dosya	C:\Users\user\AppData\Roaming	Yok

2	Rssr.exe	Dosya	C:\Users\user\AppData\Roaming\Rss Folder	Yok
3	Rss	Registry	HKCU\Software\Rss	Yok
4	{B6A807N6-42DF-4W02-93E5-B156B3FA8AL1}	Registry	HKCU\Software\Microsoft\Windows\Current Version\Run	Yok
5	Kayseri2.scr	MFT	C:\$MFT	Yok
6	Kayseri2.scr	LogFile	C:\$LogFile	Yok
7	Rssr.exe	MFT	C:\$MFT	Yok
8	Rssr.exe	LogFile	C:\$LogFile	Yok
9	KAYSERI2.SCR-28265EBD.pf	Prefetch	C:\Windows\Prefetch	Yok
10	KAYSERI2.SCR-28265EBD.pf	MFT	C:\$MFT	Yok
11	KAYSERI2.SCR-28265EBD.pf	LogFile	C:\$LogFile	Yok
12	Windows Defender – 3004	Event	C:\Windows\System32\winevt\Logs\System.evtx	Yok

Tablo 16. Kayseri.rar izleri ve Delil 3'te tespiti

Yukarıdaki 12 izden, net iz bulunamamış fakat kısmi olarak iki iz bulunabilmiştir. Delil 3 bilgisayarında tespit edilebilen bu izler şu şekildedir:

a. 1 numaralı izin kendisi tespit edilememiş fakat dosya ismi disk üzerindeki unallocated cluster denilen kullanılmayan alanda tespit edilmiştir.
b. 4 numaralı iz ile ilgili olarak, otomatik çalıştırma registry değer adı tespit edilmiş fakat registry değerinin farklı olduğu görülmüştür.



Şekil 122. Kayseri.rar delil 3 otomatik çalıştırma kaydı

"Kayseri2.scr" dosyasının çalıştırılması sonrası oluşan ve yukarıda sıralanan 12 izden net olarak hiç birine ulaşılamaması, kısmi olarak bulunan 2 izin de "kayseri2.scr" dosyanın çalıştırılması ile oluşmayıp, başka bir zararlı yazılım tarafından oluşturulmuş olma ihtimali yüksek olduğu için, "kayseri2.scr" dosyasının bilgisayar üzerinde çalıştırılmadığı kanaatine varılmıştır.

Zararlı Yazılım Analiz Sonucu

Yapılan incelemeler sonucunda; ilgili bilgisayar kullanıcılarını özel olarak hedef olan sosyal mühendislik saldırılarının mevcut olduğu, bu saldırılarla ile gönderilen zararlı yazılımların uzaktan yönetim ve dosya atma kabiliyetlerinin bulunduğu ve bu zararlı yazılımların kısa bir süre de olsa aktif olarak ilgili bilgisayarlarda çalıştığı kanaatine varılmıştır. Bu zararlı yazılımlar vasıtasıyla ilgili bilgisayarlara uzaktan dosya aktarma işleminin yapılmış olması mümkündür. Fakat bahse konu olan dosyaların bu zararlı yazılımlar vasıtasıyla geldiğini veya gelmediği konusunda yorum yapabilmek için, dosya üstverilerindeki uyumsuzluk tespit edilmesi ve dosyaların varlığından kullanıcıların haberdar olduğunu işaret eden işletim sistemi izlerinin de incelenmesi gerekmektedir. Bu konulardaki ayrıntılı incelemeler cevap 5 bölümde her dosya için ayrı ayrı yapılmıştır.

Soru 13.)

Sanık müdafilerince soruşturma ve kovuşturma aşamasında haricen aldırılarak dosyaya sunulan ve ekli olarak gönderilen özel görüş raporlarının, soruşturma aşamasında C.Savcılığı tarafından aldırılan teknik raporların ayrı ayrı irdelenerek, özel görüş raporları ve teknik raporlar hakkında açıklama ve değerlendirmede bulunulması?

Cevap 13.)

Analiz sürecinde mahkeme tarafından teslim edilen;

- "07.04.2011" tarihli Boğaziçi Üniversitesi tarafından hazırlanan adli analiz raporu,
- "25.08.2011" tarihli Emniyet Genel Müdürlüğü tarafından hazırlanan adli analiz raporu ve "AYRINTILI TEKNİK RAPOR" başlıklı adli analiz raporu,
- "21.10.2011" tarihli ODTÜ Üniversitesi tarafından hazırlanan adli analiz raporu,
- "16.12.2011" tarihli Yıldız Teknik Üniversitesi raporu,
- "21.12.2011" tarihli DataDevastation raporu ve
- "22.12.2011" tarihli Yıldız Teknik Üniversitesi raporu

incelenmiştir. Genel olarak bu raporlarda, bahse konu olan dokümanların el konulan bilgisayarlar kullanıcılarına ait olup olmadığı; bu dosyaların hangi yollarla bu bilgisayarlara gelmiş olabileceği; bu dosyalar kullanıcının bilgisi dışında, uzaktan yönetim ve dosya atma özelliği bulunan zararlı yazılımlar ve benzeri yöntemler ile gelmiş olabilir mi; bu dosyalar delil niteliği taşır mı ve benzeri sorulara cevaplar verilmeye çalışılmaktadır. Bu sorulara yeterli cevap verebilmek için en azından ilgili bilgisayarlarda şu incelemelerin yapılması gerekmektedir:

- Bahse konu olan dosyaların ilgili imajlarda oluşturulduğuna, değiştirildiğine, açıldığına veya bilgisayar kullanıcısı tarafından orada olduğuna dair herhangi bir bulgu mevcut mu?
- Bahse konu olan dosyalar hangi yollarla bu bilgisayarlara gelmiş olabilir?
- İlgili bilgisayar kullanıcılarını özel olarak hedef almış olan uzaktan yönetim ve dosya atma amaçlı kullanılabilecek zararlı yazılım yükleme saldırıları mevcut mu? Bu saldırılar başarılı olmuş mu?
- Bahse konu olan dosyaların, hedefli saldırılar ile gönderilmiş ve kullanıcılar tarafından çalıştırılmış olduğuna, uzaktan yönetim ve dosya atma özelliği bulunan zararlı yazılımlar vasıtasıyla gönderildiğine dair herhangi bir bulgu var mı? Dosyaya ait üstverilerde herhangi bir uyumsuzluk mevcut mu?

Bu bağlamda yazılan bilirkişi raporları incelendiğinde:

- Boğaziçi Üniversitesi, Emniyet Genel Müdürlüğü, ODTÜ Üniversitesi ve Yıldız Teknik Üniversitesinin hazırladığı raporlarda;, bahse konu olan dosyaların kullanıcılar tarafından mevcudiyetinin bilindiğine dair bulgulardan veya açıldığında işletim sistemi üzerinde oluşacak izlerin araştırıldığından bahsedilmemektedir.
- Emniyet raporlarında bilgisayarlarda bulunan zararlı yazılımlar ve bu bilgisayar kullanıcılarını özel olarak hedef alan sosyal mühendislik saldırılarının olası etkileri üzerinde durulmamıştır. Boğaziçi Üniversitesi, Emniyet Genel Müdürlüğü ve ODTÜ Üniversitesi ve Yıldız Teknik Üniversitesinin hazırladığı raporlarda ise kullanıcıları hedef alan sosyal mühendislik saldırıları ile gönderilen zararlı yazılımlar ayrıntılı bir şekilde incelenmemiştir. Özellikle Yıldız Teknik raporlarında hedefli sosyal mühendislik saldırılarından hiç bahsedilmemiştir. Boğaziçi raporunda ise, bilirkişilerin ellerinde bilgisayar imajı bulunmadığı için, birçok kritik analizin yanında zararlı yazılımlar ve hedefli saldırılar hakkında bir araştırma yapılamamıştır.
- Emniyet raporlarında ve zararlı yazılımlara atıf yapan DataDevastation raporunda bahse konu olan dosyaların bu zararlı yazılımlar ile gelmiş olduğuna dair herhangi bir bulgudan bahsedilmemiştir. Yıldız Teknik raporlarında ise bahse konu dosyaların zararlı yazılımlar ile gönderilmiş olduğuna dair delil olarak sunulan bulguların tamamına yakını adli analiz kaideleri içinde yeterli ve doğru değildir. Aynı şekilde, Boğaziçi raporunda bu konuda bulgu olarak atfedilen yorumlar doğru değildir. Bu iddialar ve açıklamaları ayrıntılı bir şekilde aşağıda verilmiştir.

Bilirkişi raporlarında bahsi konu olan dosyaların zararlı yazılımlar ile gönderildiğine veya değiştirildiğine dair bulgu olduğu iddia edilerek yapılan belli başlı hatalar ve açıklamaları aşağıda verilmiştir:

1. Yorum ve Cevap

Boğaziçi raporunda, silinmiş dosyaları inceleme amacıyla kullanılmış olan “Active Undelete” programı adli analiz amacıyla kullanılan ve bu konuda kabul görmüş bir araç değildir. Raporda birkaç dosya için verilen “Dosya siliniş tarih ve zamanı”, dosyaların gerçek silinme zamanını yansıtmamaktadır. Windows XP işletim sistemi ve NTFS dosya sisteminde bir dosyanın silindiği zamanın bilgisi tutulmamaktadır. Bu kuralın bir istisnası olarak çöp kutusuna gönderme durumu verilebilir ama ilgili dosyalarda bu durum söz konusu değildir.

2. Yorum ve Cevap

DataDevastation raporunda silinmiş komut dosyaları (Deleted Command Files) olarak tespit edilen “C:\Windows” klasörü altındaki “sed.exe” ve “grep.exe” dosyalarının virüs sahipleri tarafından konulmuş veya kullanılmış olabileceği iddia edilmiştir. Bu dosyaların zararlı

yazılım sahipleri tarafından konulmuş ve kullanılmış ihtimali vardır. Fakat bilgisayar üzerinde kurulmuş olduğu tespit edilen ve zararlı yazılım temizleme aracı olarak kullanılan "ComboFix"[18] programı ile gelmiş olma ihtimalinin daha yüksek olduğu değerlendirilmektedir. "C:\ComboFix.txt" dosyasının MFT kaydı son değiştirme zamanının "12/27/10 15:08:19" olması ve "sed.exe" ve "grep.exe" dosyalarının da MFT son değiştirme zamanlarının buna çok yakın bir zaman olan "12/27/10 14:49:21" olması bunu desteklemektedir.

3. Yorum ve Cevap

16.12.2011 tarihli Yıldız Teknik raporunda geçen: "Dosyaya son yazım tarihi, dosyanın disk üzerindeki yaratılma tarihinden eskidir. Bu durum, bu dosyanın kesinlikle incelenen bilgisayarda oluşturulmadığını, bir başka bilgisayarda hazırlandığını ve incelenen bilgisayarda hiç değiştirilmediğini göstermektedir." ifadesi teknik olarak doğru değildir. Bu konuda ayrıntılı bilgi cevap 5'te verilmiştir.

4. Yorum

16.12.2011 tarihli Yıldız Teknik raporunda; *"koz.doc", "Fabrikatör.doc","Ulusal Medya.doc", "Tv Analiz Proje.doc", "Reosta Operasyonu.doc", "toplantı.doc", "teRTEmiz.doc", "Bilinçlendirme.doc" ve "Sn.Komutanım.doc" dosyalarının silinen alanlarında "mbvd.exe", "9b9w3.exe", "b00ijwpu.exe", "mbdm.exe" olarak bilinen virüslerin izlerine rastlandığı, "mbvd.exe", "9b9w3.exe", "b00ijwpu.exe", "mbdm.exe" virüslerinin kullanıcının isteği dışında yabancı adreslere internet bağlantısı kurma, bilgisayarda çalışan diğer uygulamalara karışma, bilgisayardaki dosyalar üzerinde işlem yapma, bilgisayara dosya kopyalama, dosya silme gibi işlemler yapabilme kabiliyetinin olduğu, ayrıca yukarıda adı geçen dosyaların silinmesinde bu virüslerin rol oynadığının mütalaa edildiği* bildirilmiştir.

4. Cevap

Yapılan incelemeler sonucunda zararlı yazılım izi olarak adlandırılan verilerin, yukarıda belirtilen "doc" uzantılı dosyalardan önce sabit diskin aynı yerini kullanmış, içinde açık metin (clear text) olarak "mbvd.exe", "9b9w3.exe", "b00ijwpu.exe", "mbdm.exe" isimlerinin geçtiği eski dosyaların kalıntıları olduğu tespit edilmiştir. Bu eski dosya kalıntılarına, "doc" uzantılı dosyaların dosya boşluğunda (file slack) rastlanmıştır. Dosya boşluğu, bir dosyanın kullandığı son sabit disk sektöründe, sektör boyutunun bu alana yazılacak dosya verisinden fazla olmasından kaynaklanan boş alandır. Bu boş alanda da daha önceden bu sektörü kullanan dosyaların kalıntıları olabilmektedir. Bir dosyanın dosya boşluğu alanında (file slack) bulunan verilerle o dosyanın bir ilişkisi yoktur. Bu yüzden yukarıda listenen "doc" uzantılı dosyaların, içinde açık metin olarak bazı dosya isimlerinin geçtiği daha eski dosyalarla

[18] http://www.combofix.org/

herhangi bir ilişkisi bulunmamaktadır. Ayrıca bir zararlı yazılımın kullandığı dosya isimlerinin bir dosyada geçmesi ile bu zararlı yazılımın o bilgisayarda çalışmış olduğu anlaşılamaz. Bu konuda daha fazla bilgi için cevap 12 incelenebilir.

"mbvd.exe" [19], "9b9w3.exe"[20], "b00ijwpu.exe"[21], "mbdm.exe"[22] dosya isimlerini kullanan zararlı yazılımlar araştırılmış ve bu isimdeki dosyaları kullanan zararlı yazılımın çevrimiçi oyun şifrelerini çalmak için kullanılan bir zararlı yazılım türü olduğu tespit edilmiştir [23]. Bu zararlı yazılım uzaktan dosya atma amaçlı kullanılamamaktadır.

Sonuç olarak, adı geçen "doc" dosyaları ile alakası olmayan, sadece açık metin olarak virüs dosya isimlerinin geçtiği eski dosya kalıntılarından yola çıkarak ve bu dosya isimleri kullanan zararlı yazılımın da sadece çevrimiçi oyun hesaplarını çalmak için kullanıldığı göz önünde bulundurulduğunda, ilgili dosyaların silinmesinde herhangi bir zararlı yazılımın rol oynadığını mütalaa etmek mümkün değildir.

5. Yorum

16.12.2011 tarihli Yıldız Teknik raporunda; "Nedim.doc" dosyasının yaratılma ve son erişim tarihleri, "koz.doc" dosyası ile birebir aynı olduğu, ancak bu iki dosyaya ait ve aynı olan tarih kayıtları, aynı klasörde silinmiş olarak bulunan başka ve klasörlerle aynı olmadığı, bu durumun iki dosyanın aynı anda silindiğini gösterdiği iddia edilmiştir.

5. Cevap

Bir dosya silindiği zaman MFT tarihlerinde bir değişiklik olmamaktadır. Bu yüzden bir dosyanın ne zaman silindiği veya hangi dosyayla beraber silindiği ortak olan yaratılma ve son erişim tarihlerinden anlaşılamaz.

6. Yorum

16.12.2011 tarihli Yıldız Teknik raporunda, *"simon son.doc" dosyasının disk üzerinde silinmiş ya da silinmemiş olarak mevcut olmadığı, "simon son.doc" dizgesinin ham imaj kaydı üzerinde aranması ile, sadece $MFT ve $Logfile dosyalarının yazıldığı disk alanlarında geçtiği, ancak $MFT ve $Logfile dosyaların çözümlenmesinde, incelenen dosya ile ilgili herhangi bir kayda rastlanmadığı, bu durumun normal kullanıcı davranışları ile oluşmayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceğini düşündükleri* belirtilmiştir.

[19] http://r.virscan.org/e64758b3902710575aae89d36b665d1d
[20] http://r.virscan.org/c692ed2823c04070556d4bf0a1d07b55
[21] http://r.virscan.org/35f3c40bd854e5dfcce7fe34b4712ffe
[22] http://r.virscan.org/b506e1446641864e199c90f63fb695a7
[23] www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fTaterf.B

6. Cevap

"simon son.doc" dosyası içerik olarak "Unallocated clusters" alanında mevcuttur. $MFT dosyasında bir kaydı yoktur. $logfile dosyasında kaydı mevcuttur ve bu kayıt ile "Unallocated clusters" alanındaki dosya verisine ulaşım mümkündür. Ayrıntılı bilgi için cevap 5 incelenebilir. Silinmiş bir dosyanın $MFT kaydının üzerine yazılmış olduğu bir durumda, $logfile dosyasındaki kaydının üzerine yazılmamış olması ve dosya verisinin "Unallocated clusters" alanında duruyor olması normal kullanıcı davranışlarıyla uyumludur, herhangi bir zararlı yazılım işlemiyle ilişkilendirilemez.

7. Yorum

16.12.2011 tarihli Yıldız Teknik raporunda, "EK-D MİLİ EĞİTİM.doc", "Konuşma Notu.doc", "KADROLAŞMA KONUŞMA NOTU(OCAK 2004).doc", "KADROLAŞMA EK_C.doc", "KADROLAŞMA EK_A.doc", "Kardolaşma Bilgi Notu (Ocxak 2004)", "EK-E AKP'nin ATAMALARI.xls", "Prj_60.doc", "Yalçın hoca.doc" ve "SY.doc" dosyalarının disk üzerinde silinmiş ya da silinmemiş olarak mevcut olmadığı, dosya isim dizgelerinin ham imaj kaydı üzerinde aranması ile sadece $logfile dosyasının yazıldığı disk alanında ve boş disk alanında geçtiği ve $MFT dosyasında kayıtlarının olmadığı, $Logfile dosyasının çözümlenmesinde, incelenen dosyalar ile ilgili herhangi bir kayda rastlanmadığı, bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceğini düşündükleri belirtilmiştir.

7. Cevap

"EK-D MİLİ EĞİTİM.doc", "KADROLAŞMA KONUŞMA NOTU(OCAK 2004).doc" dosyalarının $logfile dosyasında iki farklı ve "Konuşma Notu.doc", "KADROLAŞMA EK-C.doc", "KADROLAŞMA EK-A.doc", "Kardolaşma Bilgi Notu (Ocxak 2004)", "EK-E AKP'nin ATAMALARI.xls", "Prj_60.doc", "Yalçın hoca.doc", "SY.doc" dosyalarının $logfile dosyasında birer adet kaydı bulunmaktadır**.** Bunun yanında "EK-D MİLİ EĞİTİM.doc", "KADROLAŞMA KONUŞMA NOTU(OCAK 2004).doc", "Konuşma Notu.doc" , "Kadrolaşma Bilgi Notu (Ocxak 2004)", "Prj_60.doc", "Yalçın hoca.doc", "SY.doc" dosyası olduğu düşünülen dosyalar "unallocated Clusters" alanından kurtarılmıştır. Bu konudaki ekran görüntülerine ve ayrıntılı açıklamalara cevap 5'ten ulaşılabilir.

Silinmiş dosyaların $MFT kayıtlarının ve disk üzerindeki verilerinin üzerine yazılmış olması ve $logfile dosyasında kayıtlarının üzerinde yazılmamış olması olağan bir durumdur. Bu durum normal kullanıcı davranışlarıyla uyumludur, herhangi bir zararlı yazılım işlemiyle ilişkilendirilmesi mümkün değildir.

8. Yorum

16.12.2011 tarihli Yıldız Teknik raporunda, “Ulusal Medya.doc”, ”Fabrikatör.doc”, “Tv Analiz Proje.doc”, “Reosta Operasyonu.doc”, “Panzehir.doc”, “mit medya.doc”, “mafia.doc”, “Ulusal Medya 2010.doc” dosyalarının bilgisayarda yaratılma ve son erişim tarihlerinin birebir aynı olduğu, dosyaya son yazım tarihlerinin ise aynı veya çok yakın olduğu, bu durumun normal kullanıcı davranışlarıyla oluşturulmasının mümkün görünmediği, dosyaların çok benzer tarih özelliklerine sahip olmasının, yaratılma ya da kopyalama ve silme işlemlerinin virüs faaliyeti ile gerçekleştiğine işaret ettiği iddia edilmiştir.

8. Cevap

“Ulusal Medya.doc”, “Fabrikatör.doc”, “Tv Analiz Proje.doc”, “Reosta Operasyonu.doc”, “Panzehir.doc”, “mit medya.doc”, “mafia.doc” dosyalarının hepsinin STD yaratılma ve son erişim tarihleri birebir aynı değil, mikro saniye değerlerinde genelde farklılıklar mevcuttur. Bu durum birden çok dosya aynı anda kopyalandığında karşılaşılan normal bir durumdur. Aynı şekilde dosyalar toplu şekilde kopyalandığında dosya son erişim zamanları da, yeni değer olarak kopyalama zamanını almaktadır.

Dosya son yazım tarihleri ise (son değiştirme zamanı), son değiştirme zamanının aktarımını desteklemeyen protokoller veya uygulamalar (eposta, internet tarayıcıları) aracılığı ile dosya aktarımı yapıldığında değişebilmektedir ve istemci tarafa aktarıldığı zamanın değerini almaktadır. Bu yüzden dosya son yazım tarihinin değişmesi için bir kullanıcının dosya üzerinde değişiklik yapması zorunlu değildir. Dosyaların son yazım tarihlerinin aynı veya yakın olması da olağan dışı bir durum değildir. Sonuç olarak dosyaların çok benzer oluşturma, erişim veya son değiştirme zaman değerlerine sahip olması, yaratılma ya da kopyalama ve silme işlemlerinin zararlı yazılım faaliyeti ile gerçekleştiğine işaret etmez. Bu zaman değerlerinin nasıl yorumlanabileceği hususunda cevap 5 incelenebilir.

9. Yorum

16.12.2011 tarihli Yıldız Teknik raporunda, “Kadrolaşma en son0610170003.doc” dizgesinin disk üzerinde yer almadığı iddia edilmiştir.

9. Cevap

“Kadrolaşma en son0610170003.doc” dosyasının kayıtlarına $logfile dosyasında rastlanmıştır. Bununla birlikte dosyanın kendisi de kurtarılabilmiştir. Geri dönüştürülen dosya içeriği, ekran görüntüleri ve daha ayrıntılı bilgi için cevap 5 incelenebilir.

10. Yorum

16.12.2011 tarihli Yıldız Teknik raporunda, "Kadrolaşma Bilgi Notu (ocxak 2004).doc" dosya isminin, "D:\Documents and Settings\EXPER\Belgelerim\Avid Liquid\Data\Media\Reels\@Imported Files0.P001001FC\20492414P 21073809P A1.WAV.pk" dosyasının içinde geçtiği ve bu dosyada aynı zamanda hjvjte.exe virüsüne ait izlerin tespit edildiği belirtilmiştir.

10. Cevap

"20492414P 21073809P A1.WAV.pk" dosyası silinmiş bir dosyadır ve daha önce kullanmış olduğu disk alanını daha sonra başka dosyalar kullanmıştır. "20492414P 21073809P A1.WAV.pk" dosyasının silindikten sonra, daha önce kullanmış olduğu disk alanını kullanan dosyalarla bir ilişkisi bulunmamaktadır. Bu disk alanını kullanan diğer dosyalar arasında da bir ilişki kurulması mümkün değildir. Aynı şekilde dosya isimlerinin silinmiş bir dosyanın disk alanında, özellikle de farklı sektörlerde bulunması ile bu iki dosya arasında bağlantı kurulamaz.

11. Yorum

16.12.2011 tarihli Yıldız Teknik raporunda; "C:\Documents and Settings\Türker\Belgelerim\Documents\aysegül\trt.doc", "C:\Documents and Settings\Türker\Desktop\temizlenecek\CHP.doc", "Hanefi.doc" ve "Sn. komutanım.doc" dosyaları için; $MFT dosyasında işli bulunan son erişim tarihinin, $MFT kayıt tarihinden ileri olduğunun görüldüğü, bu durumun, dosyaya kullanıcı müdahalesi dışında normal olmayan bir yolla erişim yapıldığını gösterdiği iddia edilmiştir.

11. Cevap

Normal kullanıcı işlemlerinden olan dosya erişim ve okuma işlemleri sırasında dosya son erişim tarihi güncellenirken, $MFT kaydı değişim tarihi işletim sistemi tarafından güncellenmek zorunda değildir. Gerçekleştirilen testler sonucunda; Windows XP işletim sisteminde, "doc" uzantılı dosyaların, Microsoft Ofis 2003 programı ile açılmaları neticesinde son erişim tarihinin güncellendiği, fakat $MFT kaydı değişim tarihinin güncellenmediği tespit test edilmiştir.

12. Yorum

16.12.2011 tarihli Yıldız Teknik raporunda; "C:\Documents and Settings\Türker\Desktop\CHP.doc" dosyasının son yazım tarihinin, dosyanın disk üzerindeki yaratılma tarihi ile birebir aynı olduğu, bu durumun, bu dosyanın kesinlikle incelenen bilgisayarda oluşturulmadığını, bir başka ortamdan kopyalandığını gösterdiği, dosyanın

bilgisayara hangi kaynaktan nasıl geldiğininse disk imajından elde edilen verilerle kesin olarak söylenemeyeceği iddia edilmiştir.

12. Cevap

Bu dosya için son değiştirme zamanı, dosya oluşturma zamanı ile birebir aynı değildir. Arada mili saniye mertebesinde de olsa fark vardır ve son değiştirme zamanı ileridedir. Microsoft ofis 2003 programı direk olarak çalıştırılabilir dosyasından (exe) veyahut bu dosyanın kısayolundan açıldıktan sonra hazırlanan doküman ilk defa kaydedildiğinde dosya son değiştirme zamanı ile dosya oluşturma zamanı arasında mili saniye mertebesinde fark oluştuğu ve son değiştirme zamanın daha ileri olduğu yapılan testlerle de kontrol edilmiştir. Sonuç olarak bu işlem ve bu durum normal bir kullanıcı davranışıdır. Diğer taraftan bu dosyanın, bilgisayar kullanıcısı tarafından oluşturulmuş ve değiştirilmiş olabileceğine dair bulgular tespit edilmiştir. Bu bulgular için cevap 5 incelenebilir.

13. Yorum

22.12.2011 tarihli Yıldız Teknik raporunda; "prj_60.doc", "Ulusal Medya 2010.doc", "teRTEmiz.doc", "Bilinçlendirme.doc" ve "Sn.Komutanım.doc" dosyalarının $MFT kaydının bulunmadığı, bunun da dosyaların normal kullanıcı işlemleri ile kaydedilmediğini gösterdiği iddia edilmiştir.

13. Cevap

"prj_60.doc", "Ulusal Medya 2010.doc", "teRTEmiz.doc", "Bilinçlendirme.doc", "Sn.Komutanım.doc" dosyalarının MHV2060BH_NW18T6229459'de sadece $logfile dosya sistemi dosyasında isimleri geçmektedir. Bu konuda ayrıntılı bilgi için cevap 5 incelenebilir. Bir dosyanın mft kaydının üzerine yazılmış olması ve logfile kaydı üzerine yazılmamış olması dosya sisteminde sıkça karşılaşılan normal bir durumdur. Bu sebeple bu durum ilgili dosyaların normal kullanıcı işlemleri ile kaydedilmediğini göstermez.

14. Yorum

22.12.2011 tarihli Yıldız Teknik raporunda; "Ulusal Medya 2010.doc", "Bilinçlendirme.doc" ve "Sn.Komutanım.doc" dizgelerinin ham imaj üzerinde aranması ile, bu dizgelerin sadece $Logfile dosyalarının yazıldığı disk alanlarında geçtiğinin görüldüğü, diskte incelenen dosya ile ilgili herhangi bir kayda rastlanmadığı, bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceğini düşündükleri belirtilmiştir.

14. Cevap

"Ulusal Medya 2010.doc", "Bilinçlendirme.doc" ve "Sn.Komutanım.doc" dosyalarının isimleri MHV2060BH_NW18T6229459 seri numaralı imajda $logfile dosya sistemi dosyasında geçmektedir fakat dosyaların kendisi kurtarılamamıştır. Bu konuda ayrıntılı bilgi için cevap 5 incelenebilir. Bir dosyanın isminin $logfile dosyasında geçmesi fakat "Unallocated clusters" da bulunamaması bu dosya verisini bulunduran disk bölgesinin üzerine başka dosya verilerinin yazıldığı anlamına gelmektedir. Bu durum dosya sistemlerinde sıkça karşılaşılan normal bir durumdur. Zararlı yazılım kaynaklı bir işlemle yapıldığını düşündürecek herhangi bir bulgu yoktur.

15. Yorum

22.12.2011 tarihli Yıldız Teknik raporunda; "prj_60.doc" dizgesinin ham imaj üzerinde aranması ile, sadece $MFT ve $Logfile dosyalarının yazıldığı disk alanlarında geçtiğinin görüldüğü, ancak $MFT ve $Logfile dosyalarının çözümlenmesinde incelenen dosya ile ilgili herhangi bir kayda rastlanmadığı, bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceği düşüncesinde oldukları belirtilmiştir.

15. Cevap

"prj_60.doc" dosya ismi $logfile dosya sistemi dosyasının çözümlenmesi neticesinde tespit edilmiştir. Bu konuda ayrıntılı bilgi için cevap 5 incelenebilir.

