



T.C.  
YILDIZ TEKNİK ÜNİVERSİTESİ  
Elektrik - Elektronik Fakültesi Dekanlığı

Sayı : B.30.2.YIL.0.28.00.00/2002  
Konu :

Tarih : 16/12/2011

Sayın Av.Dr. Duygun YARSUVAT  
Av. Hüseyin ERSÖZ

İlgi: 10.11.2011 tarihli yazınız.

İlgi yazınız ile talep etmiş olduğunuz teknik rapor hazırlanarak ekte sunulmuştur.

Bilgilerinizi rica ederim.

Saygılarımla,

Prof. Dr. Celal KOCATEPE  
DEKAN

Eki: Rapor

T.C.

**Yıldız Teknik Üniversitesi**

**Elektrik Elektronik Fakültesi Dekanlığı'na**

15/12/2011

## I-Konu:

Av.Dr. Duygun Yarsuvat ve Av. Hüseyin Ersöz'ün dekanlığımıza vermiş olduğu 10.11.2011 tarihli (Dekanlık 11.11.2011 tarih/275 kayıtlı) talep yazısı ile Müvekkili Hüseyin Soner Yalçın için CMK'nun 67/6 maddesi uyarınca Bilirkişi İncelemesi yaptırmak istemiştir. Bu amaçla dilekçe ekinde bir usb içinde verilen Arama ve El Koyma tutanağında tanımlı hard disk imaj üzerinde inceleme yapılarak, ilişkin dilekçelerinde belirttikleri 6 konuda (soruda) cevap ve teknik değerlendirme içeren rapor hazırlamasını istemiştir.

## II-İstem:

İlgili dilekçede:

Arama ve el koyma tutanağında Seagate Marka "ST3120827AS\_4MS1TF89" Seri Numaralı, imaj alma tutanağında HASH değerleri SHA1:d09a547f2ae2714ecaf7e365695e7d36bd98f5d8 ve MD5:5d533c43c70eccd368539c5107c63439 olarak verilen hard diske ait olduğu belirtilen disk imajı, Accessdata firmasının üretilen "FTK Imager" programının en güncel sürümü olan 3.1.0.1514 numaralı versiyonu ile incelenmiştir. Yöneltilen sorular ve ilişkin cevaplarımız ve değerlendirmelerimiz aşağıdadır.

### III- İnceleme ve değerlendirme:

#### Soru 1

a) Yukarıda bilgileri verilen Hard Disk içerisinde, aşağıda belirtilen dijital veriler, silinmiş veya silinmemiş olarak yer almakta mıdır?

"Ermeni Dosyası.doc", "Koz.doc", "Nedim.doc", "simon son.doc", "ABDULKADİR AYGAN.pdf", "EK-D MİLİ EĞİTİM.doc", "YBelgesi.doc", "Fabrikatör.doc", "Ulusal Medya.doc", "Tv Analiz Proje.doc", "Reosta Operasyonu.doc", "panzehir.doc", "mit medya.doc", "mafia.doc", "Sabri Uzun.doc", "Konuşma Notu.doc", "KADROLAŞMA KONUŞMA NOTU(OCAK 2004).doc", "Kadrolaşma en son0610170003.doc", "KADROLAŞMA EK-C.doc", "KADROLAŞMA EK-A.doc", "Kadrolaşma Bilgi Notu (Ocxak 2004).doc", "EK-E AKP'NİN ATAMALARI.xls", "EK-D MİLİ EĞİTİM.doc", "radikal dini gurupların faaliyet alanları.pdf", "000KITAP.docx", "trt.doc", "Ulusal Medya 2010.doc", "toplanti.doc", "prj\_60.doc", "CHP.doc", "Yalçın hoca.doc", "SY.doc", "teRTEmiz.doc", "Hanefi.doc", "Bilinçlendirme.doc", "Sn.Komutanım.doc"

b) Bu dijital dokümanların metadata (üstveri) bilgileri nedir? Bu bilgiler Adli Bilişim esasları çerçevesinde kesinlik taşımakta mıdır?

c) Söz konusu dijital verilerin NTFS dosya sistemindeki "MFT Kayıt Tarihi" nedir? Ayrıca yukarıda isimleri belirtilen dijital dokümanlarda işletim sistemi tarafından tutulan başka tarih alanları bulunmakta mıdır? Bu tarihler metadata bilgileri ile uyumluluk taşımakta mıdır? Elde edilen bulgular çerçevesinde dijital dokümanlara ilişkin değerlendirmeleriniz nelerdir?

#### Cevap 1)

Yukarıda bilgileri verilen hard disk imajı üzerinde adli bilişim esaslarınca gerçekleştirdiğimiz inceleme neticesinde adı geçen dosyaların, a şıkında istenen disk üzerinde bulunup bulunmaması ile ilgili sonuçlar, b şıkında istenen metadata bilgileri ve c şıkında istenen MFT Kayıt Tarihi bilgileri her bir dosya için ayrı bir tablo şeklinde aşağıda sunulmuştur. Dosyalar için MFT kayıt tarihi haricinde tutulan tarih bilgileri de yine tablolarda yer almaktadır. Bu alanlar hakkında ayrıntılı bilgi aşağıda verilmiştir.

"Dosya Adı" alanı, soruda belirtilen dosyanın disk imajı üzerinde aranan dizgesidir.

"Diskte Kaydı Var mı?" alanı, aranan dizgenin disk imajı üzerinde bulunup bulunmadığını gösterir.

"Dosya mı?" alanı, aranan dizgenin gerçek bir dosya olup olmadığını gösterir.

“Silinmiş mi?” alanı, dosyanın diskten silinip silinmediğini gösterir.

“Diskteki konumu” alanı, dosyanın disk üzerinde (silinmişse silinmeden önce) bulunduğu yeri gösterir.

“Şifreli mi?” alanı, dosyanın şifreli olup olmadığını gösterir.

“Gizli mi?” alanı, dosyanın gizli olup olmadığını gösterir.

“Son Erişim Tarihi” alanı, bilgisayar üzerinde herhangi bir işlem için kullanıcı, işletim sistemi veya herhangi bir uygulama tarafından dosyaya son erişilen tarihi gösterir. Bu alanın güncellenip güncellenmemesi, Windows işletim sisteminde Registry olarak bilinen sistem ayarları mekanizması ile belirlenir. Dosyalar üzerinde işlem yapan virüsler genellikle Registry kayıtlarında bu alanın güncellenmemesi için değişiklik yaparlar.

“Yaratılma Tarihi” alanı, dosyanın disk üzerinde ilk yaratılma veya başka bir ortamdan diske ilk kopyalanma tarihini gösterir.

“Dosyaya Son Yazım Tarihi” alanı, dosya üzerinde ilgili program ile açılarak içeriğinin değiştirilmesi suretiyle işlem yapıldığı son tarihi gösterir.

“MFT Kayıt Tarihi” alanı, dosyanın disk üzerinde bulunan \$MFT sistem kayıt dosyasına eklenme tarihini gösterir. MFT (Master File Table), Microsoft firmasının geliştirdiği ve Windows işletim sistemlerinde standart olarak kullanılan NTFS dosya sisteminde tüm dosyaların kaydının tutulduğu bir sistem dosyasıdır. “MFT Kayıt tarihi”, herhangi bir dosyaya ilgili olarak MFT içinde tutulan kayıttaki en son değişiklik tarihidir. Bu değişiklik; dosyanın içeriğinin değiştirilmesi veya dosya ile ilgili tutulan tarih bilgilerinin herhangi birinin değiştirilmesi şeklinde olabilir.

“MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?” alanı, MFT dosyasındaki kayıt tarihi bilgileri ile dosyanın metadata’sında yer alan diğer tarih bilgilerinin uyumlu olup olmadığını gösterir.

