

D.

HAKİM - 40026

22.01.2014

MEL

DİJİTAL ADLİ ANALİZ RAPORU

20 OCAK 2014

Hazırlayan

Erdem ALPARSLAN
Burak AKOĞUZ
Osman PAMUK

B

o

✓

İÇİNDEKİLER

1	KONU.....	2
1.1	KAPSAM.....	2
1.2	TALEP EDİLEN ANALİZLER	2
1.3	İNCELENEN DELİLLER.....	2
2	İNCELEME	3
2.1	KULLANILAN ARAÇLAR.....	3
2.2	METODOLOJİ	3
2.3	İNCELEME SONUÇLARI.....	3
2.3.1	ADLİ BİLİŞİM İNCELEME METODOLOJİSİ VE ADLİ BİLİŞİM RAPORLARI	3
2.3.2	5 NUMARALI DİSKE AİT GENEL BİLGİLER	9
2.3.3	İŞLETİM SİSTEMİ.....	12
2.3.4	DOSYA SİSTEMİ	22
2.3.5	MICROSOFT OFFICE PROGRAMI ÖZELLİKLERİ.....	30
2.3.6	ZARARLI YAZILIM İNCELEMELERİ	69
	SONUÇ	72

1 KONU

1.1 Kapsam

T.C. İstanbul 12. Ağır Ceza Mahkemesi'nin 2010/34 sayılı davası kapsamında tarafımıza iletilmiş 5 no'lu sabit diskin dijital adli analiz incelemesi ile daha önce yazılmış bilirkişi raporlarının değerlendirmelerini de içerecek genel kapsamlı bir çalışma gerçekleştirilmiştir.

1.2 Talep Edilen Analizler

Mahkeme dilekçesinde belirtilen ve bir kısım sanıklar ve müdafilerin talep dilekçeleri ve bu dilekçelerine ekledikleri bilirkişi mütalaalarında (rapor) iddia ettikleri hususları içerir bir heyet raporu tanzim edilmesi.

1.3 İncelenen Deliller

Aşağıda özellikleri belirtilen sabit diskin¹ imajı:

- **Marka/Model:** SAMSUNG SP0802N
- **Seri Numarası:** 0637J2FWA19210
- **Firmware Sürümü:** TK100-23
- **Kapasite (in sectors reported Pwr-ON):** 156,368,016 (80.0 GB)
- **Kapasite (in sectors reported by HPA):** 156,368,016 (80.0 GB)
- **Kapasite (in sectors reported by DCO):** 156,368,016 (80.0 GB)
- **HPA kullanımda mı:** Hayır
- **DCO kullanımda mı:** Hayır
- **ATA Şifreleme kullanımda mı:** Hayır
- **Arayüz:** IDE
- **ATA PIO mode:** PIO 4
- **ATA DMA mode:** UDMA 5
- **MD5 hash value:** cb063b2c013a53cab2c8ed2afe091ff0
- **SHA1 hash value:** 3b745642d7c24856adc0ef0dfecf206bf37f91ec

¹ İmaj alma aracı Tableau TD2 loglarından sabit diskle alakalı elde edilen bilgiler

2 İNCELEME

2.1 Kullanılan araçlar

Kullanılan araçlar şu şekildedir:

- **Tableau TD2:** Dijital imaj alma donanımı
- **SIFT 2.14:** Dijital adli analiz programlarını içeren Linux İşletim Sistemi Dağıtımı
- **Encase 7.05.33.33:** Dijital adli analiz programı
- **FTK Imager 3.0.1:** Dijital adli analiz programı
- **TSK (The Sleuth Kit):** "File Systems Forensics" kitabı yazarı Brian Carrier tarafından hazırlanan araçlar
- **Exiftool:** Dosya iç üst verisini elde etmek için kullanılan program

2.2 Metodoloji

Tarafımıza iletilen sabit diskin imajı üzerinde incelemeler yapılmış ve önceden hazırlanmış bilirkişi raporları detaylı olarak değerlendirilmiştir.

Öncelikle literatürde ve kurumsal kaynaklarda konu ile ilgili araştırmalar yapılmıştır. Bununla beraber laboratuvar ortamında farklı konfigürasyondaki sistemler üzerinde normal kullanıcı ve sistem davranışları modellenmiştir. İncelemeler sonunda elde edilen bulgular, modeller üzerinde sınanmıştır.