16. Yorum

22.12.2011 tarihli Yıldız Teknik raporunda; "teRTEmiz.doc" dizgesinin ham imaj üzerinde aranması ile $Logfile dosyasının yazıldığı disk alanında ve "D:\BARIS YEDEK 1112209" klasörü dosya sistemi index dosyasında ($I30) geçtiğinin görüldüğü, index kaydında yer almasına rağmen diskte mevcut bulunmayan dosyanın normal kullanıcı davranışları ile silinmediğinin anlaşıldığı, bu bulgulara rağmen diskte incelenen dosya ile ilgili herhangi bir kayda rastlanmadığı, bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceği düşüncesinde oldukları belirtilmiştir.

16. Cevap

"teRTEmiz.doc" ve "Sn.Komutanım.doc" dosya isimleri "D:\BARIS YEDEK 1112209" klasörü index dosyasında, kullanılmayan alan (unused space) olarak işaretlenen bölümde geçmektedir[24]. Bu durum daha önceden bu klasörde bulunan "teRTEmiz.doc" ve "Sn.Komutanım.doc" isimli dosyaların bu klasörden silindiği anlamına gelmektedir ve sıkça

[24] File System Forensic Analysis by Barian Carrier, Chapter 13, Index Attributes and Data Structures

karşılaşılan normal bir durumdur. “teRTEmiz.doc” ve “Sn.Komutanım.doc” dosya isimlerinin herhangi bir klasörün index dosyasının kullanılmayan alanında geçmesi ve bu dosya verilerinin disk üzerinde bulunamaması, bu dosyaların silindiği ve dosya verilerinin üzerine başka dosyaların yazıldığı anlamına gelmektedir. Bu durum normal kullanıcı davranışlarıyla oluşabilen bir durumdur ve herhangi bir zararlı yazılım tarafından gerçekleştirildiğine dair bir bulgu mevcut değildir.

Soru 14.)

Sanık Müdafilerince ve Sanık HANEFİ AVCI tarafından dosyaya sunulan, ekli olarak gönderilen dilekçelerde belirtilen konularla ilgili olarak, açıklama ve değerlendirmede bulunulması rica olunur.

Cevap 14.)

Dilekçelerde yöneltilen sorulara yönelik açıklama ve değerlendirmeler aşağıda verilmiştir.

Av. Celal Ülgen'in 30.01.2012 tarihli dilekçesinde yönelttiği sorular

Soru 1.)

"Trojen" (Truva Ati), "Spam", "Virüs" ve "Zombi Bilgisayar" kavramları ne anlama gelmektedir? Bir bilgisayarda "Trojen", "Spam" ve "Virüs" gibi zararlı yazılımların tespit edilmesi halinde söz konusu bilgisayara kötü niyetli 3. kişiler tarafından uzaktan erişim sağlanması mümkün müdür? Bu durumda o bilgisayar üzerinde kötü niyetli 3. kişiler tarafından hangi işlemler yapılabilecektir? Bu işlemler arasında doküman ekleme, silme ve değiştirme olanağı bulunmakta mıdır?

Cevap 1.)

Truva atı (Trojan horse)

Truva atı ya da trojan kendisini olduğundan farklı ve tehlikesiz göstererek gizleyebilen zararlı bir programdır. Bu programlar kullanıcıya arzu edilen bir fonksiyonu yerine getirecek bir yazılım olarak görünen, aslında kullanıcının bilgisayarına izinsiz erişimleri kolaylaştıran bir kötücül yazılımdır. Truva atları kendilerini kopyalamazlar.[25]

Spam

Uluslararası alanda kesin kabul görmüş, üzerinde mutabakat sağlanmış ve çerçevesi tam olarak belirlenmiş bir spam tanımı bulunmamaktadır. Bununla birlikte, aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere zorlayıcı nitelikte gönderilmesine spam denmektedir. İstek dışı haberleşme olarak da adlandırılmaktadır.[26]

[25] BTK, "Köle Bilgisayar ve Köle Bilgisayar Ağları", http://www.cybersecurity.gov.tr/publications/kba.pdf, Şubat 2010

[26] BTK, "E-posta'larda Spam Sorunu ve Çözüm Önerileri", http://www.btk.gov.tr/kutuphane_ve_veribankasi/tezler/Ozgur_OZTURK.PDF, Temmuz 2009

Virüs

Kendi kendini kopyalayabilen ve erişim iznine ihtiyaç duymaksızın sistemlere bulaşabilen programlardır. Virüs kavramı genellikle ve yanlışlıkla reklam ve casus yazılımları gibi kendisini yenileme becerisi olmayan diğer kötücül yazılımları ifade etmek için de kullanılmaktadır. Gerçek bir virüs, bir bilgisayardan başka bir bilgisayara ancak bir kullanıcının o virüsü ağ veya internet üzerinden göndermesiyle, ya da disket, cd, dvd veya taşınabilir veri depolama cihazlarıyla taşınmasıyla bulaşabilmektedir.

Zombi Bilgisayar

Bilgisayar dünyasında, sahibinin haberi olmadan kendisine kötücül bir yazılım bulaşmış, uzaktan erişen yetkisiz kullanıcılara kendisini kullanma ve kontrol etme yeteneği veren ve bunlardan dolayı tehlike arz eden bilgisayar "zombi" olarak adlandırılmaktadır. Ele geçirilen bir bilgisayar genellikle yüzlerden, binlerden veya milyonlardan oluşan bir köle bilgisayar ağındaki bilgisayarlardan sadece biridir ve kötücül görevlerin yapılmasında kullanılmaktadır. Kullanıcıları bilgisayarlarının ele geçirildiğinin farkında olmamalarından dolayı bu bilgisayarlar mecazi olarak zombilere benzetilmektedir.

Zararlı yazılımlar normal bir kullanıcının yapabildiği işlemlerin birçoğunu gerçekleştirebilirler. Uzaktan erişim sağlamak da bunlardan birisidir. Fakat yapılan her işlem sonucunda işletim sistemi üzerinde izler kalmaktadır. Bu izler, işletim sistemine ait olay kayıtlarında, dosya sistemine ait sistem dosyaları olan $MFT, $Logfile dosyasında ve işletim sisteminin olağan çalışması sırasında otomatik olarak oluşturulan diğer dosya ve kayıtlarda olabilir.

Ayrıntılı bir analiz yapılarak bahsedilen kötücül yazılımların etkileri araştırıldıktan sonra, bilgisayar üzerindeki izleri kontrol edilerek bunların çalıştırılıp çalıştırılmadığı, çalıştırılmış ise gerçekleştirdiği işlemler delil imajları üzerinde tespit edilmeye çalışılarak delil üzerindeki etkileri hususunda daha güvenilir bir karara varılabilir.

Soru 2.)

Bir bilgisayarda "Trojen" tespit edilmiş ise bu durumda o bilgisayarda yaratılmış olan dijital dokümanların delil olma güvenilirliği ve sağlığından söz edilebilir mi? Bu durumda söz konusu bilgisayarda kayıtlı olan dijital dokümanların mutlak suretle ve bilimsel bir kesinlikle bilgisayarın kayıtlı kullanıcıları tarafından oluşturulduğu söylenebilir mi?

Cevap 2.)

Diğer zararlı yazılımlar gibi trojanlar da; elde edilmiş e-posta adres listeleri, kötücül yazılım dağıtımında kullanılan enfekte edilmiş web siteleri ve programlar gibi değişik yollar

kullanılarak, en geniş kullanıcı sayısına ulaşma adına kullanıcı veya bilgisayar ayırt etmeden internet üzerinden dağıtılmaktadırlar. Bu zararlı yazılımlardan bazıları, bulaştıkları bilgisayarlar üzerinde yüklü antivirüs yazılımları tarafından engellenmesine rağmen, bu yazılımlara yakalanmadan da çalışabilmektedirler. Dolayısıyla, günümüz internet kullanıcılarının önemli bir kısmının bilgisayarlarında zararlı yazılımlar bulunmaktadır. Zararlı yazılımların büyük çoğunluğunun; spam gönderilmesi, internet bankacılık ve kredi kartı bilgilerinin çalınması, hizmet dışı bırakma saldırılarında kullanılması, reklam yayınlanması gibi genel olarak maddi çıkar sağlama amacıyla oluşturulup, merkezi bir şekilde yönetildiği bilinmektedir. Delil olarak değerlendirilen disklerde bulunan zararlı yazılımların analizi yapılmadan, içinde trojan bulunan delillerin güvenilmez olduğu iddia edilemez. Ayrıca bir zararlı yazılım üzerinden bilgisayara dosya atılmış olabilmesi için kötücül yazılımın;

- Hedefli bir saldırı sonucu gelmiş olması,
- Genel amaçlı olmayıp, özel olarak konfigüre edilebilip, uzaktan yönetim olanağı sağlayabilen türden olması,
- Geldiği tarihin, uzaktan atıldığı iddia edilen dosyalarla uyumlu olması veya bu dosyaların üstverilerinin değiştirildiğine dair bir bulgunun olmaması,
- Üzerinden atıldığı iddia edilen dosyalarda normal kullanıcı faaliyetlerinin gerçekleşmemiş olması, yani kullanıcının bu dosyaların varlığından haberdar olduğuna dair bulguların olmaması,

gibi özelliklere sahip olması gerekmektedir.

Soru 3.)

16.12.2011 ve 06.01.2012 tarihli Yıldız Teknik Üniversitesi Bilirkişi Raporlarında aşağıda tablo halinde gösterilen dokümanlarda, karşılarında yer alan virüslerin izlerine rastlandığı belirtilmektedir. Bu durum ne anlama gelmektedir? Söz konusu dijital dokümanların manipülatif bir niteliğe sahip olduğunu söylemek mümkün müdür?

DİJİTAL DOKÜMANIN İSMİ	VİRÜSÜN CİNSİ	VİRÜSÜN ÖZELLİĞİ
Koz.doc	**mbvd.exe**	Bilgisayara dosya kopyalama, değiştirme ve silme.
Fabrikatör.doc	**b00ijwpu.exe**	Bilgisayara dosya kopyalama, değiştirme ve silme.
Ulusal Medya.doc	**mbvd.exe**	Bilgisayara dosya kopyalama, değiştirme ve silme.
Tv Analiz Proje.doc	**mbvd.exe**	Bilgisayara dosya kopyalama, değiştirme ve silme.
Reosta Operasyonu.doc	**9b9w3.exe**	Bilgisayara dosya kopyalama, değiştirme ve silme.
Kadrolaşma Bilgi Notu (Ocxak 2004).doc	**hjvjte.exe**	Bilgisayara dosya kopyalama, değiştirme ve silme.
toplantı.doc	**mbdm.exe**	Bilgisayara dosya kopyalama, değiştirme ve silme.
teRTEmiz.doc	**9b9w3.exe**	Bilgisayara dosya kopyalama, değiştirme ve silme.
Bilinçlendirme.doc	**b00ijwpu.exe**	Bilgisayara dosya kopyalama, değiştirme ve silme.
Sn.komutanım.doc	**9b9w3.exe**	Bilgisayara dosya kopyalama, değiştirme ve silme.
Kılıçdaroğlu'na Destek Zorunlu	**srgo.exe**	Bilgisayara dosya kopyalama, değiştirme ve silme

Cevap 3.)

Müzekkere 13. sorudaki 4. yoruma verilen cevapta açıklanmıştır.

Soru 4.)

Yıldız Teknik Üniversitesi Öğretim Üyeleri olan Prof. Dr. Coşkun SÖNMEZ ve Dr. Göksel BİRİCİK tarafından hazırlanmış olan 16.12.2011 tarihli Bilirkişi Raporu'nda diğer dokümanların ise ".exe" uzantılı virüs tespit edilen dokümanlar ile yaratılma ve son erişirn tarihlerinin ayni olduğu ancak bu iki dosyaya ait ve ayni olan tarih kayıtları, ayni klasörde silinmiş olarak bulunan başka dosya ve klasörlerle ise farklı olduğu, bu durumun iki dosyanın ayni anda silindiğini gösterdiği belirtilmiştir.

Yine bir önceki dosyanın silinmesinde virüs etkisi olduğu göz önüne alındığında, bu dosya üzerinde de virüs ile işlem yapıldığı mütalaa edilmiştir. Değerlendirmelerin devamında son yazım tarihlerinin, dosyanın disk üzerindeki yaratılma tarihinden eski olduğu tespiti yapılarak bu durumun, dosyanın kesinlikle incelenen bilgisayarda oluşturulmadığı ve bir başka bilgisayarda hazırlandığını ve incelenen bilgisayarda hiç değiştirilmediğini gösterdiği vurgulanmıştır. Yapmış olduğunuz incelemeler neticesinde sizin ulaştığınız bulgular nelerdir?

Bu bulgular Yıldız Teknik Üniversitesi Raporunda yer alan tespitler ile paralellik taşımakta mıdır?

Cevap 4.)

Müzekkere 13. Soruda cevabı verilmiştir.

Soru 5.)

Bilgisayarlarda kayıtlı olan dijital dokümanların metadata (üstveri) bilgilerinde yer alan "yazar", "oluşturma tarih", "değiştirme tarihi", "son kaydetme tarihi", "şirket" ve "son erişim tarihi" bilgileri söz konusu dokümanın dosya kapsamında sanık olan kişiler tarafından

oluşturulmuş olduğu noktasında "kesin" bir tespit yapılabilir mi? Üst veri bilgileri sağlıklı ve değiştirilmez bilgiler midir?

Söz konusu bilgisayarlarda çok sayıda "spam" ve "virüs" tespit edilmiş olması bu dokümanların adli bilim esasları çerçevesinde mahkemelerin güvenebileceği bir kanıt olma niteliğine etkisi nedir?

Cevap 5.)

Müzekkere 3. ve 4. sorunun cevaplarında ve Avukat Celal Ülgen tarafından sorulan 2. Sorunun cevabında detaylı olarak açıklanmıştır.

Soru 6.)

21.12.2011 tarihli DataDevastation Bilirkişi Raporu'nda silinmiş "sed" ve "grep" komut dosyaları tespit edilmiştir. Bilirkişi UNIX ve LINUX komutları olan bu dosyaların incelenen ODATV Bilgisayarında bulunmasının olağan olmadığı tespitini yapmış ve bunun virüs yada virüs sahibi tarafından yaratışmış olabileceğini değerlendirmiştir.

Ayni raporda çok sayıda Trojen ve diğer Kötü Amaçlı Yazılımlar tespit edildiğini belirtmiş ve incelenen bilgisayarda yer alan hiçbir dokümana güvenilemeyeceği değerlendirmiştir. İnceleme sonucu elde ettiğiniz bulgular ışığında 21.12.2011 tarihli DataDevastation Raporunda yapılan tespitlere siz de katılıyor musunuz? Gerekçeniz nedir?

Cevap 6.)

Müzekkere 13. Soruda 2. İddiaya verilen cevapta detaylı olarak açıklanmıştır.

Soru 7.)

21.12.2011 tarihli DataDevastation Bilirkişi Raporu'nda harddiskte kayıtlı olan bir e-mail ile ilgili olarak u değerlendirmeler yer almaktadır: "Bu e-posta meşru mudur? Hayır. chp.org.tr ile ilgisi bulunmayan e-posta sunucuları kullanmaktadır. Jangomail, chp. org. tr 'nin kullandığı bir posta sunucusu değildir. Dolayısı ile bu, birçok ülkede cezaya tabi bir suç teşkil eden, aldatma amaçlı bir e-postadır. Bunun da ötesinde, söz konusu iki e-postaya KAY yüklenmiştir ve bu da, Türkiye'nin de İmzalamış olduğu Avrupa Konseyi Siber suçlar Antlaşması kanunlarını ihlal etmektedir." Yaptığınız inceleme neticesinde elde edilen bulgular çerçevesinde hard diskte bu şekilde aldatma amaçlı bir e-mail tespit edilmiş midir? Bu e-mailde Kötü Amaçlı Yazılım tespit edilmiş midir? Bu e-mailin kim tarafından gönderildiği tespit etmek mümkün müdür? Bu tarz e-mailler ne amaçla gönderilmektedir? Söz konusu e-mailin gönderildiği sunucu ve IP adresi nedir ve hangi ülkede bulunmaktadır?

Cevap 7.)

DataDevastation raporunda konu olan e-posta yolu ile gönderilen "Ataturk_Ekrankoruma.scr" ve "Duyuru.pdf" dosyaları ve bu dosyaların gönderildiği e-postalar incelenmiştir. Bu dosyaların kötücül yazılım olduğu tespit edilmiştir. Bu kötücül yazılımların özellikleri Soru 12'de detaylı olarak açıklanmıştır.

Kötücül Yazılım İçeren E-postalarının Kaynağının Tespiti

E-postaların kim tarafından gönderildiğini tespit etmeye yönelik olarak, yapılan analiz sırasında e-posta ile gönderilen kötücül yazılımın bağlanmaya çalıştığı "adobupdate.serveftp.com" ve "adobupdate.servehttp.com" adreslerinin alan adı kayıtları sorgulanmıştır. Yapılan sorgulama sonucu, "serveftp.com" ve "servehttp.com" alan adlarının A.B.D'de bulunan Vitalwerks Internet Solutions LLC (No-IP.com) şirketine kayıtlı olduğu görülmüştür.

```
Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: SERVEFTP.COM
   Registrar: VITALWERKS INTERNET SOLUTIONS LLC DBA NO-IP
   Whois Server: whois.no-ip.com
   Referral URL: http://www.no-ip.com
   Name Server: NF1.NO-IP.COM
   Name Server: NF2.NO-IP.COM
   Name Server: NF3.NO-IP.COM
   Name Server: NF4.NO-IP.COM
   Status: ok
   Updated Date: 12-mar-2010
   Creation Date: 01-jun-2001
   Expiration Date: 01-jun-2013
```

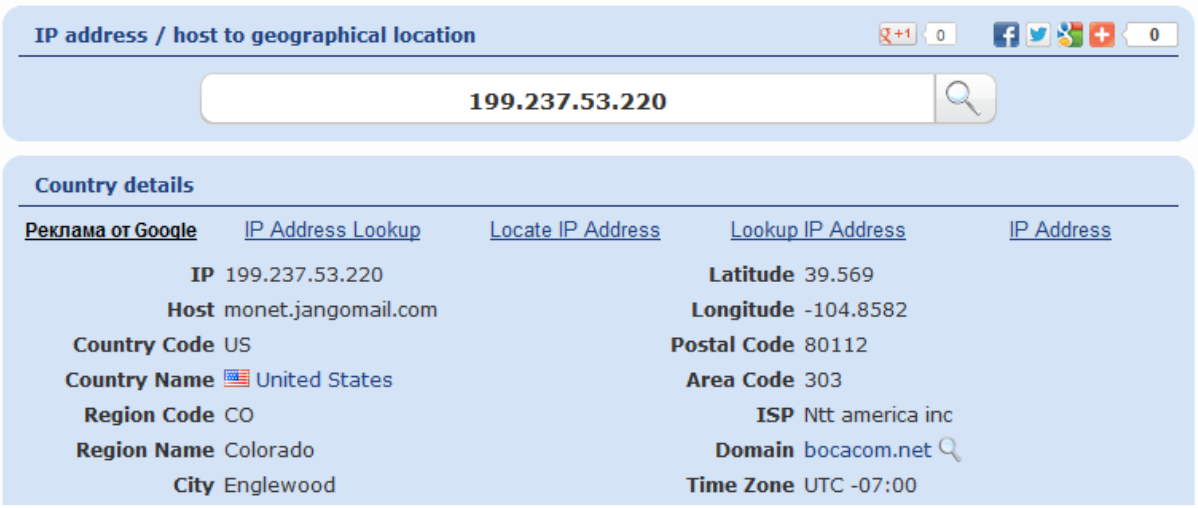
Şekil 123. Serveftp.com adresinin kaydı

No-ip.com adıyla bilinen bu şirket tarafından dinamik DNS hizmeti verilmekte, DSL ve kablolu internet kullanıcılarında yaygın olan dinamik IP adresinin veya statik IP adresinin bu şirkete ait bir alt alan adına eşlemesi yapılmaktadır. Genellikle kötücül yazılım yazarları, kimliklerinin tespitine imkân verebilecek şekilde doğrudan IP adresi kullanmak yerine bu alt alan adlarını kullanarak, hem kimliklerini gizlemekte hem de IP adreslerinin değişmesi ihtimaline karşı alan adı kullanarak bilgisayarlara olan erişimlerinin kesilmesine karşı önlem almaktadırlar. İlgili alt alan adının kullanımı hesabın açık kaldığı sürece devam etmekte ve hesap kapatılınca bitmektedir.

"Adobupdate.serveftp.com" ve "adobupdate.servehttp.com" alt alan adlarının şu an için kullanımda olmadığı görülmüştür. Eldeki veriler ışığında, bu alt alan adlarının hangi IP

adresleri tarafından kullanıldığının ve bu yolla kimin tarafından gönderildiğinin tespiti, No-ip.com şirketi tarafından bu bilgiler paylaşılmadıkça mümkün gözükmemektedir.

"Duyuru.pdf" dosyasının gönderildiği e-postanın başlık bilgileri kontrol edildiğinde, "Received: from" alanı yardımıyla e-postanın gönderildiği sunucunun adının monet.jangomail.com ve IP adresinin 199.237.53.220 olduğu görülmüştür. Bu IP adresi sorgulandığında, bu adresin A.B.D'de bulunduğu tespit edilmiştir.



Şekil 124. 199.237.53.220 IP adresinin yeri

Jangomail şirketi kullanıcıların hesap oluşturup, toplu e-posta göndermelerine veya sahip olmadıkları bir e-posta adresinden geliyor izlenimi vererek yanıltıcı e-posta yollamalarına imkân vermektedir. "Duyuru.pdf" dosyasının gönderildiği e-postanın başlık bilgileri kontrol edildiğinde, e-postayı gönderen Jangomail kullanıcısının adresi "Return-Path:" alanında "winnerr51@jangomail.com" olarak görülebilmektedir. Fakat eldeki veriler ışığında, Jangomail tarafından bu hesabı kullanan kullanıcının IP adresi paylaşılmadan, bu e-postanın kim tarafından gönderildiğinin tespiti mümkün gözükmemektedir.

Bu tarz e-postalar, aldatmaca veya oltalama adı verilen e-posta sınıflarına girmekte ve internet bankacılık ve kredi kartı bilgilerinin çalınması, hizmet dışı bırakma saldırılarında kullanılması, reklam yayınlanması gibi kullanıcının kandırılarak, çeşitli yollardan genellikle maddi çıkar sağlamaya yönelik olarak hazırlanmış kötücül yazılımları bulaştırmak amacıyla gönderilmektedir.

Soru 8.)

Barış PEHLIVAN'a ait Fujitsu Marka "MHV2060BH_NW1 8T6229459" Seri Numaralı Hard Disk üzerinde Yıldız Teknik Üniversitesi'nce görevli bilirkişiler Prof. Dr. Coşkun SONMEZ ve Dr. Göksel BIRICIK tarafından yapılan inceleme sonucu hazırlanan 23.12.2011 tarihli Bilirkişi Raporu'nda, incelenen bilgisayarda; bilgisayara uzaktan bağlantı kurma, bilgisayarı kullanıcısının bilgisi dışında uzaktan yönetme, bilgisayardaki dosyalara erişme-yükleme-silme, uzaktan dosya yükleme gibi işlemler yapabilen toplam 13 (onüç) adet trojan ve virus tipinde zararlı yazılımın bulunduğu tespiti yapılmıştır.

Söz konusu raporda yapılan tespitler ve inceleme neticesinde elde ettiğiniz bulgular çerçevesinde, bilgisayarda silinmiş bir şekilde bulunan dijital dokümanların metadata bilgilerinin, isnatlara dayanak dokümanların Barış Pehlivan'a aidiyeti noktasında kesinlik taşıyıp - taşımayacağı hususundaki bilimsel değerlendirmeniz nedir?

Cevap 8.)

Avukat Celal Ülgen tarafından sorulan 2. Sorunun cevabında ve Müzekkere 5. Sorunun cevabında detaylı olarak açıklanmıştır.

Soru 9.)

Arama ve el koyma sırasında imaj alınması neyin güvencesini sağlar? Kim ile kim arasında güven oluşturur? Salt CD ya da DVD ya da Hard diskler üzerine paraf atılması o dijital veriye sonradan kötü niyetli kişilerce ekleme yapılmasına engel oluşturur mu?

Cevap 9.)

Aram ve el koyma sırasında imaj alınması, imajı alınan diskteki verilerin imajın aktarıldığı diskteki verilerle birebir aynı olması amacını taşımaktadır. İmaj alma işleminin neticesinde, hem imajı alınan hem de imajı aktarılan diskteki verilerin hash değerleri hesaplatılır. Bu iki değerin aynı olması, o iki diskteki verilerin birbiriyle aynı olduğunu göstermektedir. Buradan hareketle, imajı aktarılan diskte yapılan incelemeler, o imajın alındığı orijinal diskte yapılan incelemelerle aynı değerlendirmeye tabi tutulabileceğini gösterir. İmaj alınması işlemi incelemeyi yaptıran makamların imajın orijinalini veremediği durumlarda incelemeyi yapan tetkikçi, imajın alındığı orijinal verinin sahibi ve imajı yaptıran makam arasında güven ilişkisi oluşturur.

CD, DVD veya hard diskler üzerine paraf atılması işlemi, (hash değerlerinin hesaplatılıp kaydedilmesi) o diskteki verilerin orijinalleriyle aynı olduğunun göstergesi ve güvencesi olarak yapılmaktadır. İmaj alındıktan ve hash değeri hesaplatıldıktan sonra imajın tekrar

açılması ve üzerinde değişiklik yapılması hash değerini değiştirecektir. Değişiklik yapılan diskin hash değeri tekrar hesaplatılırsa farklı bir sonuç oluşacaktır. Dolayısıyla imajı alınmış ve hash değeri doğru şekilde hesaplatılmış bir diskin üzerinde değişiklik yapılması durumunda bu durum hash değerlerinin tutarsız olacağından kolaylıkla anlaşılabilir.

Soru 10.)

İmaj almaya ara verilmesi, imaj almanın arama sırasında değil de sonradan kollukta alınması, ya da imajın şüpheli ve vekillerinden geri alınarak uzun süre kollukta bekletildikten sonra iade edilmesi delil sağlığı ve delil bütünlüğünü bozar mı? Bu durumda hukuka uygun bir kanıttan söz edebilme olanağı var mıdır? Açık ve gerekçeleriyle açıklar mısınız?

Cevap 10.)

İmaj alınma işlemleri, imajı alınan orijinal verilerle imajın aktarıldığı disklerin aynılığına kanıt olacağından önemli bir süreçtir. Bu işlemlerin olabildiğince hızlı, usulüne uygun ve mümkünse olay yerinde gerçekleştirilmesi en doğru yöntem olacaktır.

Ancak bununla beraber imaj alma işlemleri oldukça uzun süren ve zahmetli bir iştir. Çoğu zaman saatler mertebesinde süren bu işlemler, verinin yeni diske kopyalanması, orijinal disk ve kopyalandığı diskin hash değerlerinin hesaplatılması işlerini kapsamaktadır.

Burada dikkat edilmesi gereken nokta orijinal disk üzerinde hiçbir yazma işleminin yapılmamasıdır. İmajı alınan delilin sağlığı ve değişmezliği, imajın alındığı zaman ve lokasyondan, imaj alma sırasında işlemlere ara vermekten bağımsızdır. Önemli olan, imaj alma işleminden önce orijinal veriye herhangi bir yazma erişiminin olmamasıdır. Dolayısıyla imaj alma işlemlerinin mümkünse delil sahibi ile birlikte ve gözetiminde yapılması, orijinal delilin taşınması esnasında mühürlü torbaların ve zarfların kullanılması önem arz etmektedir.

Bu durumlara dikkat edildiği takdirde imajın ne zaman alındığı veya imaj alma işlemlerine ara verilmesi delil bütünlüğünü etkileyecek durumlar değildir.

Yarsuvat&Yarsuvat hukuk bürosunun 31.02.2012 tarihli dilekçesinde yönelttiği sorular

Hüseyin Soner Yalçın'ın müdafileri Av. Dr. Duygun Yarsavut, Av. Nurcan Çöl ve Av. Hüseyin Ersöz'ün hazırladığı dilekçede yönelttiği sorular, bir önceki bölümde detaylı olarak açıklanan Av. Celal Ülgen'in 30.01.2012 tarihli dilekçesindeki sorular ile birebir aynıdır. Cevaplar ve açıklamalar için bahsi geçen bölüm incelenebilir.

Av. Refik Ali Uçarcı'nın 12.03.2012 tarihli dilekçesinde yönelttiği sorular

Soru 1.)

Yıldız Teknik Üniversite raporunun 1. maddesi 5. sayfasında; simonson.doc isimli dosyanın sadece isim olarak var olduğunu ne normal ne de silinmiş alanda (unallocated) bu dosya ile ilgili bir ize rastlanmadığı belirtilmektedir.

Polis bilirkişi bu dosyanın var olduğunu söylemişler, ancak bu dosyanın kağıda dökümünü yapmamışlar, ancak bu dosya yerine bununla ayni olduğunu iddia ettikleri Unallocted clusters 49.doc isimli dosyayı print etmişlerdir. Simonson.doc dosyası mevcut ise kağıda print edilmesi, mümkün değil ise bunun nasıl olabileceğini , dosyanın adının mevcut olmasına karşın datasının olmaması nasıl ve neyle izah edilebilir?

