13/07/2013

Sayın Av. Hüseyin ERSÖZ,

Bilimsel inceleme talebiniz için, İstanbul 12. Ağır Ceza Mahkemesi'nde görülmekte olan 2010/34 esas sayılı davaya kanıt olan ÇYDD Kadıköy Şubesi 40 GB Sığalı Maxtor marka, 25B6201H10T7IY seri numaralı sabit disk imajında bilimsel inceleme yapılmıştır.

İnceleme sonucunda bu raporda ayrıntılı olarak anlatılan bulgulara ulaşılmıştır.

Adli Bilirkişi
Tevfik Koray Peksayar
Mak. Müh. Lis. - Bilgi Tekn. Y. Lis.
İTÜ Diploma No: 76 - 387



Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

Bilirkişi Hakkında

1975 İstanbul doğumluyum.

Hazırlık, ortaokul ve lise eğitimimi Nişantaşı Anadolu Lisesi'nde tamamladım. Nişantaşı Anadolu Lisesi Fen-Matematik bölümünden mezun oldum.

İstanbul Üniversitesi Mühendislik Fakültesi Makine Mühendisliği bölümünde lisans eğitimimi tamamladım.

İstanbul Teknik Üniversitesi Bilişim Enstitüsü Bilgi Teknolojileri Yüksek Lisans programıyla yüksek lisans eğitimi gördüm.

Elektronik, bilgisayar ve ağ sistemleri üzerine çalışmaya ortaokul yıllarında amatör olarak başladım.

Lise yıllarının sonunda bu çalışmalarım profesyonelliğe yöneldi.

Lisans eğitimimin son 3 yılında ve yüksek lisans eğitimim boyunca bilgisayar ve ağ sistemleri üzerine yaptığım çalışmalara profesyonel olarak devam ettim. Bu süre zarfında birden fazla işletmede, özellikle web uygulamaları, ağ ve intranet sistemleri ve bilişim sistemlerinin iyileştirilmesi konularında çalıştım.

1998 yılından itibaren sistem başarımı, güvenilirliği ve güvenliği üzerine çalışmalarda bulunmaya başladım.

Bu çalışmalarım sırasında Windows işletim sisteminin birçok sürümü, popüler uygulama yazılımları ve bu yazılımlarının belgelenmemiş çalışma şekil ve davranışları konusunda deneyim kazandım.

1999 yılından itibaren Windows tabanlı sistemlerin yanısıra Linux işletim sistemi üzerine yoğunlaştım.

2000 yılından beri kendime ait şahıs firmam ile profesyonel hayatıma devam etmekteyim.

2010 yılından günümüze İstanbul Adli Yargi İlk Derece Mahkemesi Bilirkişi listesinde bilgi teknolojileri konusunda kayıtlı yeminli bilirkişiyim.

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

Bilimsel İnceleme ve Bilirkişi Görüşü

1. Giriş

İnceleme ÇYDD Kadıköy Şubesi 40 GB Sığalı Maxtor marka 25B6201H10T7IY seri numaralı sabit diskin C: sürücüsünde silinmiş alanda bulunan

1. Documents and Settings/KCYDD/Desktop/Üye/İbadet Yerleri.XLS
2. GENEL/BELGE/EK16.pdf
3. GENEL/ÇAĞDAŞ taslak/liste açıklma.docx
4. GENEL/ÇAĞDAŞ taslak/LİSTE.xls
5. GENEL/ÇAĞDAŞ taslak/türrkan saylana ön yazı.docx
6. GENEL/ÇEV/ÇEV_ÇALIŞMA.xls
7. GENEL/ÇEV/çev_uyesinin_meslek-diger_yakınlarının yakınları.xls
8. GENEL/ÇEV/diğer.xls
9. GENEL/ÇEV/dz.xls
10. GENEL/ÇEV/emn_azıınlıklar.xlsx
11. GENEL/ÇEV/hv.xls
12. GENEL/ÇEV/jngk.xls
13. GENEL/ÇEV/kkk.xls
14. GENEL/ÇEV/sivil-örgüt/hepsi.xls
15. GENEL/ÇEV/sivil-örgüt/örgüt.xls
16. GENEL/ÇEV/sivil-örgüt/sivil.xls
17. GENEL/ÇYDD/ÇYDD_JÇİMEN.xls
18. GENEL/ÇYDD/DİĞER_ ÇYDD.xls
19. GENEL/ÇYDD/DZKK_DZ.K.K.xls
20. GENEL/ÇYDD/HV.K.K_ÇYDD.xls
21. GENEL/ÇYDD/KKK_ÇYDD.xls
22. GENEL/ÇYDD/MİT_ÇYDD.xls
23. GENEL/ÇYDD/MÜLKİ_İDARİ_ÇYDD.xls
24. GENEL/ÇYDD/ÖRGÜT_ÇYDD.xls
25. GENEL/ÇYDD/TÜM_ÇYDD.xls
26. GENEL/ÇYDD/YARGI_ÇYDD.xls
27. GENEL/Gamze KONA/ETM.PPT
28. GENEL/Gamze KONA/IRAKGE.DOC
29. GENEL/Gamze KONA/SVL.XLS
30. GENEL/listeler/05.11.30-CYDD OGRENCI BİLGİ.xls
31. GENEL/listeler2/2008 toplantıözeti.doc
32. GENEL/listeler2/cumhuriyet evi.xls
33. GENEL/listeler2/Listeler.xls
34. GENEL/listeler2/USA.doc
35. GENEL/Türkan SAYLAN/okan amiral/LİSTE.xls
36. GENEL/Türkan SAYLAN/okan amiral/MEKTUP(Türkan SAYLAN).doc
37. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 1.doc
38. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 2.doc
39. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 3.doc

dosyaları ile bu dosyaları içeren imaj üzerinde yapılmıştır.

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

2. İnceleme Yapılan Kütük Bilgileri

İnceleme ÇYDD Kadıköy Şubesi 40 GB Sığalı Maxtor marka 25B6201H10T7IY seri numaralı sabit disk imaj dosyası üzerinde yapılmıştır.

Bu disk bu raporun devamında kısaca "*sabit disk*", sabir disk imajı ise kısaca "*sabit disk imajı*" olarak anılmıştır.

2.1. ÇYDD Kadıköy Şubesi 40 GB Sığalı Maxtor Marka 25B6201H10T7IY Seri Numaralı Sabit Disk İmajı

Söz konusu sabit disk daha önce tarafıma inceleme için verilmiş, fakat diskin sıfırlanarak tekrar sistem kurulduğu görüldüğünden inceleme yapılmamıştır. Bu sebeple adli emanetten el konulma sonrası alınan imaj temin edilerek inceleme yapılması için tarafıma iletilmiştir.

Sabit diskin adli emanetten gelen imajının Kadikoy_CYDD_Maxtor_25B6201H10T7IY_40GB.E01 ~ E11 dosya adlı 11 parça Expert Witness Compression Format dosyaları olduğu görülmüştür.

İmaj dosyasının MD5 sayısal imzası *ca5b7799678855a8ace30aabeb05a79e* olarak belirlenmiştir.

İmaj dosyasının SHA1 sayısal imzası *49c5232b0b6ecc4b98ecfb4a871ef3db4df21951* olarak belirlenmiştir.

İmajın geçerliliği, adli emanet tarafından teslim edilen imaj dosyası içerisinde depolanan sayısal imzayla kıyaslanıp doğrulanmıştır.

Ancak kütüğün ele geçirilme anında imajının oluşturulduğuna dair bilgi yoktur. Dolayısıyla alınan imajla özgün kütük arasında birbirlerine denklikleri açısından bir bilgi sağlanamamaktadır.

Ayrıca 13/04/2009 tarihli arama ve el koyma tutanağının 1. sayfasında inceleme konusu sabit disk seri numarasının "25B6201H10T7IY" yerine "25B6201H10T71Y" olarak kayda geçirildiği görülmektedir.

İmaj Dosyası	Kadikoy_CYDD_Maxtor_25B6201H10T7IY_40GB.E01 ~ Kadikoy_CYDD_Maxtor_25B6201H10T7IY_40GB.E11
İmaj Tarihi	19/02/2013 02:25:23
İmajın Alındığı Uygulama	EnCase v6.15
Sağlanan md5 İmzası	ca5b7799678855a8ace30aabeb05a79e
Bulunan md5 İmzası	ca5b7799678855a8ace30aabeb05a79e
Sağlanan sha1 Sayısal İmzası	49c5232b0b6ecc4b98ecfb4a871ef3db4df21951
Bulunan sha1 Sayısal İmzası	49c5232b0b6ecc4b98ecfb4a871ef3db4df21951

İnceleme için önce Expert Witness Compression Format tipindeki dosyalardan Linux ewfexport komutuyla ham imaj dosyası elde edilmiştir.