Dosya Adı	Ermeni Dosyası.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\snrylcn\proje\Ermeni Dosyası.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	28/09/2010 11.54.42
Yaratılma Tarihi	28/09/2010 11.54.42
Dosyaya Son Yazım Tarihi	12/02/2009 13.08.10
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	28/09/2010 11.54.42
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"><li>Dosyaya son yazım tarihi, dosyanın disk üzerindeki yaratılma tarihinden eskidir. Bu durum, bu dosyanın kesinlikle incelenen bilgisayarda oluşturulmadığını,</li></ul>





	bir başka bilgisayarda hazırlandığını ve incelenen bilgisayarda hiç değiştirilmediğini göstermektedir. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.
--	---

Dosya Adı	Koz.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\Koz.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	16/08/2010 10.32.20
Yaratılma Tarihi	16/08/2010 10.32.20
Dosyaya Son Yazım Tarihi	04/08/2010 10.49.56
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	16/08/2010 10.32.20
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"><li>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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li><li>Silinen dosyanın bıraktığı alanda mbvd.exe olarak bilinen virüsün izlerine rastlanmıştır. Bu durum ile ilgili ekran görüntüsü Ek-1'de verilmiştir. Mbvd.exe 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 yapabilen bir virüstür. Virüs ile ilgili detaylı bilgi Ek-2'deki internet sayfasında verilmiştir. Bu dosyanın silinmesinde mbvd.exe virüsünün rol oynadığı mütalaa edilmektedir.</li></ul>

JCH

JCH

Dosya Adı	Nedim.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\Nedim.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	16/08/2010 10.32.20
Yaratılma Tarihi	16/08/2010 10.32.20
Dosyaya Son Yazım Tarihi	09/08/2010 06.35.18
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	16/08/2010 10.32.20
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"> <li>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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li> <li>Dosyanın yaratılma ve son erişim tarihleri, bir önceki incelenen dosya ile birebir aynıdır. Ancak bu iki dosyaya ait ve aynı olan tarih kayıtları, aynı klasörde silinmiş olarak bulunan başka dosya ve klasörlerle aynı değildir. Bu durum iki dosyanın aynı anda silindiğini göstermektedir. Bir önceki dosyanın silinmesinde virüs etkisi olduğu göz önüne alındığında, bu dosya üzerinde de virüs ile işlem yapıldığı mütalaa edilmektedir.</li> </ul>

Dosya Adı	simon son.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Hayır
Silinmiş mi?	Diskte mevcut değildir.
Diskteki konumu	Diskte mevcut değildir.
Şifreli mi?	Diskte mevcut değildir.
Gizli mi?	Diskte mevcut değildir.
Son Erişim Tarihi	Diskte mevcut olmadığından tespit edilemez.
Yaratılma Tarihi	Diskte mevcut olmadığından tespit edilemez.
Dosyaya Son Yazım Tarihi	Diskte mevcut olmadığından tespit edilemez.
Ek Açıklamalar	Aranan dizgenin, işletim sistemine ait \$LogFile ve

*[Handwritten signature]*

*[Handwritten signature]*

	ŞMFT dosyalarında izi olduğu, ancak iki dosyada da aranan dosyaya ilişkin bir kayıt girdisi olmadığı tespit edilmiştir.
MFT Kayıt Tarihi	Mevcut bulunmamaktadır.
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Mevcut olmadığı için tespit edilemez.
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosya disk üzerinde silinmiş ya da silinmemiş olarak mevcut değildir. "simon son.doc" dizgesinin ham imaj kaydı üzerinde aranması ile, sadece ŞMFT ve ŞLogfile dosyalarının yazıldığı disk alanlarında geçtiği görülmüştür. Ancak, ŞMFT ve ŞLogfile dosyaların çözümlenmesinde, incelenen dosya ile ilgili herhangi bir kayda rastlanmamıştır. Bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceği düşüncesindeyiz.</li> </ul>

Dosya Adı	ABDULKADİR AYGAN.pdf
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\sncyl\ABDULKADİR AYGAN.pdf
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	20/12/2010 08.28.46
Yaratılma Tarihi	20/12/2010 08.28.45
Dosyaya Son Yazım Tarihi	25/05/2008 22.21.34
Ek Açıklamalar	Dosyanın işletim sistemine ait ŞLogFile ve ŞMFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	20/12/2010 08.28.46
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosyaya son yazım tarihi, dosyanın disk üzerindeki yaratılma tarihinden eskidir. Bu durum, bu dosyanın kesinlikle incelenen bilgisayarda oluşturulmadığını, bir başka bilgisayarda hazırladığını ve incelenen bilgisayarda hiç değiştirilmediğini göstermektedir. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li> </ul>

Dosya Adı	EK-D MİLİ EĞİTİM.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Hayır

SH

SH

Silinmiş mi?	Diskte mevcut değildir.
Diskteki konumu	Diskte mevcut değildir.
Şifreli mi?	Diskte mevcut değildir.
Gizli mi?	Diskte mevcut değildir.
Son Erişim Tarihi	Diskte mevcut olmadığından tespit edilemez.
Yaratılma Tarihi	Diskte mevcut olmadığından tespit edilemez.
Dosyaya Son Yazım Tarihi	Diskte mevcut olmadığından tespit edilemez.
Ek Açıklamalar	Aranan dizgenin işletim sistemine ait \$LogFile dosyasında ve disk boş alanında kayıt izleri olduğu tespit edilmiştir. Ancak dosyanın \$MFT dosyasında kaydı yoktur. Bu durum dosyanın diske kaydedilmediğini göstermektedir.
MFT Kayıt Tarihi	Mevcut bulunmamaktadır.
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Mevcut olmadığı için tespit edilemez.
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosya disk üzerinde silinmiş ya da silinmemiş olarak mevcut değildir. "EK-D MİLİ EĞİTİM.doc" dizgesinin ham imaj kaydı üzerinde aranması ile, sadece \$Logfile dosyasının yazıldığı disk alanında ve boş disk alanında geçtiği, \$MFT dosyasında kaydı olmadığı görülmüştür. \$Logfile dosyasının çözümlenmesinde, incelenen dosya ile ilgili herhangi bir kayda rastlanmamıştır. Bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceği düşüncesindeyiz.</li> </ul>

Dosya Adı	Ybelgesi.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\Nedim\YBelgesi.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	27/09/2010 13.34.57
Yaratılma Tarihi	27/09/2010 13.34.57
Dosyaya Son Yazım Tarihi	09/07/2009 12.20.00
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	27/09/2010 13.34.57
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosyaya son yazım tarihi, dosyanın disk üzerindeki yaratılma tarihinden eskidir. Bu durum, bu dosyanın kesinlikle incelenen bilgisayarda oluşturulmadığını, bir başka bilgisayarda hazırlandığını ve</li> </ul>

*[Handwritten signature]*

*[Handwritten signature]*

	incelenen bilgisayarda hiç değiştirilmediğini göstermektedir. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.
--	--

Dosya Adı	Fabrikatör.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\snrcyln\proje\Fabrikatör.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	28/09/2010 11.54.42
Yaratılma Tarihi	28/09/2010 11.54.42
Dosyaya Son Yazım Tarihi	12/02/2009 13.08.10
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	28/09/2010 11.54.42
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"><li>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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li><li>Silinen dosyanın bıraktığı alanda b00ijwpu.exe olarak bilinen virüsün izlerine rastlanmıştır. Bu durum ile ilgili ekran görüntüsü Ek-3'te verilmiştir. b00ijwpu.exe 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 yapabilen bir virüstür. Virüs ile ilgili detaylı bilgi Ek-4'teki internet sayfasında verilmiştir. Bu dosyanın silinmesinde b00ijwpu.exe virüsünün rol oynadığı mütalaa edilmektedir.</li></ul>





Dosya Adı	Ulusal Medya.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\snrcyl\proje\Ulusal Medya.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	28/09/2010 11.54.42
Yaratılma Tarihi	28/09/2010 11.54.42
Dosyaya Son Yazım Tarihi	12/02/2009 13.08.12
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	28/09/2010 11.54.42
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"><li>• 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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li><li>• Dosyanın bilgisayarda yaratılma ve son erişim tarihleri, bir önceki dosya ile birebir aynıdır. Dosyaya son yazım tarihi ise bir önceki dosyadan sadece iki saniye farklıdır. Bu durumun normal kullanıcı davranışlarıyla oluşturulması mümkün görünmemektedir. Her iki dosyanın da çok benzer tarih özelliklerine sahip olması, yaratılma ya da kopyalama ve silme işlemlerinin virüs faaliyeti ile gerçekleştiğine işaret eder.</li><li>• Silinen dosyanın bıraktığı alanda mbvd.exe olarak bilinen virüsün izlerine rastlanmıştır. Bu durum ile ilgili ekran görüntüsü Ek-5'te verilmiştir. Mbvd.exe 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 yapabilen bir virüstür. Virüs ile ilgili detaylı bilgi Ek-2'deki internet sayfasında verilmiştir. Bu dosyanın silinmesinde mbvd.exe virüsünün rol oynadığı</li></ul>

JST

HU

	mütalaa edilmektedir.
--	-----------------------

Dosya Adı	<b>Tv Analiz Proje.doc</b>
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\snrcyln\proje\Tv Analiz Proje.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	28/09/2010 11.54.42
Yaratılma Tarihi	28/09/2010 11.54.42
Dosyaya Son Yazım Tarihi	12/02/2009 13.08.12
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	28/09/2010 11.54.42
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"><li>• 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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li><li>• Dosyanın bilgisayarda yaratılma, son erişim ve dosyaya son yazım tarihleri, bir önceki dosya ile birebir aynıdır. Bu durumun normal kullanıcı davranışlarıyla oluşturulması mümkün görünmemektedir. Her iki dosyanın da aynı tarih özelliklerine sahip olması, yaratılma ya da kopyalama ve silme işlemlerinin virüs faaliyeti ile gerçekleştiğine işaret eder.</li><li>• Silinen dosyanın bıraktığı alanda <b>mbvd.exe</b> olarak bilinen virüsün izlerine rastlanmıştır. Bu durum ile ilgili ekran görüntüsü Ek-6'da verilmiştir. Mbvd.exe 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 yapabilen bir virüstür. Virüs ile ilgili detaylı bilgi Ek-2'deki internet sayfasında</li></ul>

JET,

AD

	verilmiştir. Bu dosyanın silinmesinde mbvd.exe virüsünün rol oynadığı mütalaa edilmektedir.
--	---