Cevap 1.)

Soruda bahsi geçen simon son.doc dosyası için detaylı inceleme ve analizler müzerekkere 5. soruda detaylı şekilde cevaplanmıştır.

İlgili dosya silinmiş alan olarak tabir edilen (unallocated clusters) bölümünde tespit edilmiştir. Dosyanın ST3120927AS_4MS1TF89 nolu imajda izi olmadığı gibi bir ifade gerçeği yansıtmamaktadır.

$MFT yapısı ve unallocated clusters bölümünün en anlama geldiği müzekkere kapsamında detaylı olarak cevaplanmıştır. Kısaca bahsetmek gerekirse, NTFS dosya sisteminde dosyalar üstveri ve dosyanın kendisi olmak üzere 2 bölümden oluşmaktadır, denilebilir.

Silinen dosyaların üzerine zaman içerisinde başka veriler yazılabilir. Bu durum hem $MFT bölümü hem de dosyanın veri bölümü üzerinde gerçekleşebilmektedir. $MFT kısmı silinen ve üzerine başka veriler yazılan dosyaların veri kısmı (artık $MFT kayıtları kaybolduğu için) bundan sonra unallocated clusters olarak tabir edilen bölümde tutulmaktadır. Bilgisayarın doğal çalışma süreci içerisinde bu unallocated clusters alanı üzerine başka veriler yazılmış olabilir, ancak henüz yazılmamış da olabilir. Simon son.doc dosyası, unallocated clusters alanında işte bu şekilde henüz üzerine yazılmamış alanlarda tespit edilmiştir. Dosyanın $MFT kaydının üzerine başka veriler yazılmış olduğu için, dosyanın görüntülebilmesinin tek yolu unallocated clusters alanındaki verilerin gösterilmesi şeklinde olabilir. Unallocated clusters alanında tespit edilen dosyalara ait clusterların bir kısmı üzerine başka veriler yazılmış olabilir. Bu nedenle analiz edilen dosyaların görüntülenebilenhali, orijinal haliyle

birebir aynı olmayabilir. Ancak bu durum dosyanın tamamının daha önce ilgili hard diskte bulunmadığı anlamını da taşımamaktadır.

Soru 2.)

Polis bilirkişileri simonson.doc Ile Unallocted clusters 49.doc aynı dosya diyor. Ancak verdikleri raporda K-50 dizin 397 de Unallocted clusters 49.doc dosyanın Logical Size (büyüklüğü) 3312 KB denmekte iken, K-45 Dizin 37 de simonson.doc' un Logical size 3391488 KB olarak gösterilmektedir. Bin kat büyüklük farkına rağmen nasıl olur da bu iki dosya aynı nicelik ve nitelikte kabul edilebilir?

Cevap 2.)

Simon son.doc dosyası ile ilişkin yukarıda atıf yapılan klasörler incelenmiştir. 50. Klasör dizin 397'de yer alan Unallocated Clusters 49.doc dosyasının alanının 3312 KB olduğu görülmüştür. Soruda da bu şekilde ifade edilmiştir.

Ancak 45. Klasör dizin 37'de verilen 3391488 sayısıyla ilgili Logical Size (büyüklük) birimi verilmemiştir. Bilgisayarlarda dosya büyüklüklerini ifade eden birimlerle ilgili kısaca bilgi vermek gerekirse; büyüklüklerine göre byte, kilobyte(KB), megabyte(MB), gigabyte(GB) .. şeklinde sıralandıkları söylenebilir. Bu birimler, 1024 ile çarpılarak büyümektedir. Dolayısıyla 1 KB veri, 1024 byte'a tekabül etmektedir.

45. Klasör dizin 37'de **Logical Size** sütununda verilen 3391488 değerinin **byte** cinsinden yazıldığı tespit edilmiştir. Bu tespit yapılırken aynı tabloda yer alan diğer dosyaların boyutları da incelenmiş ve ilgili dosyaların orijinalleri referans alınarak bu kanıya varılmıştır. Bu listedeki verilerinin tamamının byte cinsinden olduğu görülmüştür. Burada verilen değerleri kilobyte cinsinden yazdığımızda aşağıdaki durum ortaya çıkmıştır.

3391488 sayısını 1024 ile böldüğümüzde 3312 sayısını buluruz ki bu bize ilgili dosyanın **kilobyte** cinsinden karşılığını vermektedir. 50. Klasör'de yer alan değer de 3312 KB olarak görülmektedir.

Dolayısıyla bu 2 dosyanın aynı boyutta olduğu tespit edilmiştir. Herhangi bir tutarsızlık söz konusu değildir.

Soru 3.)

Unallocted clusters 49.doc dosyayı Hanefi Avci'nın yazdığı Haliçte Yaşayan Simonlar isimli kitabın tam bitmemiş pdf formatındaki nüshasının copy paste yöntemi ile Word'e atılmış şekli olduğu anlaşılmaktadır. Mahkeme huzurunda da denendiğinde pdf dosyası word'e kopyalanınca aynı şekilde sayfa düzenin bozulduğu tüm başlıkların yok olduğu, içerisindeki grafik ve çizgilerin yok olduğu, díp notların yazı içerisine girdíği, bazı sayfa numaralarının yazının içerisine girip satir sonuna girdiği, en önemlisi de yazi içerisindeki fotograf gibi olan belgelerin (imzali mühürlü olanlarinin) yazi içerisine kopyalanamadığı ve sayfa numaralari ile boş kaldıkları görülmüştür.

Ayni şekilde polis bilirkişilerinin kağıda döktüğü orjinal kitabin 597 sayfa olmasina karşın, bu metnin 318 sayfa olduğu, ayni şekilde taslak dizin K48 dizin 403,402,399,387,346,341,330 dip notların yazi içerisine girdiğinin görüldüğü, yine (Taslaktaki sayfa nolan dip notlar: 284, 300, 345, 304,525,565 sayfalari içerisinde yaziya karışık olduğu görüldüğü) bu dip notlar orjinal kitapta ve orjinal taslakta 277, 285, 293, 338, 484, 497, 517, 557 sayfalarda ana metinden çizgi lie ayrılmış sayfa altında ayrışmış bulunduğu,

Yine Unallocted clusters 49.doc taslakta 458 sayfa 461, 462, 463 sayfalarda olmasi gereken belgeler olmadığı, sayfalarin boş olduğu 467 sayfanin yarım olduğu çünkü yarim belge olduğu, bu belgenin orijinal kitapta 451,454,455,456,457 ve 460 sayfalarda görülen belgeler olduğu,

Bu taslağın yayin evinin 06.08.2010 tarihli pdf formatli taslağı olduğu tespit edilmiştir. Bu dosyanın buradan kopyalanması haricinde oluşma imkani var mıdır?

Cevap 3.)

Unallocated clusterlarda tespit edilen bu dosya ile ilgili detay bilgiler müzekkerinin 5. sorusuna verilen cevaplarda, simon son.doc başlığı altında incelenmiştir.

Yukarıda yöneltilen ifadeler ve soruları incelemek için ilk olarak unallocated cluster kavramına ve disk dosya yapısına değinmek gerekir. Raporumuzda çeşitli yerlerde izah edilen ve özellikle müzekkerenin 10. sorusuna verilen cevapta açıklanan kavramlar incelenerek unallocated clusterlar hakkında bilgi edinilebilir.

Yukarıda yöneltilen soru özelinde yorum yapmak gerekirse, unallocated cluster alanında tespit edilen verilerin geri dönüşümü ve ekranda görüntülenmesi esnasında çeşitli format

bozuklukları ve okunmaz-anlaşılmaz karakterlerle karşılaşılabilir. Bu durumun bir kaç sebebi olabilir.

İlki, düzyazı formatı dışındaki (fotoğraf, ses, video vb.) verilerin, kendi formatlarında tutulduğu için gözle okunamamasıdır. Karışık ve anlamsız gibi görünen karakter dizesi şeklinde dururlar. Bu nedenle gözle bakıldığında formatları bozuk görünür.

İkincisi, Microsoft Word uygulamasının bir metin editörü olmasına karşın, uygulamada kaydedilen yazılara çeşitli formatlar atayabilmesidir. Örnek vermek gerekirse, kalın harflerle ve italik yazılan, alt ve üst başlıkları olan, dipnotlar atanan ve büyük küçük harf gibi ayrımları olan bir yazı, unallocated clusters alanından geri döndürüldüğünde bütün bu formatları **kaybeder.** Sebebi, unallocated clusters alanında verilerin ancak ham halinin görüntülenebiliyor olmasıdır. Bir önceki cümlede bahsi geçen bütün yazı formatları ancak Word uygulamasının açabileceği şekilde kaydedilmiştir. Bu izler ve işaretler Word uygulaması tarafından yorumlanamadığı için ve unallocated cluster alanından sadece ham veri (ham halde duran yazı) geri dönüşümü yapılabildiği için, hiçbir yazı tipi ve format görüntülemez. Dosyanın tamamının görsel özelliklerini de koruyarak geri dönüşümünün yapılabilmesi için $MFT kaydının silinmemiş olması gerekmektedir. Ancak simon son.doc dosyasının $MFT kaydı silindiği için bunu sağlamak mümkün değildir.

Üçüncüsü ise, unallocated clusters alanında dosya bütünlüğünün garanti edilememesidir. İlgili dosya silinmiş olduğundan, dosyanın kaydedilmiş olduğu alanın (clusterların) üzerine, kısmen veya tamamen başka bir veri yazılmış olabilir. Bu durumun gerçekleşmesi halinde dosyanın bir kısmının geri dönüşümü yapılamayacaktır.

Değinilmesi gereken bir diğer nokta, özellikle geniş hacimli ve birçok kilobyte'dan oluşan dosyaların, diskte farklı clusterlarda kaydedilmiş olma ihtimalinin bulunmasıdır. Silinmemiş dosyalarda $MFT kaydı referans alınarak dosyanın kaydedilmiş olduğu bütün clusterlar ve adresleri bilindiğinden, dosya görüntülemede hiçbir sorun yaşanmaz.

Ancak dosyalar silindiğinde ve özellikle $MFT kaydı silinerek üzerine başka veriler yazıldığında, dosyanın kayıtlı olduğu clusterlar arasındaki ilişki kaybedilmiş olur. Bu durumda dosyanın hiç görüntülememesi ihtimali olduğu gibi, ancak bir kısmının görüntülenebilmesi ve geri döndürülebilmesi ihtimali de mevcuttur.

Yukarıda açıklanan verilerden hareketle; unallocated clusters alanında tespit edilen verilerin format bozukluğu, bir kısmının eksik olması, okunamaması ve sayfa sayısının az olması vb. gibi durumlar olağandır. Bu durumlar, dosyanın geçmişte bir PDF dokümanından Word'e copy paste ile aktarıldığı anlamına gelmemektedir. Dolayısıyla diskte Word dökümanı olarak

tespit edilen dosyanın, copy paste ile mi oluşturulduğu veya bu diskte mi hazırlandığı konusunda bir yargıya varılamaz.

Soru 4.)

Bu şekilde Unaltocted clusters 49.doc'dan yeniden bu kitabi üretmek ne kadar zaman içerisinde mümkün olabilir?

Cevap 4.)

Unallocated clusterlardan veri üretmek, ilgili clusterlarda bulunan verilerin ortaya çıkarılması ve birleştirilmesiyle mümkündür. Bu işleme recover (geri dönüşüm) denmektedir. Kitabın üretilmesinden ne kastedildiği anlaşılamamıştır, clusterlardan veri dönüşümü ile ilgili işlemler otomatize veya manuel işlemlerle mümkün olabileceğinden herhangi bir zaman diliminden bahsetmek mümkün değildir.

Soru 5.)

a.) Hanefi.doc isimli dosya önce 12.07.2010 da başka bir bilgisayarda oluşturulmuş, sonra 26.07.2010 tarihinde ODATV'ye taşınmış ama ODATV'de hiç açılıp okunmamış olduğu görülmektedir.

b.) Nedim.doc isimli dosyada önce 09.08.2010 tarihinde başka bir bilgisayarda oluşturulmuş, sonra 16.08.2010 da ODATV bilgisayarina taşınmış gözükmektedir. Hiç açılıp okunmamış olduğu görülmektedir.

Bu dosyaların bulunduğu bilgisayarda oluşturan olarak gözüken soner isimli bir kullanıcı bulunmamaktadır. Ayrıca soner isimli dosyanin sahibi olduğu iddiasında bulunulan kişi 2010 yılı Ağustos ayı boyunca Bodrum'da olduğunu hiç Istanbul'a gelmediğini belgeleyebileceğini belirttiğine göre, bu dosya nasıl oluşmuş, ya da oluşturulmuş olabilir? Bu oluşum konusunda nasıl, neden ve ne tür bir işlem ile yapılabileceğini açıklayabilir misiniz?

Cevap 5.)

a.) Hanefi.doc isimli dosya ile ilgili ayrıntılı bilgiler 5. sorunun cevabında verilmiştir. Buna göre dosyanın soner isimli bir kullanıcı tarafından oluşturulduğu ve en son yine aynı kullanıcı tarafından değişikliğe uğradığı görülmüştür. Ancak bu dosyanın incelenen ODATV diskinde hiç açılmadığı gibi bir yorum gerçeği yansıtmamaktadır. İlgili dosyaya 2011-01-26 tarih ve

12:07:37 dakika-saniyesinde erişim yapıldığı tespit edilmiştir. Bununla ilgili kayıtlar 5. Sorunun Hanefi.doc başlığında detaylı olarak gösterilmiştir.

b.) Nedim.doc isimli dosya ile ilgili bilgiler 5. sorunun cevabında verilmiştir. Dosyanın soner isimli bir kullanıcı tarafından oluşturulduğu ve en son yine aynı kullanıcı tarafından değişikliğe uğradığı görülmüştür.

Bu dosyalar soner isimli bir kullanıcı tarafından oluşturulmuş ve değiştirilmiş görünmektedir. İncelenen ODATV hard diskinde bu isimle oluşturulmuş dosyaların bulunması, bu dosyaların soner isimli bir kullanıcının bilgisayarında oluşturulup ODATV bilgisayarına aktarıldığı kanısını oluşturmaktadır. Dosyaların zaman tarih verileri ve içerdikleri üstverilerinin analizi neticesinde herhangi bir anormallik ve sıradışı durum tespit edilememiştir.

Soru 6.)

Polis bilirkişilerinin raporuna göre K-45 dizin 37 den 32 e kadar listeledikleri bilgisayarda bulunan $Logfail dosyalarının oluşum tarihine bakildiğinda 08.07.2010 günü saat: 16:17:13 ile 14. Saniyelerde, 115 dosyanin hemde büyük kısmının scanner ile taramali büyük hacimli dosyanin oluşturulduğu görülmektedir. Büyük ihtimalle buraya kopyalandığı anlaşılmaktadır.

Ancak CD-DVD ve USB gibi veri tarayıcıları ile yapilan yaklaşik 100 dosyanin kopyalanmasinda iki saniyede kopyalamanin mümkün olmadığı en az 10 saniye ve üstü, hatta CD-DVD bir kaç dakika aldığı görülmüştür. Bu konu Mahkemede huzurunda da eylemsel olarak gösterilmiştir. Ancak bu uygulamanin bilgisayarin içerisinde diskin bir dayrektörüden, başka dayrektörüye aktarilirken mümkün olduğu görülmüştür. ODATV bilgisayarinda bir kopya suret olduğuna göre, 115 dosyanin iki saniyede kopyalanmasi nasil olabilir?

Bu dosyalar sıkıştırılmış zipli.rar uzantili dosyalar halinde virüsle gönderme, veya başka bir yöntemle kopyalanmış olabilirmi? Cevap evet ise bu kopyalama metodu hakkında açıklamalarda bulunurmusunuz.?

Cevap 6.)

Bahsi geçen dosyalar incelendiğinde $LogFile zamanlarının 2 sn. farkla oluştuğu görülmektedir. Bu durum, dosyaların başka bir kaynaktan kopyalanarak geldiğine işaret ediyor olabilir. Ancak kopyalama kaynağının ne olduğu konusunda net bir yorum yapmak mümkün değildir. Aynı bilgisayara ait farklı bir dizinden kopyalama işlemi yapılmış olabileceği gibi, sıkıştırılmış bir dosyadan çıkarılarak da oluşmuş olabilir. Bunun yanı sıra, aynı ağdan bulunan başka bir bilgisayarın paylaşım klasöründen de kopyalanmış olabilir. Buna benzer

örnekler çoğaltılabilir. Burada üzerinde durulması gereken nokta, ilgili dosyaların detaylı analiz çıktılarıdır. Dosyaların hangi kaynaktan geldiği, sıkıştırılmış bir dosyadan gelip gelmediği, sıkıştırılmış dosyadan geldiyse bunun zararlı yazılımlar aracılığıyla olup olmadığı detaylı inceleme konusudur. Bununla ilgili çalışmalar 5. Ve 12. Soruda detaylı şekilde izah edilmiştir.

Sonuç olarak, bahsi geçen 115 dosyaya ait kayıtların 2 sn. içinde görünüyor olması, bu dosyaların sıkıştırılmış bir dosya ile virüs aracılığıyla geldiğine dair tek başına bir delil olamaz. Dosyaların 2 sn. de oluşmuş olması, başka bir çok sebeple de oluşabilecek bir durumdur. İlgili dosyaların bir zararlı yazılım aracılığıyle gelip gelmediği konusunda, zararlı yazılımların statik ve dinamik analizine kadar derin araştırmalar yapılması gerekmektedir. Bu çalışmaların sonuçları raporun 5 ve 12. sorularında detaylı şekilde açıklanmıştır.

Soru 7.)

Hiçbir dosyanın Hash değerinin diğerleri Ile aynı olamayacağı bir tek harf ve/veya nokta eklense hash değerinin değişeceği belirtilmesine rağmen K-50 dizin 395 ve 385 bulunan Emníyet Bilirkişileri tarafından çıkarılan birbirinin benzeri olduğu söylenen Unallocted clusters 40.doc ile ulusal medya 2010.doc dosyalarının büyüklükleri farkli olmasına, arada (2. KB)'den fazla fark olmasına rağmen aynı hash değerlerinde olmaları nasıl mümkün olabilir?

Neden farklı dosyaların farklı büyüklüklüklerine rağmen ayni hash değerinde olmaları nasıl mümkün olabilir? Eger hash değerlerinin aynı olması mümkün ise teknik olarak bu hususu nasil açıklayabilirsiniz?

Cevap 7.)

Bir dosyanın hash değeri hesaplandıktan sonra, o dosyaya tek bir harf bile eklense yeni bir hash değeri oluşacaktır. Bu iki değerin birbiriyle aynı olması söz konusu değildir.

Emniyetin bilirkişi raporunda bahsi geçen 2 dosyaya ait veriler incelendiğinde ise; Unallocated clusters 40.doc dosyasının 63.50 KB, Ulusal Medya 2010.doc dosyasının 65024 BYTE olduğu görülmüştür. 1 KB 1024 BYTE'a tekabül ettiği için, 63.50 KB'ın BYTE karşılığı 65024 olacaktır. Bu değer de Ulusal Medya 2010.doc dosyasında belirtilmiş olan değerle aynıdır. Dolayısıyla bu iki dosyanın boyutlarının aynı olduğu görülmektedir.

Sn. Hanefi Avcı'nın 26.01.2012 tarihli dilekçesinde yönelttiği sorular

Soru A-2)

Bilgisayarlar üzerinde emniyet mensuplarınca yapılan ilk inceleme ve raporlar adli bilişim incelemeleri usulüne uygun mudur? Yeterli ve tam bir inceleme yapılarak tüm bilgiler toplanmış mıdır? Eksik inceleme yapılmış ise olması gereken incelemeleri maddeler halinde sayılması

Cevap A-2)

Diğer bilirkişi raporları ile ilgili detaylı değerlendirmeler raporun 14. Sorusunda cevaplanmıştır.

Soru A-3.)

İncelenen bilgisayarda virüs olup olmadığının araştırılmadan, internet, antivirüs ve diğer log kayıtları incelenmeden, bilgisayarda antivirüs ve diğer güvenlik yazılımları olup olmadığı ve onların log kayıtları incelenmeden, ADSL modem kayıtlarının imajı alınmadan, bilgisayarın tüm yazılım ve donanımı tespit edilip incelenmeden adli bilişim raporu yazılması normal midir, yoksa bunlar yapılmadan yapılan inceleme eksik, yanıltıcı hatta yanlış midir?

Cevap A-3.)

Adli bilişim raporları, bilirkişilerden rapor isteyen makamın inceleme talepleri ve sorularına yönelik hazırlanmaktadır. İncelenmesi gereken adli deliller, bilirkişilere yöneltilen sorulara cevap bulunabilmesi için gerekli tetkiklere ve araştırmalara tabi tutulurlar. Burada yönlendirici olan, bilirkişiden rapor hazırlanmasını isteyen makamın talepleridir. Bu taleplere cevap verebilmek için ihtiyaç duyulan deliller (hard disk imajı vb.) taleple birlikte bilirkişilere iletilir. Bilirkişi raporları bu doğrultuda hazırlanır ve teslim edilir.

Bilirkişilerden istenen inceleme talepleri çeşitlenebilir. Analiz edilmesi gereken verilere göre farklı çalışmalar yapılır ve rapor hazırlanır. Dolayısıyla her bilirkişi raporunda olması gereken sabit bir inceleme yoktur. Bilirkişilerden cevaplanması istenen sorularda; ilgili bilgisayara ait virüs-antivirüs araştırması, internet erişim bilgileri ve analizi, detaylı donanım ve yazılım özelliklerinin raporlanması gibi talepler yoksa bu başlıkların incelenmesine gerek olmayacaktır. Sadece sorulan soruların cevaplarının olduğu bir rapor tanzim edilmesi bu nedenle doğaldır, bu durum hazırlanan bilirkişi raporunun eksikliğini göstermemektedir.

Ancak bu durumla beraber gözetilmesi gereken çeşitli hassasiyetlerden bahsedilebilir. Söz gelimi, talep kapsamında bir hard disk imajının virüs içerdiği iddia ediliyorsa, veya herhangi bir dosyanın virüs ile oluşturulduğuna yönelik araştırma talep edildiyse; o diskte bulunan bütün virüslerin analizi, antivirüs logları, internet erişim bilgileri vb. gibi bütün bilgiler tespit edilmelidir. Virüslerin statik-dinamik analizi de yapılarak bir yargıya varılmaya çalışılmalıdır. Böyle bir araştırma kapsamında bahsi geçen veriler düzenlenerek rapor tanzim edilebilir. Bununla beraber her bilirkişi incelemesinde bu analizlerin yapılmasına ihtiyaç yoktur.

Av. Nebi Doğan'ın 01.02.2012 tarihli dilekçesinde yönelttiği sorular

Soru A-1.)

İnceleme yapılan diskte gizli bölümler var mıdır?

Cevap A-1.)

İnceleme yapılan diskteki herhangi bir gizli bölüme rastlanılmamıştır.

Soru A-2.)

Disklerde kriptolama yapılarak dosyalar koruma altına alınmış mıdır?

Cevap A-2.)

Disklerde kriptolu saklanan ve korunan bir dosyaya rastlanmamıştır.

Soru 2.)

Hard Disk imajlarını almak için kullanılan yazılım ya da donanımlar uluslararası geçerli sertifikalara sahip midir?

Cevap 2.)

Soruya ilişkin cevaplar Müzekkere 1. Soru'da ayrıntılı olarak açıklanmıştır.

Soru 3.)

Alınan imaj dosyasının sonradan değiştirilip değiştirilmediği anlaşılabilir mi? Anlamanın yöntemi nedir? Hard disk üzerinde olmayan bir dosyanın alınan hard disk imajı içinde bulunabilmesi teknik olarak mümkün müdür. Böyle bir işlemin yöntemi nedir?

Cevap 3.)

Hard disk imajları ve özellikleri hakkında detaylı bilgi 1. Soruda verilmiştir. Özetlemek gerekirse; hard disk imaj dosyasının değişmezliği hash değeri ile anlaşılabilir. Arama el-koyma esnasında veya daha sonra kollukta yapılan imaj alma işlemi sırasında hem orijinal hem de imajı alınan diskin hash değerlerinin alınması ve birbiriyle aynılığının teyidi, verilerin değişmezliği sağlayacak bir kontroldür. Hard diskte olmayan bir dosyanın hard disk imajında bulunabilmesi, hash değerlerinin birbirinin aynı olması durumunda imkânsızdır.

Soru 4.)

Ekteki iddianamede belirtilen 4 dosya imajlarda var mıdır? Var ise, belgelerin oluşturulma ve silinme tarihleri nedir? Bunlara güvenilir mi? Bu belgeler bilgisayar mı oluşmuş, yoksa dışarda mı? Tespiti yapılmalı. Dijital dosyanın kim tarafından oluşturulduğu nasıl tespit edilebilir? Mümkünse tespiti. Bilgisayarlara sahibinin isteği dışında yüklenmesi mümkün mü? Mümkünse hangi yöntemlerle.

Cevap 4.)

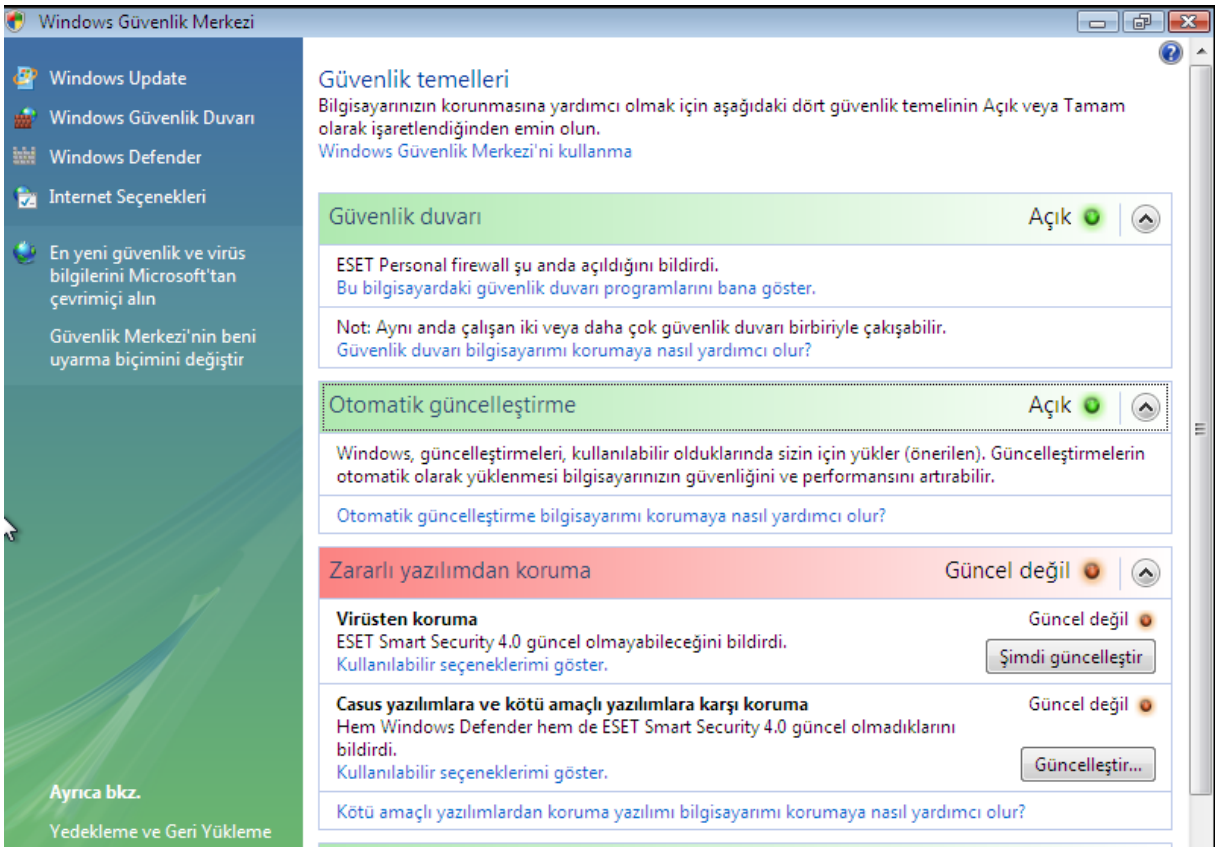
Bu sorular müzekkere kapsamında detaylı şekilde cevaplanmıştır. 3.4.5.7.8 ve 12. Sorular incelenebilir.

Soru 5.)

İlgili sistemlerde antivirüs ve firewall yüklü mü? Kuruluysa, dışardan yapılan müdahaleleri engellemek için yeterli mi? Antivirüs ve firewall loglarının incelenmesi. Virus var mı, araştırılması? Virüs var ise, geldiği tarih saatlerin belirtilmesi.