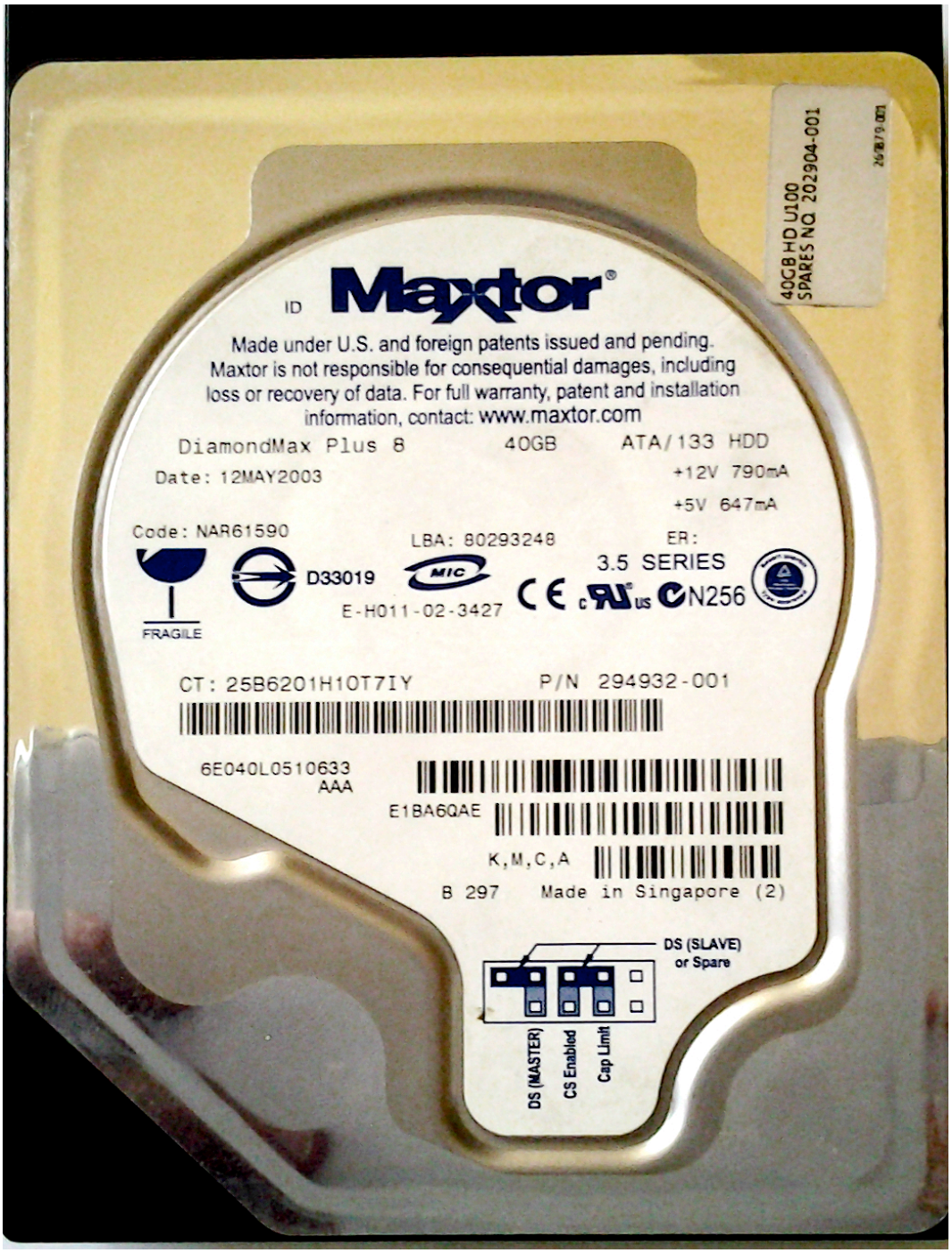
İnceleme yapılan dosyalar silinmiş oldukları için bu ham imajdan R-Studio ile kurtarılmıştır.

Adli emanetçe sağlanan Expert Witness Compression Format dosyaları da "*Sleuthkit Autopsy"* inceleme yazılımı kullanılarak kurtarılan bu dosyaların imajdaki halleriyle eşitliği doğrulanmıştır.

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

3. Sabit Disk Hakkında Genel Bilgiler

3.1. Disk Donanımı



Markası	Maxtor
Sığası	40 GB
Modeli	DiamondMax Plus 8
Ürün Numarası	294932-001
Seri Numarası	25B6201H10T7IY (İKİ BEŞ B ALTI İKİ SIFIR BİR H BİR SIFIR T YEDİ I Y)
Üretim Tarihi	12/05/2003

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

3.2. Dosya Sistemi

Disk üzerinde 1 bölüm bulunmuştur.

Bölüm	1 (C: sürücüsü)
Etiket	SISTEM
Boyut	40 GB
Dosya Sistemi	NTFS
Birim Seri Numarası	EA382F29382EF46B
Oluşturan İşletim Sistemi	Windows XP
Oluşturulma Tarihi	21/02/2009 23:05:34
Kurulu İşletim Sistemi	Windows XP Service Pack 2 build 2600

3.3. Kurulu İşletim Sistemi

İşletim Sistemi Sürümü	Windows XP Service Pack 2 build 2600 (2600.xpsp.051011-1528)
Kurulum Tarihi	21/02/2009
Kurulum Naşlangıcı	21:10:23 (setuplog.txt dosyasına göre)
Kurulum Sonu	23:39:15
Kurulum Kaynağı	HL-DT-ST DVD-ROM GDR8161B (D:\I386)
Kurulum Yolu	C:\WINDOWS
Dil	Türkçe
Kayıtlı Kullanıcı	USER
Kayıtlı Firma	USER
Ürün Kimliği	55896-640-8365391-23987
Son Açılma Tarihi	10/04/2009 20:47:46
Son Kapatılma Tarihi	10/04/2009 20:48:18
Sistem Güvenlik Tanımlayıcısı (SID)	S-1-5-21-329068152-1580818891-682003330

3.4. Kurulu Microsoft Office sürümü

Kurulu Microsoft Office uygulaması sürümünün Office 11 (Office 2003) olduğu tespit edilmiştir.

3.5. Kurulu Anti-virüs Yazılımı

Kurulu anti-virüs yazılımın ESET NOD32 olduğu tespit edilmiştir.

3.6. Sistemin Son Kullanıldığı Tarih

Yapılan incelemede sistemin son kez 10/04/2009 20:47:46 tarihinde açıldığı ve son kez 10/04/2009 20:48:18 tarihinde kapatıldığı tespit edilmiştir.

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

3.7. Ağ Bağlantısı

Sisteme 10.0.0.103 IP adresinin atandığı ve makine isminin "*KCYDD3*" olduğu tespit edilmiştir.

3.8. Tanımlı Kullanıcılar

Sistem kayıt defterinde yapılan incelemede sistemde 2 kullanıcının tanımlı olduğu tespit edilmiştir.

Kullanıcı Adı	Kullanıcı Kimliği (SID)	Son Giriş Tarihi	Son Parola Değişikliği
Administrator	S-1-5-21-329068152-1580818891-682003330-500	21/02/2009 21:40:56	21/02/2009 23:28:55
KCYDD	S-1-5-21-329068152-1580818891-682003330-1001	10/04/2009 20:47:50	Parola yok - Hiç bir zaman

3.9. Diğer Veri Depolama Cihazları

Yapılan incelemede hizmet süresi içinde "*KCYDD3*" adlı bilgisayara 3 farklı USB depolama cihazları takıldığı tespit edilmiştir.