Dosya Adı	Reosta Operasyonu.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\snrcyln\proje\Reosta Operasyonu.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	28/09/2010 11.54.42
Yaratılma Tarihi	28/09/2010 11.54.42
Dosyaya Son Yazım Tarihi	12/02/2009 13.08.12
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	28/09/2010 11.54.42
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"><li>• 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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li><li>• Dosyanın bilgisayarda yaratılma, son erişim ve dosyaya son yazım tarihleri, bir önceki dosya ile birebir aynıdır. Bu durumun normal kullanıcı davranışlarıyla oluşturulması mümkün görünmemektedir. Her iki dosyanın da aynı tarih özelliklerine sahip olması, yaratılma ya da kopyalama ve silme işlemlerinin virüs faaliyeti ile gerçekleştiğine işaret eder.</li><li>• Silinen dosyanın bıraktığı alanda 9b9w3.exe olarak bilinen virüsün izlerine rastlanmıştır. Bu durum ile ilgili ekran görüntüsü Ek-7'de verilmiştir. 9b9w3.exe 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</li></ul>

*[Handwritten signature]*

*[Handwritten signature]*

	yapabilen bir virüstür. Virüs ile ilgili detaylı bilgi Ek-8'deki internet sayfasında verilmiştir. Bu dosyanın silinmesinde 9b9w3.exe virüsünün rol oynadığı mütalaa edilmektedir.
--	---

Dosya Adı	panzehir.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\snrcyl\proje\panzehir.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	28/09/2010 11.54.42
Yaratılma Tarihi	28/09/2010 11.54.42
Dosyaya Son Yazım Tarihi	12/02/2009 13.08.12
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	28/09/2010 11.54.42
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"><li>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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li><li>Dosyanın bilgisayarda yaratılma, son erişim ve dosyaya son yazım tarihleri, bir önceki dosya ile birebir aynıdır. Bu durumun normal kullanıcı davranışlarıyla oluşturulması mümkün görünmemektedir. Her iki dosyanın da aynı tarih özelliklerine sahip olması, yaratılma ya da kopyalama ve silme işlemlerinin virüs faaliyeti ile gerçekleştiğine işaret eder.</li></ul>

Dosya Adı	mit medya.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\snrcyl\proje\mit medya.doc





Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	28/09/2010 11.54.42
Yaratılma Tarihi	28/09/2010 11.54.42
Dosyaya Son Yazım Tarihi	12/02/2009 13.08.10
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	28/09/2010 11.54.42
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"> <li>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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li> <li>Dosyanın bilgisayarda yaratılma ve son erişim tarihleri, bir önceki dosya ile birebir aynıdır. Dosyaya son yazım tarihi ise sadece iki saniye farklıdır. Bu durumun normal kullanıcı davranışlarıyla oluşturulması mümkün görünmemektedir. Her iki dosyanın da çok benzer tarih özelliklerine sahip olması, yaratılma ya da kopyalama ve silme işlemlerinin virüs faaliyeti ile gerçekleştiğine işaret eder.</li> </ul>

Dosya Adı	mafia.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\snrcyl\proje\mafia.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	28/09/2010 11.54.42
Yaratılma Tarihi	28/09/2010 11.54.42
Dosyaya Son Yazım Tarihi	12/02/2009 13.08.10
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	28/09/2010 11.54.42
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosyaya son yazım tarihi, dosyanın disk üzerindeki yaratılma tarihinden eskidir.</li> </ul>





	<p>Bu durum, bu dosyanın kesinlikle incelenen bilgisayarda oluşturulmadığını, bir başka bilgisayarda hazırlandığını ve incelenen bilgisayarda hiç değiştirilmediğini göstermektedir. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</p> <ul style="list-style-type: none"> <li>• Dosyanın bilgisayarda yaratılma ve son erişim tarihleri, bir önceki dosya ile birebir aynıdır. Dosyaya son yazım tarihi ise sadece iki saniye farklıdır. Bu durumun normal kullanıcı davranışlarıyla oluşturulması mümkün görünmemektedir. Her iki dosyanın da çok benzer tarih özelliklerine sahip olması, yaratılma ya da kopyalama ve silme işlemlerinin virüs faaliyeti ile gerçekleştiğine işaret eder.</li> </ul>
--	--

Dosya Adı	Sabri Uzun.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\Sabri Uzun.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	20/12/2010 09.46.21
Yaratılma Tarihi	20/12/2010 09.46.21
Dosyaya Son Yazım Tarihi	20/12/2010 09.35.20
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	20/12/2010 09.46.21
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"> <li>• 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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li> </ul>

Dosya Adı	Konuşma Notu.doc
Diskte Kaydı Var mı?	Evet

*[Handwritten signature]*

*[Handwritten signature]*

Dosya mı?	Hayır
Silinmiş mi?	Diskte mevcut değildir.
Diskteki konumu	Diskte mevcut değildir.
Şifreli mi?	Diskte mevcut değildir.
Gizli mi?	Diskte mevcut değildir.
Son Erişim Tarihi	Diskte mevcut olmadığından tespit edilemez.
Yaratılma Tarihi	Diskte mevcut olmadığından tespit edilemez.
Dosyaya Son Yazım Tarihi	Diskte mevcut olmadığından tespit edilemez.
Ek Açıklamalar	Aranan dizgenin işletim sistemine ait \$LogFile dosyasında ve disk boş alanında kayıt izleri olduğu tespit edilmiştir. Ancak dosyanın \$MFT dosyasında kaydı yoktur. Bu durum dosyanın diske kaydedilmediğini göstermektedir.
MFT Kayıt Tarihi	Mevcut bulunmamaktadır.
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Mevcut olmadığı için tespit edilemez.
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosya disk üzerinde silinmiş ya da silinmemiş olarak mevcut değildir. "Konuşma Notu.doc" dizgesinin ham imaj kaydı üzerinde aranması ile, sadece \$Logfile dosyasının yazıldığı disk alanında ve boş disk alanında geçtiği, \$MFT dosyasında kaydı olmadığı görülmüştür. \$Logfile dosyasının çözümlenmesinde, incelenen dosya ile ilgili herhangi bir kayda rastlanmamıştır. Bu durum normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceği düşüncesindeyiz.</li> </ul>

Dosya Adı	KADROLAŞMA KONUŞMA NOTU(OCAK 2004).doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Hayır
Silinmiş mi?	Diskte mevcut değildir.
Diskteki konumu	Diskte mevcut değildir.
Şifreli mi?	Diskte mevcut değildir.
Gizli mi?	Diskte mevcut değildir.
Son Erişim Tarihi	Diskte mevcut olmadığından tespit edilemez.
Yaratılma Tarihi	Diskte mevcut olmadığından tespit edilemez.
Dosyaya Son Yazım Tarihi	Diskte mevcut olmadığından tespit edilemez.
Ek Açıklamalar	Aranan dizgenin işletim sistemine ait \$LogFile dosyasında ve disk boş alanında kayıt izleri olduğu tespit edilmiştir. Ancak dosyanın \$MFT dosyasında kaydı yoktur. Bu durum dosyanın diske kaydedilmediğini göstermektedir.
MFT Kayıt Tarihi	Mevcut bulunmamaktadır.
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Mevcut olmadığı için tespit edilemez.
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosya disk üzerinde silinmiş ya da silinmemiş olarak mevcut değildir.</li> </ul>

	<p>“KADROLAŞMA KONUŞMA NOTU(OCAK 2004).doc” dizgesinin ham imaj kaydı üzerinde aranması ile, sadece \$Logfile dosyasının yazıldığı disk alanında ve boş disk alanında geçtiği, \$MFT dosyasında kaydı olmadığı görülmüştür. \$Logfile dosyasının çözümlenmesinde, incelenen dosya ile ilgili herhangi bir kayda rastlanmamıştır. Bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceği düşüncesindeyiz.</p>
--	---

Dosya Adı	Kadrolaşma en son061017003.doc
Diskte Kaydı Var mı?	Hayır
Dosya mı?	Hayır
Silinmiş mi?	Diskte mevcut değildir.
Diskteki konumu	Diskte mevcut değildir.
Şifreli mi?	Diskte mevcut değildir.
Gizli mi?	Diskte mevcut değildir.
Son Erişim Tarihi	Diskte mevcut olmadığından tespit edilemez.
Yaratılma Tarihi	Diskte mevcut olmadığından tespit edilemez.
Dosyaya Son Yazım Tarihi	Diskte mevcut olmadığından tespit edilemez.
Ek Açıklamalar	Aranan dizgenin diskte hiçbir kaydı bulunmamaktadır.
MFT Kayıt Tarihi	Mevcut bulunmamaktadır.
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Mevcut olmadığı için tespit edilemez.
Değerlendirmeler	<ul style="list-style-type: none"> <li>“Kadrolaşma en son061017003.doc” dizgesi disk üzerinde yer almamaktadır.</li> </ul>