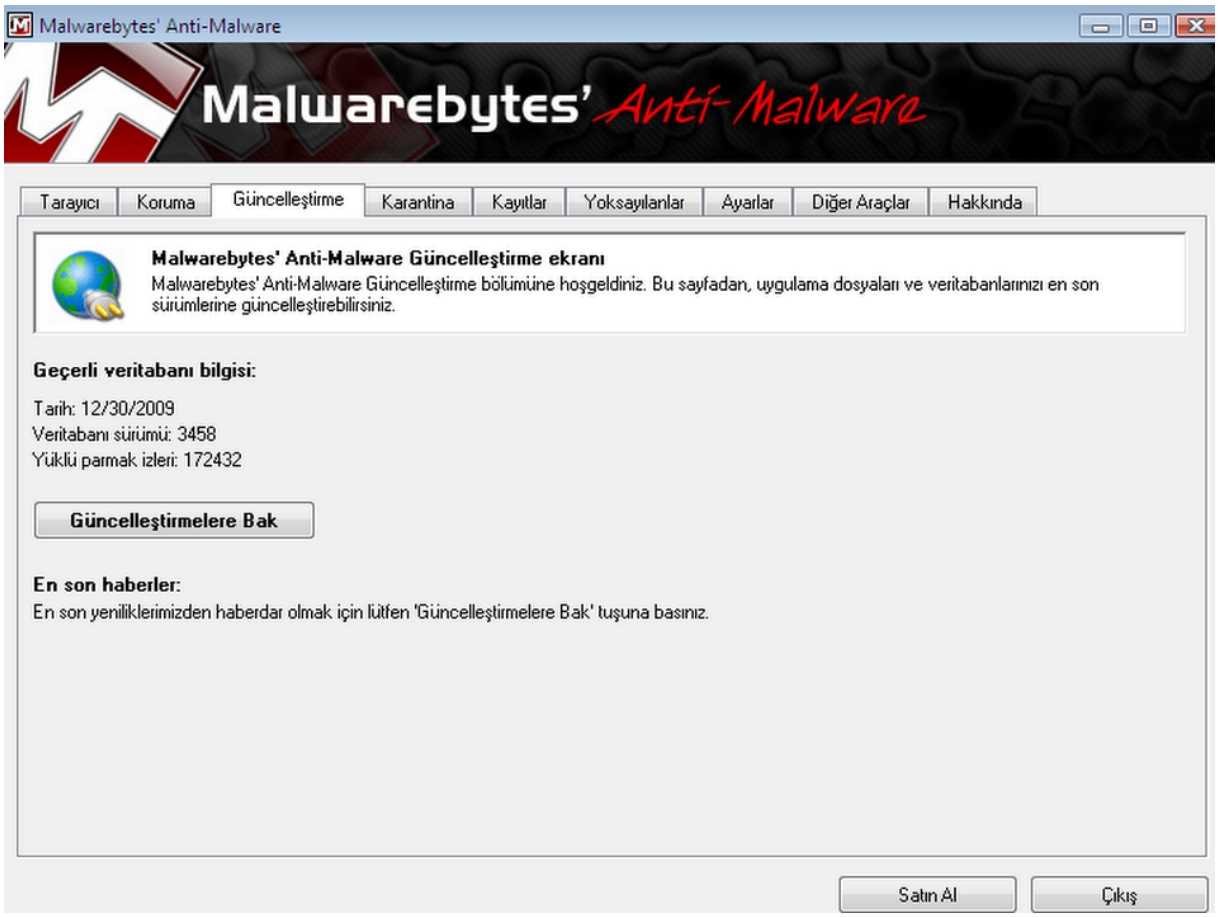
Cevap 5.)

S17HJ90Q816726 seri nolu hard disk imajı üzerinde “ESET Smart Security 4” isimli antivirüs uygulamasının çalıştığı, güvenlik duvarının (firewall) aktif olduğu ve kötücül yazılımlara karşı “Malwarebytes Anti-Malware” uygulamasının çalıştığı tespit edilmiştir. Antivirüs programının en son 28.08.2010 tarihinde, Anti-Malware uygulamasının ise en son 30.12.2009 tarihinde güncellendiği görülmektedir. Kurulu olan bu uygulamalar, dışarıdan müdahaleleri büyük oranda durdurabilse de tamamen engelleyemez.



Şekil 125 - S17HJ90Q816726 Güvenlik Duvarı Bilgileri

Şekil 126 - S17HJ90Q816726 Antivirüs Güncellenme Bilgileri



Şekil 127 - S17HJ90Q816726 Anti-Malware Uygulaması Güncellenme Bilgileri

Soru 6.)

muyesserugur@mynet.com muyesseryildiz@yahoo.com'daki maillerde virüs var mı? Virüs varsa ve bilgisayara bulaşmışsa herhangi bir işlem yapılmış mı? EK-1'deki dosyaların bu yolla gelmesi mümkün mü?

Cevap 6.)

Bu sorular müzekkere kapsamında detaylı şekilde cevaplanmıştır. Soru 5'de ilgili dosyaların olduğu bölümler incelenebilir. Ayrıca Soru 12'de bulunan zararlı yazılımlar ve virüslerle ilgili açıklamalara başvurulabilir.

Soru 7.)

İddianamede yer alan ve Müyesser Uğur'un ilgili dosyalarda gerçekleştirdiği iddia edilen işlemlerle ilgili kesinlik ifade eden yargılarda bulunulması mümkün mü? Bahsi geçen dosyaların hangi yöntemlerle iletildiği tespit edilebilir mi?

Cevap 7.)

İnceleme ve analizler neticesinde, bahsi geçen dosyaların ilgili tarihlerde belirtilen kullanıcılar tarafından oluşturulduğu/değiştirildiği görülse de, bu verilere sadece belge üstverilerinden yola çıkarak ulaşılabilmektedir. Ancak dosya sistemi üstverileri incelendiğinde, Müyesser Uğur'dan alınan imajda bulunan dosyaların dosya sistemi üstverilerinde bazı farklılıklar tespit edilmiştir. Konuyla ilgili olarak zararlı yazılım analizi ve dosya üstverilerinin yorumlanması çalışmaları yapılmıştır. Müzekkere kapsamında bu konular detaylı olarak açıklanmıştır. Bu bağlamda 5.6.7.8.9 ve 12. sorular incelenebilir.

İlgili cevaplarda detayı verilen bulgular neticesinde, iddianamede belirtilen bu ifade için kesinlikten bahsedilemeyeceği kanısı oluşmuştur.

4 SONUÇ

İnceleme kapsamında ST3120927AS_4MS1TF89 (delil 1), MHV2060BH_NW18T6229459 (delil 2) ve S17HJ90Q816726 (delil 3) seri numaralı sabit disklerin imajlarında EK-1 dosya listesinde belirtilen dosyaların kime ait olduğu, ilgili bilgisayarlara nereden gelmiş olduğu, bilgisayarlara zararlı yazılımlar vasıtasıyla mı geldiği hususlarında adli analiz çalışması gerçekleştirilmiştir.

Adli analiz çalışmasında gerçekleştirilen adımlar aşağıda sıralanmıştır.

- İlgili bilgisayar kullanıcılarına özel olarak gönderilen (hedefli saldırı) zararlı yazılımlar incelenmiştir.
- Hedefli saldırılarda kullanılan zararlı yazılımların uzaktan yönetim ve dosya atma kabiliyeti olup olmadığı ve bilgisayarda çalışmış olup olmadığı incelenmiştir.
- EK-1 dosya llistesinde yer alan dosyaların bu zararlı yazılımlarla ilişkisi olup olmadığını tespit etmek için dosya üstverileri ve işletim sistemi izleri incelenmiştir.
- Üstveri incelemesinde, bahse konu dosyalarda herhangi bir uyumsuzluk olup olmadığı ve ilgili bilgisayar kullanıcısının bu dosyalardan haberdar olup olmadığı anlaşılmaya çalışılmıştır.

İlgili bilgisayarlarda çok sayıda zararlı yazılımın izine rastlanmıştır. Tespit edilen bu izlerin büyük çoğunluğunun aktif olma şansı bulamamış veya uzaktan dosya atma özelliği bulunmayan zararlı yazılımlara ait olduğu görülmüştür. Geri kalan zararlı yazılım izleri içinden de, imajları incelenen bilgisayarların kullanıcılarını özel olarak hedef almış olan zararlı yazılımlara ait izler ayrıntılı bir şekilde incelenmiştir. Bu incelemenin sonucunda, uzaktan dosya atabilme özelliğine sahip ve ilgili bilgisayar kullanıcılarını hedef almış olan zararlı yazılımların çalışmış olduğu kanısına varılmıştır.

Ek-1 dosya listesinde belirtilen dosyaların belge üstverileri, dosya sistemi üstverileri ve işletim sistemi izleri incelenmiştir. İncelemeler sonucunda, **Ek-1 de listelenen dosyalardan sy.doc ve prj_60.doc dosyaları dışındakilerin ilgili bilgisayarlarda oluşturulduğuna veya değiştirildiğine dair bir bulguya rastlanmamıştır.** sy.doc ve prj_60.doc dosyalarının delil 2 bilgisayarında değiştirilmiş olma ihtimali mevcuttur. Bu iki dosya dışındaki dosyaların bilgisayar kullanıcıları tarafından açıldığında, işletim sistemi üzerinde oluşabilecek izler incelenmiş ve ilgili bilgisayar kullanıcıları tarafından açıldıklarına dair kuvvetli bir bulgu olmadığı tespit edilmiştir. Dosya üstverileri arasında uyumsuzluklar araştırılmış ve sadece

delil 3 üzerindeki 4 dosya için, normal kullanıcı davranışları ile oluşması zor, dosya sistemi üstverilerinde bulunan bir uyumsuzluğa rastlanmıştır. Bu uyumsuzluğun normal koşullarda oluşma ihtimalinin düşük olduğu değerlendirilmektedir. Bunun yanında bu uyumsuzluğun dosya sistemi üstverilerinin dışarıdan bir müdahale ile değiştirilmesi sonucu oluşması ihtimali ise daha kuvvetlidir. Bu müdahale zararlı bir yazılım aracılığıyla uzaktan erişim yöntemi ile gerçekleştirilebileceği gibi, bilgili bir kullanıcı tarafından da gerçekleştirilme ihtimali mevcuttur. Delil 3 bilgisayarını bu yetkinliğe sahip bir kullanıcının da kullandığına dair izlere rastlanmıştır. Delil 1 ve delil 2 hakkında hazırlanmış bilirkişi raporlarının, Ek-1 dosya listesindeki dosyaların üstverilerinde ve dosya sistemi izlerinde bulunduğunu ve zararlı yazılımlar vasıtasıyla oluşmuş olduğunu savundukları uyumsuzluk iddiaları ayrıntılı bir şekilde incelenmiştir. Bu inceleme sonucunda, dosya üstverilerinde ve dosya sistemi izlerinde iddia edilen herhangi bir uyumsuzluğun olmadığı ve delillerde tespit edilen zararlı yazılımlar ile ilişkilendirilemeyeceği açıklanmıştır.

Ek-1 listesinde yer alan dosyaların ilgili bilgisayarlara nereden gelmiş olabileceği incelenmiştir. Listedeki dosyaların büyük çoğunluğunun oluşturma tarihinin sadece saniye seviyesinde saklandığı, FAT formatındaki bir sürücüden kopyalanmış olması veya “zip”, “rar” benzeri arşiv dosyalarından çıkarılmış olması veya CD, DVD tarzı bir veri aygıtından gelmiş olma olasılığı mevcuttur. Özellikle delil 2 de Ek-1 dosya listesinde ismi geçen birçok dosyanın “rar” uzantılı dosyalardan çıkarılmış olduğuna işaret eden dosya sistemi izlerine rastlanmıştır. Fakat bu arşiv dosyalarına erişilemediği için nereden gelmiş olabilecekleri hususunda bir fikir yürütülememektedir. Bunun yanında delil 1 ve delil 2 bilgisayarlarında aynı USB veri depolama cihazlarının kullanılmış olduğu ve üç bilgisayarda da “Team Viewer” uygulamasının kurulu olduğu ve bu programın kayıtlarında ortak bağlantı adreslerinin de olduğu tespit edilmiştir. Dosyaların bu bilgisayarlara aktarılması için bu USB veri depolama cihazları veyahut “TeamViwer” uygulaması da kullanılmış olabilir.

Sonuç olarak, Delil 3 teki dosya sistemi üstveri uyumsuzlukları ve bu bilgisayar kullanıcısına başarılı bir şekilde gerçekleştirilmiş olduğu değerlendirilen hedefli zararlı yazılım gönderme saldırısının zamanlaması, **Delil 3 bilgisayarındaki dosyaların zararlı yazılım vasıtasıyla gönderilmiş olma ihtimalini güçlendirmektedir**. Delil 1 ve Delil 2 bilgisayarlarında da, özel hedefli sosyal mühendislik saldırıları ile gönderilen, uzaktan dosya atma özelliği bulunan zararlı yazılımların çalışmış olduğu tespit edilmiştir ve Ek-1 dosya listesindeki dosyalar

üzerinde ilgili bilgisayar kullanıcıları tarafından bir işlem gerçekleştirdildiğine dair tatmin edici izlere rastlanmamıştır. Bunun yanında Ek-1 dosya listesindeki dosyaların üstverilerinde ve işletim sistemi izlerinde, bu dosyaların zararlı yazılımlar vasıtasıyla bu bilgisayarlara gönderilmiş olduğuna dair herhangi bir bulguya da rastlanmamıştır. Bu sebeple **bu dosyaların zararlı yazılımlar vasıtasıyla geldiğine veya gelmediğine dair kesin bir yargıya varılamamıştır**. .

Osman PAMUK	**Ünal TATAR**	**Emin ÇALIŞKAN**
Bilirkişi	**Bilirkişi**	**Bilirkişi**

5 EKLER

EK-1 ST3120827AS_4MS1TF89 seri nolu hard disk imajında gerçekleştirilen güncelleştirmeler

Name	Description	Installed By	Installation Date	Update Type	Application	Last Modified Time
KB2229593	Windows XP için Güvenlik Güncelleştirmesi (KB2229593)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:56
KB835221WXP	High Definition Audio Driver Package - KB835221	Türker	03.04.2008	Update	Windows XP OOB	03.04.2008 18:39
KB893803v2	Windows Installer 3.1 (KB893803)	Türker	07.10.2008	Update	Windows XP	07.10.2008 12:32
KB898461	Windows XP için Güncelleştirme (KB898461)	SYSTEM	28.12.2010	Update	Windows XP	28.12.2010 19:47
KB923561	Windows XP için Güvenlik Güncelleştirmesi (KB923561)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:44
KB925720	Windows XP için Güncelleştirme (KB925720)	SYSTEM	31.12.2010	Update	Windows XP	31.12.2010 19:12
KB926239	Hotfix for Windows XP (KB926239)	Türker	07.10.2008	Update	Windows XP	07.10.2008 12:43
KB929399	Hotfix for Windows Media Format 11 SDK (KB929399)		N/A		Windows Media Format 11 SDK	29.12.2010 19:51
KB929399		SYSTEM	29.12.2010	Update	Windows Media Format 11 SDK	29.12.2010 19:51
KB939683	Windows Media Player 11 (KB939683) için Düzeltme		N/A		Windows Media Player 11	29.12.2010 19:50
KB939683		SYSTEM	29.12.2010	Update	Windows Media Player 11	29.12.2010 19:50
KB941569	Windows XP (KB941569) için Güvenlik Güncelleştirmesi		N/A		Windows XP	29.12.2010 19:52
KB941569		SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:52
KB944338-v2	Windows XP için Güvenlik Güncelleştirmesi (KB944338-v2)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010

						19:44
KB946102	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB946102)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB946457	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB946457)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB946573	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB946573)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB946648	Windows XP için Güvenlik Güncelleştirmesi (KB946648)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:59
KB947317	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB947317)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB948233	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB948233)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB948233v2	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB948233)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB948646	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB948646)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB949226	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB949226)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB949777	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB949777)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB950230	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB950230)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service	31.12.2010 19:10

					Pack 2	
KB950762	Windows XP için Güvenlik Güncelleştirmesi (KB950762)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:52
KB950974	Windows XP için Güvenlik Güncelleştirmesi (KB950974)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:56
KB950986	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB950986)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB951113	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB951113)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB951376-v2	Windows XP için Güvenlik Güncelleştirmesi (KB951376-v2)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 20:00
KB951748	Windows XP için Güvenlik Güncelleştirmesi (KB951748)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:47
KB952004	Windows XP için Güvenlik Güncelleştirmesi (KB952004)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:53
KB952069_WM9	Windows Media Player (KB952069) için Güvenlik Güncelleştirmesi		N/A		Windows Media Player	29.12.2010 19:54
KB952069_WM9		SYSTEM	29.12.2010	Update	Windows Media Player	29.12.2010 19:54
KB952287	Windows XP için Düzeltme (KB952287)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:51
KB952324	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB952324)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB952346	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB952346)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB952883	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB952883)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB952954	Windows XP için Güvenlik Güncelleştirmesi (KB952954)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 20:00

KB954154_WM11	Windows Media Player 11 (KB954154) için Güvenlik Güncelleştirmesi		N/A		Windows Media Player 11	29.12.2010 19:44
KB954154_WM11		SYSTEM	29.12.2010	Update	Windows Media Player 11	29.12.2010 19:44
KB954155_WM9	Windows Media Player (KB954155) için Güvenlik Güncelleştirmesi		N/A		Windows Media Player	29.12.2010 19:58
KB954155_WM9		SYSTEM	29.12.2010	Update	Windows Media Player	29.12.2010 19:58
KB954550-v5	Hotfix for Windows XP (KB954550-v5)	SYSTEM	30.12.2010	Update	Windows XP	30.12.2010 11:35
KB955069	Windows XP için Güvenlik Güncelleştirmesi (KB955069)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:45
KB955759	Windows XP için Güncelleştirme (KB955759)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:58
KB956572	Windows XP için Güvenlik Güncelleştirmesi (KB956572)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:55
KB956802	Windows XP için Güvenlik Güncelleştirmesi (KB956802)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:45
KB956803	Windows XP için Güvenlik Güncelleştirmesi (KB956803)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:59
KB956844	Windows XP için Güvenlik Güncelleştirmesi (KB956844)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:54
KB958470	Windows XP için Güvenlik Güncelleştirmesi (KB958470)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:46
KB958481	Hotfix for Microsoft .NET Framework 2.0 Service Pack 2 (KB958481)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB958483	Hotfix for Microsoft .NET Framework 3.0 Service Pack 1 (KB958483)	SYSTEM	N/A		Microsoft .NET Framework 3.0 Service Pack 2	30.12.2010 11:45
KB958484	Hotfix for Microsoft .NET Framework 3.5 SP1 (KB958484)	SYSTEM	N/A		Microsoft .NET Framework 3.5 SP1	30.12.2010 11:46
KB958644	Windows XP için Güvenlik Güncelleştirmesi (KB958644)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:45

KB958869	Windows XP için Güvenlik Güncelleştirmesi (KB958869)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:59
KB959426	Windows XP için Güvenlik Güncelleştirmesi (KB959426)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:59
KB960225	Windows XP için Güvenlik Güncelleştirmesi (KB960225)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:55
KB960803	Windows XP için Güvenlik Güncelleştirmesi (KB960803)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:46
KB960859	Windows XP için Güvenlik Güncelleştirmesi (KB960859)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:59
KB961118	Windows XP için Düzeltme (KB961118)	SYSTEM	31.12.2010	Update	Windows XP	31.12.2010 19:16
KB961501	Windows XP için Güvenlik Güncelleştirmesi (KB961501)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:54
KB961503	Windows XP için Güncelleştirme (KB961503)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:56
KB963707	Update for Microsoft .NET Framework 3.5 SP1 (KB963707)	SYSTEM	N/A		Microsoft .NET Framework 3.5 SP1	31.12.2010 19:12
KB967715	Windows XP için Güncelleştirme (KB967715)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:51
KB968389	Windows XP için Güncelleştirme (KB968389)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:44
KB969059	Windows XP için Güvenlik Güncelleştirmesi (KB969059)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:56
KB970238	Windows XP için Güvenlik Güncelleştirmesi (KB970238)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:47
KB970430	Windows XP için Güvenlik Güncelleştirmesi (KB970430)	SYSTEM	30.12.2010	Update	Windows XP	30.12.2010 20:08
KB971032	Windows XP için Güvenlik Güncelleştirmesi (KB971032)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:45
KB971468	Windows XP için Güvenlik Güncelleştirmesi (KB971468)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:59
KB971657	Windows XP için Güvenlik Güncelleştirmesi (KB971657)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:55
KB971	Windows XP için Güncelleştirme	SYST	30.12.	Upda	Windows XP	30.12.2

737	(KB971737)	EM	2010	te		010 20:01
KB971961	Windows XP için Güvenlik Güncelleştirmesi (KB971961)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:47
KB972270	Windows XP için Güvenlik Güncelleştirmesi (KB972270)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:55
KB973507	Windows XP için Güvenlik Güncelleştirmesi (KB973507)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:52
KB973540_WM9L	Windows Media Player (KB973540) için Güvenlik Güncelleştirmesi		N/A		Windows Media Player	29.12.2010 19:53
KB973540_WM9L		SYSTEM	29.12.2010	Update	Windows Media Player	29.12.2010 19:53
KB973687	Windows XP için Güncelleştirme (KB973687)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:52
KB973815	Windows XP için Güncelleştirme (KB973815)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:45
KB973869	Windows XP için Güvenlik Güncelleştirmesi (KB973869)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:54
KB973904	Windows XP için Güvenlik Güncelleştirmesi (KB973904)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:51
KB974112	Windows XP için Güvenlik Güncelleştirmesi (KB974112)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:55
KB974318	Windows XP için Güvenlik Güncelleştirmesi (KB974318)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:56
KB974392	Windows XP için Güvenlik Güncelleştirmesi (KB974392)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:50
KB974417	Security Update for Microsoft .NET Framework 2.0 Service Pack 2 (KB974417)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB974571	Windows XP için Güvenlik Güncelleştirmesi (KB974571)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:53
KB975025	Windows XP için Güvenlik Güncelleştirmesi (KB975025)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:53
KB975467	Windows XP için Güvenlik Güncelleştirmesi (KB975467)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:44
KB975	Windows XP için Güvenlik	SYST	29.12.	Upda	Windows XP	29.12.2

560	Güncelleştirmesi (KB975560)	EM	2010	te		010 19:53
KB975 561	Windows XP için Güvenlik Güncelleştirmesi (KB975561)	SYST EM	29.12. 2010	Upda te	Windows XP	29.12.2 010 19:54
KB975 562	Windows XP için Güvenlik Güncelleştirmesi (KB975562)	SYST EM	29.12. 2010	Upda te	Windows XP	29.12.2 010 19:45
KB975 713	Windows XP için Güvenlik Güncelleştirmesi (KB975713)	SYST EM	29.12. 2010	Upda te	Windows XP	29.12.2 010 19:55
KB976 576	Update for Microsoft .NET Framework 2.0 Service Pack 2 (KB976576)	SYST EM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2 010 19:14
KB976 765v2	Security Update for Microsoft .NET Framework 2.0 Service Pack 2 (KB976765)	SYST EM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2 010 19:10
KB976 769v2	Security Update for Microsoft .NET Framework 3.0 Service Pack 1 (KB976769)	SYST EM	N/A		Microsoft .NET Framework 3.0 Service Pack 2	31.12.2 010 19:11
KB977 354v2	Update for Microsoft .NET Framework 3.0 Service Pack 1 (KB977354)	SYST EM	N/A		Microsoft .NET Framework 3.0 Service Pack 2	31.12.2 010 19:15
KB977 816	Windows XP için Güvenlik Güncelleştirmesi (KB977816)	SYST EM	29.12. 2010	Upda te	Windows XP	29.12.2 010 19:52
KB977 914	Windows XP için Güvenlik Güncelleştirmesi (KB977914)	SYST EM	29.12. 2010	Upda te	Windows XP	29.12.2 010 19:47
KB978 037	Windows XP için Güvenlik Güncelleştirmesi (KB978037)	SYST EM	29.12. 2010	Upda te	Windows XP	29.12.2 010 19:55
KB978 338	Windows XP için Güvenlik Güncelleştirmesi (KB978338)	SYST EM	29.12. 2010	Upda te	Windows XP	29.12.2 010 19:55
KB978 542	Windows XP için Güvenlik Güncelleştirmesi (KB978542)	SYST EM	29.12. 2010	Upda te	Windows XP	29.12.2 010 19:47
KB978 601	Windows XP için Güvenlik Güncelleştirmesi (KB978601)	SYST EM	29.12. 2010	Upda te	Windows XP	29.12.2 010 19:51
KB978 695_W M9	Windows Media Player (KB978695) için Güvenlik Güncelleştirmesi		N/A		Windows Media Player	29.12.2 010 19:46
KB978		SYST	29.12.	Upda	Windows	29.12.2

695_WM9		EM	2010	te	Media Player	010 19:46
KB978706	Windows XP için Güvenlik Güncelleştirmesi (KB978706)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:46
KB979309	Windows XP için Güvenlik Güncelleştirmesi (KB979309)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:46
KB979482	Windows XP için Güvenlik Güncelleştirmesi (KB979482)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:46
KB979559	Windows XP için Güvenlik Güncelleştirmesi (KB979559)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:51
KB979683	Windows XP için Güvenlik Güncelleştirmesi (KB979683)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:59
KB979909	Security Update for Microsoft .NET Framework 2.0 Service Pack 2 (KB979909)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB980195	Windows XP için Güvenlik Güncelleştirmesi (KB980195)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:58
KB980218	Windows XP için Güvenlik Güncelleştirmesi (KB980218)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 20:00
KB980232	Windows XP için Güvenlik Güncelleştirmesi (KB980232)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:58
KB980773	Security Update for Microsoft .NET Framework 2.0 Service Pack 2 (KB980773)	SYSTEM	N/A		Microsoft .NET Framework 2.0 Service Pack 2	31.12.2010 19:10
KB981350	Windows XP için Güvenlik Güncelleştirmesi (KB981350)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:58
KB981793	Windows XP için Düzeltme (KB981793)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:51
KB982381	Windows XP için Güvenlik Güncelleştirmesi (KB982381)	SYSTEM	29.12.2010	Update	Windows XP	29.12.2010 19:45
MSCompPackV1	Microsoft Compression Client Pack 1.0 for Windows XP	Türker	07.10.2008	Update	Windows XP	07.10.2008 12:43
WIC		SYSTEM	30.12.2010	Update	Windows XP	30.12.2010 11:16
WMFDist11		Türker	07.10.2008	Update	Windows Media	07.10.2008

					Format 11 runtime	12:42
wmp11		Türker	07.10.2008	Update	Windows Media Player 11	07.10.2008 12:43
Wudf01000		Türker	07.10.2008	Update	Windows XP	07.10.2008 12:41

EK-2 MHV2060BH_NW18T6229459 seri nolu hard disk imajında gerçekleştirilen güncelleştirmeler

Name	Description	Installed By	Installation Date	Display Version	Update Type	Application	Last Modified Time
ie8		Barış	11.12.2009	20.090.308.140.743	Update	Windows XP	11.12.2009 14:03
KB888111WXPSP2		Barış	11.12.2009	20.040.219.000.000	Update	Windows XP	11.12.2009 12:03
KB893803v2	Windows Installer 3.1 (KB893803)	Barış	11.12.2009	03.Oca	Update	Windows XP	11.12.2009 14:33
WIC		Barış	24.07.2010	3.0.0.0	Update	Windows XP	24.07.2010 14:58
XpsEPSC		Barış	24.07.2010		Update	XML Paper Specification Shared Components Pack 1.0	24.07.2010 15:01
XpsEPSC	XML Paper Specification Shared Components Pack 1.0		N/A			XML Paper Specification Shared Components Pack 1.0	24.07.2010 15:00

EK-3 S17HJ90Q816726 seri nolu hard disk imajında gerçekleştirilen güncelleştirmeler