Tipi	Disk sürücüsü
Marka	Kingston
Model	DataTraveler 2.0 Rev 1.00
Eşsiz Kimlik	0604171741332&0
Kurulum Yeri	\??\Volume{a3c6d5ca-002e-11de-a93b-000802150421}

Tipi	Disk sürücüsü
Marka	Kingston
Model	Kingston DataTraveler 2.0 USB Device
Eşsiz Kimlik	20070620000000000591897 57&0
Kurulum Yeri	\??\??\Volume{40be8089-16ca-11de-a949-000802150421} E:

Tipi	Disk sürücüsü
Marka	Kingston
Model	DataTraveler 2.0 PMAP
Eşsiz Kimlik	001D0F1314D55B8715150456&0
Kurulum Yeri	??\Volume{9fe197a0-0647-11de-a941-000802150421}

3.10. Virüs Etkinliği

Dosya sisteminde Clam Antivirus ile yapılan taramada etkin olarak çalışan birden fazla virüse rastlanmıştır.

Bulunan virüslü dosyalar Virustotal.com ile denetlenip içerdikleri virüs tipi tespiti doğrulanmıştır.

Bulunan bu virüslü dosyalar aşağıdaki tabloda listelenmiştir.

Virüs Tipi	**Dosya**	**Silinmiş**
Worm:Win32/Taterf.B	2.com gbha.bat	Hayır
INF.Autorun-96	autorun.inf d1vmq.exe Aynı dosyaların otomatik yedeklenmiş halleri	Evet
Trojan.OnlineGames-6063	WINDOWS/system32/optyhww1.dll Aynı dosyanın otomatik yedeklenmiş halleri	Hayır
Win.Trojan.Agent-116401	Documents and Settings/KCYDD/Local Settings/Temp/ker11.tmp	Hayır
Win.Trojan.Magania-1590	Documents and Settings/KCYDD/Local Settings/Temp/nmf11.tmp	Hayır

Bu zararlı yazılmalardan
1. Worm:Win32/Taterf.B
2. Trojan.OnlineGames-6063
3. Win.Trojan.Agent-116401
4. Win.Trojan.Magania-1590

olarak tanımlanan virüsler İnternet yoluyla otomatik olarak dosya indirebilen yazılımlardır.

Yapılan incelemede özellikle "*Worm:Win32/Taterf.B*" tarafından "*help.rar*" adlı dosyanın defalarca diske indirildiği görülmüştür.

İndirilmeye çalışılan bu dosya başka bir zararlı yazılım olabileceği gibi başka dosyaları indirmesini sağlayan "*emir*" dosyası da olabilir.

Ancak bu virüsün eski tarihli olması sebebiyle indirmeye çalıştıkları dosyalar halen İnternet'te yer almamaktadır.

Bu sebeple, bu virüsler yoluyla söz konusu sistemin uzaktan kontrol edildiğini kesin olarak tepit etmek mümkün değildir.

Ancak, "*INF.Autorun-96*" olarak sınıflandırılan virüsün 22/03/2009 tarihi saat 17:36:34'e kadar sistemde etkin olarak çalıştığı görülmektedir.

Bu virüsün sürekli çalışabilirliğinin sağlanması için kendisinin kopyasını çıkardığı, "*d1vmq.exe*" dosyasını 14/03/2009 23:12:35 diskte oluşturulma tarihini, "*autorun.inf*" dosyasını diskte oluşturulma tarihi 01/03/2009 12:00:32 olacak şekilde geri tarihli işlemle kendisini tekrar diske yazdığı ve sistem tarafından da otomatik olarak yedeklendiği görülmektedir.

3.11. Sistem Hakkında Diğer Bilgiler

İncelenen sabit disk imajında bulunan Windows sisteminin Windows Kayıt Defteri "*HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\FileSystem*" ve "*HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Control\FileSystem*" anahtarlarının "*NtfsDisableLastAccessUpdate*" değerinin 1 olduğu, bu sebeple dosya son erişim tarihlerinin diskte güncellenmesinin kapalı olduğu tespit edilmiştir.

Ancak, bu ayarı saklayan "WINDOWS/system32/config/system" kayıt defteri dosyasının diskte son değişiklik tarihi 10/04/2009 20:47:46 olarak görülmektedir ve bu tarih sistemin son kez açıldığı tarihtir.

Bu dosyanın verisindeki değişiklik ise 10/04/2009 20:48:17 tarihini göstermektedir.

Dosyaya son erişim tarihi ise güncellenmiştir. Son erişim tarihi 10/04/2009 20:48:17'dir ve bu tarih sistemin son kez kapatıldığı tarihtir.

Bu ayarın sistemin son kez kullanılarak kapatıldığı 10/04/2009 tarihinde saat 20:47:46 ile 20:48:17 arasında yapıldığı anlaşılmaktadır.

Bu sebeple, sistemin son kapatıldığı tarihten sonra, bu sistem kullanılarak yapılan dosya işlemlerinde dosya erişim tarihlerinin diskte güncellenmemesi beklenilen durumdur.

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

4. Dosya İncelemesi

4.1. 02.06.2010 tarihli "*İNCELEME VE DEĞERLENDİRME RAPORU*"

02.06.2010 tarihli "*İNCELEME VE DEĞERLENDİRME RAPORU*"nda sistemin kurulduğu ve son kapatıldığı tarihler yer almaktadır.

Bilgisayar Hard diski üzerinde bulunan işletim sistemi, ismi ve özellikleri aşağıdaki gibidir.

InstallDate	02/21/09 09:38:55PM
ProductName	Microsoft Windows XP
RegisteredOrganization	USER
RegisteredOwner	USER
CurrentVersion	5.1
CurrentBuildNumber	2600
SystemRoot	C:\WINDOWS
SourcePath	D:\I386
PathName	C:\WINDOWS
ProductId	55896-640-8365391-23987
CSDVersiyon	Service Pack 2
Last Shut Down Time	04/10/09 08:48:17PM

Aynı yazıda bir kısım dosyaların üst verileriyle sağlanan bir kısım bilgilerin tespitinin yapıldığı, ancak tüm bilgilerin tespit edilmediği görülmektedir.

"*İNCELEME VE DEĞERLENDİRME RAPORU*"ndaki üst veri tespitiyle ilgili bir örnek aşağıda verilmiştir.

4- "liste açıklma.docx" isimli MSword dosyasının özellikleri aşağıya çıkartılmıştır.

Name	liste açıklma.docx
File Created	12/30/08 12:46:42
Logical Size	11.773
Full Path	C\GENEL\ÇAĞDAŞ taslak\liste açıklma.docx
Hash Value	6eb19f9a0fbacada4076908502c61017

Adli bilişim çalışmalarında, üst veri incelemelerinin amacı sayısal dosyalar hakkında bilgi sağlamaktır.

Üst verilerden temin edilen bilgilerin başta dosyaların kişi/kişilere aitliği, tarih ve yer bağlantısı olmak üzere değerli bilgi sağlayabileceği şüphesizdir.

Üst veri incelemelerini destekleyen ve yapılması şart olan diğer tespit, sayısal dosyaların bulundukları kütük üzerindeki dosya sistemince sağlanan işlem tarihleridir.

Dosya sisteminde kayıtlı bilgilerin incelenmesiyle dosyaların kütükte oluşumları, yer değişimleri ve kütüğün bağlı olduğu sistemle ilişkileri tespit edilerek değerli bulgulara ulaşılır.

Bahsedilen bu dosya sistemi incelemesinin 02.06.2010 tarihli "*İNCELEME VE DEĞERLENDİRME RAPORU*"nda hiçbir dosya için yapılmadığı açıkça görülmektedir.

Bu durum, söz konusu "*İNCELEME VE DEĞERLENDİRME RAPORU*" başlıklı yazının eksik bir inceleme ve değerlendirme sonucunda oluşturulduğunu göstermektedir.