Dosya Adı	KADROLAŞMA EK-C.doc
Diskte Kaydı Var mı?	Hayır
Dosya mı?	Hayır
Silinmiş mi?	Diskte mevcut değildir.
Diskteki konumu	Diskte mevcut değildir.
Şifreli mi?	Diskte mevcut değildir.
Gizli mi?	Diskte mevcut değildir.
Son Erişim Tarihi	Diskte mevcut olmadığından tespit edilemez.
Yaratılma Tarihi	Diskte mevcut olmadığından tespit edilemez.
Dosyaya Son Yazım Tarihi	Diskte mevcut olmadığından tespit edilemez.
Ek Açıklamalar	Aranan dizgenin işletim sistemine ait \$LogFile dosyasında kayıt izleri olduğu tespit edilmiştir. Ancak dosyanın \$MFT dosyasında kaydı yoktur. Bu durum dosyanın diske kaydedilmediğini göstermektedir.
MFT Kayıt Tarihi	Mevcut bulunmamaktadır.
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Mevcut olmadığı için tespit edilemez.
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosya disk üzerinde silinmiş ya da silinmemiş olarak mevcut değildir.</li> </ul>





	<p>“KADROLAŞMA EK-C.doc” dizgesinin ham imaj kaydı üzerinde aranması ile, sadece \$Logfile dosyasının yazıldığı disk alanında geçtiği, \$MFT dosyasında kaydı olmadığı görülmüştür. \$Logfile dosyasının çözümlenmesinde, incelenen dosya ile ilgili herhangi bir kayda rastlanmamıştır. Bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceği düşüncesindeyiz.</p>
--	---

<b>Dosya Adı</b>	<b>KADROLAŞMA EK-A.doc</b>
<b>Diskte Kaydı Var mı?</b>	Hayır
<b>Dosya mı?</b>	Hayır
<b>Silinmiş mi?</b>	Diskte mevcut değildir.
<b>Diskteki konumu</b>	Diskte mevcut değildir.
<b>Şifreli mi?</b>	Diskte mevcut değildir.
<b>Gizli mi?</b>	Diskte mevcut değildir.
<b>Son Erişim Tarihi</b>	Diskte mevcut olmadığından tespit edilemez.
<b>Yaratılma Tarihi</b>	Diskte mevcut olmadığından tespit edilemez.
<b>Dosyaya Son Yazım Tarihi</b>	Diskte mevcut olmadığından tespit edilemez.
<b>Ek Açıklamalar</b>	Aranan dizgenin işletim sistemine ait \$LogFile dosyasında kayıt izleri olduğu tespit edilmiştir. Ancak dosyanın \$MFT dosyasında kaydı yoktur. Bu durum dosyanın diske kaydedilmediğini göstermektedir.
<b>MFT Kayıt Tarihi</b>	Mevcut bulunmamaktadır.
<b>MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?</b>	Mevcut olmadığı için tespit edilemez.
<b>Değerlendirmeler</b>	<ul style="list-style-type: none"> <li>Dosya disk üzerinde silinmiş ya da silinmemiş olarak mevcut değildir. “KADROLAŞMA EK-A.doc” dizgesinin ham imaj kaydı üzerinde aranması ile, sadece \$Logfile dosyasının yazıldığı disk alanında geçtiği, \$MFT dosyasında kaydı olmadığı görülmüştür. \$Logfile dosyasının çözümlenmesinde, incelenen dosya ile ilgili herhangi bir kayda rastlanmamıştır. Bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceği düşüncesindeyiz.</li> </ul>

<b>Dosya Adı</b>	<b>Kadrolaşma Bilgi Notu (Ocxak 2004).doc</b>
<b>Diskte Kaydı Var mı?</b>	Evet
<b>Dosya mı?</b>	Hayır
<b>Silinmiş mi?</b>	Diskte mevcut değildir.
<b>Diskteki konumu</b>	Diskte mevcut değildir.
<b>Şifreli mi?</b>	Diskte mevcut değildir.

*[Handwritten signature]*

*[Handwritten signature]*

Gizli mi?	Diskte mevcut değildir.
Son Erişim Tarihi	Diskte mevcut olmadığından tespit edilemez.
Yaratılma Tarihi	Diskte mevcut olmadığından tespit edilemez.
Dosyaya Son Yazım Tarihi	Diskte mevcut olmadığından tespit edilemez.
Ek Açıklamalar	Aranan dizgenin işletim sistemine ait \$LogFile dosyasında, disk üzerinde silinmiş olan bir dosyada ve disk boş alanında kayıt izleri olduğu tespit edilmiştir. Ancak dosyanın \$MFT dosyasında kaydı yoktur. Bu durum dosyanın diske kaydedilmediğini göstermektedir.
MFT Kayıt Tarihi	Mevcut bulunmamaktadır.
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Mevcut olmadığı için tespit edilemez.
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosya disk üzerinde silinmiş ya da silinmemiş olarak mevcut değildir. "KADROLAŞMA KONUŞMA NOTU(OCAK 2004).doc" dizgesinin ham imaj kaydı üzerinde aranması ile, sadece \$Logfile dosyasının yazıldığı disk alanında ve boş disk alanında geçtiği, \$MFT dosyasında kaydı olmadığı görülmüştür. \$Logfile dosyasının çözümlenmesinde, incelenen dosya ile ilgili herhangi bir kayda rastlanmamıştır. Bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceği düşüncesindeyiz.</li> <li>Dizge bir de "D:\ Documents and Settings\EXPER\Belgelerim\Avid Liquid\Data\Media\Reels\@Imported Files0.P001001FC\2049241P 21073809P A1.WAV.pk" dosyasının içinde geçmektedir. Bu dosyada aynı zamanda hjvjte.exe virüsüne ait izler de tespit edilmiştir. Bu durum ile ilgili ekran görüntüsü Ek-9'da verilmiştir. hjvjte.exe 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 yapabilen bir virüstür. Virüs ile ilgili detaylı bilgi Ek-10'daki internet sayfasında verilmiştir.</li> </ul>

Dosya Adı	EK-E AKP'NİN ATAMALARI.xls
Diskte Kaydı Var mı?	Hayır
Dosya mı?	Hayır
Silinmiş mi?	Diskte mevcut değildir.
Diskteki konumu	Diskte mevcut değildir.

*[Handwritten signature]*

*[Handwritten signature]*

Şifreli mi?	Diskte mevcut değildir.
Gizli mi?	Diskte mevcut değildir.
Son Erişim Tarihi	Diskte mevcut olmadığından tespit edilemez.
Yaratılma Tarihi	Diskte mevcut olmadığından tespit edilemez.
Dosyaya Son Yazım Tarihi	Diskte mevcut olmadığından tespit edilemez.
Ek Açıklamalar	Aranan dizgenin işletim sistemine ait \$LogFile dosyasında kayıt izleri olduğu tespit edilmiştir. Ancak dosyanın \$MFT dosyasında kaydı yoktur. Bu durum dosyanın diske kaydedilmediğini göstermektedir.
MFT Kayıt Tarihi	Mevcut bulunmamaktadır.
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Mevcut olmadığı için tespit edilemez.
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosya disk üzerinde silinmiş ya da silinmemiş olarak mevcut değildir. "EK-E AKP'NİN ATAMALARI.xls" dizgesinin ham imaj kaydı üzerinde aranması ile, sadece \$Logfile dosyasının yazıldığı disk alanında geçtiği, \$MFT dosyasında kaydı olmadığı görülmüştür. \$Logfile dosyasının çözümlenmesinde, incelenen dosya ile ilgili herhangi bir kayda rastlanmamıştır. Bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceği düşüncesindeyiz.</li> </ul>

Dosya Adı	<b>EK-D MİLİ EĞİTİM.doc</b>
Diskte Kaydı Var mı?	Evet
Dosya mı?	Hayır
Silinmiş mi?	Diskte mevcut değildir.
Diskteki konumu	Diskte mevcut değildir.
Şifreli mi?	Diskte mevcut değildir.
Gizli mi?	Diskte mevcut değildir.
Son Erişim Tarihi	Diskte mevcut olmadığından tespit edilemez.
Yaratılma Tarihi	Diskte mevcut olmadığından tespit edilemez.
Dosyaya Son Yazım Tarihi	Diskte mevcut olmadığından tespit edilemez.
Ek Açıklamalar	Aranan dizgenin işletim sistemine ait \$LogFile dosyasında ve disk boş alanında kayıt izleri olduğu tespit edilmiştir. Ancak dosyanın \$MFT dosyasında kaydı yoktur. Bu durum dosyanın diske kaydedilmediğini göstermektedir.
MFT Kayıt Tarihi	Mevcut bulunmamaktadır.
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Mevcut olmadığı için tespit edilemez.
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosya disk üzerinde silinmiş ya da silinmemiş olarak mevcut değildir. "EK-D MİLİ EĞİTİM.doc" dizgesinin ham imaj kaydı üzerinde aranması ile, sadece \$Logfile dosyasının yazıldığı disk alanında ve boş disk alanında geçtiği, \$MFT dosyasında kaydı olmadığı görülmüştür.</li> </ul>

*[Handwritten signature]*

*[Handwritten signature]*

	<p>ŞLogfile dosyasının çözümlenmesinde, incelenen dosya ile ilgili herhangi bir kayda rastlanmamıştır. Bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceği düşüncesindeyiz.</p>
--	---

Dosya Adı	radikal dini grupların faaliyet alanları.pdf
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\snrcyln\kozinoğlu3\radikal dini grupları faaliyetleri\radikal dini grupların faaliyet alanları.pdf
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	20/12/2010 08.28.47
Yaratılma Tarihi	20/12/2010 08.28.47
Dosyaya Son Yazım Tarihi	16/12/2007 22.10.50
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	20/12/2010 08.28.47
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"> <li>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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li> </ul>

Dosya Adı	000KITAP.docx
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\Yeni Klasör\S.U\000KITAP.docx
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	10/01/2011 13.24.13
Yaratılma Tarihi	10/01/2011 13.24.13
Dosyaya Son Yazım Tarihi	17/12/2010 11.51.56
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT

JOH.