Name	Description	Installation Date	Update Type	Last Modified Time
	Definition Update for Windows Defender - KB915597 (Definition 1.99.322.0)	01.03.2011 19:09	AutomaticUpdates	01.03.2011 22:09
	Definition Update for Windows Defender - KB915597 (Definition 1.99.94.0)	25.02.2011 19:19	AutomaticUpdates	25.02.2011 22:19
	Definition Update for Windows Defender - KB915597 (Definition 1.97.2292.0)	22.02.2011 06:45	Windows Defender	22.02.2011 09:45
	Definition Update for Windows Defender - KB915597 (Definition 1.97.2020.0)	18.02.2011 09:58	AutomaticUpdates	18.02.2011 12:58
	Definition Update for Windows Defender - KB915597 (Definition 1.97.1752.0)	15.02.2011 16:24	AutomaticUpdates	15.02.2011 19:24
	Definition Update for Windows Defender - KB915597 (Definition 1.97.1491.0)	11.02.2011 20:04	AutomaticUpdates	11.02.2011 23:04
	Definition Update for Windows Defender - KB915597 (Definition 1.97.1233.0)	08.02.2011 10:42	AutomaticUpdates	08.02.2011 13:42
	Definition Update for Windows Defender - KB915597 (Definition 1.97.984.0)	04.02.2011 19:02	AutomaticUpdates	04.02.2011 22:02
	Definition Update for Windows Defender - KB915597 (Definition 1.97.757.0)	01.02.2011 06:35	AutomaticUpdates	01.02.2011 09:35
	Definition Update for Windows Defender - KB915597 (Definition 1.97.544.0)	28.01.2011 12:46	AutomaticUpdates	28.01.2011 15:46
	Definition Update for Windows Defender - KB915597 (Definition 1.97.286.0)	25.01.2011 11:15	Windows Defender	25.01.2011 14:15
	Definition Update for Windows Defender - KB915597 (Definition 1.97.22.0)	22.01.2011 07:21	AutomaticUpdates	22.01.2011 10:21
	Definition Update for Windows Defender - KB915597 (Definition 1.95.4180.0)	18.01.2011 18:55	AutomaticUpdates	18.01.2011 21:55
	Definition Update for Windows Defender - KB915597 (Definition 1.95.3914.0)	14.01.2011 13:33	AutomaticUpdates	14.01.2011 16:33
	Definition Update for Windows Defender - KB915597 (Definition 1.95.3662.0)	11.01.2011 20:46	AutomaticUpdates	11.01.2011 23:46
	Definition Update for Windows Defender - KB915597 (Definition 1.95.3426.0)	07.01.2011 23:12	AutomaticUpdates	08.01.2011 02:12
	Definition Update for Windows Defender - KB915597 (Definition 1.95.3177.0)	05.01.2011 03:56	AutomaticUpdates	05.01.2011 06:56
	Definition Update for Windows Defender - KB915597 (Definition 1.95.2986.0)	31.12.2010 07:04	AutomaticUpdates	31.12.2010 10:04
	Definition Update for Windows Defender - KB915597 (Definition 1.95.2903.0)	30.12.2010 10:50	AutomaticUpdates	30.12.2010 13:50
	Definition Update for Windows Defender - KB915597 (Definition 1.95.2722.0)	28.12.2010 15:03	AutomaticUpdates	28.12.2010 18:03
	Definition Update for Windows Defender - KB915597 (Definition 1.95.2533.0)	25.12.2010 02:39	AutomaticUpdates	25.12.2010 05:39
	Definition Update for Windows Defender - KB915597 (Definition 1.95.2197.0)	21.12.2010 05:38	AutomaticUpdates	21.12.2010 08:38
	Definition Update for Windows Defender -	17.12.201	AutomaticU	17.12.2010

	KB915597 (Definition 1.95.1996.0)	0 17:33	pdates	20:33
	Definition Update for Windows Defender - KB915597 (Definition 1.95.1764.0)	15.12.201 0 20:10	AutomaticU pdates	15.12.2010 23:10
	Definition Update for Windows Defender - KB915597 (Definition 1.95.1522.0)	10.12.201 0 13:01	AutomaticU pdates	10.12.2010 16:01
	Definition Update for Windows Defender - KB915597 (Definition 1.95.1304.0)	07.12.201 0 19:53	AutomaticU pdates	07.12.2010 22:53
	Definition Update for Windows Defender - KB915597 (Definition 1.95.1100.0)	04.12.201 0 02:13	AutomaticU pdates	04.12.2010 05:13
	Definition Update for Windows Defender - KB915597 (Definition 1.95.861.0)	30.11.201 0 06:17	AutomaticU pdates	30.11.2010 09:17
	Definition Update for Windows Defender - KB915597 (Definition 1.95.656.0)	26.11.201 0 16:40	AutomaticU pdates	26.11.2010 19:40
	Definition Update for Windows Defender - KB915597 (Definition 1.95.422.0)	25.11.201 0 18:50	AutomaticU pdates	25.11.2010 21:50
	Definition Update for Windows Defender - KB915597 (Definition 1.95.191.0)	19.11.201 0 18:15	AutomaticU pdates	19.11.2010 21:15
	Definition Update for Windows Defender - KB915597 (Definition 1.93.1985.0)	16.11.201 0 11:53	AutomaticU pdates	16.11.2010 14:53
	Definition Update for Windows Defender - KB915597 (Definition 1.93.1733.0)	13.11.201 0 01:54	AutomaticU pdates	13.11.2010 04:54
	Definition Update for Windows Defender - KB915597 (Definition 1.93.1456.0)	09.11.201 0 12:16	AutomaticU pdates	09.11.2010 15:16
	Definition Update for Windows Defender - KB915597 (Definition 1.93.1238.0)	05.11.201 0 23:24	AutomaticU pdates	06.11.2010 02:24
	Definition Update for Windows Defender - KB915597 (Definition 1.93.1130.0)	04.11.201 0 08:35	AutomaticU pdates	04.11.2010 11:35
	Definition Update for Windows Defender - KB915597 (Definition 1.93.948.0)	02.11.201 0 17:23	AutomaticU pdates	02.11.2010 20:23
	Definition Update for Windows Defender - KB915597 (Definition 1.93.695.0)	29.10.201 0 06:29	Windows Defender	29.10.2010 09:29
	Definition Update for Windows Defender - KB915597 (Definition 1.93.468.0)	26.10.201 0 23:18	AutomaticU pdates	27.10.2010 02:18
	Definition Update for Windows Defender - KB915597 (Definition 1.93.284.0)	22.10.201 0 09:17	AutomaticU pdates	22.10.2010 12:17
	Definition Update for Windows Defender - KB915597 (Definition 1.93.26.0)	20.10.201 0 01:45	AutomaticU pdates	20.10.2010 04:45
	Definition Update for Windows Defender - KB915597 (Definition 1.91.1817.0)	15.10.201 0 17:35	AutomaticU pdates	15.10.2010 20:35
	Definition Update for Windows Defender - KB915597 (Definition 1.91.1591.0)	12.10.201 0 06:42	AutomaticU pdates	12.10.2010 09:42
	Definition Update for Windows Defender - KB915597 (Definition 1.91.1370.0)	08.10.201 0 21:28	AutomaticU pdates	09.10.2010 00:28
	Definition Update for Windows Defender - KB915597 (Definition 1.91.1122.0)	05.10.201 0 11:41	AutomaticU pdates	05.10.2010 14:41
	Definition Update for Windows Defender - KB915597 (Definition 1.91.961.0)	02.10.201 0 05:28	AutomaticU pdates	02.10.2010 08:28
	Definition Update for Windows Defender - KB915597 (Definition 1.91.902.0)	01.10.201 0 08:19	AutomaticU pdates	01.10.2010 11:19
	Definition Update for Windows Defender - KB915597 (Definition 1.91.724.0)	28.09.201 0 23:07	Windows Defender	29.09.2010 02:07
	Definition Update for Windows Defender -	24.09.201	Windows	24.09.2010

	KB915597 (Definition 1.91.452.0)	0 13:18	Defender	16:18
	Definition Update for Windows Defender - KB915597 (Definition 1.91.253.0)	21.09.2010 16:54	AutomaticUpdates	21.09.2010 19:54
	Definition Update for Windows Defender - KB915597 (Definition 1.91.14.0)	17.09.2010 20:03	AutomaticUpdates	17.09.2010 23:03
	Definition Update for Windows Defender - KB915597 (Definition 1.89.1620.0)	14.09.2010 09:52	AutomaticUpdates	14.09.2010 12:52
	Definition Update for Windows Defender - KB915597 (Definition 1.89.1411.0)	11.09.2010 00:25	AutomaticUpdates	11.09.2010 03:25
	Definition Update for Windows Defender - KB915597 (Definition 1.89.1145.0)	07.09.2010 10:19	AutomaticUpdates	07.09.2010 13:19
	Definition Update for Windows Defender - KB915597 (Definition 1.89.901.0)	03.09.2010 06:19	AutomaticUpdates	03.09.2010 09:19
	Definition Update for Windows Defender - KB915597 (Definition 1.89.660.0)	31.08.2010 15:34	AutomaticUpdates	31.08.2010 18:34
	Definition Update for Windows Defender - KB915597 (Definition 1.89.471.0)	28.08.2010 01:07	AutomaticUpdates	28.08.2010 04:07
	Definition Update for Windows Defender - KB915597 (Definition 1.89.207.0)	24.08.2010 06:14	Windows Defender	24.08.2010 09:14
	Definition Update for Windows Defender - KB915597 (Definition 1.89.175.0)	23.08.2010 16:53	AutomaticUpdates	23.08.2010 19:53
	Definition Update for Windows Defender - KB915597 (Definition 1.87.2231.0)	19.08.2010 15:55	AutomaticUpdates	19.08.2010 18:55
	Definition Update for Windows Defender - KB915597 (Definition 1.87.1998.0)	16.08.2010 22:47	Windows Defender	17.08.2010 01:47
	Definition Update for Windows Defender - KB915597 (Definition 1.87.1828.0)	13.08.2010 16:53	AutomaticUpdates	13.08.2010 19:53
	Definition Update for Windows Defender - KB915597 (Definition 1.87.1764.0)	12.08.2010 19:34	AutomaticUpdates	12.08.2010 22:34
	Definition Update for Windows Defender - KB915597 (Definition 1.87.1528.0)	09.08.2010 19:48	AutomaticUpdates	09.08.2010 22:48
	Definition Update for Windows Defender - KB915597 (Definition 1.87.1293.0)	05.08.2010 17:34	AutomaticUpdates	05.08.2010 20:34
	Definition Update for Windows Defender - KB915597 (Definition 1.87.1042.0)	02.08.2010 20:00	AutomaticUpdates	02.08.2010 23:00
	Definition Update for Windows Defender - KB915597 (Definition 1.87.836.0)	29.07.2010 15:01	AutomaticUpdates	29.07.2010 18:01
	Definition Update for Windows Defender - KB915597 (Definition 1.87.582.0)	27.07.2010 05:13	AutomaticUpdates	27.07.2010 08:13
	Definition Update for Windows Defender - KB915597 (Definition 1.87.362.0)	22.07.2010 23:05	AutomaticUpdates	23.07.2010 02:05
	Definition Update for Windows Defender - KB915597 (Definition 1.87.146.0)	20.07.2010 08:06	AutomaticUpdates	20.07.2010 11:06
	Definition Update for Windows Defender - KB915597 (Definition 1.85.2136.0)	15.07.2010 19:14	AutomaticUpdates	15.07.2010 22:14
	Definition Update for Windows Defender - KB915597 (Definition 1.85.1905.0)	12.07.2010 23:21	Windows Defender	13.07.2010 02:21
	Definition Update for Windows Defender - KB915597 (Definition 1.85.1714.0)	09.07.2010 09:35	AutomaticUpdates	09.07.2010 12:35
	Definition Update for Windows Defender - KB915597 (Definition 1.85.1476.0)	06.07.2010 19:15	AutomaticUpdates	06.07.2010 22:15
	Definition Update for Windows Defender -	02.07.201	AutomaticU	02.07.2010

	KB915597 (Definition 1.85.1218.0)	0 07:04	pdates	10:04
	Definition Update for Windows Defender - KB915597 (Definition 1.85.967.0)	28.06.201 0 19:54	AutomaticU pdates	28.06.2010 22:54
	Definition Update for Windows Defender - KB915597 (Definition 1.85.753.0)	25.06.201 0 01:09	AutomaticU pdates	25.06.2010 04:09
	Definition Update for Windows Defender - KB915597 (Definition 1.85.532.0)	22.06.201 0 01:35	Windows Defender	22.06.2010 04:35
	Definition Update for Windows Defender - KB915597 (Definition 1.85.81.0)	17.06.201 0 17:42	AutomaticU pdates	17.06.2010 20:42
	Definition Update for Windows Defender - KB915597 (Definition 1.83.1826.0)	14.06.201 0 22:39	Windows Defender	15.06.2010 01:39
	Definition Update for Windows Defender - KB915597 (Definition 1.83.1506.0)	10.06.201 0 23:07	AutomaticU pdates	11.06.2010 02:07
	Definition Update for Windows Defender - KB915597 (Definition 1.83.1268.0)	07.06.201 0 14:16	AutomaticU pdates	07.06.2010 17:16
	Definition Update for Windows Defender - KB915597 (Definition 1.83.1076.0)	03.06.201 0 19:53	AutomaticU pdates	03.06.2010 22:53
	Definition Update for Windows Defender - KB915597 (Definition 1.83.848.0)	01.06.201 0 01:09	AutomaticU pdates	01.06.2010 04:09
	Definition Update for Windows Defender - KB915597 (Definition 1.83.642.0)	27.05.201 0 15:52	Windows Defender	27.05.2010 18:52
	Definition Update for Windows Defender - KB915597 (Definition 1.83.398.0)	24.05.201 0 16:35	AutomaticU pdates	24.05.2010 19:35
	Definition Update for Windows Defender - KB915597 (Definition 1.83.160.0)	20.05.201 0 23:03	Windows Defender	21.05.2010 02:03
	Definition Update for Windows Defender - KB915597 (Definition 1.81.1898.0)	18.05.201 0 01:07	AutomaticU pdates	18.05.2010 04:07
	Definition Update for Windows Defender - KB915597 (Definition 1.81.1622.0)	14.05.201 0 05:42	AutomaticU pdates	14.05.2010 08:42
	Definition Update for Windows Defender - KB915597 (Definition 1.81.1347.0)	10.05.201 0 15:28	AutomaticU pdates	10.05.2010 18:28
	Definition Update for Windows Defender - KB915597 (Definition 1.81.1110.0)	06.05.201 0 23:30	Windows Defender	07.05.2010 02:30
	Definition Update for Windows Defender - KB915597 (Definition 1.81.874.0)	03.05.201 0 22:50	Windows Defender	04.05.2010 01:50
	Definition Update for Windows Defender - KB915597 (Definition 1.81.660.0)	29.04.201 0 14:50	AutomaticU pdates	29.04.2010 17:50
	Definition Update for Windows Defender - KB915597 (Definition 1.81.438.0)	26.04.201 0 17:11	AutomaticU pdates	26.04.2010 20:11
	Definition Update for Windows Defender - KB915597 (Definition 1.81.149.0)	23.04.201 0 01:58	AutomaticU pdates	23.04.2010 04:58
	Definition Update for Windows Defender - KB915597 (Definition 1.81.0.0)	20.04.201 0 15:20	AutomaticU pdates	20.04.2010 18:20
	Definition Update for Windows Defender - KB915597 (Definition 1.79.2152.0)	19.04.201 0 18:43	AutomaticU pdates	19.04.2010 21:43
	Definition Update for Windows Defender - KB915597 (Definition 1.79.1918.0)	15.04.201 0 22:56	Windows Defender	16.04.2010 01:56
	Definition Update for Windows Defender - KB915597 (Definition 1.79.1631.0)	13.04.201 0 01:08	AutomaticU pdates	13.04.2010 04:08
	Definition Update for Windows Defender - KB915597 (Definition 1.79.1432.0)	09.04.201 0 07:57	Windows Defender	09.04.2010 10:57
	Definition Update for Windows Defender -	06.04.201	AutomaticU	06.04.2010

	KB915597 (Definition 1.79.1220.0)	0 01:24	pdates	04:24
	Definition Update for Windows Defender - KB915597 (Definition 1.79.953.0)	02.04.201 0 14:08	AutomaticU pdates	02.04.2010 17:08
	Definition Update for Windows Defender - KB915597 (Definition 1.79.702.0)	29.03.201 0 14:31	AutomaticU pdates	29.03.2010 17:31
	Definition Update for Windows Defender - KB915597 (Definition 1.79.495.0)	25.03.201 0 21:34	AutomaticU pdates	26.03.2010 00:34
	Definition Update for Windows Defender - KB915597 (Definition 1.79.308.0)	22.03.201 0 16:32	AutomaticU pdates	22.03.2010 19:32
	Definition Update for Windows Defender - KB915597 (Definition 1.79.130.0)	19.03.201 0 02:09	AutomaticU pdates	19.03.2010 05:09
	Definition Update for Windows Defender - KB915597 (Definition 1.77.1038.0)	15.03.201 0 18:09	AutomaticU pdates	15.03.2010 21:09
	Definition Update for Windows Defender - KB915597 (Definition 1.77.834.0)	11.03.201 0 17:46	AutomaticU pdates	11.03.2010 20:46
	Definition Update for Windows Defender - KB915597 (Definition 1.77.575.0)	08.03.201 0 20:37	AutomaticU pdates	08.03.2010 23:37
	Definition Update for Windows Defender - KB915597 (Definition 1.77.353.0)	04.03.201 0 21:13	AutomaticU pdates	05.03.2010 00:13
	Definition Update for Windows Defender - KB915597 (Definition 1.77.174.0)	01.03.201 0 21:45	AutomaticU pdates	02.03.2010 00:45
	Definition Update for Windows Defender - KB915597 (Definition 1.77.30.0)	26.02.201 0 02:17	AutomaticU pdates	26.02.2010 05:17
	Definition Update for Windows Defender - KB915597 (Definition 1.77.0.0)	25.02.201 0 07:09	AutomaticU pdates	25.02.2010 10:09
	Definition Update for Windows Defender - KB915597 (Definition 1.75.1050.0)	22.02.201 0 20:56	AutomaticU pdates	22.02.2010 23:56
	Definition Update for Windows Defender - KB915597 (Definition 1.75.924.0)	19.02.201 0 05:27	AutomaticU pdates	19.02.2010 08:27
	Definition Update for Windows Defender - KB915597 (Definition 1.75.798.0)	15.02.201 0 18:31	AutomaticU pdates	15.02.2010 21:31
	Definition Update for Windows Defender - KB915597 (Definition 1.75.657.0)	11.02.201 0 16:12	AutomaticU pdates	11.02.2010 19:12
	Definition Update for Windows Defender - KB915597 (Definition 1.75.517.0)	09.02.201 0 02:40	AutomaticU pdates	09.02.2010 05:40
	Definition Update for Windows Defender - KB915597 (Definition 1.75.377.0)	05.02.201 0 01:55	AutomaticU pdates	05.02.2010 04:55
	Definition Update for Windows Defender - KB915597 (Definition 1.75.203.0)	02.02.201 0 04:37	AutomaticU pdates	02.02.2010 07:37
	Definition Update for Windows Defender - KB915597 (Definition 1.75.94.0)	28.01.201 0 16:45	Windows Defender	28.01.2010 19:45
	Definition Update for Windows Defender - KB915597 (Definition 1.75.4.0)	27.01.201 0 02:16	AutomaticU pdates	27.01.2010 05:16
	Definition Update for Windows Defender - KB915597 (Definition 1.71.2521.0)	21.01.201 0 17:08	AutomaticU pdates	21.01.2010 20:08
	Definition Update for Windows Defender - KB915597 (Definition 1.71.2357.0)	18.01.201 0 18:57	AutomaticU pdates	18.01.2010 21:57
	Definition Update for Windows Defender - KB915597 (Definition 1.71.2204.0)	14.01.201 0 20:00	AutomaticU pdates	14.01.2010 23:00
	Definition Update for Windows Defender - KB915597 (Definition 1.71.2030.0)	12.01.201 0 04:46	AutomaticU pdates	12.01.2010 07:46
	Definition Update for Windows Defender -	07.01.201	AutomaticU	07.01.2010

	KB915597 (Definition 1.71.1885.0)	0 17:05	pdates	20:05
	Definition Update for Windows Defender - KB915597 (Definition 1.71.1705.0)	04.01.201 0 17:01	AutomaticU pdates	04.01.2010 20:01
	Definition Update for Windows Defender - KB915597 (Definition 1.71.1568.0)	01.01.201 0 04:33	AutomaticU pdates	01.01.2010 07:33
	Definition Update for Windows Defender - KB915597 (Definition 1.71.1433.0)	28.12.200 9 21:18	AutomaticU pdates	29.12.2009 00:18
	Definition Update for Windows Defender - KB915597 (Definition 1.71.1326.0)	24.12.200 9 20:56	AutomaticU pdates	24.12.2009 23:56
	Definition Update for Windows Defender - KB915597 (Definition 1.71.1143.0)	22.12.200 9 08:00	AutomaticU pdates	22.12.2009 11:00
	Definition Update for Windows Defender - KB915597 (Definition 1.71.992.0)	17.12.200 9 17:37	AutomaticU pdates	17.12.2009 20:37
	Definition Update for Windows Defender - KB915597 (Definition 1.71.833.0)	14.12.200 9 16:18	AutomaticU pdates	14.12.2009 19:18
	Definition Update for Windows Defender - KB915597 (Definition 1.71.700.0)	11.12.200 9 01:10	AutomaticU pdates	11.12.2009 04:10
	Definition Update for Windows Defender - KB915597 (Definition 1.71.570.0)	08.12.200 9 02:17	AutomaticU pdates	08.12.2009 05:17
	Definition Update for Windows Defender - KB915597 (Definition 1.71.471.0)	03.12.200 9 20:09	AutomaticU pdates	03.12.2009 23:09
	Definition Update for Windows Defender - KB915597 (Definition 1.71.346.0)	30.11.200 9 16:52	AutomaticU pdates	30.11.2009 19:52
	Definition Update for Windows Defender - KB915597 (Definition 1.71.269.0)	26.11.200 9 15:54	AutomaticU pdates	26.11.2009 18:54
	Definition Update for Windows Defender - KB915597 (Definition 1.71.129.0)	23.11.200 9 23:57	Windows Defender	24.11.2009 02:57
	Definition Update for Windows Defender - KB915597 (Definition 1.71.26.0)	20.11.200 9 02:09	AutomaticU pdates	20.11.2009 05:09
	Definition Update for Windows Defender - KB915597 (Definition 1.69.995.0)	16.11.200 9 23:35	Windows Defender	17.11.2009 02:35
	Definition Update for Windows Defender - KB915597 (Definition 1.69.881.0)	12.11.200 9 21:57	AutomaticU pdates	13.11.2009 00:57
	Definition Update for Windows Defender - KB915597 (Definition 1.69.725.0)	10.11.200 9 07:02	AutomaticU pdates	10.11.2009 10:02
	Definition Update for Windows Defender - KB915597 (Definition 1.69.643.0)	07.11.200 9 04:14	AutomaticU pdates	07.11.2009 07:14
	Definition Update for Windows Defender - KB915597 (Definition 1.69.443.0)	02.11.200 9 17:46	Windows Defender	02.11.2009 20:46
	Definition Update for Windows Defender - KB915597 (Definition 1.69.301.0)	29.10.200 9 14:54	Windows Defender	29.10.2009 17:54
	Definition Update for Windows Defender - KB915597 (Definition 1.69.144.0)	27.10.200 9 00:27	AutomaticU pdates	27.10.2009 03:27
	Definition Update for Windows Defender - KB915597 (Definition 1.69.18.0)	22.10.200 9 16:51	AutomaticU pdates	22.10.2009 19:51
	Definition Update for Windows Defender - KB915597 (Definition 1.67.940.0)	19.10.200 9 23:04	AutomaticU pdates	20.10.2009 02:04
	Definition Update for Windows Defender - KB915597 (Definition 1.67.841.0)	15.10.200 9 19:57	AutomaticU pdates	15.10.2009 22:57
	Definition Update for Windows Defender - KB915597 (Definition 1.67.698.0)	13.10.200 9 04:00	AutomaticU pdates	13.10.2009 07:00
	Definition Update for Windows Defender -	08.10.200	AutomaticU	08.10.2009

	KB915597 (Definition 1.67.543.0)	9 19:07	pdates	22:07
	Windows Update Aracısı 7.4.7600.226	07.10.200 9 01:39	AutomaticU pdates	07.10.2009 04:39
	Definition Update for Windows Defender - KB915597 (Definition 1.67.379.0)	06.10.200 9 01:41	AutomaticU pdates	06.10.2009 04:41
	Windows Vista İçin Internet Explorer 8	03.10.200 9 18:49	AutomaticU pdates	03.10.2009 21:49
	Microsoft Office Uyumluluk Paketi Service Pack 2 (SP2)	03.10.200 9 16:21	AutomaticU pdates	03.10.2009 19:21
	Microsoft Office 2003 Service Pack 3 (SP3)	03.10.200 9 16:20	AutomaticU pdates	03.10.2009 19:20
	Definition Update for Windows Defender - KB915597 (Definition 1.67.321.0)	02.10.200 9 22:49	AutomaticU pdates	03.10.2009 01:49
	Definition Update for Windows Defender - KB915597 (Definition 1.67.136.0)	28.09.200 9 17:42	AutomaticU pdates	28.09.2009 20:42
	Definition Update for Windows Defender - KB915597 (Definition 1.67.10.0)	27.09.200 9 00:39	AutomaticU pdates	27.09.2009 03:39
	Definition Update for Windows Defender - KB915597 (Definition 1.65.586.0)	10.09.200 9 20:16	AutomaticU pdates	10.09.2009 23:16
	Definition Update for Windows Defender - KB915597 (Definition 1.65.477.0)	07.09.200 9 23:23	Windows Defender	08.09.2009 02:23
	Definition Update for Windows Defender - KB915597 (Definition 1.65.330.0)	04.09.200 9 04:45	AutomaticU pdates	04.09.2009 07:45
	Definition Update for Windows Defender - KB915597 (Definition 1.65.146.0)	31.08.200 9 18:10	AutomaticU pdates	31.08.2009 21:10
	Definition Update for Windows Defender - KB915597 (Definition 1.63.2059.0)	28.08.200 9 16:09	Windows Defender	28.08.2009 19:09
	Definition Update for Windows Defender - KB915597 (Definition 1.63.1861.0)	24.08.200 9 19:25	AutomaticU pdates	24.08.2009 22:25
	Definition Update for Windows Defender - KB915597 (Definition 1.63.1684.0)	20.08.200 9 17:24	AutomaticU pdates	20.08.2009 20:24
	Definition Update for Windows Defender - KB915597 (Definition 1.63.1552.0)	18.08.200 9 02:12	AutomaticU pdates	18.08.2009 05:12
	Definition Update for Windows Defender - KB915597 (Definition 1.63.1394.0)	15.08.200 9 21:52	AutomaticU pdates	16.08.2009 00:52
	Definition Update for Windows Defender - KB915597 (Definition 1.63.1207.0)	10.08.200 9 15:42	AutomaticU pdates	10.08.2009 18:42
	Definition Update for Windows Defender - KB915597 (Definition 1.63.1021.0)	07.08.200 9 15:12	AutomaticU pdates	07.08.2009 18:12
	Definition Update for Windows Defender - KB915597 (Definition 1.63.812.0)	04.08.200 9 08:39	AutomaticU pdates	04.08.2009 11:39
	Definition Update for Windows Defender - KB915597 (Definition 1.63.604.0)	30.07.200 9 23:04	AutomaticU pdates	31.07.2009 02:04
	Definition Update for Windows Defender - KB915597 (Definition 1.63.422.0)	27.07.200 9 17:24	Windows Defender	27.07.2009 20:24
	Definition Update for Windows Defender - KB915597 (Definition 1.63.118.0)	23.07.200 9 21:28	AutomaticU pdates	24.07.2009 00:28
	Definition Update for Windows Defender - KB915597 (Definition 1.63.67.0)	23.07.200 9 01:46	AutomaticU pdates	23.07.2009 04:46
	Definition Update for Windows Defender - KB915597 (Definition 1.61.1958.0)	20.07.200 9 16:10	AutomaticU pdates	20.07.2009 19:10
	Definition Update for Windows Defender -	17.07.200	AutomaticU	17.07.2009

	KB915597 (Definition 1.61.1700.0)	9 11:00	pdates	14:00
	Definition Update for Windows Defender - KB915597 (Definition 1.61.1497.0)	13.07.200 9 16:08	AutomaticU pdates	13.07.2009 19:08
	Definition Update for Windows Defender - KB915597 (Definition 1.61.1304.0)	09.07.200 9 19:47	AutomaticU pdates	09.07.2009 22:47
	Definition Update for Windows Defender - KB915597 (Definition 1.61.1063.0)	06.07.200 9 18:56	AutomaticU pdates	06.07.2009 21:56
	Definition Update for Windows Defender - KB915597 (Definition 1.61.835.0)	02.07.200 9 14:56	AutomaticU pdates	02.07.2009 17:56
	Definition Update for Windows Defender - KB915597 (Definition 1.61.601.0)	29.06.200 9 18:00	AutomaticU pdates	29.06.2009 21:00
	Definition Update for Windows Defender - KB915597 (Definition 1.61.369.0)	25.06.200 9 23:22	Windows Defender	26.06.2009 02:22
	Definition Update for Windows Defender - KB915597 (Definition 1.61.149.0)	23.06.200 9 01:24	AutomaticU pdates	23.06.2009 04:24
	Definition Update for Windows Defender - KB915597 (Definition 1.59.1480.0)	18.06.200 9 21:20	AutomaticU pdates	19.06.2009 00:20
	Definition Update for Windows Defender - KB915597 (Definition 1.59.1267.0)	15.06.200 9 22:38	Windows Defender	16.06.2009 01:38
	Definition Update for Windows Defender - KB915597 (Definition 1.59.1107.0)	11.06.200 9 23:06	Windows Defender	12.06.2009 02:06
	Definition Update for Windows Defender - KB915597 (Definition 1.59.918.0)	11.06.200 9 00:29	AutomaticU pdates	11.06.2009 03:29
	Definition Update for Windows Defender - KB915597 (Definition 1.59.789.0)	05.06.200 9 03:48	AutomaticU pdates	05.06.2009 06:48
	Definition Update for Windows Defender - KB915597 (Definition 1.59.659.0)	01.06.200 9 19:36	AutomaticU pdates	01.06.2009 22:36
	Definition Update for Windows Defender - KB915597 (Definition 1.59.458.0)	28.05.200 9 14:12	AutomaticU pdates	28.05.2009 17:12
	Definition Update for Windows Defender - KB915597 (Definition 1.59.251.0)	26.05.200 9 02:09	AutomaticU pdates	26.05.2009 05:09
	Definition Update for Windows Defender - KB915597 (Definition 1.59.52.0)	22.05.200 9 08:20	AutomaticU pdates	22.05.2009 11:20
	Definition Update for Windows Defender - KB915597 (Definition 1.57.1556.0)	18.05.200 9 22:34	Windows Defender	19.05.2009 01:34
	Definition Update for Windows Defender - KB915597 (Definition 1.57.1329.0)	14.05.200 9 22:34	Windows Defender	15.05.2009 01:34
	Definition Update for Windows Defender - KB915597 (Definition 1.57.1094.0)	11.05.200 9 21:26	AutomaticU pdates	12.05.2009 00:26
	Definition Update for Windows Defender - KB915597 (Definition 1.57.963.0)	07.05.200 9 18:31	AutomaticU pdates	07.05.2009 21:31
	Definition Update for Windows Defender - KB915597 (Definition 1.57.806.0)	05.05.200 9 00:04	Windows Defender	05.05.2009 03:04
	Definition Update for Windows Defender - KB915597 (Definition 1.57.619.0)	01.05.200 9 21:44	AutomaticU pdates	02.05.2009 00:44
	Definition Update for Windows Defender - KB915597 (Definition 1.57.408.0)	28.04.200 9 09:13	AutomaticU pdates	28.04.2009 12:13
	Definition Update for Windows Defender - KB915597 (Definition 1.57.181.0)	23.04.200 9 23:10	Windows Defender	24.04.2009 02:10
	Definition Update for Windows Defender - KB915597 (Definition 1.55.1987.0)	21.04.200 9 22:53	AutomaticU pdates	22.04.2009 01:53
	Definition Update for Windows Defender -	13.04.200	Windows	13.04.2009