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

Suç kanıtı olarak kabul edilen ve söz konusu davanın iddianamesinde bahsi geçen;

1. Documents and Settings/KCYDD/Desktop/Üye/İbadet Yerleri.XLS
2. GENEL/BELGE/EK16.pdf
3. GENEL/ÇAĞDAŞ taslak/liste açıklma.docx
4. GENEL/ÇAĞDAŞ taslak/LİSTE.xls
5. GENEL/ÇAĞDAŞ taslak/türrkan saylana ön yazı.docx
6. GENEL/ÇEV/ÇEV_ÇALIŞMA.xls
7. GENEL/ÇEV/çev_uyesinin_meslek-diger_yakınlarının yakınları.xls
8. GENEL/ÇEV/diğer.xls
9. GENEL/ÇEV/dz.xls
10. GENEL/ÇEV/emn_azıınlıklar.xlsx
11. GENEL/ÇEV/hv.xls
12. GENEL/ÇEV/jngk.xls
13. GENEL/ÇEV/kkk.xls
14. GENEL/ÇEV/sivil-örgüt/hepsi.xls
15. GENEL/ÇEV/sivil-örgüt/örgüt.xls
16. GENEL/ÇEV/sivil-örgüt/sivil.xls
17. GENEL/ÇYDD/ÇYDD_JÇİMEN.xls
18. GENEL/ÇYDD/DİĞER_ ÇYDD.xls
19. GENEL/ÇYDD/DZKK_DZ.K.K.xls
20. GENEL/ÇYDD/HV.K.K_ÇYDD.xls
21. GENEL/ÇYDD/KKK_ÇYDD.xls
22. GENEL/ÇYDD/MİT_ÇYDD.xls
23. GENEL/ÇYDD/MÜLKİ_İDARİ_ÇYDD.xls
24. GENEL/ÇYDD/ÖRGÜT_ÇYDD.xls
25. GENEL/ÇYDD/TÜM_ÇYDD.xls
26. GENEL/ÇYDD/YARGI_ÇYDD.xls
27. GENEL/Gamze KONA/ETM.PPT
28. GENEL/Gamze KONA/IRAKGE.DOC
29. GENEL/Gamze KONA/SVL.XLS
30. GENEL/listeler/05.11.30-CYDD OGRENCI BİLGİ.xls
31. GENEL/listeler2/2008 toplantıözeti.doc
32. GENEL/listeler2/cumhuriyet evi.xls
33. GENEL/listeler2/Listeler.xls
34. GENEL/listeler2/USA.doc
35. GENEL/Türkan SAYLAN/okan amiral/LİSTE.xls
36. GENEL/Türkan SAYLAN/okan amiral/MEKTUP(Türkan SAYLAN).doc
37. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 1.doc
38. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 2.doc
39. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 3.doc

dosyalarının üst veri incelemesi okumakta olduğunuz bu raporun yazımı öncesi titizlikle yapılarak

1. Dosya üst verilerinden,
2. Excel dosyalarının BIFF kayıtlarından,
3. Excel dosyalarının son kullanıcı kayıtlarından,
4. Word dosyalarının son kaydedilme zaman damgalarından,
5. Dosya sisteminden,
6. NTFS dosya sistemi LogFile kayıtlarından

elde edilen bilgi ve bulgular "*Ek-1*"de sunulmuş ve bu raporda ayrıntılandırılmıştır.

Dosya sistemi incelemesinin değerlendirmesi de bu raporun ilgili bölümünde sunulmuştur.

4.2. Dosya İncelemesi Bulguları

İncelenen dosyaların üst verilerinden ve dosya sisteminden elde edilen tarih bilgileri incelendiğinde, incelenen 39 dosyanın tümünün diskte oluşturulma tarihinin diskin formatlandığı tarihten geride olduğu görülmektedir.

Bu bulgu dosyaların tümünün geri tarihli işlemlerle sabit diskte kopyalanarak oluşturulduğuna işaret etmektedir.

Dosya sistemi incelemesi de bu bulguyu doğrulamaktadır.

İnceleme sonucunda başka bulgulara ve tutarsızlıklarla da karşılaşılmıştır.

Dosyaların diskte oluşturulma tarihleri, MFT girdi numaraları, LogFile girdi numaraları ve MFT girdisi kullanım sayılarını gösteren dökümler "*Ek-2*", "*Ek-3*" ve "*Ek-4*"te sunulmuştur.

4.2.1. Üst Verideki Oluşturulma Tarihi Sabit Diskin Formatlandığı Tarihten Geride Olan Dosyalar

Aşağıda listesi verilen dosyaların üst verilerinden elde edilen oluşturulma tarihi sabit diskin formatlanarak dosya sisteminin oluşturulduğu tarihten geridedir.

1. Documents and Settings/KCYDD/Desktop/Üye/İbadet Yerleri.XLS
2. GENEL/BELGE/EK16.pdf
3. GENEL/ÇEV/emn_azıınlıklar.xlsx
4. GENEL/Gamze KONA/ETM.PPT
5. GENEL/Gamze KONA/IRAKGE.DOC
6. GENEL/Gamze KONA/SVL.XLS
7. GENEL/listeler/05.11.30-CYDD OGRENCI BİLGİ.xls
8. GENEL/listeler2/2008 toplantıözeti.doc
9. GENEL/listeler2/cumhuriyet evi.xls
10. GENEL/Türkan SAYLAN/okan amiral/LİSTE.xls
11. GENEL/Türkan SAYLAN/okan amiral/MEKTUP(Türkan SAYLAN).doc
12. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 1.doc
13. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 2.doc
14. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 3.doc

Üst verinin itibar edilebilir olduğu varsayıldığında, bu bulgu listelenen dosyaların incelenen sabit diskte başka bir kaynaktan kopyalanarak oluşturulduğuna işaret etmektedir.

4.2.2. Üst Verideki Son Değişiklik Tarihi Diskin Formatlandığı Tarihten Geride Olan Dosyalar

Aşağıda listesi verilen dosyaların üst verilerinden elde edilen son değişiklik tarihi sabit diskin formatlanarak dosya sisteminin oluşturulduğu tarihten geridedir.

1. Documents and Settings/KCYDD/Desktop/Üye/İbadet Yerleri.XLS
2. GENEL/BELGE/EK16.pdf
3. GENEL/ÇAĞDAŞ taslak/liste açıklma.docx
4. GENEL/ÇAĞDAŞ taslak/LİSTE.xls
5. GENEL/ÇAĞDAŞ taslak/türrkan saylana ön yazı.docx
6. GENEL/Gamze KONA/ETM.PPT
7. GENEL/Gamze KONA/IRAKGE.DOC
8. GENEL/listeler/05.11.30-CYDD OGRENCI BİLGİ.xls
9. GENEL/listeler2/cumhuriyet evi.xls
10. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 1.doc
11. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 2.doc
12. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 3.doc

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

Üst verinin itibar edilebilir olduğu varsayıldığında, bu bulgu listelenen dosyaların incelenen sabit diskte başka bir kaynaktan kopyalanarak oluşturulduğuna işaret etmektedir.

4.2.3. Üst Verideki Son Değişiklik Tarihi Oluşturulma Tarihinden Geride Olan Dosyalar

Aşağıda listesi verilen dosyaların üst verilerinden elde edilen son değişiklik tarihi dosyaların üst verilerinden elde edilen oluşturulma tarihlerinden geridedir.

1. GENEL/ÇAĞDAŞ taslak/liste açıklma.docx
2. GENEL/ÇAĞDAŞ taslak/türrkan saylana ön yazı.docx
3. GENEL/listeler2/2008 toplantıözeti.doc
4. GENEL/listeler2/Listeler.xls
5. GENEL/listeler2/USA.doc

Bu bulgu tarih manipülasyonuna ve dosya üst verilerinde değişikliğe işaret etmektedir.

4.2.4. Oluşturuldukları ve/veya Son Kaydedildikleri Microsoft Office Sürümü Sistemde Kurulu Sürümle Uyumlu Olmayan Dosyalar

Sabit diskte kurulu olan Microsoft Office uygulaması sürümünün Office 11 (Office 2003) olduğu tespit edilmiş ve "*3.4. Kurulu Microsoft Office sürümü*" bölümünde raporlanmıştır.

Aşağıda listelenen dosyaların son kaydedildikleri ve/veya oluşturuldukları tespit edilen Microsoft Office sürümü sistemde kurulu olan sürümle uyumlu değildir.