JOH

	dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	10/01/2011 13.24.13
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"> <li>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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li> </ul>

Dosya Adı	trt.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Hayır
Diskteki konumu	C:\Documents and Settings\Türker\Belgelerim\Documents\ayşegül\trt.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	14/10/2010 14.58.03
Yaratılma Tarihi	19/03/2008 15.11.18
Dosyaya Son Yazım Tarihi	19/03/2008 15.15.08
Ek Açıklamalar	<p>Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.</p> <p>"trt.doc" dizgesi ayrıca "C:\Documents and Settings\türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (barisp)\Inbox\5DB624C9-00001FEC.eml" ve "C:\Documents and Settings\türker\Local Settings\Application Data\Microsoft\Windows Live Mail\Odatv (barisp)\Inbox\27037685-00004057.eml" dosyalarında kayıtlı bulunan e-posta mesajlarında da geçtiği tespit edilmiştir.</p>
MFT Kayıt Tarihi	22/07/2010 09.55.46
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Hayır
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosyanın disk üzerindeki yaratılma tarihi ve dosyaya son yazım tarihi, birbirine yakın ve tutarlıdır.</li> <li>\$MFT dosyasında işli bulunan son erişim tarihi Temmuz 2010 iken, dosyaya son erişim tarihi Ekim 2010 olarak görünmektedir. Bu durum, dosyaya kullanıcı müdahalesi dışında normal olmayan bir yolla erişim yapıldığını</li> </ul>





göstermektedir.

Dosya Adı	Ulusal Medya 2010.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\AÇIL SUSAM AÇIL\snrcyln\proje\Ulusal Medya 2010.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	28/09/2010 11.54.42
Yaratılma Tarihi	28/09/2010 11.54.42
Dosyaya Son Yazım Tarihi	27/09/2010 12.33.10
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	28/09/2010 11.54.42
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"><li>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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li><li>Dosyanın bilgisayarda yaratılma ve son erişim tarihleri, aynı klasörde silinmiş olarak bulunan diğer dosyalarla birebir aynıdır. Bu durumun normal kullanıcı davranışlarıyla oluşturulması mümkün görünmemektedir. Dosyaların aynı tarih özelliklerine sahip olması, yaratılma ya da kopyalama ve silme işlemlerinin virüs faaliyeti ile gerçekleştiğine işaret eder.</li></ul>

Dosya Adı	toplantı.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\ toplantı.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	24/12/2010 11.09.03
Yaratılma Tarihi	26/04/2010 08.36.39
Dosyaya Son Yazım Tarihi	25/04/2010 11.33.56
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT

	dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	26/04/2010 08.36.39
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"> <li>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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li> <li>Silinen dosyanın bıraktığı alanda <b>mbdm.exe</b> olarak bilinen virüsün izlerine rastlanmıştır. Bu durum ile ilgili ekran görüntüsü Ek-11'de verilmiştir. mbdm.exe kullanıcının isteği dışında yabancı adreslere internet bağlantısı kurma, bilgisayarda çalışan diğer uygulamalara karışma, <b>bilgisayardaki dosyalar üzerinde işlem yapma, bilgisayara dosya kopyalama, dosya silme gibi işlemler yapabilen bir virüstür.</b> Virüs ile ilgili detaylı bilgi Ek-12'deki internet sayfasında verilmiştir. Bu dosyanın silinmesinde mbdm.exe virüsünün rol oynadığı mütalaa edilmektedir.</li> </ul>

Dosya Adı	<b>prj_60.doc</b>
Diskte Kaydı Var mı?	Evet
Dosya mı?	Hayır
Silinmiş mi?	Diskte mevcut değildir.
Diskteki konumu	Diskte mevcut değildir.
Şifreli mi?	Diskte mevcut değildir.
Gizli mi?	Diskte mevcut değildir.
Son Erişim Tarihi	Diskte mevcut olmadığından tespit edilemez.
Yaratılma Tarihi	Diskte mevcut olmadığından tespit edilemez.
Dosyaya Son Yazım Tarihi	Diskte mevcut olmadığından tespit edilemez.
Ek Açıklamalar	Aranan dizgenin işletim sistemine ait \$LogFile dosyasında kayıt izleri olduğu tespit edilmiştir. Ancak dosyanın \$MFT dosyasında kaydı yoktur. Bu durum dosyanın diske kaydedilmediğini göstermektedir.
MFT Kayıt Tarihi	Mevcut bulunmamaktadır.
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Mevcut olmadığı için tespit edilemez.
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosya disk üzerinde silinmiş ya da silinmemiş olarak mevcut değildir.</li> </ul>

*[Handwritten signature]*

*[Handwritten signature]*

	<p>“prj_60.doc” dizgesinin ham imaj kaydı üzerinde aranması ile, sadece \$Logfile dosyasının yazıldığı disk alanında geçtiği, \$MFT dosyasında kaydı olmadığı görülmüştür. \$Logfile dosyasının çözümlenmesinde, incelenen dosya ile ilgili herhangi bir kayda rastlanmamıştır. Bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceği düşüncesindeyiz.</p>
--	--

Dosya Adı	CHP.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Hayır
Diskteki konumu	C:\Documents and Settings\türker\Desktop\CHP.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	28/01/2011 17.37.54
Yaratılma Tarihi	24/01/2011 14.01.26
Dosyaya Son Yazım Tarihi	24/01/2011 14.01.26
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	24/01/2011 14.01.29
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosyaya son yazım tarihi, dosyanın disk üzerindeki yaratılma tarihi ile birebir aynıdır. Bu durum, bu dosyanın kesinlikle incelenen bilgisayarda oluşturulmadığını, bir başka ortamdan kopyalandığını göstermektedir. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li> <li>Dosyaya son erişim tarihi son yazım ve oluşturulma tarihlerinden ileridedir. Bu da dosyaya bu bilgisayardan erişim yapıldığını ancak hiçbir değişiklik yapılmadığını gösterir. Dosyaya işletim sisteminde herhangi bir uygulama ile mi yoksa kullanıcı tarafından mı erişildiği ise kesin olarak tespit edilemez.</li> </ul>
Dosya Adı	CHP.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Hayır
Diskteki konumu	C:\Documents and

JH.

ld

	Settings\türker\Desktop\temizlenecek\CHP.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	28/01/2011 17.30.46
Yaratılma Tarihi	28/09/2010 13.27.14
Dosyaya Son Yazım Tarihi	05/11/2010 09.17.21
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	23/11/2010 07.14.35
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosya 28 Eylül 2010'da yaratılmış, 05 Kasım 2010'da içeriğinde değişiklik yapılmıştır. \$MFT kayıt tarihi ise 23 Kasım 2010'dur, yani son değişiklik tarihinden ileridedir. Ancak dosyaya son erişim tarihi 28 Ocak 2011 olarak görünmektedir. Bu da dosyaya kullanıcının kontrolü ve işletim sistemi yöntemleri dışında bir yoldan erişildiğini gösterir.</li> </ul>