	KB915597 (Definition 1.55.1579.0)	9 19:07	Defender	22:07
	Definition Update for Windows Defender - KB915597 (Definition 1.55.1119.0)	07.04.200 9 15:29	AutomaticU pdates	07.04.2009 18:29
	Definition Update for Windows Defender - KB915597 (Definition 1.55.933.0)	03.04.200 9 11:01	AutomaticU pdates	03.04.2009 14:01
	Definition Update for Windows Defender - KB915597 (Definition 1.55.736.0)	30.03.200 9 23:07	Windows Defender	31.03.2009 02:07
	Definition Update for Windows Defender - KB915597 (Definition 1.55.543.0)	27.03.200 9 03:52	AutomaticU pdates	27.03.2009 06:52
	Definition Update for Windows Defender - KB915597 (Definition 1.55.314.0)	23.03.200 9 17:29	AutomaticU pdates	23.03.2009 20:29
	Definition Update for Windows Defender - KB915597 (Definition 1.55.103.0)	19.03.200 9 22:54	AutomaticU pdates	20.03.2009 01:54
	Definition Update for Windows Defender - KB915597 (Definition 1.53.638.0)	17.03.200 9 07:39	AutomaticU pdates	17.03.2009 10:39
	Definition Update for Windows Defender - KB915597 (Definition 1.53.431.0)	15.03.200 9 12:33	AutomaticU pdates	15.03.2009 15:33
	Definition Update for Windows Defender - KB915597 (Definition 1.53.288.0)	11.03.200 9 00:15	AutomaticU pdates	11.03.2009 03:15
	Definition Update for Windows Defender - KB915597 (Definition 1.53.256.0)	10.03.200 9 00:09	Windows Defender	10.03.2009 03:09
	Definition Update for Windows Defender - KB915597 (Definition 1.53.92.0)	05.03.200 9 20:23	AutomaticU pdates	05.03.2009 23:23
	Definition Update for Windows Defender - KB915597 (Definition 1.51.1279.0)	03.03.200 9 05:47	AutomaticU pdates	03.03.2009 08:47
	Definition Update for Windows Defender - KB915597 (Definition 1.51.1145.0)	27.02.200 9 00:25	AutomaticU pdates	27.02.2009 03:25
	Definition Update for Windows Defender - KB915597 (Definition 1.51.937.0)	23.02.200 9 15:02	AutomaticU pdates	23.02.2009 18:02
	Definition Update for Windows Defender - KB915597 (Definition 1.51.768.0)	19.02.200 9 16:46	AutomaticU pdates	19.02.2009 19:46
	Definition Update for Windows Defender - KB915597 (Definition 1.51.627.0)	17.02.200 9 01:02	AutomaticU pdates	17.02.2009 04:02
	Definition Update for Windows Defender - KB915597 (Definition 1.51.484.0)	13.02.200 9 08:49	AutomaticU pdates	13.02.2009 11:49
	Definition Update for Windows Defender - KB915597 (Definition 1.51.391.0)	09.02.200 9 23:59	Windows Defender	10.02.2009 02:59
	Definition Update for Windows Defender - KB915597 (Definition 1.51.303.0)	05.02.200 9 21:48	AutomaticU pdates	06.02.2009 00:48
	Definition Update for Windows Defender - KB915597 (Definition 1.51.124.0)	03.02.200 9 07:24	AutomaticU pdates	03.02.2009 10:24
	Definition Update for Windows Defender - KB915597 (Definition 1.49.2750.0)	30.01.200 9 02:52	AutomaticU pdates	30.01.2009 05:52
	Definition Update for Windows Defender - KB915597 (Definition 1.49.2551.0)	26.01.200 9 21:13	AutomaticU pdates	27.01.2009 00:13
	Definition Update for Windows Defender - KB915597 (Definition 1.49.2376.0)	22.01.200 9 23:55	Windows Defender	23.01.2009 02:55
	Definition Update for Windows Defender - KB915597 (Definition 1.49.2195.0)	19.01.200 9 19:08	AutomaticU pdates	19.01.2009 22:08
	Definition Update for Windows Defender - KB915597 (Definition 1.49.2011.0)	15.01.200 9 20:40	AutomaticU pdates	15.01.2009 23:40
	Definition Update for Windows Defender -	13.01.200	AutomaticU	13.01.2009

	KB915597 (Definition 1.49.1841.0)	9 14:56	pdates	17:56
	Definition Update for Windows Defender - KB915597 (Definition 1.49.1662.0)	09.01.200 9 06:50	AutomaticU pdates	09.01.2009 09:50
	Definition Update for Windows Defender - KB915597 (Definition 1.49.1455.0)	06.01.200 9 12:15	AutomaticU pdates	06.01.2009 15:15
	Definition Update for Windows Defender - KB915597 (Definition 1.49.1289.0)	01.01.200 9 18:02	AutomaticU pdates	01.01.2009 21:02
	Definition Update for Windows Defender - KB915597 (Definition 1.49.1123.0)	30.12.200 8 04:03	Windows Defender	30.12.2008 07:03
	Definition Update for Windows Defender - KB915597 (Definition 1.49.989.0)	25.12.200 8 21:05	AutomaticU pdates	26.12.2008 00:05
	Definition Update for Windows Defender - KB915597 (Definition 1.49.864.0)	22.12.200 8 23:30	Windows Defender	23.12.2008 02:30
	Definition Update for Windows Defender - KB915597 (Definition 1.49.701.0)	19.12.200 8 04:40	AutomaticU pdates	19.12.2008 07:40
	Definition Update for Windows Defender - KB915597 (Definition 1.49.523.0)	17.12.200 8 04:06	AutomaticU pdates	17.12.2008 07:06
	Definition Update for Windows Defender - KB915597 (Definition 1.49.369.0)	11.12.200 8 23:47	Windows Defender	12.12.2008 02:47
	Definition Update for Windows Defender - KB915597 (Definition 1.49.217.0)	09.12.200 8 08:04	AutomaticU pdates	09.12.2008 11:04
	Definition Update for Windows Defender - KB915597 (Definition 1.49.88.0)	05.12.200 8 00:03	AutomaticU pdates	05.12.2008 03:03
	Definition Update for Windows Defender - KB915597 (Definition 1.47.966.0)	02.12.200 8 14:46	AutomaticU pdates	02.12.2008 17:46
	Definition Update for Windows Defender - KB915597 (Definition 1.47.864.0)	27.11.200 8 20:53	AutomaticU pdates	27.11.2008 23:53
	Windows Update Aracısı 7.2.6001.788	26.11.200 8 03:09	AutomaticU pdates	26.11.2008 06:09
	Definition Update for Windows Defender - KB915597 (Definition 1.47.708.0)	25.11.200 8 04:15	AutomaticU pdates	25.11.2008 07:15
	Definition Update for Windows Defender - KB915597 (Definition 1.47.567.0)	21.11.200 8 03:13	AutomaticU pdates	21.11.2008 06:13
	Definition Update for Windows Defender - KB915597 (Definition 1.47.487.0)	20.11.200 8 03:43	AutomaticU pdates	20.11.2008 06:43
	Definition Update for Windows Defender - KB915597 (Definition 1.47.283.0)	15.11.200 8 04:42	AutomaticU pdates	15.11.2008 07:42
	Definition Update for Windows Defender - KB915597 (Definition 1.47.167.0)	12.11.200 8 23:43	AutomaticU pdates	13.11.2008 02:43
	Definition Update for Windows Defender - KB915597 (Definition 1.47.15.0)	08.11.200 8 05:06	AutomaticU pdates	08.11.2008 08:06
	Definition Update for Windows Defender - KB915597 (Definition 1.45.1466.0)	06.11.200 8 20:00	Windows Defender	06.11.2008 23:00
	Definition Update for Windows Defender - KB915597 (Definition 1.45.1403.0)	05.11.200 8 10:16	AutomaticU pdates	05.11.2008 13:16
	Definition Update for Windows Defender - KB915597 (Definition 1.45.1246.0)	31.10.200 8 21:47	AutomaticU pdates	01.11.2008 00:47
	Definition Update for Windows Defender - KB915597 (Definition 1.45.1162.0)	29.10.200 8 21:31	AutomaticU pdates	30.10.2008 00:31
	Definition Update for Windows Defender - KB915597 (Definition 1.45.1012.0)	26.10.200 8 09:56	AutomaticU pdates	26.10.2008 12:56
	Definition Update for Windows Defender -	17.10.200	AutomaticU	18.10.2008

	KB915597 (Definition 1.45.731.0)	8 22:55	pdates	01:55
	Definition Update for Windows Defender - KB915597 (Definition 1.45.430.0)	10.10.200 8 22:32	Windows Defender	11.10.2008 01:32
	Definition Update for Windows Defender - KB915597 (Definition 1.45.380.0)	09.10.200 8 20:57	AutomaticU pdates	09.10.2008 23:57
	Definition Update for Windows Defender - KB915597 (Definition 1.45.280.0)	08.10.200 8 01:21	AutomaticU pdates	08.10.2008 04:21
	Definition Update for Windows Defender - KB915597 (Definition 1.45.124.0)	02.10.200 8 21:33	AutomaticU pdates	03.10.2008 00:33
	Definition Update for Windows Defender - KB915597 (Definition 1.43.801.0)	28.09.200 8 21:55	AutomaticU pdates	29.09.2008 00:55
	Windows Update Aracısı 7.2.6001.784	01.01.200 5 19:30	AutomaticU pdates	01.01.2005 22:30
KB21 64913	Microsoft Silverlight için Güncelleştirme (KB2164913)	04.09.201 0 00:01	AutomaticU pdates	04.09.2010 03:01
KB22 02122	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB2202122)	15.07.201 0 00:01	AutomaticU pdates	15.07.2010 03:01
KB22 51399	Microsoft Office Word 2003 Güvenlik Güncelleştirmesi (KB2251399)	13.08.201 0 00:03	AutomaticU pdates	13.08.2010 03:03
KB22 64403	Microsoft Office Excel 2003 Güvenlik Güncelleştirmesi (KB2264403)	13.08.201 0 00:03	AutomaticU pdates	13.08.2010 03:03
KB22 77947	2007 Microsoft Office Sistemi Güvenlik Güncelleştirmesi (KB2277947)	13.08.201 0 00:00	AutomaticU pdates	13.08.2010 03:00
KB22 79246	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB2279246)	13.08.201 0 00:01	AutomaticU pdates	13.08.2010 03:01
KB22 84695	Microsoft Office Publisher 2003 Güvenlik Güncelleştirmesi (KB2284695)	16.12.201 0 01:01	AutomaticU pdates	16.12.2010 04:01
KB22 88613	Microsoft Office 2003 Güvenlik Güncelleştirmesi (KB2288613)	16.09.201 0 00:00	AutomaticU pdates	16.09.2010 03:00
KB22 89158	Microsoft Office 2007 Sistemi Güvenlik Güncelleştirmesi (KB2289158)	11.11.201 0 01:02	AutomaticU pdates	11.11.2010 04:02
KB22 89163	Microsoft Office 2003 Güvenlik Güncelleştirmesi (KB2289163)	16.12.201 0 01:02	AutomaticU pdates	16.12.2010 04:02
KB22 89187	Microsoft Office 2003 Güvenlik Güncelleştirmesi (KB2289187)	11.11.201 0 01:02	AutomaticU pdates	11.11.2010 04:02
KB22 91595	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB2291595)	16.09.201 0 00:02	AutomaticU pdates	16.09.2010 03:02
KB22 93428	Microsoft Office Outlook 2003 Güvenlik Güncelleştirmesi (KB2293428)	16.09.201 0 00:02	AutomaticU pdates	16.09.2010 03:02
KB23 44875	2007 Microsoft Office Sistemi Güvenlik Güncelleştirmesi (KB2344875)	15.10.201 0 00:07	AutomaticU pdates	15.10.2010 03:07
KB23 44893	Microsoft Office Excel 2003 Güvenlik Güncelleştirmesi (KB2344893)	15.10.201 0 00:03	AutomaticU pdates	15.10.2010 03:03
KB23 44911	Microsoft Office Word 2003 Güvenlik Güncelleştirmesi (KB2344911)	15.10.201 0 00:06	AutomaticU pdates	15.10.2010 03:06
KB23 45043	2007 Microsoft Office Sistemi Güvenlik Güncelleştirmesi (KB2345043)	15.10.201 0 00:06	AutomaticU pdates	15.10.2010 03:06
KB24 10707	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB2410707)	15.10.201 0 00:05	AutomaticU pdates	15.10.2010 03:05
KB24 13304	Microsoft Office PowerPoint 2003 Güvenlik Güncelleştirmesi (KB2413304)	11.11.201 0 01:01	AutomaticU pdates	11.11.2010 04:01
KB24	Microsoft Silverlight için Güncelleştirme	30.09.201	AutomaticU	30.09.2010

16427	(KB2416427)	0 00:01	pdates	03:01
KB24 35682	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB2435682)	11.11.201 0 01:00	AutomaticU pdates	11.11.2010 04:00
KB24 49798	Microsoft Office Outlook 2003 Güncelleştirmesi (KB2449798)	16.12.201 0 01:02	AutomaticU pdates	16.12.2010 04:02
KB24 66074	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB2466074)	16.12.201 0 01:02	AutomaticU pdates	16.12.2010 04:02
KB24 77244	Microsoft Silverlight için Güncelleştirme (KB2477244)	19.12.201 0 01:01	AutomaticU pdates	19.12.2010 04:01
KB24 92441	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB2492441)	11.02.201 1 08:33	AutomaticU pdates	11.02.2011 11:33
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Şubat 2011 (KB890830)	11.02.201 1 08:33	AutomaticU pdates	11.02.2011 11:33
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Ocak 2011 (KB890830)	11.01.201 1 20:58	AutomaticU pdates	11.01.2011 23:58
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Aralık 2010 (KB890830)	16.12.201 0 01:01	AutomaticU pdates	16.12.2010 04:01
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Kasım 2010 (KB890830)	11.11.201 0 01:02	AutomaticU pdates	11.11.2010 04:02
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Ekim 2010 (KB890830)	15.10.201 0 00:05	AutomaticU pdates	15.10.2010 03:05
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Eylül 2010 (KB890830)	16.09.201 0 00:02	AutomaticU pdates	16.09.2010 03:02
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Ağustos 2010 (KB890830)	13.08.201 0 00:02	AutomaticU pdates	13.08.2010 03:02
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Temmuz 2010 (KB890830)	15.07.201 0 00:02	AutomaticU pdates	15.07.2010 03:02
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Haziran 2010 (KB890830)	10.06.201 0 00:02	AutomaticU pdates	10.06.2010 03:02
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Mayıs 2010 (KB890830)	13.05.201 0 00:03	AutomaticU pdates	13.05.2010 03:03
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Nisan 2010 (KB890830)	16.04.201 0 00:02	AutomaticU pdates	16.04.2010 03:02
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Mart 2010 (KB890830)	11.03.201 0 01:03	AutomaticU pdates	11.03.2010 04:03
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Şubat 2010 (KB890830)	10.02.201 0 01:03	AutomaticU pdates	10.02.2010 04:03
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Ocak 2010 (KB890830)	14.01.201 0 01:02	AutomaticU pdates	14.01.2010 04:02
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Aralık 2009 (KB890830)	11.12.200 9 01:02	AutomaticU pdates	11.12.2009 04:02
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Kasım 2009 (KB890830)	12.11.200 9 01:02	AutomaticU pdates	12.11.2009 04:02
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Ekim 2009 (KB890830)	15.10.200 9 00:05	AutomaticU pdates	15.10.2009 03:05
KB89 0830	Windows Kötü Amaçlı Yazılımları Temizleme Aracı - Eylül 2009 (KB890830)	03.10.200 9 18:51	AutomaticU pdates	03.10.2009 21:51
KB90 5866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Nisan 2010] (KB905866)	16.04.201 0 00:01	AutomaticU pdates	16.04.2010 03:01
KB90 5866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Mart 2010] (KB905866)	11.03.201 0 01:04	AutomaticU pdates	11.03.2010 04:04
KB90	Windows Mail Önemsiz E-posta Filtresi	10.02.201	AutomaticU	10.02.2010

5866	Güncelleştirmesi [Şubat 2010] (KB905866)	0 01:01	pdates	04:01
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Ocak 2010] (KB905866)	14.01.2010 01:02	AutomaticUpdates	14.01.2010 04:02
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Aralık 2009] (KB905866)	11.12.2009 01:01	AutomaticUpdates	11.12.2009 04:01
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Kasım 2009] (KB905866)	12.11.2009 01:00	AutomaticUpdates	12.11.2009 04:00
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Ekim 2009] (KB905866)	15.10.2009 00:03	AutomaticUpdates	15.10.2009 03:03
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Eylül 2009] (KB905866)	10.09.2009 00:01	AutomaticUpdates	10.09.2009 03:01
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Ağustos 2009] (KB905866)	13.08.2009 00:00	AutomaticUpdates	13.08.2009 03:00
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Temmuz 2009] (KB905866)	16.07.2009 00:00	AutomaticUpdates	16.07.2009 03:00
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Haziran 2009] (KB905866)	11.06.2009 00:01	AutomaticUpdates	11.06.2009 03:01
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Mayıs 2009] (KB905866)	14.05.2009 00:00	AutomaticUpdates	14.05.2009 03:00
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Nisan 2009] (KB905866)	17.04.2009 00:02	AutomaticUpdates	17.04.2009 03:02
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Mart 2009] (KB905866)	11.03.2009 01:00	AutomaticUpdates	11.03.2009 04:00
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Şubat 2009] (KB905866)	11.02.2009 01:00	AutomaticUpdates	11.02.2009 04:00
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Ocak 2009] (KB905866)	15.01.2009 01:00	AutomaticUpdates	15.01.2009 04:00
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Aralık 2008] (KB905866)	14.12.2008 01:01	AutomaticUpdates	14.12.2008 04:01
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Kasım 2008] (KB905866)	13.11.2008 01:00	AutomaticUpdates	13.11.2008 04:00
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Ekim 2008] (KB905866)	15.10.2008 00:01	AutomaticUpdates	15.10.2008 03:01
KB905866	Windows Mail Önemsiz E-posta Filtresi Güncelleştirmesi [Eylül 2008] (KB905866)	29.09.2008 00:04	AutomaticUpdates	29.09.2008 03:04
KB907417	Office 2003 için Güncelleştirme (KB907417)	03.10.2009 18:53	AutomaticUpdates	03.10.2009 21:53
KB921598	Microsoft Office 2003 Güvenlik Güncelleştirmesi (KB921598)	03.10.2009 16:18	AutomaticUpdates	03.10.2009 19:18
KB925902	Windows Vista Güvenlik Güncelleştirmesi (KB925902)	29.09.2008 00:01	AutomaticUpdates	29.09.2008 03:01
KB929123	Windows Vista için Windows Mail Toplu Güvenlik Güncelleştirmesi (KB929123)	29.09.2008 00:33	AutomaticUpdates	29.09.2008 03:33
KB929399	Windows Vista için Windows Media Format 11 SDK Güncelleştirmesi (KB929399)	29.09.2008 00:21	AutomaticUpdates	29.09.2008 03:21
KB929916	Microsoft .NET Framework Sürüm 2.0 Güvenlik Güncelleştirmesi (KB929916)	14.12.2008 01:00	AutomaticUpdates	14.12.2008 04:00
KB929916	Microsoft .NET Framework Sürüm 2.0 Güvenlik Güncelleştirmesi (KB929916)	29.09.2008 00:15	AutomaticUpdates	29.09.2008 03:15
KB930178	Windows Vista Güvenlik Güncelleştirmesi (KB930178)	14.12.2008 01:01	AutomaticUpdates	14.12.2008 04:01
KB93	Windows Vista Güvenlik Güncelleştirmesi	29.09.200	AutomaticU	29.09.2008

0178	(KB930178)	8 00:29	pdates	03:29
KB93 0857	Windows Vista Güncelleştirmesi (KB930857)	29.09.200 8 00:17	AutomaticU pdates	29.09.2008 03:17
KB93 1099	Windows Vista Güncelleştirmesi (KB931099)	29.09.200 8 00:26	AutomaticU pdates	29.09.2008 03:26
KB93 1213	Windows Vista Güvenlik Güncelleştirmesi (KB931213)	29.09.200 8 00:02	AutomaticU pdates	29.09.2008 03:02
KB93 1573	Windows Vista Güncelleştirmesi (KB931573)	29.09.200 8 00:01	AutomaticU pdates	29.09.2008 03:01
KB93 2471	.NET Framework 3.0 Güncelleştirmesi: x86 (KB932471)	29.09.200 8 00:30	AutomaticU pdates	29.09.2008 03:30
KB93 3579	Windows Vista Güvenlik Güncelleştirmesi (KB933579)	29.09.200 8 00:06	AutomaticU pdates	29.09.2008 03:06
KB93 3729	Windows Vista Güvenlik Güncelleştirmesi (KB933729)	29.09.200 8 00:02	AutomaticU pdates	29.09.2008 03:02
KB93 3928	Windows Vista Güncelleştirmesi (KB933928)	29.09.200 8 00:06	AutomaticU pdates	29.09.2008 03:06
KB93 5807	Windows Vista Güvenlik Güncelleştirmesi (KB935807)	29.09.200 8 00:20	AutomaticU pdates	29.09.2008 03:20
KB93 6021	Windows Vista Güvenlik Güncelleştirmesi (KB936021)	29.09.200 8 00:17	AutomaticU pdates	29.09.2008 03:17
KB93 6181	Microsoft XML Core Services 4.0 Service Pack 2 Güvenlik Güncelleştirmesi (KB936181)	29.09.200 8 00:01	AutomaticU pdates	29.09.2008 03:01
KB93 6357	Windows Vista Güncelleştirmesi (KB936357)	29.09.200 8 00:23	AutomaticU pdates	29.09.2008 03:23
KB93 6782	Windows Vista Güvenlik Güncelleştirmesi (KB936782)	29.09.200 8 00:19	AutomaticU pdates	29.09.2008 03:19
KB93 6824	Windows Vista Güncelleştirmesi (KB936824)	29.09.200 8 00:25	AutomaticU pdates	29.09.2008 03:25
KB93 6825	Windows Vista Güncelleştirmesi (KB936825)	29.09.200 8 00:08	AutomaticU pdates	29.09.2008 03:08
KB93 7077	Windows Vista Güncelleştirmesi (KB937077)	29.09.200 8 00:03	AutomaticU pdates	29.09.2008 03:03
KB93 7287	Windows Vista Güncelleştirmesi (KB937287)	01.10.200 8 00:00	AutomaticU pdates	01.10.2008 03:00
KB93 8123	Windows Vista Güvenlik Güncelleştirmesi (KB938123)	29.09.200 8 00:29	AutomaticU pdates	29.09.2008 03:29
KB93 8127	Windows Vista Güvenlik Güncelleştirmesi (KB938127)	29.09.200 8 00:02	AutomaticU pdates	29.09.2008 03:02
KB93 8194	Windows Vista Güncelleştirmesi (KB938194)	29.09.200 8 00:35	AutomaticU pdates	29.09.2008 03:35
KB93 8371	Windows Vista Güncelleştirmesi (KB938371)	29.09.200 8 00:10	AutomaticU pdates	29.09.2008 03:10
KB93 8464	Windows Vista Güvenlik Güncelleştirmesi (KB938464)	29.09.200 8 00:16	AutomaticU pdates	29.09.2008 03:16
KB93 8979	Windows Vista Güncelleştirmesi (KB938979)	29.09.200 8 00:05	AutomaticU pdates	29.09.2008 03:05
KB93 9159	Windows Vista Güncelleştirmesi (KB939159)	29.09.200 8 00:00	AutomaticU pdates	29.09.2008 03:00
KB94 0510	Windows Vista Güncelleştirmesi (KB940510)	30.09.200 8 00:01	AutomaticU pdates	30.09.2008 03:01

KB941569	Windows Vista Güvenlik Güncelleştirmesi (KB941569)	29.09.2008 00:07	AutomaticUpdates	29.09.2008 03:07
KB941649	Windows Vista Güncelleştirmesi (KB941649)	29.09.2008 00:32	AutomaticUpdates	29.09.2008 03:32
KB941651	Windows Vista Güncelleştirmesi (KB941651)	29.09.2008 00:21	AutomaticUpdates	29.09.2008 03:21
KB941693	Windows Vista Güvenlik Güncelleştirmesi (KB941693)	29.09.2008 00:08	AutomaticUpdates	29.09.2008 03:08
KB941833	Microsoft XML Core Services 4.0 Service Pack 2 Güncelleştirmesi (KB941833)	30.09.2008 00:01	AutomaticUpdates	30.09.2008 03:01
KB942624	Windows Vista Güvenlik Güncelleştirmesi (KB942624)	29.09.2008 00:03	AutomaticUpdates	29.09.2008 03:03
KB943055	Windows Vista Güvenlik Güncelleştirmesi (KB943055)	29.09.2008 00:03	AutomaticUpdates	29.09.2008 03:03
KB943078	Windows Vista Güvenlik Güncelleştirmesi (KB943078)	29.09.2008 00:01	AutomaticUpdates	29.09.2008 03:01
KB943411	Windows Vista Güncelleştirmesi (KB943411)	29.09.2008 00:04	AutomaticUpdates	29.09.2008 03:04
KB943899	Windows Vista Güncelleştirmesi (KB943899)	29.09.2008 00:18	AutomaticUpdates	29.09.2008 03:18
KB943973	Microsoft Works Suite 2005 Güvenlik Güncelleştirmesi (KB943973)	03.10.2009 16:21	AutomaticUpdates	03.10.2009 19:21
KB945185	Office 2003 Güvenlik Güncelleştirmesi (KB945185)	03.10.2009 16:20	AutomaticUpdates	03.10.2009 19:20
KB945432	Microsoft Office Outlook 2003 Güvenlik Güncelleştirmesi (KB945432)	03.10.2009 16:21	AutomaticUpdates	03.10.2009 19:21
KB945553	Windows Vista Güvenlik Güncelleştirmesi (KB945553)	29.09.2008 00:03	AutomaticUpdates	29.09.2008 03:03
KB946026	Windows Vista Güvenlik Güncelleştirmesi (KB946026)	29.09.2008 00:31	AutomaticUpdates	29.09.2008 03:31
KB946041	Windows Vista Güncelleştirmesi (KB946041)	29.09.2008 00:25	AutomaticUpdates	29.09.2008 03:25
KB946456	Windows Vista Güvenlik Güncelleştirmesi (KB946456)	29.09.2008 00:15	AutomaticUpdates	29.09.2008 03:15
KB947319	Microsoft Office Web Components Güvenlik Güncelleştirmesi (KB947319)	04.10.2009 16:44	AutomaticUpdates	04.10.2009 19:44
KB948590	Windows Vista Güvenlik Güncelleştirmesi (KB948590)	29.09.2008 00:07	AutomaticUpdates	29.09.2008 03:07
KB948881	Windows Vista için ActiveX Kill Bitleri Güvenlik Güncelleştirmesi (KB948881)	10.02.2009 15:29	AutomaticUpdates	10.02.2009 18:29
KB948988	Microsoft Office PowerPoint 2003 Güvenlik Güncelleştirmesi (KB948988)	03.10.2009 16:20	AutomaticUpdates	03.10.2009 19:20
KB949810	Office Orijinal Ürün Avantajı Bildirimleri (KB949810) tr	03.10.2009 16:21	AutomaticUpdates	03.10.2009 19:21
KB949939	Windows Vista Güncelleştirmesi (KB949939)	29.09.2008 00:01	AutomaticUpdates	29.09.2008 03:01
KB950124	Windows Vista Güncelleştirmesi (KB950124)	29.09.2008 00:19	AutomaticUpdates	29.09.2008 03:19
KB950125	Windows Vista Güncelleştirmesi (KB950125)	29.09.2008 00:01	AutomaticUpdates	29.09.2008 03:01
KB950126	Windows Vista için Media Center Toplu Güncelleştirmesi (KB950126)	29.09.2008 00:02	AutomaticUpdates	29.09.2008 03:02