1. Documents and Settings/KCYDD/Desktop/Üye/İbadet Yerleri.XLS
2. GENEL/ÇAĞDAŞ taslak/liste açıklma.docx
3. GENEL/ÇAĞDAŞ taslak/LİSTE.xls
4. GENEL/ÇAĞDAŞ taslak/türrkan saylana ön yazı.docx
5. GENEL/ÇEV/ÇEV_ÇALIŞMA.xls
6. GENEL/ÇEV/çev_uyesinin_meslek-diger_yakınlarının yakınları.xls
7. GENEL/ÇEV/diğer.xls
8. GENEL/ÇEV/dz.xls
9. GENEL/ÇEV/emn_azıınlıklar.xlsx
10. GENEL/ÇEV/hv.xls
11. GENEL/ÇEV/jngk.xls
12. GENEL/ÇEV/kkk.xls
13. GENEL/ÇEV/sivil-örgüt/hepsi.xls
14. GENEL/ÇEV/sivil-örgüt/örgüt.xls
15. GENEL/ÇEV/sivil-örgüt/sivil.xls
16. GENEL/ÇYDD/ÇYDD_JÇİMEN.xls
17. GENEL/ÇYDD/DİĞER_ ÇYDD.xls
18. GENEL/ÇYDD/DZKK_DZ.K.K.xls
19. GENEL/ÇYDD/HV.K.K_ÇYDD.xls
20. GENEL/ÇYDD/KKK_ÇYDD.xls
21. GENEL/ÇYDD/MİT_ÇYDD.xls
22. GENEL/ÇYDD/MÜLKİ_İDARİ_ÇYDD.xls
23. GENEL/ÇYDD/ÖRGÜT_ÇYDD.xls
24. GENEL/ÇYDD/TÜM_ÇYDD.xls
25. GENEL/ÇYDD/YARGI_ÇYDD.xls
26. GENEL/Gamze KONA/IRAKGE.DOC
27. GENEL/Gamze KONA/SVL.XLS
28. GENEL/listeler/05.11.30-CYDD OGRENCI BİLGİ.xls
29. GENEL/listeler2/2008 toplantıözeti.doc
30. GENEL/listeler2/cumhuriyet evi.xls
31. GENEL/listeler2/Listeler.xls
32. GENEL/listeler2/USA.doc

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

33. GENEL/Türkan SAYLAN/okan amiral/LİSTE.xls
34. GENEL/Türkan SAYLAN/okan amiral/MEKTUP(Türkan SAYLAN).doc
35. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 2.doc
36. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 3.doc

Bu bulgu listelenen dosyaların incelenen sabit diskte kurulu Microsoft Office sürümünden başka bir sürümün kurulu olduğu bir bilgisayarda oluşturulup, bu diskte kopyalanarak oluşturulduğuna işaret etmektedir.

4.2.5. Türkiye Dışında Oluşturulan veya Son Kez Kaydedilen Dosyalar

İncelenen;
1. Documents and Settings/KCYDD/Desktop/İbadet Yerleri.XLS
2. GENEL/listeler2/cumhuriyet evi.xls
3. GENEL/listeler2/Listeler.xls

Excel dosyalarının BIFF kayıtlarından elde edilen bilgi, dosyayı kaydeden sistemin bulunduğu ülkenin Amerika Birleşik Devletleri olduğunu ve kullanılan Excel yazılımının Amerika Birleşik Devletleri için çıkarılmış sürüm olduğunu göstermektedir.

Bu bulgu listelenen Excel dosyalarının Türkiye dışında oluşturulduğuna ya da son kez Türkiye dışında kaydedildiğine işaret etmektedir.

Bu BIFF kayıtlarının elde edilmesinde kullanılan PHP dilinde yazılmış kod "Ek-7"de sunulmuştur.

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

5. Dosya Sistemi İncelemesi Bulguları

5.1. NTFS Dosya Sistemlerinde Ana Dosya Tablosu (MFT) Hakkında Bilgi

Bir dosya sistemi, üzerine kaydedilecek dosyaların düzenli olarak depolanmasını ve kolay erişim sağlanmasını amaçlar.

NTFS dosya sistemlerinde dosyalar öbek (İng.: cluster) tabir edilen yapılarla saklanır.

Öbeklerin boyutları sabittir ve bir disk ilk kez kullanıma hazırlandığında (formatlandığında) diskin toplam boyutuna göre dosyalara en uygun erişim ve sistem başarımının sağlanması için önceden belirlenir.

Dosyalar disk üzerinde bu öbeklere parçalanarak depolanır. Bilgisayarlarda tüm işlemlerin 2'li sayı sistemi ile yapılmasından dolayı bir dosyanın kapladığı öbek sayısı her zaman tam sayıdır.

Örneğin 5.3 kilobayt boyutunda bir dosya 4 kilobayt boyutunda öbek tanımı olan bir FAT dosya sisteminde 2 öbekle depolanır. Diğer bir deyişle dosya disk üzerinde 8 kilobayt yer kaplar.

Öbekler disk üzerinde serbestçe yerleştirilebilir, disk üzerinde yer alan bir öbekten sonra gelen öbeğin bir önceki öbeğin depoladığı dosya parçasını içeriyor olması şart değildir.

Ana dosya tablosu (İng.: master file table / İng. Kıs.: MFT) ya da dosya yerleşim tablosu, öbekler hakkında bilginin depolandığı yapıdır. Dosya yerleşim tablosunda her öbeğin nasıl kullanıldığı hakkında girdi depolanır. Bu girdilerle işletim sistemine dosyaların depolandığı öbeklerin numaraları, diskin hangi bölümlerinin dosyalar tarafından kullanıldığını ve hangi bölümlerinin kullanım için serbest olduğu bilgisi sağlanır.

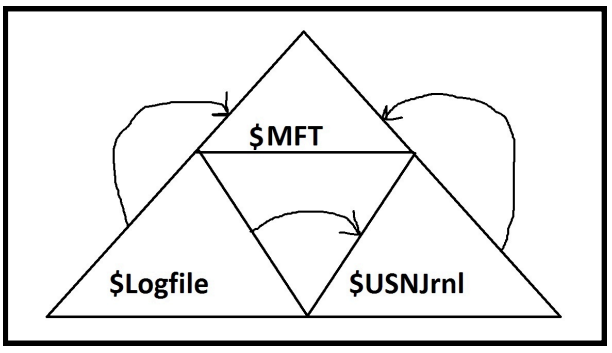
Bu dosya yerleşim tablosu girdileri, işletim sistemi tarafından kullanılarak öbeklere zincir şeklinde erişilip dosyaların okunmasını sağlar. İşletim sistemi bir dosyanın ard arda hangi öbeklerde depolandığını dosya yerleşim tablosundan öğrenip öbekleri sırayla okuyarak depolanmış dosyaya erişir.

Öbekler disk üzerine rastgele yazılmalarına rağmen dosya yerleşim tablosunda öbeklerin numaralanması her zaman birbirini takip eder.

MFT girdileri dosya oluşturulma tarihleriyle uyumluluk içinde sayıları ardışık olarak artarak birbirini takip ederler.

Bu girdi numaraları takip edilerek hangi dosyanın hangisinden sonra oluşturulduğu kolaylıkla belirlenebilir. Dolayısıyla, dosyaların işlem tarihlerinden bağımsız olarak bu girdi numaralarından kayıt sıraları kolayca tespit edilebilir.

LogFile adlı sistem dosyası bu girdilerin işlem sırasını depolamakta, bu işlemleri, eğer işletim sisteminde etkinleştirilmişse, $USNJrnl adlı jurnal dosyasına da yazmaktadır.



Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

LogFile yapısında sıra numaraları kullanılarak, sürücü üzerinde yapılan dosya işlemlerinin kaydı tutulur.

Yukarıda da anlatıldığı üzere, disk üzerine yeni dosyalar kaydedildikçe MFT girdi numaraları artmaktadır. Bu girdiler üzerinde yapılan değişiklikler ise LogFile sıra numaralarında artış olarak görünmektedir.

Böylece, MFT girdi numaraları ve LogFile sıra numaraları takip edilerek dosya kayıt işlemlerinin ayrıntısına ulaşmak kolaylaşır.

Disk üzerinde yer kalmayınca ve dosya sistemi üzerinde tanımlanabilecek dosya sayısının sonuna ulaşılmışsa daha önce silinmiş olan girdi numaraları ve dosyaların kapladığı öbekler kullanılmaya başlanır.

NTFS dosya sistemi yerleşim tablosunda en çok 4,294,967,295 (dört milyon iki yüz doksan dört bin iki yüz doksan beş) dosya tanımlanabilir.

5.2. Dosya İşlem Tarihlerindeki Çelişkiler

Suç kanıtı olarak kabul edilen 39 dosyanın 38'ini içeren "*GENEL*" dizini MFT girdisinin dosya sisteminde oluşturulma tarihi 26/02/2006 15:07:06 ve 1'ini içeren içeren silinmiş "*Documents and Settings/KCYDD/Desktop/Üye*" dizini MFT girdisinin dosya sisteminde oluşturulma tarihi 30/12/2008 16:01:43'tür.