Dosya Adı	Yalçın hoca.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Hayır
Silinmiş mi?	Diskte mevcut değildir.
Diskteki konumu	Diskte mevcut değildir.
Şifreli mi?	Diskte mevcut değildir.
Gizli mi?	Diskte mevcut değildir.
Son Erişim Tarihi	Diskte mevcut olmadığından tespit edilemez.
Yaratılma Tarihi	Diskte mevcut olmadığından tespit edilemez.
Dosyaya Son Yazım Tarihi	Diskte mevcut olmadığından tespit edilemez.
Ek Açıklamalar	Aranan dizgenin işletim sistemine ait \$LogFile dosyasında kayıt izleri olduğu tespit edilmiştir. Ancak dosyanın \$MFT dosyasında kaydı yoktur. Bu durum dosyanın diske kaydedilmediğini göstermektedir.
MFT Kayıt Tarihi	Mevcut bulunmamaktadır.
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Mevcut olmadığı için tespit edilemez.
Değerlendirmeler	<ul style="list-style-type: none"> <li>Dosya disk üzerinde silinmiş ya da silinmemiş olarak mevcut değildir. "Yalçın hoca.doc" dizgesinin ham imaj kaydı üzerinde aranması ile, sadece \$Logfile dosyasının yazıldığı disk alanında geçtiği, \$MFT dosyasında kaydı olmadığı görülmüştür. \$Logfile dosyasının çözümlenmesinde, incelenen dosya ile ilgili herhangi bir kayda rastlanmamıştır. Bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan</li> </ul>

	izlerin virüs kaynaklı bir işlemle yapılabileceği düşüncesindeyiz.
--	--

Dosya Adı	SY.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Hayır
Silinmiş mi?	Diskte mevcut değildir.
Diskteki konumu	Diskte mevcut değildir.
Şifreli mi?	Diskte mevcut değildir.
Gizli mi?	Diskte mevcut değildir.
Son Erişim Tarihi	Diskte mevcut olmadığından tespit edilemez.
Yaratılma Tarihi	Diskte mevcut olmadığından tespit edilemez.
Dosyaya Son Yazım Tarihi	Diskte mevcut olmadığından tespit edilemez.
Ek Açıklamalar	Aranan dizgenin işletim sistemine ait \$LogFile dosyasında kayıt izleri olduğu tespit edilmiştir. Ancak dosyanın \$MFT dosyasında kaydı yoktur. Bu durum dosyanın diske kaydedilmediğini göstermektedir.
MFT Kayıt Tarihi	Mevcut bulunmamaktadır.
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Mevcut olmadığı için tespit edilemez.
Değerlendirmeler	<ul style="list-style-type: none"><li>Dosya disk üzerinde silinmiş ya da silinmemiş olarak mevcut değildir. "SY.doc" dizgesinin ham imaj kaydı üzerinde aranması ile, sadece \$Logfile dosyasının yazıldığı disk alanında geçtiği, \$MFT dosyasında kaydı olmadığı görülmüştür. \$Logfile dosyasının çözümlenmesinde, incelenen dosya ile ilgili herhangi bir kayda rastlanmamıştır. Bu durumun normal kullanıcı davranışları ile oluşamayacağı, bulunan izlerin virüs kaynaklı bir işlemle yapılabileceği düşüncesindeyiz.</li></ul>

Dosya Adı	teRTEmiz.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\yeni\teRTEmiz.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	26/07/2010 09.55.57
Yaratılma Tarihi	26/07/2010 09.55.57
Dosyaya Son Yazım Tarihi	09/10/2008 11.12.18
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	26/07/2010 09.55.57
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet



<b>Değerlendirmeler</b>	<ul style="list-style-type: none"> <li>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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li> <li>Silinen dosyanın bıraktığı alanda <b>9b9w3.exe</b> olarak bilinen virüsün izlerine rastlanmıştır. Bu durum ile ilgili ekran görüntüsü Ek-13'te verilmiştir. 9b9w3.exe kullanıcının isteği dışında yabancı adreslere internet bağlantısı kurma, bilgisayarda çalışan diğer uygulamalara karışma, <b>bilgisayardaki dosyalar üzerinde işlem yapma, bilgisayara dosya kopyalama, dosya silme</b> gibi işlemler yapabilen bir virüstür. Virüs ile ilgili detaylı bilgi Ek-8'deki internet sayfasında verilmiştir. Bu dosyanın silinmesinde 9b9w3.exe virüsünün rol oynadığı mütalaa edilmektedir.</li> </ul>
-------------------------	--

<b>Dosya Adı</b>	<b>Hanefi.doc</b>
<b>Diskte Kaydı Var mı?</b>	Evet
<b>Dosya mı?</b>	Evet
<b>Silinmiş mi?</b>	Evet
<b>Diskteki konumu</b>	D:\Yedek\desktop\yeni\Hanefi.doc
<b>Şifreli mi?</b>	Hayır
<b>Gizli mi?</b>	Hayır
<b>Son Erişim Tarihi</b>	26/01/2011 12.07.37
<b>Yaratılma Tarihi</b>	26/07/2010 09.55.57
<b>Dosyaya Son Yazım Tarihi</b>	12/07/2010 09.17.48
<b>Ek Açıklamalar</b>	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
<b>MFT Kayıt Tarihi</b>	26/07/2010 09.55.57
<b>MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?</b>	Evet
<b>Değerlendirmeler</b>	<ul style="list-style-type: none"> <li>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. Dosyanın bilgisayara hangi kaynaktan</li> </ul>

*[Handwritten signature]*

*[Handwritten signature]*

	<p>nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</p> <ul style="list-style-type: none"> <li>• Dosyanın \$MFT kayıt tarihi Temmuz 2010 iken, son erişim tarihi Ocak 2011'dir. Bu da dosyaya kullanıcının kontrolü ve işletim sistemi yöntemleri dışında bir yoldan erişildiğini gösterir.</li> </ul>
--	---

Dosya Adı	Bilinçlendirme.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\yeni\Bilinçlendirme.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	26/07/2010 09.55.57
Yaratılma Tarihi	26/07/2010 09.55.57
Dosyaya Son Yazım Tarihi	24/03/2010 23.15.04
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	26/07/2010 09.55.57
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"> <li>• 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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li> <li>• Silinen dosyanın bıraktığı alanda b00ijwpu.exe olarak bilinen virüsün izlerine rastlanmıştır. Bu durum ile ilgili ekran görüntüsü Ek-14'te verilmiştir. b00ijwpu.exe 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 yapabilen bir virüstür. Virüs ile ilgili detaylı bilgi Ek-4'teki internet sayfasında verilmiştir. Bu dosyanın silinmesinde b00ijwpu.exe virüsünün rol oynadığı mütalaa edilmektedir. Dosyanın yaratılma ve son erişim tarihlerinin aynı klasörde silinmiş</li> </ul>

JH

JH

	olarak bulunan "teRTEmiz.doc" isimli dosya ile birebir aynı olması, dosya üzerinde virüs vasıtası ile işlem yapıldığını doğrulamaktadır.
--	--

Dosya Adı	Sn.komutanım.doc
Diskte Kaydı Var mı?	Evet
Dosya mı?	Evet
Silinmiş mi?	Evet
Diskteki konumu	D:\Yedek\desktop\yeni\Sn.Komutanım.doc
Şifreli mi?	Hayır
Gizli mi?	Hayır
Son Erişim Tarihi	24/12/2010 11.08.23
Yaratılma Tarihi	26/07/2010 09.55.57
Dosyaya Son Yazım Tarihi	01/07/2010 14.19.34
Ek Açıklamalar	Dosyanın işletim sistemine ait \$LogFile ve \$MFT dosyalarında da kayıt izleri olduğu tespit edilmiştir.
MFT Kayıt Tarihi	26/07/2010 09.55.57
MFT Kayıt Tarihi Diğer Tarihlerle Uyumlu mu?	Evet
Değerlendirmeler	<ul style="list-style-type: none"><li>• 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. Dosyanın bilgisayara hangi kaynaktan nasıl geldiği ise disk imajından elde edilen verilerle kesin olarak söylenemez.</li><li>• Silinen dosyanın bıraktığı alanda 9b9w3.exe olarak bilinen virüsün izlerine rastlanmıştır. Bu durum ile ilgili ekran görüntüsü Ek-15'te verilmiştir. 9b9w3.exe 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 yapabilen bir virüstür. Virüs ile ilgili detaylı bilgi Ek-8'deki internet sayfasında verilmiştir. Bu dosyanın silinmesinde 9b9w3.exe virüsünün rol oynadığı mütalaa edilmektedir.</li><li>• Dosyanın yaratılma tarihlerinin aynı klasörde silinmiş olarak bulunan "teRTEmiz.doc" ve "Bilinçlendirme.doc" isimli dosyalar ile birebir aynı olması,</li></ul>

	<p>dosya üzerinde virüs vasıtası ile işlem yapıldığını doğrulamaktadır.</p> <ul style="list-style-type: none"><li>• Dosyanın son erişim tarihinin ŞMFT kayıt tarihinden yaklaşık 6 ay ileride olması da dosyaya kullanıcı ya da işletim sistemi üzerinden değil, farklı bir yoldan erişildiğini gösterir.</li></ul>
--	---

## Soru 2

**Bir dijital dokümanın metadatasında (üstverisinde) yer alan yazar bilgileri aidiyeti sağlamak noktasında yeterli bir bilgi midir? Bir dijital dokümanın bir şahıs tarafından yaratıldığını ispatlayan, gösteren ve yasal geçerliliği olan veriler nelerdir?**

## Cevap 2)

Dijital dokümanlar format ve tiplerine bağlı olarak, işletim sisteminin her dosya için tuttuğu metadata dışında, kendi içlerinde tanımlayıcı üstveriler taşıyabilirler. Bu üstveriler her programın formatına ve dosya tipine bağlı olarak değişir, tüm dijital dokümanlarda aynı değildir. Örneğin kelime işlemci olarak tabir edilen Microsoft Word isimli program, “.doc” veya “.docx” uzantısına sahip tipte, kendi formatında dosyalar oluşturur ve veriyi bu dosyalarda kendine has üstverilerle birlikte tutar. .doc uzantılı bir dosyada Word programının kendine has olarak tuttuğu üstveri bilgileri aşağıda listelenmiştir.