KB950213	Microsoft Office Publisher 2003 Güvenlik Güncelleştirmesi (KB950213)	03.10.2009 16:22	AutomaticUpdates	03.10.2009 19:22
KB950582	Windows Vista Güvenlik Güncelleştirmesi (KB950582)	29.09.2008 00:28	AutomaticUpdates	29.09.2008 03:28
KB950762	Windows Vista Güvenlik Güncelleştirmesi (KB950762)	29.09.2008 00:04	AutomaticUpdates	29.09.2008 03:04
KB950974	Windows Vista Güvenlik Güncelleştirmesi (KB950974)	30.09.2008 00:01	AutomaticUpdates	30.09.2008 03:01
KB951066	Windows Vista için Windows Mail Güvenlik Güncelleştirmesi (KB951066)	14.12.2008 01:00	AutomaticUpdates	14.12.2008 04:00
KB951066	Windows Vista için Windows Mail Güvenlik Güncelleştirmesi (KB951066)	29.09.2008 00:02	AutomaticUpdates	29.09.2008 03:02
KB951072	Windows Vista Güncelleştirmesi (KB951072)	29.09.2008 00:24	AutomaticUpdates	29.09.2008 03:24
KB951376	Windows Vista Güvenlik Güncelleştirmesi (KB951376)	29.09.2008 00:10	AutomaticUpdates	29.09.2008 03:10
KB951535	Microsoft Office 2003 Güvenlik Güncelleştirmesi (KB951535)	04.10.2009 16:43	AutomaticUpdates	04.10.2009 19:43
KB951698	Windows Vista Güvenlik Güncelleştirmesi (KB951698)	29.09.2008 00:02	AutomaticUpdates	29.09.2008 03:02
KB951847	Microsoft .NET Framework 3.5 Service Pack 1 (KB951847) x86 Dil Paketi	16.08.2009 01:43	AutomaticUpdates	16.08.2009 04:43
KB951847	Microsoft .NET Framework 3.5 Service Pack 1 ve .NET Framework 3.5 Ailesi Güncelleştirmesi (KB951847) x86	09.08.2009 00:18	AutomaticUpdates	09.08.2009 03:18
KB952004	Windows Vista Güvenlik Güncelleştirmesi (KB952004)	17.04.2009 00:02	AutomaticUpdates	17.04.2009 03:02
KB952069	Windows Vista Güvenlik Güncelleştirmesi (KB952069)	13.12.2008 01:00	AutomaticUpdates	13.12.2008 04:00
KB952287	Windows Vista Güncelleştirmesi (KB952287)	29.09.2008 00:07	AutomaticUpdates	29.09.2008 03:07
KB953155	Windows Vista Güvenlik Güncelleştirmesi (KB953155)	30.10.2008 01:00	AutomaticUpdates	30.10.2008 04:00
KB953404	Microsoft Office 2003 Güvenlik Güncelleştirmesi (KB953404)	03.10.2009 16:22	AutomaticUpdates	03.10.2009 19:22
KB953432	Microsoft Office Outlook 2003 Güncelleştirmesi (KB953432)	03.10.2009 18:53	AutomaticUpdates	03.10.2009 21:53
KB953733	Windows Vista Güvenlik Güncelleştirmesi (KB953733)	29.09.2008 00:36	AutomaticUpdates	29.09.2008 03:36
KB953838	Windows Vista için Internet Explorer 7 Toplu Güvenlik Güncelleştirmesi (KB953838)	29.09.2008 00:12	AutomaticUpdates	29.09.2008 03:12
KB953839	Windows Vista için ActiveX Kill Bitleri Toplu Güvenlik Güncelleştirmesi (KB953839)	29.09.2008 00:03	AutomaticUpdates	29.09.2008 03:03
KB954154	Windows Vista Güvenlik Güncelleştirmesi (KB954154)	29.09.2008 00:22	AutomaticUpdates	29.09.2008 03:22
KB954155	Windows Vista İçin Windows Media Format Çalışma Zamanı 11 Güvenlik Güncelleştirmesi (KB954155)	15.10.2009 00:00	AutomaticUpdates	15.10.2009 03:00
KB954211	Windows Vista Güvenlik Güncelleştirmesi (KB954211)	15.10.2008 00:01	AutomaticUpdates	15.10.2008 03:01
KB954366	Windows Vista Güncelleştirmesi (KB954366)	29.09.2008 00:34	AutomaticUpdates	29.09.2008 03:34

KB954430	Microsoft XML Core Services 4.0 Service Pack 2 Güvenlik Güncelleştirmesi (KB954430)	13.11.2008 01:00	AutomaticUpdates	13.11.2008 04:00
KB954459	Windows Vista Güvenlik Güncelleştirmesi (KB954459)	13.11.2008 01:00	AutomaticUpdates	13.11.2008 04:00
KB954464	Microsoft Office Word 2003 Güvenlik Güncelleştirmesi (KB954464)	03.10.2009 18:50	AutomaticUpdates	03.10.2009 21:50
KB954478	Office 2003 Güvenlik Güncelleştirmesi (KB954478)	03.10.2009 18:50	AutomaticUpdates	03.10.2009 21:50
KB955020	Windows Vista Güncelleştirmesi (KB955020)	29.09.2008 00:14	AutomaticUpdates	29.09.2008 03:14
KB955069	Windows Vista Güvenlik Güncelleştirmesi (KB955069)	13.11.2008 01:00	AutomaticUpdates	13.11.2008 04:00
KB955430	Windows Vista Güncelleştirmesi (KB955430)	02.05.2009 00:00	AutomaticUpdates	02.05.2009 03:00
KB955439	Access Snapshot Viewer 2003 Güvenlik Güncelleştirmesi (KB955439)	03.10.2009 16:18	AutomaticUpdates	03.10.2009 19:18
KB955466	Microsoft Office Excel 2003 Güvenlik Güncelleştirmesi (KB955466)	03.10.2009 18:52	AutomaticUpdates	03.10.2009 21:52
KB955519	Windows Vista için Media Center Toplu Güncelleştirmesi (KB955519)	30.10.2008 01:00	AutomaticUpdates	30.10.2008 04:00
KB955839	Windows Vista Güncelleştirmesi (KB955839)	13.12.2008 01:03	AutomaticUpdates	13.12.2008 04:03
KB956390	Windows Vista için Internet Explorer 7 Toplu Güvenlik Güncelleştirmesi (KB956390)	15.10.2008 00:00	AutomaticUpdates	15.10.2008 03:00
KB956391	Windows Vista için ActiveX Kill Bitleri Toplu Güvenlik Güncelleştirmesi (KB956391)	15.10.2008 00:02	AutomaticUpdates	15.10.2008 03:02
KB956572	Windows Vista Güvenlik Güncelleştirmesi (KB956572)	17.04.2009 00:01	AutomaticUpdates	17.04.2009 03:01
KB956744	Windows Vista Güvenlik Güncelleştirmesi (KB956744)	13.08.2009 00:01	AutomaticUpdates	13.08.2009 03:01
KB956802	Windows Vista Güvenlik Güncelleştirmesi (KB956802)	14.12.2008 01:01	AutomaticUpdates	14.12.2008 04:01
KB956841	Windows Vista Güvenlik Güncelleştirmesi (KB956841)	15.10.2008 00:01	AutomaticUpdates	15.10.2008 03:01
KB957095	Windows Vista Güvenlik Güncelleştirmesi (KB957095)	15.10.2008 00:01	AutomaticUpdates	15.10.2008 03:01
KB957097	Windows Vista Güvenlik Güncelleştirmesi (KB957097)	14.12.2008 01:01	AutomaticUpdates	14.12.2008 04:01
KB957097	Windows Vista Güvenlik Güncelleştirmesi (KB957097)	13.11.2008 01:00	AutomaticUpdates	13.11.2008 04:00
KB957321	Windows Vista Güncelleştirmesi (KB957321)	14.12.2008 01:00	AutomaticUpdates	14.12.2008 04:00
KB957321	Windows Vista Güncelleştirmesi (KB957321)	27.11.2008 01:00	AutomaticUpdates	27.11.2008 04:00
KB957388	Windows Vista Güncelleştirmesi (KB957388)	14.12.2008 01:01	AutomaticUpdates	14.12.2008 04:01
KB957784	Microsoft Office PowerPoint 2003 Güvenlik Güncelleştirmesi (KB957784)	04.10.2009 16:45	AutomaticUpdates	04.10.2009 19:45
KB958215	Windows Vista için Internet Explorer 7 Toplu Güvenlik Güncelleştirmesi (KB958215)	13.12.2008 01:01	AutomaticUpdates	13.12.2008 04:01
KB958484	Hotfix for Microsoft .NET Framework 3.5 SP1 (KB958484)	N/A		09.08.2009 03:16

KB958623	Windows Vista Güvenlik Güncelleştirmesi (KB958623)	14.12.2008 01:00	AutomaticUpdates	14.12.2008 04:00
KB958624	Windows Vista Güvenlik Güncelleştirmesi (KB958624)	13.12.2008 01:01	AutomaticUpdates	13.12.2008 04:01
KB958644	Windows Vista Güvenlik Güncelleştirmesi (KB958644)	27.10.2008 04:27	AutomaticUpdates	27.10.2008 07:27
KB958687	Windows Vista Güvenlik Güncelleştirmesi (KB958687)	15.01.2009 01:00	AutomaticUpdates	15.01.2009 04:00
KB958690	Windows Vista Güvenlik Güncelleştirmesi (KB958690)	11.03.2009 01:00	AutomaticUpdates	11.03.2009 04:00
KB958869	Windows Vista Güvenlik Güncelleştirmesi (KB958869)	15.10.2009 00:03	AutomaticUpdates	15.10.2009 03:03
KB959108	Windows Vista Güncelleştirmesi (KB959108)	27.11.2008 01:00	AutomaticUpdates	27.11.2008 04:00
KB959130	Windows Vista Güncelleştirmesi (KB959130)	27.11.2008 01:00	AutomaticUpdates	27.11.2008 04:00
KB959426	Windows Vista Güvenlik Güncelleştirmesi (KB959426)	17.04.2009 00:01	AutomaticUpdates	17.04.2009 03:01
KB959772	Windows Vista Güncelleştirmesi (KB959772)	11.03.2009 01:00	AutomaticUpdates	11.03.2009 04:00
KB960225	Windows Vista Güvenlik Güncelleştirmesi (KB960225)	11.03.2009 01:00	AutomaticUpdates	11.03.2009 04:00
KB960544	Windows Vista için Media Center Toplu Güncelleştirmesi (KB960544)	17.02.2009 01:00	AutomaticUpdates	17.02.2009 04:00
KB960714	Windows Vista için Internet Explorer 7 Güvenlik Güncelleştirmesi (KB960714)	19.12.2008 01:00	AutomaticUpdates	19.12.2008 04:00
KB960715	Windows Vista için ActiveX Kill Bitleri Güncelleştirme Paketi (KB960715)	11.02.2009 01:00	AutomaticUpdates	11.02.2009 04:00
KB960803	Windows Vista Güvenlik Güncelleştirmesi (KB960803)	17.04.2009 00:02	AutomaticUpdates	17.04.2009 03:02
KB961260	Windows Vista için Internet Explorer 7 Toplu Güvenlik Güncelleştirmesi (KB961260)	11.02.2009 01:01	AutomaticUpdates	11.02.2009 04:01
KB961371	Windows Vista Güvenlik Güncelleştirmesi (KB961371)	16.07.2009 00:00	AutomaticUpdates	16.07.2009 03:00
KB961501	Windows Vista Güvenlik Güncelleştirmesi (KB961501)	11.06.2009 00:02	AutomaticUpdates	11.06.2009 03:02
KB963027	Windows Vista İçin Internet Explorer 7 Toplu Güvenlik Güncelleştirmesi (KB963027)	17.04.2009 00:01	AutomaticUpdates	17.04.2009 03:01
KB963707	Update for Microsoft .NET Framework 3.5 SP1 (KB963707)	N/A		02.09.2009 03:00
KB963707	.NET Framework Assistant 1.0 x86 için .NET Framework 3.5 Service Pack 1 Güncelleştirmesi (KB963707)	02.09.2009 00:00	AutomaticUpdates	02.09.2009 03:00
KB967632	Windows Vista İçin Media Center Toplu Güncelleştirmesi (KB967632)	14.06.2009 22:25	AutomaticUpdates	15.06.2009 01:25
KB967723	Windows Vista Güvenlik Güncelleştirmesi (KB967723)	10.09.2009 00:02	AutomaticUpdates	10.09.2009 03:02
KB968389	Windows Vista Güncelleştirmesi (KB968389)	25.08.2009 00:00	AutomaticUpdates	25.08.2009 03:00
KB968537	Windows Vista Güvenlik Güncelleştirmesi (KB968537)	11.06.2009 00:02	AutomaticUpdates	11.06.2009 03:02
KB968816	Windows Vista İçin Windows Media Format Çalışma Zamanı 11 Güvenlik	10.09.2009 00:02	AutomaticUpdates	10.09.2009 03:02

	Güncelleştirmesi (KB968816)			
KB969603	Microsoft Office Word 2003 Güvenlik Güncelleştirmesi (KB969603)	04.10.2009 16:43	AutomaticUpdates	04.10.2009 19:43
KB969613	2007 Microsoft Office Sistemi Güvenlik Güncelleştirmesi (KB969613)	04.10.2009 16:43	AutomaticUpdates	04.10.2009 19:43
KB969618	Microsoft Office Sistemi 2007 Güvenlik Güncelleştirmesi (KB969618)	04.10.2009 16:44	AutomaticUpdates	04.10.2009 19:44
KB969679	2007 Microsoft Office Sistemi Güvenlik Güncelleştirmesi (KB969679)	04.10.2009 16:45	AutomaticUpdates	04.10.2009 19:45
KB969681	Microsoft Office Excel 2003 Güvenlik Güncelleştirmesi (KB969681)	04.10.2009 16:44	AutomaticUpdates	04.10.2009 19:44
KB969897	Windows Vista İçin Internet Explorer 7 Toplu Güvenlik Güncelleştirmesi (KB969897)	11.06.2009 00:01	AutomaticUpdates	11.06.2009 03:01
KB969898	Windows Vista için ActiveX Kill Bitleri Güncelleştirme Paketi (KB969898)	11.06.2009 00:01	AutomaticUpdates	11.06.2009 03:01
KB969947	Windows Vista Güvenlik Güncelleştirmesi (KB969947)	12.11.2009 01:01	AutomaticUpdates	12.11.2009 04:01
KB970238	Windows Vista Güvenlik Güncelleştirmesi (KB970238)	11.06.2009 00:01	AutomaticUpdates	11.06.2009 03:01
KB970430	Windows Vista Güncelleştirmesi (KB970430)	11.12.2009 01:02	AutomaticUpdates	11.12.2009 04:02
KB970653	Windows Vista Güncelleştirmesi (KB970653)	29.08.2009 00:01	AutomaticUpdates	29.08.2009 03:01
KB970710	Windows Vista Güvenlik Güncelleştirmesi (KB970710)	10.09.2009 00:02	AutomaticUpdates	10.09.2009 03:02
KB971468	Windows Vista Güvenlik Güncelleştirmesi (KB971468)	10.02.2010 01:03	AutomaticUpdates	10.02.2010 04:03
KB971486	Windows Vista Güvenlik Güncelleştirmesi (KB971486)	15.10.2009 00:04	AutomaticUpdates	15.10.2009 03:04
KB971557	Windows Vista Güvenlik Güncelleştirmesi (KB971557)	13.08.2009 00:01	AutomaticUpdates	13.08.2009 03:01
KB971657	Windows Vista Güvenlik Güncelleştirmesi (KB971657)	13.08.2009 00:01	AutomaticUpdates	13.08.2009 03:01
KB971737	Windows Vista Güncelleştirmesi (KB971737)	11.12.2009 01:03	AutomaticUpdates	11.12.2009 04:03
KB971961	Windows Vista İçin Jscript 5.8 Güvenlik Güncelleştirmesi (KB971961)	04.10.2009 16:45	AutomaticUpdates	04.10.2009 19:45
KB971961	Windows Vista İçin Jscript 5.7 Güvenlik Güncelleştirmesi (KB971961)	10.09.2009 00:01	AutomaticUpdates	10.09.2009 03:01
KB972036	Windows Vista Güncelleştirmesi (KB972036)	04.09.2009 00:00	AutomaticUpdates	04.09.2009 03:00
KB972145	Windows Vista Güncelleştirmesi (KB972145)	29.10.2009 01:01	AutomaticUpdates	29.10.2009 04:01
KB972260	Windows Vista İçin Internet Explorer 7 Toplu Güvenlik Güncelleştirmesi (KB972260)	30.07.2009 00:01	AutomaticUpdates	30.07.2009 03:01
KB972270	Windows Vista Güvenlik Güncelleştirmesi (KB972270)	14.01.2010 01:02	AutomaticUpdates	14.01.2010 04:02
KB972580	Microsoft Office 2003 Güvenlik Güncelleştirmesi (KB972580)	15.10.2009 00:02	AutomaticUpdates	15.10.2009 03:02
KB972581	2007 Microsoft Office Sistemi Güvenlik Güncelleştirmesi (KB972581)	15.10.2009 00:02	AutomaticUpdates	15.10.2009 03:02
KB97	Windows Vista için ActiveX Kill Bitleri Toplu	16.07.200	AutomaticU	16.07.2009

3346	Güvenlik Güncelleştirmesi (KB973346)	9 00:00	pdates	03:00
KB973443	Microsoft Office Word 2003 Güvenlik Güncelleştirmesi (KB973443)	12.11.2009 01:01	AutomaticUpdates	12.11.2009 04:01
KB973475	Microsoft Office Excel 2003 Güvenlik Güncelleştirmesi (KB973475)	12.11.2009 01:03	AutomaticUpdates	12.11.2009 04:03
KB973507	Windows Vista Güvenlik Güncelleştirmesi (KB973507)	13.08.2009 00:01	AutomaticUpdates	13.08.2009 03:01
KB973515	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB973515)	03.10.2009 18:50	AutomaticUpdates	03.10.2009 21:50
KB973525	Windows Vista İçin ActiveX Kill Bitleri Toplu Güvenlik Güncelleştirmesi (KB973525)	15.10.2009 00:01	AutomaticUpdates	15.10.2009 03:01
KB973540	Windows Vista Güvenlik Güncelleştirmesi (KB973540)	13.08.2009 00:01	AutomaticUpdates	13.08.2009 03:01
KB973565	Windows Vista Güvenlik Güncelleştirmesi (KB973565)	12.11.2009 01:00	AutomaticUpdates	12.11.2009 04:00
KB973687	Windows Vista Güncelleştirmesi (KB973687)	26.11.2009 01:02	AutomaticUpdates	26.11.2009 04:02
KB973688	Microsoft XML Core Services 4.0 Service Pack 2 Güncelleştirmesi (KB973688)	26.11.2009 01:01	AutomaticUpdates	26.11.2009 04:01
KB973704	2007 Microsoft Office Sistemi Güvenlik Güncelleştirmesi (KB973704)	12.11.2009 01:02	AutomaticUpdates	12.11.2009 04:02
KB973705	Microsoft Office Outlook 2003 Güvenlik Güncelleştirmesi (KB973705)	15.10.2009 00:05	AutomaticUpdates	15.10.2009 03:05
KB973768	Windows Vista Güvenlik Güncelleştirmesi (KB973768)	10.09.2009 00:01	AutomaticUpdates	10.09.2009 03:01
KB973917	Windows Vista Güncelleştirmesi (KB973917)	11.03.2010 01:01	AutomaticUpdates	11.03.2010 04:01
KB973917	Windows Vista Güncelleştirmesi (KB973917)	11.12.2009 16:13	AutomaticUpdates	11.12.2009 19:13
KB974145	Windows Vista Güvenlik Güncelleştirmesi (KB974145)	10.02.2010 01:01	AutomaticUpdates	10.02.2010 04:01
KB974306	Windows Vista İçin Media Center Toplu Güncelleştirmesi (KB974306)	15.10.2009 00:02	AutomaticUpdates	15.10.2009 03:02
KB974318	Windows Vista Güvenlik Güncelleştirmesi (KB974318)	11.12.2009 01:00	AutomaticUpdates	11.12.2009 04:00
KB974455	Windows Vista İçin Internet Explorer 8 Toplu Güvenlik Güncelleştirmesi (KB974455)	15.10.2009 00:02	AutomaticUpdates	15.10.2009 03:02
KB974467	Windows Vista İçin Microsoft .NET Framework 2.0 Service Pack 2 Güvenlik Güncelleştirmesi (KB974467)	15.10.2009 00:03	AutomaticUpdates	15.10.2009 03:03
KB974554	Microsoft Office 2003 Güvenlik Güncelleştirmesi (KB974554)	15.10.2009 00:03	AutomaticUpdates	15.10.2009 03:03
KB974571	Windows Vista Güvenlik Güncelleştirmesi (KB974571)	15.10.2009 00:01	AutomaticUpdates	15.10.2009 03:01
KB974771	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB974771)	15.10.2009 00:01	AutomaticUpdates	15.10.2009 03:01
KB975051	Microsoft Office 2003 Güvenlik Güncelleştirmesi (KB975051)	11.12.2009 01:03	AutomaticUpdates	11.12.2009 04:03
KB975364	Windows Vista için Internet Explorer 8 Uyumluluk Görünümü Listesi Güncelleştirmesi (KB975364)	29.10.2009 01:01	AutomaticUpdates	29.10.2009 04:01
KB97	Windows Vista Güvenlik Güncelleştirmesi	15.10.200	AutomaticU	15.10.2009

5467	(KB975467)	9 00:05	pdates	03:05
KB975517	Windows Vista Güvenlik Güncelleştirmesi (KB975517)	15.10.2009 00:01	AutomaticUpdates	15.10.2009 03:01
KB975560	Windows Vista Güvenlik Güncelleştirmesi (KB975560)	10.02.2010 01:01	AutomaticUpdates	10.02.2010 04:01
KB975561	Windows Vista İçin Movie Maker 6.0 Güvenlik Güncelleştirmesi (KB975561)	11.03.2010 01:04	AutomaticUpdates	11.03.2010 04:04
KB975929	Windows Vista Güncelleştirmesi (KB975929)	25.02.2010 01:01	AutomaticUpdates	25.02.2010 04:01
KB975958	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB975958)	12.11.2009 01:01	AutomaticUpdates	12.11.2009 04:01
KB976098	Windows Vista Güncelleştirmesi (KB976098)	26.11.2009 01:02	AutomaticUpdates	26.11.2009 04:02
KB976325	Windows Vista İçin Internet Explorer 8 Toplu Güvenlik Güncelleştirmesi (KB976325)	11.12.2009 01:02	AutomaticUpdates	11.12.2009 04:02
KB976382	Microsoft Office 2003 Güvenlik Güncelleştirmesi (KB976382)	13.05.2010 00:03	AutomaticUpdates	13.05.2010 03:03
KB976470	Windows Vista Güncelleştirmesi (KB976470)	26.11.2009 01:01	AutomaticUpdates	26.11.2009 04:01
KB976662	Windows Vista Güncelleştirmesi (KB976662)	25.02.2010 01:02	AutomaticUpdates	25.02.2010 04:02
KB976749	Update for Internet Explorer 8 for Windows Vista (KB976749)	04.11.2009 13:06	AutomaticUpdates	04.11.2009 16:06
KB976881	Microsoft Office PowerPoint 2003 Güvenlik Güncelleştirmesi (KB976881)	10.02.2010 01:01	AutomaticUpdates	10.02.2010 04:01
KB976882	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB976882)	11.12.2009 01:03	AutomaticUpdates	11.12.2009 04:03
KB977165	Windows Vista Güvenlik Güncelleştirmesi (KB977165)	10.02.2010 01:02	AutomaticUpdates	10.02.2010 04:02
KB977713	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB977713)	10.02.2010 01:03	AutomaticUpdates	10.02.2010 04:03
KB977816	Windows Vista Güvenlik Güncelleştirmesi (KB977816)	16.04.2010 00:01	AutomaticUpdates	16.04.2010 03:01
KB977840	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB977840)	14.01.2010 01:02	AutomaticUpdates	14.01.2010 04:02
KB978207	Windows Vista İçin Internet Explorer 8 Toplu Güvenlik Güncelleştirmesi (KB978207)	23.01.2010 01:01	AutomaticUpdates	23.01.2010 04:01
KB978251	Windows Vista Güvenlik Güncelleştirmesi (KB978251)	10.02.2010 01:00	AutomaticUpdates	10.02.2010 04:00
KB978262	Windows Vista İçin ActiveX Kill Bitleri Toplu Güvenlik Güncelleştirmesi (KB978262)	10.02.2010 01:02	AutomaticUpdates	10.02.2010 04:02
KB978338	Windows Vista Güvenlik Güncelleştirmesi (KB978338)	16.04.2010 00:01	AutomaticUpdates	16.04.2010 03:01
KB978380	2007 Microsoft Office Sistemi Güvenlik Güncelleştirmesi (KB978380)	11.03.2010 01:02	AutomaticUpdates	11.03.2010 04:02
KB978474	Microsoft Office Excel 2003 Güvenlik Güncelleştirmesi (KB978474)	11.03.2010 01:04	AutomaticUpdates	11.03.2010 04:04
KB978506	Windows Vista için Internet Explorer 8 Uyumluluk Görünümü Listesi Güncelleştirmesi (KB978506)	28.01.2010 01:00	AutomaticUpdates	28.01.2010 04:00
KB978551	Update for Microsoft Office 2003 (KB978551)	19.12.2009 01:00	AutomaticUpdates	19.12.2009 04:00

KB978601	Windows Vista Güvenlik Güncelleştirmesi (KB978601)	14.04.2010 00:00	AutomaticUpdates	14.04.2010 03:00
KB979099	Update for Rights Management Services Client for Windows Vista (KB979099)	25.02.2010 01:02	AutomaticUpdates	25.02.2010 04:02
KB979306	Windows Vista Güncelleştirmesi (KB979306)	25.02.2010 01:02	AutomaticUpdates	25.02.2010 04:02
KB979309	Windows Vista Güvenlik Güncelleştirmesi (KB979309)	14.04.2010 00:00	AutomaticUpdates	14.04.2010 03:00
KB979683	Windows Vista Güvenlik Güncelleştirmesi (KB979683)	16.04.2010 00:03	AutomaticUpdates	16.04.2010 03:03
KB979771	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB979771)	11.03.2010 01:04	AutomaticUpdates	11.03.2010 04:04
KB980182	Windows Vista İçin Internet Explorer 8 Toplu Güvenlik Güncelleştirmesi (KB980182)	01.04.2010 00:01	AutomaticUpdates	01.04.2010 03:01
KB980232	Windows Vista Güvenlik Güncelleştirmesi (KB980232)	16.04.2010 00:03	AutomaticUpdates	16.04.2010 03:03
KB980302	Windows Vista için Internet Explorer 8 Uyumluluk Görünümü Listesi Güncelleştirmesi (KB980302)	25.03.2010 01:01	AutomaticUpdates	25.03.2010 04:01
KB980373	Microsoft Office Outlook 2003 Güvenlik Güncelleştirmesi (KB980373)	15.07.2010 00:03	AutomaticUpdates	15.07.2010 03:03
KB980469	Microsoft Office Publisher 2003 Güvenlik Güncelleştirmesi (KB980469)	16.04.2010 00:00	AutomaticUpdates	16.04.2010 03:00
KB980923	Microsoft Office InfoPath 2003 Güvenlik Güncelleştirmesi (KB980923)	10.06.2010 00:01	AutomaticUpdates	10.06.2010 03:01
KB981332	Windows Vista Güvenlik Güncelleştirmesi (KB981332)	16.04.2010 00:02	AutomaticUpdates	16.04.2010 03:02
KB981432	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB981432)	16.04.2010 00:01	AutomaticUpdates	16.04.2010 03:01
KB981715	2007 Microsoft Office Sistemi Güncelleştirmesi (KB981715)	16.04.2010 00:03	AutomaticUpdates	16.04.2010 03:03
KB981716	Microsoft Office Access 2003 Güvenlik Güncelleştirmesi (KB981716)	15.07.2010 00:02	AutomaticUpdates	15.07.2010 03:02
KB981725	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB981725)	13.05.2010 00:01	AutomaticUpdates	13.05.2010 03:01
KB982122	Microsoft Office Publisher 2003 Güvenlik Güncelleştirmesi (KB982122)	10.06.2010 00:03	AutomaticUpdates	10.06.2010 03:03
KB982133	Microsoft Office Excel 2003 Güvenlik Güncelleştirmesi (KB982133)	10.06.2010 00:04	AutomaticUpdates	10.06.2010 03:04
KB982134	Microsoft Office Word 2003 Güvenlik Güncelleştirmesi (KB982134)	10.06.2010 00:03	AutomaticUpdates	10.06.2010 03:03
KB982157	Microsoft Office PowerPoint 2003 Güvenlik Güncelleştirmesi (KB982157)	10.06.2010 00:01	AutomaticUpdates	10.06.2010 03:01
KB982311	Microsoft Office 2003 Güvenlik Güncelleştirmesi (KB982311)	10.06.2010 00:04	AutomaticUpdates	10.06.2010 03:04
KB982312	2007 Microsoft Office Sistemi Güvenlik Güncelleştirmesi (KB982312)	10.06.2010 00:03	AutomaticUpdates	10.06.2010 03:03
KB982331	2007 Microsoft Office Sistemi Güvenlik Güncelleştirmesi (KB982331)	10.06.2010 00:01	AutomaticUpdates	10.06.2010 03:01
KB982926	Microsoft Silverlight Güncelleştirmesi (KB982926)	04.06.2010 00:01	AutomaticUpdates	04.06.2010 03:01
KB983503	Outlook Önemsiz E-posta Filtresi 2003 Güncelleştirmesi (KB983503)	10.06.2010 00:02	AutomaticUpdates	10.06.2010 03:02