Bu iki tarih de silinmiş olan "*GENEL*" ve "*Documents and Settings/KCYDD/Desktop/Üye*" dizinlerinin bulunduğu disk bölümünün (partisyonun) formatlandığı ve MFT yapısının oluşturulma tarihi olan 21/02/2009'dan geridedir.

"*GENEL*" dizinin son erişim, son değişiklik ve dosya sisteminde değişiklik tarihleri de birbiriyle eşit olarak 18/02/2009 12:28:43'ü göstermektedir ve bu tarih de "*GENEL*" dizininin bulunduğu disk bölümünün (partisyonun) oluşturulma tarihi olan 21/02/2009'dan geridedir.

"*Documents and Settings/KCYDD/Desktop/Üye*" dizinin son erişim, son değişiklik ve dosya sisteminde değişiklik tarihleri de birbiriyle eşit olarak 18/02/2009 12:30:59'u göstermektedir ve bu tarih de "*GENEL*" dizininin bulunduğu disk bölümünün (partisyonun) oluşturulma tarihi olan 21/02/2009'dan geridedir.

Bir disk bölümü oluşturulmadan üzerine girdi kaydı yapılamayacağı için, "*GENEL*" ve "*Documents and Settings/KCYDD/Desktop/Üye*" dizinlerinin geri tarihli işlemlerle diskte oluşturulduğu anlaşılmaktadır.

"*GENEL*" ve "*Documents and Settings/KCYDD/Desktop/Üye*" dizinlerinin son değişiklik ve dosya sisteminde değişiklik tarihlerinin eşit olması da, her iki dizinin de diske kopyalandığını ve kopyalandıktan sonra bu dizinlere girilmediği, içindeki dosyaların okunmadığını göstermektedir.

Yapılan incelemede "*GENEL*" dizininin içinde, son değişiklik saati sistemin son kapatılma tarihinden sonrasını gösteren girdiler bulunduğu görülmektedir.

Bu silinmiş dosyalardan en son işlem görenler;

1. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/en yeni liste 2007-2008.xls
2. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 1.doc
3. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 2.doc
4. GENEL/Türkan SAYLAN/tükansaylan-1/a ortabaşı/Türkan SAYLAN 3.doc
5. GENEL/Türkan SAYLAN/okan amiral/_Kodlar.txt
6. GENEL/Türkan SAYLAN/okan amiral/LİSTE.xls
7. GENEL/Türkan SAYLAN/okan amiral/MEKTUP(Türkan SAYLAN).doc

dosyalarıdır.

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

Bu dosya girdilerinin diskte son değişiklik tarihleri eşit olarak 10/04/2009 23:55:16'yı göstermektedir ve bu tarih diskin takılı olduğu sistemin son kapatıldığı 10/04/2009 20:48:17'den ileridedir.

Söz konusu dosyaların silinmiş olmaları, bu dosyaların diskte daha önce yer alıp da daha sonra üstünde yeni partisyonlar oluşturulmak suretiyle silinmiş partisyonlara ait oldukları anlamına gelmemektedir. Bu dosya girdileri bu diskte son oluşturulmuş olan, sistem tarafından kullanılan ve silinmemiş partisyondaki MFT yapısında yer almaktadırlar.

Bu dosyaların disk üzerinde kapladığı öbekler (İng.: cluster) başka silinmemiş dosyalar tarafından kullanılmış durumda değildirler, MFT kayıtlarına, dosya verilerine eksiksiz olarak erişilebilmekte ve kurtarılabilemektedir.

Yukarıda sayılan sebeplerle "*GENEL*" dizininin , "*GENEL*" dizininin içerdiği dosyaların ve suç konusu olarak incelenen dosyaların diskin takılı olduğu sistem kullanılarak oluşturulması sistem tarihinin ileri-geri tarihlere ayarlanmasıyla veya özel bazı yazılımlar kullanılarak mümkündür.

Ancak, disk üzerinde kayıtlı suç kanıtı dosyalar dışındaki diğer dosyalarda benzer tutarsızlıklarla karşılaşılmamaktadır.

5.3. Son Erişim Tarihinin Disk Üzerinde Güncellenmesi

"*3.10. Sistem Hakkında Diğer Bilgiler*" bölümünde detaylandırıldığı üzere, sistemin son kapatıldığı tarihte yapılan ayarla, bu sistem kullanılarak yapılan dosya işlemlerinde dosya erişim tarihlerinin diskte güncellenmemesi beklenilen durumdur.

Ancak, incelenen bir kısım dosyanın disk üzerindeki erişim tarihlerinin güncellenmiş olduğu görülmektedir.

Örneğin "*05.11.30-CYDD OGRENCI BİLGİ.xls*" dosyasının işlem tarihleri aşağıdadır.

Diskte Son Değişiklik	10/04/2009 19:27:41
Son Erişim	11/01/2009 14:44:48
Dosyada Son Değişiklik	05/02/2006 20:14:56
Diskte Oluşturulma	05/02/2006 20:32:38
Silinme	18/02/2009 12:28:43

Bu durum, bu dosyanın diskin takılı olduğu bilgisayarda kurulu olan işletim sistemiyle değil, dosyaların son erişim tarihlerinin diskte güncellenebildiği bir başka sistemde oluşturulduğunu göstermektedir.

Ayrıca bu dosyanın son erişim tarihi dosyanın diskte oluşturulduğu tarihten ileridedir ve diğer suç konusu dosyaların disk üzerinde işlem gördükleri tarihlerde de benzer çelişkilerle karşılaşılmaktadır.

5.4. Dosya İşlem Tarihlerindeki Çelişkilerin İncelenmesi

Yukarıda detaylandırılan çelişkiler sebebiyle, dosya kayıt işlemlerinin izlerine ulaşmak için dosya sisteminde yer alan NTFS jurnali ($UsnJrnl) ve NTFS olay kayıtları (LogFile) incelenmek istenmiştir.

Kurulu Windows XP sisteminin sürümü sebebiyle NTFS jurnal kayıtlarının olmadığı görülmüştür.

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

NTFS olay kayıtlarının (LogFile) "*Sleuthkit Autopsy*" yazılımıyla incelenmesiyle, dosya sistemi üzerinde sistem tarihi geri alınarak dosya kayıt işlemleri yapıldığı şüphesi edinilmiştir.

Örneğin; son MFT dosya kaydı "*SERPİL.xls*" adlı silinmiş dosyadır.

Dosya Adı	SERPİL.xls
MFT Girdi No	12,072
Diskte Son Değişiklik	10/04/2009 23:22:35
Son Erişim	19/02/2008 16:15:02
Dosyada Son Değişiklik	17/12/2007 00:05:02
Diskte Oluşturulma	19/02/2008 16:15:02
Oluşturulma LogFile Sıra No	106,267,383
Silinme Tarihi	18/02/2009 12:28:43
Silinme LogFile Sıra No	106,319,157

Bu MFT kaydı, dosyanın diskte son değişikliğinin sistemin kapatıldığı tarihten sonra yapıldığını ve dosyanın diskin formatlandığı tarihten önce kaydedildiğini göstermektedir.

Bu bulgu, disk üzerinde tarih manipülasyonlarıyla dosya oluşturulduğunu göstermektedir.

5.5. Dosya Sistemindeki Geri Tarihli İşlemlerin LogFile Yapısında Tespiti

"*5.1. NTFS Dosya Sistemlerinde Ana Dosya Tablosu (MFT) Hakkında Bilgi*" bölümünde açıklanan bir NTFS dosya sistemi yapısı olan LogFile yapısındaki işlem kayıt numaraları her işlemde artacak şekilde tutulur.

Normalde çalışan bir bilgisayarın saati devamlı ileriye gideceği için, LogFile kayıt numaralarının artışının dosya işlem tarihleriyle uyumlu olması beklenen durumdur.

Bu işlem kayıtları, bir otel resepsiyon görevlisinin doldurduğu, hangi müşterinin, hangi odayı, hangi tarhte tuttuğu ve hangi tarihte çıkış yaptığını gösterir kayıt defterine benzetilmesi tam olarak uygun bir örnektir.

Örneğin, söz konusu otel kayıt defterinde 10 numaralı kaydın 10/06/2012 tarihini göstermesine rağmen 11 numaralı kaydın 09/06/2012 tarihini göstermesi bu kaydın geçerli bir kayıt olmadığına işaret eder.