- Dosyayı tanımlayıcı alanlar
  - Başlık (Title)
  - Konu (Subject)
  - Etiketler (Tags)
  - Kategoriler (Categories)
  - Yorumlar (Comments)
- Dosyanın sahipliği ile ilgili alanlar
  - Yazarlar (Authors)
  - En son Kaydeden (Last Saved By)
  - Revizyon Sayısı (Revision Number)
  - Versiyon Numarası (Version Number)
  - Program Adı (Program Name)
  - Şirket (Company)
  - Yönetici (Manager)
  - İçeriğin Yaratıldığı Tarih (Content Created)
  - Son Kaydedildiği Tarih (Date Last Saved)
  - Son Yazdırıldığı Tarih (Last Printed)
  - Toplam düzenleme zamanı (Total Editing Time)

- İçerik ile ilgili alanlar
  - İçerik durumu (Content Status)
  - İçerik Tipi (Content Type)
  - Kelime Sayısı (Word Count)
  - Karakter Sayısı (Character Count)
  - Satır Sayısı (Line Count)
  - Paragraf Sayısı (Paragraph Count)
  - Şablon (Template)
  - Ölçekleme (Scale)
  - Bağlantılar Bozuk Mu? (Links Dirty?)
  - Dili (Language)

Dijital bir dokümanın kendine has olarak tuttuğu üstveriler (metadata), o dokümanın kime ait olduğunu KESİNLİKLE ispatlamaz. Bu bilgilerden bazıları, kullanıcı tarafından ilgili programla (özel bir programa gerek duymadan bile) değiştirilebilir, hatta yanlış bile yazılabilir. Bunun dışında özel programlarla bu alanların tümü istendiği gibi değiştirilebilir. Bu değişiklikler kötü niyetli, virüs ya da casus programlarla da gerçekleştirilebilir. Bu sebeplerle dijital bir dokümanın kim tarafından oluşturulduğu kesin olarak tespit edilemez, ayrıca dijital dokümanın üst bilgilerinde yer alan yazar bilgileri aidiyeti sağlamak noktasında delil anlamında kesinlikle yeterli değildir.

Bir dijital dokümanın bir şahıs tarafından yaratıldığını ispatlayan, gösteren ve yasal geçerliliği olan tek veri dosyanın yaratıcısı olan şahıs tarafından kendi elektronik imzası ile imzalanması olabilir. Ancak elektronik imza da tek başına aidiyet bilgisini vermekte yetersiz kalabilir. Elektronik imza sistemleri donanımsal ya da yazılımsal olabilmektedir ve her iki türde de kullanıcının belirlediği şifre ile imza mekanizması işler. Şifrenin (veya donanımın) kaybedilmesi veyahut çalınması gibi durumlarda şifreyi ele geçirenler, bir şahsa ait olan elektronik imzayı kullanılarak, belgeleri o şahıs tarafından imzalanmış gibi gösterebilirler. Bu sebeplerle de dijital bir dokümanın bir şahıs tarafından yaratıldığını ispatlayan, gösteren ve yasal geçerliliği olan kesin bir mekanizma mevcut değildir.

### Soru 3

**Seagate Marka "ST3120827AS\_4MS1TF89" Seri Numaralı Hard Diskte hangi işletim sistemi ve virüs programı yüklüdür? Söz konusu bilgisayar "Uzaktan Yardım Bağlantılarına ve Uzaktan Denetime" açık mıdır? İşletim Sisteminin Güvenlik Özellikleri ve Virüs Programı zararlı e-posta ve yazılımlardan korumak noktasında ne kadar işlevseldir? Virüs Koruma Programlarının çalışma prensibi nedir?**

### Cevap 3)

İncelenen hard disk imajında yüklü olan işletim sistemi ve anti virüs programı ile ilgili detaylar aşağıdaki tabloda verilmiştir. Tespitte ilgili ekran görüntüsü Ek-16a ve Ek-16b'de mevcuttur.

İşletim Sistemi Adı	Microsoft Windows XP
İşletim Sistemi Tipi	Professional
Servis Paketi Seviyesi	Service Pack 2
Versiyonu	5.1
Derleme versiyonu	2600
Ürün Kodu	55896-640-0637221-23667
Dili	Türkçe
Antivirüs Programı	Eset Nod32 Antivirüs
Versiyonu	4.0.424.0
Kurulum Tarihi	04/12/2009

İncelenen bilgisayar uzaktan yardım bağlantılarına ve uzaktan denetime açıktır. Bununla ilgili ekran görüntüleri Ek 17a ve Ek-17-b'de verilmiştir.

İncelenen bilgisayarda kurulu olan işletim sisteminde, üretici firmanın özellikle güvenlik açıklarını gidermek için yüklenmesini tavsiye ettiği güncelleme paketlerinin (Service Pack) son versiyonu kurulu değildir. Bilgisayarda Service Pack 2 kuruludur. Üretici firmanın önerdiği son versiyon ise Service Pack 3'tür. Service Pack 3 kurulması ile birçok güvenlik açığı giderilmektedir. Bu güncellemeler Ek-18'de listelenmiştir.

Antivirüs yazılımlarının zararlı e-posta ve yazılımlardan koruma prensipleri için ilk olarak çalışma prensiplerinden bahsedilecektir. Bir antivirüs, bir programın ya da e-postanın ne yaptığına, yapısına bakarak onun virüs olup olmadığına karar veremez. Virüs olduğu bilinen dosyaların antivirüs yazılım üreticilerine rapor edilmeleri ile, bu üreticiler virüs gibi zararlı yazılımların bu dosyalarındaki imzalarını alırlar ve kendi veritabanlarına eklerler. Bu imzanın arama veritabanına eklenmesi ile artık o virüs ilgili antivirüs yazılımınca tanınabilir ve yakalanabilir olur. Bu çalışma prensibi sebebiyle, bir virüs tüm antivirüs programlarınca yakalanamayacağı gibi, bir antivirüs programı da tüm virüsleri yakalayamaz. Özellikle ortaya yeni çıkan virüsler; tanınıp, ihbar edilmeleri ve imzalarının veritabanlarına eklenmelerine kadar geçen sürede yayılabilir ve zarar verebilirler. Antivirüs ya da diğer güvenlik yazılımları, virüs dışında bilgisayarda "arka kapı (backdoor)" olarak bilinen ve iki yönlü veri sızdıran, zararlı kod çalıştırabilen trojan ve worm adı verilen zararlı programcıklar için de aynı prensiplerle çalışırlar. Bu sebeple de her türlü zararlı yazılıma karşı koruma sağlama prensipleri aynıdır.

Bilgisayarın işletim sistemindeki tüm güncellemelerin yapılmış olması, güncel bir virüs imza veri tabanına sahip antivirüs yazılımı kullanılması, ağ trafiğini filtreleyen güvenlik duvarı yazılımı kullanımı gibi önlemler alınsa dahi normal bir kullanıcının virüs ya da diğer zararlı yazılımlardan etkilenmemesi olanaksız değildir. İnternete bağlı ve Windows işletim sistemine sahip bir bilgisayarın %100 güvenli olması gibi bir tanım yapılması mümkün değildir.

#### Soru 4

**Bir bilgisayara normal kullanıcı yolları dışında erişim mümkün müdür? Bu hangi yollarla yapılabilmektedir? Böyle bir yasa dışı erişim halinde standart bir kullanıcı tarafından bu hususun fark edilmesi ve engellenebilmesi mümkün müdür? Böyle bir erişim mümkün ise korsan kullanıcı tarafından bilgisayar üzerinde hangi işlemlerin gerçekleştirilmesi mümkündür?**

#### Cevap 4)

Bir bilgisayara normal kullanıcı yolları dışında uzaktan erişim ve kontrol mümkündür. Windows işletim sisteminde uzaktan erişim, kontrol ve yardım için protokol bulunmaktadır ve incelenen hard diskten takılı olduğu bilgisayarda da bu özelliğin açık olduğu tespit edilmiştir.

Bilgisayara fiziksel erişim mümkünse, USB bellek ya da CD/DVD gibi ortamlarla bilgisayara zararlı programlar aktarılabilir ve yüklenebilir. Bu gibi programlar bilgisayara yüklenir ve çalıştırılırsa, kullanıcının bilgisi dışında, her türlü işlemi bilgisayar üzerinde gerçekleştirebilir.

Bu yolların dışında worm, trojan ve virüs denen zararlı yazılımlarla da kullanıcının bilgisi haricinde bilgisayara erişim yapılabilir, bir kullanıcının bilgisayarda yapabileceği her tür işlem gerçekleştirilebilir. Bu tip zararlı yazılımlar bilgisayara ağ altyapısındaki güvenlik açıkları kullanılarak ya da bilgisayar üzerindeki güvenlik açıkları kullanılarak yüklenebilir. Ayrıca internette zararlı içerik barındıran adreslere girilmesi ve bu kodların çalıştırılması ile de bilgisayara zararlı yazılımlar girebilir. Bu yöntemde örneğin, "videoyu izlemek için tıklayın ve izinleri kabul edin" yazan bir bağlantının tıklanması ile aslında zararlı program olan ancak video dosyası görüntüsü verilmiş bir bağlantının çalıştırılması yeterli olabilir. Aynı şekilde, ekinde aslında zararlı program içeren ancak normal bir Word dokümanı ya da resim dosyası görüntüsü verilmiş olan bir e-postanın kullanıcıya gönderilmesi ve kullanıcının bu dosyayı açmaya çalışması ile de zararlı yazılımlar bilgisayarı ele geçirebilir.