Q936181	Security update for MSXML4 SP2 (KB936181)	N/A		29.09.2008 03:01
Q941833	Security update for MSXML4 SP2 (KB941833)	N/A		30.09.2008 03:01
Q954430	Security update for MSXML4 SP2 (KB954430)	N/A		13.11.2008 04:00
Q973688	Security update for MSXML4 SP2 (KB973688)	N/A		26.11.2009 04:00

EK-4 ST3120827AS_4MS1TF89 seri nolu hard disk imajı üzerindeki Antivirüs uygulaması ile tarama sonucu

Dosya Adı	Kötücül Yazılım Türü
C:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\154754DE-0000B343.eml	HTML/TrojanDownloader.Agent.NBT.Gen truva atı
C:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\1D186270AC-0000B6C1.eml	HTML/Fraud.AV truva atı
C:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\23C948CC-0000B352.eml	HTML/TrojanDownloader.Agent.NBU.Gen truva atı
C:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\2F0C549B-0000B712.eml	HTML/Fraud.AV truva atı
C:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\33081EDC-0000B600.eml	HTML/Fraud.AV truva atı
C:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\4269757D-0000B79F.eml	HTML/Fraud.AV truva atı
C:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\46CF01D3-0000B35A.eml	HTML/TrojanDownloader.Agent.NBU.Gen truva atı
C:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\473E6737-0000B1A2.eml	HTML/TrojanDownloader.Agent.NBR truva atı
C:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\49442E40-0000B6A3.eml	HTML/Fraud.AV truva atı
C:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\4AFE7274-0000B803.eml	HTML/Fraud.AV truva atı
C:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\4CFF64A0-0000B605.eml	HTML/Fraud.AV truva atı
C:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\58B026CA-0000B34E.eml	HTML/TrojanDownloader.Agent.NBU.Gen truva atı
C:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\590E765F-0000B360.eml	HTML/TrojanDownloader.Agent.NBU.Gen truva atı
C:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\5BB903F4-0000B19D.eml	HTML/TrojanDownloader.Agent.NBR truva atı
C:\Documents and Settings\Türker\Local Settings\Application	HTML/Fraud.AV truva

Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\6D696A15-0000B569.eml	atı

EK-5 ST3120827AS_4MS1TF89 seri nolu hard disk imajının Güncel Antivirüs uygulaması ile tarama sonucu

Kötücül Yazılım Türü	Dosya Adı
detected: Trojan program Backdoor.Win32.Bandok.zs	file: G:\Documents and Settings\Administrator\Start Menu\Programlar\Baslangiç\MSN Messenger.exe
detected: Trojan program Backdoor.Win32.Bandok.zs	file: G:\Documents and Settings\All Users\Start Menu\Programlar\Baslangiç\MSN Messenger.exe
detected: Trojan program Backdoor.Win32.Bandok.zs	file: G:\Documents and Settings\Türker\Application Data\Adobe\svchost.exe
detected: Trojan program Backdoor.Win32.Turkojan.jgu	file: G:\Documents and Settings\Türker\Application Data\Adobereader10\Svchost.exe
detected: Trojan program Trojan-FakeAV.Win32.Agent.tv	file: G:\Documents and Settings\Türker\Belgelerim\Youtube_Jacker_2\setup.exe
detected: Trojan program Trojan-Clicker.Win32.Scorpech.ab	file: G:\Documents and Settings\Türker\Desktop\Packmatronic 1.0 TeV.exe
not found: Trojan program Trojan-Spy.HTML.Fraud.gen (modification)	file: G:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (barist)\Junk E-mail\41BB26E9-000008DB.eml
not found: Trojan program Trojan-Spy.HTML.Fraud.gen (modification)	file: G:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\0923196E-00003E85.eml
not found: Trojan program Trojan-Spy.HTML.Fraud.gen (modification)	file: G:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\2C67451C-0000C49C.eml
not found: Trojan program Trojan-Spy.HTML.Fraud.gen (modification)	file: G:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\3FD556DD-00003EAD.eml
not found: Trojan program Trojan-Spy.HTML.Fraud.gen (modification)	file: G:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\53E758BC-0000C62D.eml
not found: Trojan program Exploit.HTML.Iframe.FileDownload (modification)	file: G:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Storage Folders\Alinan Klasör\Odatv (info)\Önemsiz e-posta\44C53D41-0000008D.eml
detected: Trojan	file: G:\Documents and Settings\Türker\Start

program Backdoor.Win32.Bandok.zs	Menu\Programlar\Baslangiç\MSN Messenger.exe
detected: adware not-a-virus:AdWare.Win32.Agent.rcd	file: G:\Program Files\Avea Jet Mobil Modem\Component\BIDevManager.dll
detected: adware not-a-virus:AdWare.Win32.Agent.rce	file: G:\Program Files\Avea Jet Mobil Modem\Component\BIRas.dll
detected: adware not-a-virus:AdWare.Win32.Agent.rhg	file: G:\Program Files\Avea Jet Mobil Modem\Component\CMCOMService.dll
detected: Trojan program Trojan.Win32.VBKrypt.bbaw	file: G:\U3ROM\Driver.exe
detected: Trojan program Trojan.Win32.VBKrypt.bbaw	file: H:\U3ROM\Driver.exe
detected: Trojan program Trojan-Spy.HTML.Fraud.gen (modification)	mail body: G:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (barist)\Junk E-mail\41BB26E9-000008DB.eml/text/html
detected: Trojan program Trojan-Spy.HTML.Fraud.gen (modification)	mail body: G:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\0923196E-00003E85.eml/text/html
detected: Trojan program Trojan-Spy.HTML.Fraud.gen (modification)	mail body: G:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\2C67451C-0000C49C.eml/text/html
detected: Trojan program Trojan-Spy.HTML.Fraud.gen (modification)	mail body: G:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\3FD556DD-00003EAD.eml/text/html
detected: Trojan program Trojan-Spy.HTML.Fraud.gen (modification)	mail body: G:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (info)\Inbox\53E758BC-0000C62D.eml/text/html
detected: Trojan program Exploit.HTML.Iframe.FileDownload (modification)	mail body: G:\Documents and Settings\Türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Storage Folders\Alinan Klasör\Odatv (info)\Önemsiz e-posta\44C53D41-0000008D.eml/text/html

EK-6 MHV2060BH_NW18T6229459 seri nolu hard disk imajı üzerindeki Antivirüs uygulaması ile tarama sonucu

Dosya Adı	Kötücül Yazılım türü
C:\KURTARDIM\New Folder\SmileyCentralSetup2.1.50.3-3.exe	Win32/Toolbar.MyWebSearch.O uygulama türevi
C:\Programlar\bsp212941.rar » RAR » bsp212941\Keygen_bsp_pro2.x.exe	Win32/Keygen.AG uygulama türevi
D:\Documents and Settings\Barış\Application Data\hidserv.exe	Win32/Injector.ENH truva atı türevi
D:\Documents and Settings\Barış\Application Data\Sun\Java\Deployment\cache\6.0\45\53a44ead-673ca127 » ZIP » Polat.class	Java/TrojanDownloader.Agent.NCC truva atı
D:\Documents and Settings\Barış\Application Data\Sun\Java\Deployment\cache\6.0\60\5c2bd6bc-7e89708d » ZIP » vmain.class	Win32/Agent.FQRCZBA truva atı türevi olabilir
D:\Documents and Settings\Barış\Local Settings\Temp\dhq.dll	Win32/TrojanDropper.Small.NLW truva atı türevi
D:\Documents and Settings\Barış\Local Settings\Temp\jar_cache1819216091733354042.tmp	Win32/Injector.ENH truva atı türevi
D:\Documents and Settings\Barış\Local Settings\Temp\javafire2733307070907000575.exe	Win32/Injector.ENH truva atı türevi
D:\Documents and Settings\Barış\Local Settings\Temporary Internet Files\OLK4\Duyuru (2).pdf	JS/Exploit.Pdfka.OQB truva atı
D:\Documents and Settings\Barış\Local Settings\Temporary Internet Files\OLK4\Duyuru (3).pdf	JS/Exploit.Pdfka.OQB truva atı
D:\Documents and Settings\Barış\Local Settings\Temporary Internet Files\OLK4\Duyuru (4).pdf	JS/Exploit.Pdfka.OQB truva atı
D:\Documents and Settings\Barış\Local Settings\Temporary Internet Files\OLK4\Duyuru.pdf	JS/Exploit.Pdfka.OQB truva atı

EK-7 MHV2060BH_NW18T6229459 seri nolu hard disk imajının Güncel Antivirüs uygulaması ile tarama sonucu

Kötücül Yazılım Türü	Dosya Adı
detected: virus Worm.Win32.AutoRun.bqil	file: G:\Documents and Settings\Baris\Application Data\hidserv.exe
detected: Trojan program Trojan.Win32.Genome.nyeg	file: G:\Documents and Settings\Baris\Application Data\Microsoft\Network\svchost.exe
detected: Trojan program Trojan.Win32.Genome.oxxy	file: G:\Documents and Settings\Baris\Application Data\Microsoft\Network\wuauclt.exe
detected: Trojan program Trojan-Downloader.Java.OpenConnection.ex	file: G:\Documents and Settings\Baris\Application Data\Sun\Java\Deployment\cache\6.0\45\53a44ead-673ca127/Polat.class
detected: Trojan program Backdoor.Win32.Bandok.zs	file: G:\Documents and Settings\Baris\Local Settings\Temp\adobe1.exe
detected: Trojan program Backdoor.Win32.Bandok.zv	file: G:\Documents and Settings\Baris\Local Settings\Temp\dhq.dll
detected: Trojan program Backdoor.Win32.Bandok.zv	file: G:\Documents and Settings\Baris\Local Settings\Temp\dhq.dll//data0000
detected: virus Worm.Win32.AutoRun.bqil	file: G:\Documents and Settings\Baris\Local Settings\Temp\jar_cache1819216091733354042.tmp
detected: virus Worm.Win32.AutoRun.bqil	file: G:\Documents and Settings\Baris\Local Settings\Temp\javafire2733307070907000575.exe
detected: Trojan program Exploit.Win32.CVE-2010-2883.a	file: G:\Documents and Settings\Baris\Local Settings\Temporary Internet Files\OLK4\Duyuru (2).pdf
detected: Trojan program Exploit.Win32.CVE-2010-2883.a	file: G:\Documents and Settings\Baris\Local Settings\Temporary Internet Files\OLK4\Duyuru (2).pdf//data0013
detected: Trojan program Exploit.Win32.CVE-2010-2883.a	file: G:\Documents and Settings\Baris\Local Settings\Temporary Internet Files\OLK4\Duyuru (3).pdf
detected: Trojan program Exploit.Win32.CVE-2010-2883.a	file: G:\Documents and Settings\Baris\Local Settings\Temporary Internet Files\OLK4\Duyuru (3).pdf//data0013
detected: Trojan program Exploit.Win32.CVE-2010-2883.a	file: G:\Documents and Settings\Baris\Local Settings\Temporary Internet Files\OLK4\Duyuru (4).pdf
detected: Trojan program Exploit.Win32.CVE-2010-2883.a	file: G:\Documents and Settings\Baris\Local Settings\Temporary Internet Files\OLK4\Duyuru (4).pdf//data0013
detected: Trojan program Exploit.Win32.CVE-2010-2883.a	file: G:\Documents and Settings\Baris\Local Settings\Temporary Internet Files\OLK4\Duyuru.pdf
detected: Trojan program Exploit.Win32.CVE-2010-2883.a	file: G:\Documents and Settings\Baris\Local Settings\Temporary Internet Files\OLK4\Duyuru.pdf//data0013
detected: adware not-a-virus:AdWare.Win32.Agent.rcd	file: G:\Program Files\Avea Jet Mobil Modem\Component\BIDevManager.dll
detected: adware not-a-virus:AdWare.Win32.Agent.rce	file: G:\Program Files\Avea Jet Mobil Modem\Component\BIRas.dll
detected: adware not-a-virus:AdWare.Win32.Agent.rhg	file: G:\Program Files\Avea Jet Mobil Modem\Component\CMCOMService.dll
detected: Trojan program Trojan-FakeAV.Win32.Agent.tv	file: H:\BARIS YEDEK 11122009\DEKSTOP\BARIS\Youtube_Jacker_2.rar/Youtube_Jacker_2\setup.exe

detected: Trojan program Trojan-FakeAV.Win32.Agent.tv	file: H:\BARIS YEDEK 11122009\DEKSTOP\BARIS\Youtube_Jacker_2\setup.exe
detected: Trojan program Exploit.Win32.CVE-2010-2883.a	file: G:\Documents and Settings\Baris\Local Settings\Temporary Internet Files\OLK4\Duyuru (2).pdf//data0014
detected: Trojan program Exploit.Win32.CVE-2010-2883.a	file: G:\Documents and Settings\Baris\Local Settings\Temporary Internet Files\OLK4\Duyuru (3).pdf//data0014

EK-8 S17HJ90Q816726 seri nolu hard disk imajı üzerindeki Antivirüs uygulaması ile tarama sonucu

Dosya Adı	Kötücül Yazılım Türü
C:\Program Files\Winamp\Lang\Winamp-tr-tr.wlz » ZIP » ml_wire.lng	probably a variant of Win32/Agent trojan
C:\Users\user\yedek 04.01.2006.rar » RAR » yedek 04.01.2006\masa □st□ yedek\ilimin yeri\Obezlik.exe	Win32/Alman.NAB virus
C:\Users\user\yedek 04.01.2006.rar » RAR » yedek 04.01.2006\masa □st□ yedek\ilimin yeri\hesap makinesi.exe	Win32/Alman.NAB virus
C:\Users\user\yedek 04.01.2006.rar » RAR » yedek 04.01.2006\masa □st□ yedek\ilimin yeri\ilim nas□l biri.exe	Win32/Alman.NAB virus
C:\Users\user\AppData\Local\Temp\jar_cache3228180793729402572.tmp » ZIP » sklif/Hieeyfc.class	a variant of Java/Exploit.Agent.F trojan
C:\Users\user\AppData\Local\Temp\jar_cache3228180793729402572.tmp » ZIP » sklif/Hirwfee.class	a variant of Java/TrojanDownloader.Agent.NBA trojan
C:\Users\user\AppData\Local\Temp\jar_cache3228180793729402572.tmp » ZIP » sklif/Hiydcxed.class	a variant of Java/TrojanDownloader.Agent.NBA trojan
C:\Users\user\AppData\Local\Temp\jar_cache3746291637984595421.tmp » ZIP » wedfd/HkdfkjX.class	a variant of Java/TrojanDownloader.Agent.NBG trojan
C:\Users\user\AppData\Local\Temp\jar_cache3746291637984595421.tmp » ZIP » wedfd/KHdfsdeX.class	a variant of Java/TrojanDownloader.Agent.NAX trojan
C:\Users\user\AppData\Local\Temp\jar_cache4009429545395556072.tmp » ZIP » sklif/Hieeyfc.class	a variant of Java/Exploit.Agent.F trojan
C:\Users\user\AppData\Local\Temp\jar_cache4009429545395556072.tmp » ZIP » sklif/Hirwfee.class	a variant of Java/TrojanDownloader.Agent.NBA trojan
C:\Users\user\AppData\Local\Temp\jar_cache4009429545395556072.tmp » ZIP » sklif/Hiydcxed.class	a variant of Java/TrojanDownloader.Agent.NBA trojan
C:\Users\user\AppData\Local\Temp\jar_cache4664843006566065941.tmp » ZIP » AppletX.class	a variant of Java/Exploit.Agent.NAC trojan
C:\Users\user\AppData\Local\Temp\jar_cache5296422474143948704.tmp » ZIP » myf/y/AppletX.class	probably a variant of Win32/Agent trojan
C:\Users\user\AppData\Local\Temp\jar_cache5296422474143948704.tmp » ZIP » myf/y/LoaderX.class	a variant of Java/TrojanDownloader.Agent.NAC trojan
C:\Users\user\AppData\Local\Temp\jar_cache5296422474143948704.tmp » ZIP » myf/y/PayloadX.class	a variant of Java/TrojanDownloader.Agent.NAD trojan
C:\Users\user\AppData\Local\Temp\jar_cache6027426541994742715.tmp » ZIP » myf/y/AppletX.class	probably a variant of Win32/Agent trojan
C:\Users\user\AppData\Local\Temp\jar_cache6027426541994742715.tmp » ZIP » myf/y/LoaderX.class	a variant of Java/TrojanDownloader.Agent.NAC trojan
C:\Users\user\AppData\Local\Temp\jar_cache6027426541994742715.tmp » ZIP » myf/y/PayloadX.class	a variant of Java/TrojanDownloader.Agent.NAD trojan

C:\Users\user\AppData\Local\Temp\jar_cache63489273481 1725596.tmp » ZIP » sklif/Hieeyfc.class	a variant of Java/Exploit.Agent.F trojan
C:\Users\user\AppData\Local\Temp\jar_cache63489273481 1725596.tmp » ZIP » sklif/Hirwfee.class	a variant of Java/TrojanDownloader.Agent .NBA trojan
C:\Users\user\AppData\Local\Temp\jar_cache63489273481 1725596.tmp » ZIP » sklif/Hiydcxed.class	a variant of Java/TrojanDownloader.Agent .NBA trojan
C:\Users\user\AppData\Local\Temp\jar_cache92053019518 48269570.tmp » ZIP » sklif/Hieeyfc.class	a variant of Java/Exploit.Agent.F trojan
C:\Users\user\AppData\Local\Temp\jar_cache92053019518 48269570.tmp » ZIP » sklif/Hirwfee.class	a variant of Java/TrojanDownloader.Agent .NBA trojan
C:\Users\user\AppData\Local\Temp\jar_cache92053019518 48269570.tmp » ZIP » sklif/Hiydcxed.class	a variant of Java/TrojanDownloader.Agent .NBA trojan
C:\Users\user\AppData\LocalLow\Sun\Java\Deployment\cac he\6.0\2\59d5a6c2-62656763 » ZIP » AppleT.class	probably a variant of Win32/TrojanDownloader.Age nt trojan
C:\Users\user\AppData\LocalLow\Sun\Java\Deployment\cac he\6.0\32\22328120-6e8e24de » ZIP » sklif/Hieeyfc.class	a variant of Java/Exploit.Agent.F trojan
C:\Users\user\AppData\LocalLow\Sun\Java\Deployment\cac he\6.0\32\22328120-6e8e24de » ZIP » sklif/Hirwfee.class	a variant of Java/TrojanDownloader.Agent .NBA trojan
C:\Users\user\AppData\LocalLow\Sun\Java\Deployment\cac he\6.0\32\22328120-6e8e24de » ZIP » sklif/Hiydcxed.class	a variant of Java/TrojanDownloader.Agent .NBA trojan
C:\Users\user\AppData\LocalLow\Sun\Java\Deployment\cac he\6.0\43\45db68ab-130899b9 » ZIP » Uutecwv.class	a variant of Java/Exploit.Agent.NAC trojan
C:\Users\user\AppData\LocalLow\Sun\Java\Deployment\cac he\6.0\55\6a6cde37-52c6fc38 » ZIP » AppleT.class	probably a variant of Win32/TrojanDownloader.Age nt trojan
C:\Users\user\AppData\LocalLow\Sun\Java\Deployment\cac he\6.0\61\4493d8fd-3e3240e5 » ZIP » AppleT.class	probably a variant of Win32/TrojanDownloader.Age nt trojan
E:\Vista Crack\CRACK 1\vistacrack.exe	probably a variant of Win32/Agent trojan

EK-9 S17HJ90Q816726 seri nolu hard disk imajının Güncel Antivirüs uygulaması ile tarama sonucu

Kötücül Yazılım Türü	Dosya Adı
detected: Trojan program Trojan.Win32.Buzus.fucn	file: G:\$Recycle.Bin\S-1-5-21-3650067926-1772903394-554442032-1000\$R8NPPFM\bvid.exe
detected: Trojan program Trojan.Win32.Buzus.fyws	file: G:\$Recycle.Bin\S-1-5-21-3650067926-1772903394-554442032-1000\$R8NPPFM\tmp345.exe
detected: Trojan program Backdoor.Win32.Poison.lze	file: G:\Program Files\Winamp\Lang\Winamp-tr-tr.wlz/ml_wire.lng
detected: Trojan program Trojan.Win32.FakeAV.dshj	file: G:\Users\user\yedek 04.01.2006.rar/yedek 04.01.2006\Belgeler\setup_ares.rar/setup_ares.exe//data0037
detected: virus Virus.Win32.Alman.b	file: G:\Users\user\yedek 04.01.2006.rar/yedek 04.01.2006\masa üstü yedek\ilimin yeri\Obezlik.exe
detected: virus Virus.Win32.Alman.b	file: G:\Users\user\yedek 04.01.2006.rar/yedek 04.01.2006\masa üstü yedek\ilimin yeri\hesap makinesi.exe
detected: virus Virus.Win32.Alman.b	file: G:\Users\user\yedek 04.01.2006.rar/yedek 04.01.2006\masa üstü yedek\ilimin yeri\ilim nasil biri.exe
not found: Trojan program Trojan.Win32.FakeAV.dshj	file: G:\Users\user\yedek 04.01.2006.rar/yedek 04.01.2006\masa üstü yedek\Yeni Klasör\Belgelerim\setup_ares.rar
detected: Trojan program Trojan-Spy.Win32.SpyEyes.if	file: G:\Users\user\AppData\Local\Temp\e.exe
detected: Trojan program Exploit.Java.Agent.bw	file: G:\Users\user\AppData\Local\Temp\jar_cache27908705121 6407523.tmp/Google.class
detected: Trojan program Exploit.Java.Agent.a	file: G:\Users\user\AppData\Local\Temp\jar_cache35570030273 88380316.tmp/Keyworq.class
detected: Trojan program Exploit.Java.Agent.f	file: G:\Users\user\AppData\Local\Temp\jar_cache32281807937 29402572.tmp/sklif/Hieeyfc.class
detected: Trojan program Exploit.Java.Agent.bw	file: G:\Users\user\AppData\Local\Temp\jar_cache27908705121 6407523.tmp/GTalk.class
detected: Trojan program Exploit.Java.Agent.f	file: G:\Users\user\AppData\Local\Temp\jar_cache35570030273 88380316.tmp/Uutecwv.class
detected: Trojan program Exploit.Java.CVE-2008-5353.g	file: G:\Users\user\AppData\Local\Temp\jar_cache32281807937 29402572.tmp/sklif/Hirwfee.class
detected: Trojan program Exploit.Java.Agent.f	file: G:\Users\user\AppData\Local\Temp\jar_cache37462916379 84595421.tmp/wedfd/EoyweiX.class
detected: Trojan program Trojan-Downloader.Java.Agent.jm	file: G:\Users\user\AppData\Local\Temp\jar_cache32281807937 29402572.tmp/sklif/Hiydcxed.class
detected: Trojan program Trojan-Downloader.Java.Agent.bk	file: G:\Users\user\AppData\Local\Temp\jar_cache37462916379 84595421.tmp/wedfd/HkdfkjX.class
detected: Trojan program	file:

Exploit.Java.Agent.a	G:\Users\user\AppData\Local\Temp\jar_cache4001315816243314369.tmp/Keyworq.class
detected: Trojan program Exploit.Java.Agent.f	file: G:\Users\user\AppData\Local\Temp\jar_cache4009429545395556072.tmp/sklif/Hieeyfc.class
detected: Trojan program Exploit.Java.CVE-2009-3867.c	file: G:\Users\user\AppData\Local\Temp\jar_cache4664843006566065941.tmp/AppletX.class
detected: Trojan program Exploit.Java.Agent.f	file: G:\Users\user\AppData\Local\Temp\jar_cache4001315816243314369.tmp/Uutecwv.class
detected: Trojan program Exploit.Java.Agent.f	file: G:\Users\user\AppData\Local\Temp\jar_cache5296422474143948704.tmp/myf/y/AppletX.class
detected: Trojan program Trojan-Downloader.Java.OpenStream.af	file: G:\Users\user\AppData\Local\Temp\jar_cache5296422474143948704.tmp/myf/y/LoaderX.class
detected: Trojan program Exploit.Java.Agent.f	file: G:\Users\user\AppData\Local\Temp\jar_cache6027426541994742715.tmp/myf/y/AppletX.class
detected: Trojan program Exploit.Java.Agent.a	file: G:\Users\user\AppData\Local\Temp\jar_cache6194583195133143611.tmp/Keyworq.class
detected: Trojan program Trojan-Downloader.Java.Agent.al	file: G:\Users\user\AppData\Local\Temp\jar_cache6027426541994742715.tmp/myf/y/LoaderX.class
detected: Trojan program Exploit.Java.Agent.f	file: G:\Users\user\AppData\Local\Temp\jar_cache6194583195133143611.tmp/Uutecwv.class
detected: Trojan program Exploit.Java.Agent.bx	file: G:\Users\user\AppData\Local\Temp\jar_cache6258964244736895883.tmp/tower/Drivers.class
detected: Trojan program Exploit.Java.Agent.a	file: G:\Users\user\AppData\Local\Temp\jar_cache9056863023038247746.tmp/Keyworq.class
detected: Trojan program Exploit.Java.Agent.f	file: G:\Users\user\AppData\Local\Temp\jar_cache6348927348117255596.tmp/sklif/Hieeyfc.class
detected: Trojan program Exploit.Java.Agent.bx	file: G:\Users\user\AppData\Local\Temp\jar_cache6258964244736895883.tmp/tower/Googles.class
detected: Trojan program Exploit.Java.Agent.bx	file: G:\Users\user\AppData\Local\Temp\jar_cache6258964244736895883.tmp/tower/Updaters.class
detected: Trojan program Exploit.Java.Agent.f	file: G:\Users\user\AppData\Local\Temp\jar_cache9056863023038247746.tmp/Uutecwv.class
detected: Trojan program Exploit.Java.Agent.f	file: G:\Users\user\AppData\Local\Temp\jar_cache9205301951848269570.tmp/sklif/Hieeyfc.class
detected: Trojan program Trojan.Win32.Zapchast.frs	file: G:\Users\user\AppData\Local\Temp\NS1F7.tmp//NbIXR6BE.

	dll
detected: Trojan program Packed.Win32.Katusha.j	file: G:\Users\user\AppData\Local\Temp\NS1F99.tmp
detected: Trojan program Trojan.Win32.Zapchast.frs	file: G:\Users\user\AppData\Local\Temp\NSAE31.tmp//NbIXR6BE.dll
detected: Trojan program Packed.Win32.Krap.ao	file: G:\Users\user\AppData\Local\Temp\~TMBC64.tmp
detected: Trojan program Trojan-Dropper.Win32.TDSS.gen	file: G:\Users\user\AppData\Local\Temp\tmp0e16b14e\1283073091.exe
detected: Trojan program Trojan-Downloader.Java.Agent.cf	file: G:\Users\user\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\2\59d5a6c2-62656763/AppleT.class
detected: Trojan program Exploit.Java.Agent.f	file: G:\Users\user\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\32\22328120-6e8e24de/sklif/Hieeyfc.class
detected: Trojan program Exploit.Java.Agent.a	file: G:\Users\user\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\43\45db68ab-130899b9/Keyworq.class
detected: Trojan program Exploit.Java.Agent.f	file: G:\Users\user\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\43\45db68ab-130899b9/Uutecwv.class
detected: Trojan program Trojan-Downloader.Java.Agent.cf	file: G:\Users\user\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\55\6a6cde37-52c6fc38/AppleT.class
detected: Trojan program Trojan-Downloader.Java.Agent.cf	file: G:\Users\user\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\61\4493d8fd-3e3240e5/AppleT.class
detected: Trojan program Trojan.Win32.Agent.ezqg	file: G:\Users\user\AppData\Roaming\download2\svcnost.exe
detected: Trojan program Trojan.Win32.Llac.vop	file: G:\Users\user\AppData\Roaming\FLVPlayer\wmplayer.exe
detected: Trojan program Trojan.Win32.Llac.vop	file: G:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\wmplayer.exe
detected: Trojan program Trojan.Win32.FakeAV.dshj	file: G:\Users\user\Documents\setup_ares.rar/setup_ares.exe//data0037
detected: Trojan program Trojan.Win32.FakeAV.dshj	file: G:\Users\user\yedek 04.01.2006.rar/yedek 04.01.2006\masa üstü yedek\Yeni Klasör\Belgelerim\setup_ares.rar/setup_ares.exe
detected: Trojan program Trojan.Win32.FakeAV.dshj	file: G:\Users\user\yedek 04.01.2006.rar/yedek 04.01.2006\Belgeler\setup_ares.rar/setup_ares.exe