"*5.4. Dosya İşlem Tarihlerindeki Çelişkilerin İncelenmesi*" bölümünde verilen örnekteki ve benzer durumdaki çelişkili kayıtların görülmesinden doğan şüphenin giderilmesi için, "*NTFS Log Tracker v1.0*" yazılımı kullanılarak LogFile yapısında kayıtlı olan işlemlerin dökümü alınmıştır.

Bu dökümde olay kaydı olarak saklanan ilki 89,777,161 ve sonuncusu 106,553,708 sıra numaralı toplam 30,272 (otuz bin iki yüz yetmiş iki) kayıt olduğu tespit edilmiştir.

Bu kayıtların bir kısmı sistemde çalışan "*INF.Autorun-96*" olarak sınıflandırılan kötü amaçlı yazılım tarafından geri tarihli olarak gerçekleştirildiğini ve "*d1vmq.exe*" ile "*autorun.inf*" dosyalarının farklı aralıklarla oluşturulduğunu göstermektedir.

Yapılan incelemede, sistemin son kapatıldığı tarihteki son dosya sistemi işleminin 103,812,372 numaralı LogFile girdisinin işaret ettiği "*Documents and Settings/KCYDD/UserData/OX2ZSHAN/YL[1].xml*" dosyasının içeriğinin değişmesi olayı olduğu görülmektedir.

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

Bu olay kaydını takip eden 103,816,014 sıra numaralı olay kaydı geri tarihli olarak 17/03/2009 18:15:41 tarihini taşımaktadır ve bu olayı takip eden yine aynı tarihli 103,816,062 sıra numaralı olay sonunda "*Documents and Settings/KCYDD/Belgelerim/New Folder*" dizini oluşturulmaktadır.

Yapılan incelemede ilki 103,816,014 ve sonuncusu 106,553,708 olmak üzere toplam 9,321 dosya sistemi işleminin;

1. Sistemin son kapatıldığı tarihten sonra yapıldığı,
2. Sistem tarihi ileri ve geri alınarak önce diske suç unsuru içeren dosyaların yanısıra birçok dosyanın kopyalandığı,
3. Bu sürçete diskte toplam 1,115 (bin yüz on beş) dosyanın oluşturulduğu,
4. Daha sonra sistem tarihi değiştirilerek dosyaların silindiği

tespit edilmektedir.

Suç kanıtı olarak kabul edilen dosyaların tarihselliğini, MFT girdilerini ve LogFile sıra numaralarını gösteren dökümler "*Ek 2*", "*Ek 3*" ve "*Ek 4*"te sunulmuştur.

Bu dökümlerde dosyaların sabit diskte oluşturulma tarihleriyle LogFile ve MFT girdi numaralarında uyumsuzluk görülmektedir.

LogFile yapısından elde edilen;

1. Tarih manipülasyonu ile diske yüklenen dosyaların dökümü "*Ek 5*"te,
2. Tarih manipülasyonu içeren dosya sistemi işlemlerini gösteren döküm "*Ek 6*"da,
3. Tüm dosya sistemi işlemlerini gösteren döküm "*Ek 8*"de

sunulmuştur.

5.6. Sabit Diskin Başka Bir Bilgisayara Takılarak İşlem Yapılmasının İzleri

5.6.1. Başka Bilgisayara Ait Güvenlik Tanımlayıcısı İzi

Sabit diskin takılı olduğu "*KCYDD3*" adlı bilgisayarın güvenlik tanımlayacısının (SID) "*S-1-5-21-329068152-1580818891-682003330*" olduğu tespit edilmiş ve "*3.3. Kurulu İşletim Sistemi*" bölümünde raporlanmıştır.

Güvenlik tanımlayıcısı (SID), işletim sistemi kurulumundan sonra Windows işletim sistemi tarafından kurulduğu makineye otomatik olarak atanan ve Windows Kayıt Defteri'nde saklanan bir değerdir.

Bu değer her kurulan makine için eşsiz olacak şekilde hesaplanır ve birden fazla makinenin aynı SID değerine sahip olması imkansızdır.

"*Administrator*" adlı kullanıcının güvenlik tanımlayıcısı her zaman 500 ile biter ve başında tanımlı olduğu makinenin güvenlik tanımlayıcısı yer alır.

"*Administrator*" adlı kullanıcının;

1. Güvenlik tanımlayıcısının "*S-1-5-21-329068152-1580818891-682003330-500*",
2. Son giriş tarihinin 21/02/2009 21:40:56,
3. Son parola değişiklik tarihinin 21/02/2009 23:28:55

olduğu tespit edilmiş ve "*3.8. Tanımlı Kullanıcılar*" bölümünde raporlanmıştır.

Bu bilgiler ışığında LogFile yapısında yapılan incelemede "*Administrator*" kullanıcısıyla giriş yapılarak sistemin kapatıldığı 10/04/2009 20:48:18 tarihine kadar sistemde bazı işlemler yaptığı görülmektedir.

"*RECYCLER/S-1-5-21-329068152-1580818891-682003330-500" konumunda* "Administrator" kullanıcısının kullanımına özel bir çöp tenekesi girdisi bulunmamaktadır.

Ancak inceleme sırasında 20/03/2009 17:35:26 tarihli, 106,500,184 numaralı dizin oluşturulma LogFile kaydına sahip, "*RECYCLER/S-1-5-21-1547161642-1644491937-682003330-500*" adlı ve diskten silinmiş dosyalar içeren çöp tenekesi diziniyle karşılaşılmıştır.

Bu dizin adının "*KCYDD3*" adlı bilgisayarın "*S-1-5-21-329068152-1580818891-682003330"* güvenlik tanımlayıcısı yerine "*S-1-5-21-1547161642-1644491937-682003330"* ile belirtilen güvenlik tanımlayıcısını içermesi, söz konusu çöp tenekesi dizininin diskin takıldığı başka bir makinede oluşturulduğunu göstermektedir.

Bu çöp tenekesi dizini, içerdiği silinmiş dizin ve dosya girdileri sistemin son kapatıldığı tarihten sonrasına işaret eden oluşturulma ve silinme LogFile kayıt numaraları taşımaktadır.

Bu bulgu, diskin sistemin son kullanıldığı tarihten sonra başka bir bilgisayara takılarak üzerinde dosya oluşturma ve dosya silme işlemlerinin yapıldığını göstermektedir.

5.6.2. Başka Dilde Windows İşletim Sistemi İzi

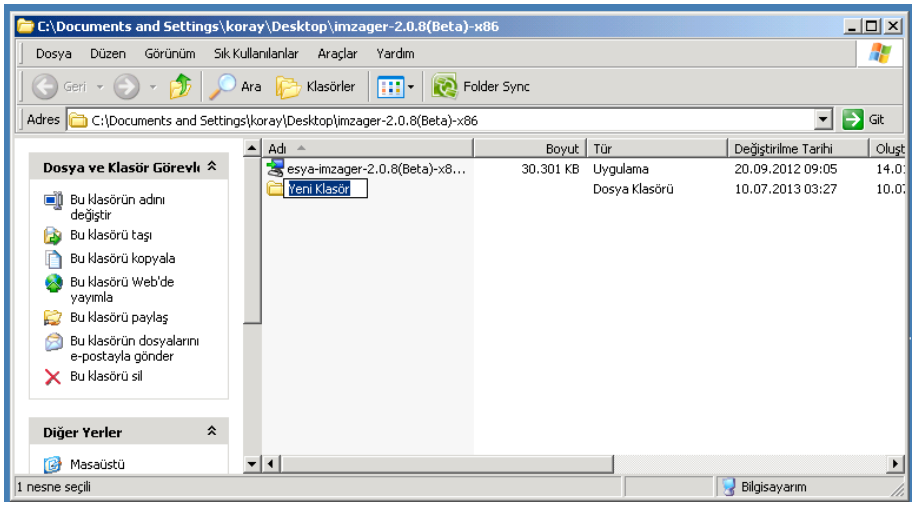
Yapılan incelemede "*KCYDD3*" adlı sistemde kullanılan Windows XP işletim sisteminin dilinin Türkçe olduğu tespit edilmiştir.

Ancak, örneğin;

1. 103,816,014
2. 103,816,038
3. 103,816,062
4. 103,817,564
5. 103,817,588
6. 103,817,638
7. 103,819,903
8. 103,819,927
9. 103,819,951
10. 103,820,210
11. 103,820,234
12. 103,820,296

numaralı LogFile kayıtlarında görülen, sabit disk üzerinde oluşturulan yeni dizinlerin ilk adının "*New Folder*" olarak verilmesidir.