Zararlı yazılımlar istedikleri kodları bilgisayar üzerinde çalıştırılabileceği için, dosyalar üzerinde normal bir kullanıcının işletim sistemini kullanarak gerçekleştiremeyeceği işlemler de yapılabilir, çalışan diğer uygulamalara sızılabilir ve bunları da etkileyebilir. Sistemde dosya oluşturma, sistemden dosya silme, sistemdeki dosyaları değiştirme yanında; sisteme internetteki dış kaynaklardan dosya kopyalama ya da sistemdeki dosyaları internette belirli adreslere yükleme, e-posta ile gönderme gibi işlemleri de yapabilir. Bunun yanında kullanıcının kişisel ve özel bilgilerini, şifrelerini, hatta klavyede bastığı her bir tuşu bile okuyup kaydedebilir, dış kaynaklara gönderebilir. Kısaca ele geçirilen bilgisayar üzerinde zararlı programın yapabilecekleri, o programı üretenin bilgisayar üzerinde yapmak istediği her şey olabilir.

Bilgisayara yasadışı erişim yapıldığında kullanıcının bunu anlamasının tek yolu, güvenlik duvarı ya da antivirüs yazılımının bir erişim olduğuna ya da bir bağlantı kurulduğuna dair kullanıcıya uyarı vermesi olabilir. Ancak zararlı yazılımlar antivirüs programını da etkileyebilirler. Antivirüs eğer zararlı yazılımın

imzasını veritabanında bulundurmuyorsa, bu durumda uyarı da vermez. İncelenen bilgisayarda kurulu olan antivirüs programının böyle bir bağlantı kurulduğunda uyarı verme özelliği mevcut değildir. İşletim sisteminin de güvenlik duvarı en son güvenlik güncelleştirmelerine sahip değildir. Bu sebeplerle incelenen bilgisayarda normal bir kullanıcının böyle bir erişimi anlamasının yolu bulunmamaktadır. Bilgisayarda kurulan ağ bağlantılarını kontrol etmek ve çalışan uygulama ve sistem servislerini kontrol etmek, bunlara ilaveten normal dışı uygulama ve-veya servisler olduğunu belirlemek sıradan bir bilgisayar kullanıcısının yapamayacağı davranışlardır. Bilgisayar korsanı olarak tanımlanan kötü niyetli kişiler, bunları fark edemeyecek kullanıcıların bilgisayarlarına virüs ya da trojan programları yüklenmesi ile ele geçirir ve kendi amaçlarına uygun olarak istedikleri gibi kullanabilirler. Bu bilgisayarlara zombi bilgisayar adı verilir ve zombi bilgisayarın gerçek kullanıcısı bilgisayarının neler yaptığının, ne amaçlar için kullanıldığının farkında değildir.

## Soru 5

**Seagate Marka "ST3120827AS\_4MS1TF89" Seri Numaralı Hard Diskin imajı üzerinde yapılan inceleme neticesinde bir güvenlik açığı ile karşılaşmış mıdır? Hard disk içinde yapılan virüs taraması sırasında zararlı bir yazılım veya virüs ile karşılaşmış mıdır? Aynı işlem Microsoft Office Outlook'da kayıtlı olan E-postalarla ilgili yapıldığında zararlı bir yazılım veya virüs ile karşılaşmış mıdır?**

## Cevap 5)

İncelenen hard diskte kurulu işletim sistemi son güvenlik güncelleştirmelerine sahip değildir. Bununla ilgili detaylı bilgiler 3.sorunun cevabında verilmiştir.

Hard disk imajında yer alan dosyaların ve e-postaların tümü bilgisayarda mevcut oldukları haliyle çıkarılarak, McAfee AntiVirus Plus ürününün 10.5 versiyonu ile taranmıştır. Bu tarama sonuçlarına göre;

- C diskinde incelenen toplam 282289 adet dosya ve e-postalarda toplam ikiyüzebeş (251) adet virüs, trojan ve exploit tipinde zararlı yazılım bulunduğu tespit edilmiştir. Tespit edilen zararlı yazılımlar ve buldukları dosyalar Ek-19'da listelenmiştir.
- D diskinde incelenen 4413 dosyada virüs tespit edilmemiştir.

## Soru 6

Yapılan güvenlik incelemeleri sonucunda, Seagate Marka "ST3120827AS\_4MS1TF89" Seri Numaralı Hard Disk İmajı içeriğinde kayıtlı olan ve yukarıda isimleri belirtilen dijital verilerin kim tarafından yaratıldığı veya yüklenmiş olabileceği hususunda kesin bir yargıya varmak Adli Bilişim esasları çerçevesinde mümkün müdür?

## Cevap 6)

İncelenen hard disk üzerinde, isimleri birinci soruda belirtilmiş olan dosyaların kim tarafından yaratıldığı veya yüklenmiş olabileceği hususunda kesin bir yargıya varmak mümkün değildir. İncelenen hard disk virüs içermektedir. Ayrıca hard diskteki e-posta mesajlarında trojan adı verilen zararlı yazılımlar mevcuttur ve bunların bilgisayarda çalıştığı tespit edilmiştir. Bu zararlı yazılımların çalıştığı bir sistemde;

- Dosyaların var olup olmadıklarının,
- Silinmiş veya yaratılmış olmalarının,
- Sahiplik bilgilerinin,
- Dosya tarihlerinin değiştirilip değiştirilmediğinin,
- Bunların hangi kaynak tarafından yapıldığının

adli bilişim esasları çerçevesinde kesin olarak belirlenebilmesi ve ispatlanarak söylenebilmesi mümkün değildir.



**Prof. Dr. A. Coşkun Sönmez**

Yıldız Teknik Üniversitesi,  
Bilgisayar Mühendisliği Bölümü



**Arş. Grv. Dr. Göksel Biricik**

Yıldız Teknik Üniversitesi,  
Bilgisayar Mühendisliği Bölümü

Yukarıda imzaları bulunanlar Fakültemizde görevli elemanlardır.



Prof. Dr. Celal KOCATERE  
DEKAN  
Elektrik-Elektronik Fakültesi

## Ekler

Ek-1 Koz.doc dosyasının silindikten sonra bıraktığı alanda mbvd.exe virüsüne ait olan izler.

Ek-2 mbvd.exe virüsünün yapabilecekleri ile ilgili bilgi

Ek-3 Fabrikatör.doc dosyasının silindikten sonra bıraktığı alanda b00ijwpu.exe virüsüne ait olan izler.

Ek-4 b00ijwpu.exe virüsünün yapabilecekleri ile ilgili bilgi

Ek-5 Ulusal Medya.doc dosyasının silindikten sonra bıraktığı alanda mbvd.exe virüsüne ait olan izler.

Ek-6 Tv Analiz Proje.doc dosyasının silindikten sonra bıraktığı alanda mbvd.exe virüsüne ait olan izler.

Ek-7 Reosta Operasyonu.doc dosyasının silindikten sonra bıraktığı alanda 9b9w3.exe virüsüne ait olan izler.

Ek-8 9b9w3.exe virüsünün yapabilecekleri ile ilgili bilgi

Ek-9 "Kadrolaşma Bilgi Notu (Ocxak 2004).doc" dizgesinin disk üzerinde bulunduğu alanda hjvjte.exe virüsüne ait olan izler.

Ek-10 hjvjte.exe virüsünün yapabilecekleri ile ilgili bilgi

Ek-11 toplantı.doc dosyasının silindikten sonra bıraktığı alanda mbdm.exe virüsüne ait olan izler.

Ek-12 mbdm.exe virüsünün yapabilecekleri ile ilgili bilgi

Ek-13 teRTEmiz.doc dosyasının silindikten sonra bıraktığı alanda 9b9w3.exe virüsüne ait olan izler.

Ek-14 Bilinçlendirme.doc dosyasının silindikten sonra bıraktığı alanda b00ijwpu.exe virüsüne ait olan izler.

Ek-15 Sn.Komutanım.doc dosyasının silindikten sonra bıraktığı alanda 9b9w3.exe virüsüne ait olan izler.

Ek-16a, Ek-16b İncelenen bilgisayarda yüklü olan işletim sistemi ve anti virüsle ilgili sistem kayıt defteri bilgileri

Ek-17a, Ek-17b İncelenen bilgisayarda uzaktan yardım bağlantılarına ve uzaktan denetime açık olduğunu gösteren sistem kayıt defteri bilgileri

Ek-18 Microsoft Windows XP Service Pack 3 Kurulumu ile giderilen güvenlik açıkları

Ek-19 İncelenen hard diskteki dosya ve e-postalarda tespit edilen virüs ve trojan tipindeki zararlı yazılımların listesi