Yeni bir dizin oluşturulurken ilgili menüden "yeni klasör" seçeneği kullanılarak sonradan adının değiştirilmesi tipik bir kullanıcı davranışıdır. Türkçe Windows işletim sistemi kullanıldığı takdirde böyle bir durumda yeni oluşturulan bir dizine "*Yeni Klasör*" adı verilmektedir.



Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

Yapılan incelemede toplam 300 dosya sistemi işleminin "*New Folder*" adına işaret ettiği tespit edilmektedir.

Bu oluşturulan dizinlerin adlarının oluşturulma sonrası değiştirildikleri için dosya sistemi üzerinde kayıtlı "*New Folder*" adlı herhangi bir dizin bulunmamaktadır.

Bu dizinlerin adlarının değiştirildikten sonra içlerine dosya kopyalandığı görülmektedir.

Söz edilen dosya ve dizin oluşturma işlemlerinin LogFile kayıt numaralarına göre sistemin son kez kapatıldığı tarihten sonra ve sistem tarihinde değişikliklerle gerçekleştirildiği tespit edilmektedir.

Bu bulgu da, diskin sistemin son kullanıldığı tarihten sonra başka bir bilgisayara takılarak üzerinde dosya oluşturma ve dosya silme işlemlerinin yapıldığını göstermektedir.

5.6.3. Diske Kaydedilen Geri Tarihli Dosyaların Son Erişim Tarihlerinin Güncellenmiş Olması

"*3.11. Sistem Hakkında Diğer Bilgiler*" bölümünde ayrıntılandırıldığı üzere, sabit diskin takılı olduğu bilgisayarın son kapatıldığı tarihten kısa bir zaman önce yapılan Windows XP işletim sistemi ayarları sebebiyle dosya erişim tarihlerinin sabit disk üzerinde güncellenmemesi beklenilen durumdur.

Ancak "*Ek 6*" ve "*Ek 8*"deki dökümlerde görülen birçok dosyanın son erişim tarihlerinin oluşturulma, değişiklik ve MFT değişikliği tarihlerinden ileride olduğu görülmektedir, dolayısıyla disk üzerinde işlem gören bu dosyaların erişim tarihlerinin güncellenmiş olduğunu göstermektedir.

Bu bulgu da sabit diskin sistemin son kapatıldığı tarihten sonra başka bir bilgisayara takılarak üzerinde tarih manipülasyonlarıyla dosya kaydı yapıldığını göstermektedir.

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

6. Özet

"*KCYDD3*" adlı sistemde takılı olarak 21/02/2009 23:39:15 ile 10/04/2009 20:48:18 tarihleri arasında kullanılan, 13/04/2009 14:30 itibariyle arama sonucu el konulmuş olan ÇYDD Kadıköy Şubesi'ne ait 40 GB Sığalı Maxtor marka, 25B6201H10T7IY seri numaralı sabit disk imajında, ilgili imajın temini öncesi yapılan el koyma tutanağında ve ilk sayısal delil incelemesi belgelerinde yapılan incelemede;

1. Sabit diskin ele geçirilme anında imajının oluşturulmadığı görüldüğünden, alınan imajla özgün kütük arasında birbirlerine denklikleri açısından somut bilgi bulunmadığı görülmüştür.

2. 02.06.2010 tarihli "*İNCELEME VE DEĞERLENDİRME RAPORU*"nda bir kısım dosyaların üst verileriyle sağlanan bir kısım bilgilerin tespitinin yapıldığı, ancak tüm bilgilerin tespit edilmediği görülmüştür.

3. 02.06.2010 tarihli "*İNCELEME VE DEĞERLENDİRME RAPORU*"nda dosya sistemi incelemesinin hiçbir dosya için yapılmadığı anlaşılmıştır.

4. Söz konusu disk üzerinde kayıtlı suç kanıtı olarak kabul edilen dosyalarda yapılan incelemede, dosyaların tümünde tarih ve üst veri tutarsızlıkları tespit edilmiştir.

5. Dosyaların bulunduğu sabit disk üzerindeki NTFS LogFile yapısında kayıtlı dosya sistemi işlemlerinden suç kanıtı sayılan dosyaları gösterir kayıtların sistemin son kullanıldığı tarihten sonra yapılan geri tarihli işlemler olduğu tespit edilmiştir.

6. Bu işlemlerle diskte toplam 1,115 dosyanın oluşturulduğu tespit edilmiştir.

7. Sabit diskin "*KCYDD3*" adlı bilgisayardaki kullanım sürecinden sonra başka bir bilgisayara takıldığının izleri tespit edilmiştir.

8. Söz konusu geri tarihli dosya kayıt işlemlerinin sabit diskin takılı olduğu bu bilgisayarda yapıldığı anlaşılmıştır.

9. Bu dosya kayıt işlemleri bittikten sonra kaydedilen dosyaların silindiği tespit edilmiştir.

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

7. Sonuç

İncelenen ÇYDD Kadıköy Şubesi'ne ait 40 GB Sığalı Maxtor marka, 25B6201H10T7IY seri numaralı sabit diskteki dosya sistemine geri tarihli işlemlerle aralarında suç kanıtı olan dosyaların da bulunduğu 1,115 dosya ve bu dosyaları içeren dizinlerin kaydedildiği tespit edilmiştir.

Sabit diskin takılı bulunduğu bilgisayarın son kez kapatıldığı 10/04/2009 tarihi saat 20:48:18'ten sonra başka bir bilgisayara takılarak bu dosya ve dizinlerin sabit diske kaydedildikleri anlaşılmıştır.

Bu kayıt işlemleri 10/04/2009 tarihi saat 20:48:18'den çok önceki tarihleri gösterecek şekilde yapıldığı ve daha sonra da kaydedilen bu dosyaların silindiği tespit edilmiştir.

Bu bulgular, söz konusu sabit diskin içeriğine kullanım tarihinden sonra, bilinmeyen bir tarihte geri tarihli işlemlerle değişiklik yapıldığını açıkça göstermektedir.

İncelenen ÇYDD Kadıköy Şubesi'ne ait 40 GB Sığalı Maxtor marka, 25B6201H10T7IY seri numaralı sabit diskin uğradığı bu içerik değişikliği dolayısıyla geçerli bir sayısal delil olma vasfını yitirdiği kanaatindeyim.

Adli Bilirkişi
Tevfik Koray Peksayar
Mak. Müh. Lis. - Bilgi Tekn. Y. Lis.
İTÜ Diploma No: 76 - 387



Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.

Ekler

Ek 1 - Dosya İnceleme Dökümü

Ek 2 - Suç Konusu Dosyaların Diskte Oluşturulma Tarihi, MFT Girdisi ve LogFile Girdisi Dökümü (Diskte Oluşturulma Tarihine Göre Sıralı)

Ek 3 - Suç Konusu Dosyaların Diskte Oluşturulma Tarihi, MFT Girdisi ve LogFile Girdisi Dökümü (LogFile Sıra Numarasına Göre Sıralı)

Ek 4 - Suç Konusu Dosyaların Diskte Oluşturulma Tarihi, MFT Girdisi ve LogFile Girdisi Dökümü (MFT Girdi Numarasına Göre Sıralı)

Ek 5 – Manipülasyon İle Diske Yüklenen Dosyaların Oluşturulma, MFT'de Değişiklik, Erişim Tarihleri ve LogFile Girdisi Dökümü

Ek 6 – Manipülasyon İçeren İşlemlerin LogFile Kayıtları

Ek 7 - Excel Dosyalarında Varolan BIFF Kayıtlarının Elde Edilmesinde Kullanılan Program Kodları (PHP Dilinde)

Ek 8 - Tüm LogFile Kayıtları

Notlar

1. Ek 6 ve Ek 8'de sunulan dökümlerdeki boş hücreler üst hücrelerle aynı olay ve olay tarihini içerir anlamına gelmektedir.

2. Ek 6 ve Ek 8'de sunulan dökümlerdeki geçici işlem kayıtlarında görülebilen saat farkları LogFile yapısında bu işlemler için saat dilimi bilgisi tutulmamasından kaynaklanmaktadır.

Bu belge 5070 sayılı Elektronik İmza Kanunu'na göre elektronik imza ile imzalanmıştır.