2.3 İNCELEME SONUÇLARI

2.3.1 ADLİ BİLİŞİM İNCELEME METODOLOJİSİ VE ADLİ BİLİŞİM RAPORLARI

2.3.1.1 Adli Bilişim Nedir

Adli bilişim, son yıllarda önemi gittikçe artan ve bilişim sektöründeki gelişmelere paralel olarak ilerleyen bir bilim dalıdır^{2 3}. Bilişim ile paralel yürüyen fakat kendine has kuralları ve prosedürleri olan bu bilim dalında uzmanlık, bilişim sektörünün diğer alanlarında olduğundan oldukça farklıdır. Disiplinler arası olarak gelişen bu bilim dalı başlarda sadece bilgisayar adli analizini (computer forensics) içerirken, son yıllarda akıllı mobil cihazların artması ve farklı teknolojilerin ortaya çıkması (bulut bilişim gibi) sonucunda birbirinden çok farklı alanları da kapsar olmuştur. Günümüzde mobil cihazlar, mobil işletim sistemleri ve hatta mobil uygulamalar bazında adli bilişimden bahsedilmektedir. Bu gelişmeler, adli bilişim konusundaki uzmanlığın yetkinlik adımlarını arttırmakta ve bir kişinin bütün adli bilişim alanlarında uzman olmasını da zorlaştırmaktadır. Bunun yanında, adli bilişim konusundaki uzman sayısının azlığından dolayı

² Adli Bilişim (Computer Forensic), edirnebarosu.org.tr/incelemeler/adli-bilisim-computer-forensic/

³ Computer Forensics, www.us-cert.gov/sites/default/files/publications/forensics.pdf

her biliřim uzmanının ya da bilgisayar/elektronik mhendisinin adli biliřimden de anlıyor olacađına dair dođru olmayan bir kanaat vardır. Bu alanda uzmanlařmak iin dnya standartlarında eđitim ve sertifikasyon hizmeti veren kuruluřlardan^{4 5 6 7 8} etkinlik sertifikası alınmalıdır. Adli biliřim konusunda uzmanlık iin sertifikalar yanında adli biliřim uzmanının tecrbesi de nemlidir. Adli biliřim konusunda tecrbe seviyesi, adli biliřim incelemeleri ya da adli biliřim konusunda laboratuvar alıřmaları yapıldıka artacaktır.

Ayrıca, adli biliřim yetkin kiřiler tarafından uygun (onaylı ya da adli biliřim sektrnce kabul grmř) programlar/aralar kullanılarak yapılmalıdır. Bu programlar/aralar hem ok pahalıdır, hem de gncel versiyonlarının takip edilmesi iin her sene ayrı lisans creti demek gerekmektedir. Hatta belli programlar iin programı alacak kiři ya da kurumların programı satan řirkete kendilerinin adli biliřim incelemeleri konusunda yetkili olduklarını ispat etme ykmllkleri de olabilmektedir⁹. Tm bu zorluklar řunu gstermektedir; adli biliřim yapacak kiři ya da kurumların kullanılacak aralar ve programlar iin belli bir yatırım yapmaları, ayrıca adli biliřim konusundaki ehliyetlerini de ispatlamaları gerekmektedir.

Adli biliřim programlarının ortak zelliđi, delil btnlđn koruyacak řekilde iřlem yapmalarıdır. Bunun yanında, adli biliřim uzmanları da sreleri dikkatli bir řekilde takip ederek delilin btnlđn bozulmamasını sađlamaya alıřmaladırlar. Ayrıca, NIST¹⁰ gibi kuruluřlar adli analiz programlarını onaylamakta ve bu onay neticesinde hangi adli analiz programlarının/aralarının ne amalarla kullanılabileceđi belirlenmektedir.

Adli biliřim temel olarak 4 ana adımdan oluřmaktadır¹¹:

- Hazırlık
- Toplama
- İnceleme
- Raporlama

⁴ SANS Institute, www.sans.org

⁵ Blackhat, <http://www.blackhat.com>

⁶ Infosec Institute, <http://www.infosecinstitute.com>,

⁷ Digital Intelligence, <http://www.digitalintelligence.com>

⁸ Seven Safe, <http://7safe.com>

⁹ XRY(www.msab.com) cep telefonu inceleme programında bazı zellikler ancak kolluk kuvvetleri tarafından kullanılabilir

¹⁰ NIST(National Institute of Standards and Technology – Amerikan Ulusal Standart Enstits), www.nist.gov

¹¹ Forensic Examination of Digital Evidence:A Guide for Law Enforcement, www.ncjrs.gov/pdffiles1/nij/199408.pdf

2.3.1.2 Adli Bilişim Aşamaları

2.3.1.2.1 Hazırlık

Hazırlık aşaması, yapılacak çalışmanın kapsamının anlaşılması ile başlayıp planlama ile devam etmektedir. Takip edilecek süreçlerin ve kullanılacak araçların belirlenmesi çok önemlidir. Adli bilişim sürecinin ilk adımı olması sebebiyle sonraki adımların düzgün bir şekilde ilerleyebilmesi bu adıma bağlıdır.

2.3.1.2.2 Toplama

Toplama aşamasında genelde kolluk kuvvetleri tarafından bilişim sistemlerinden veri toplanmaktadır. Bilişim sistemleri verileri, veri depolama birimlerinde saklarlar. Saklanan bu verilerin içindeki bilgiler toparlanıp adli bilişim incelemeleri yapacak kişi ya da kişilere verilmektedir.

Genelde veri depolama birimlerinden veri kopyalanırken kaynak veri, yazma korumalı mantıkla okunur ve orijinal veri ile kopyanın birebir aynı olduğu kontrol edilir. Orijinal diskten kopyalama işlemine "imaj alma" denilmektedir. Bu işlem ya özel yazma korumalı aygıtlar¹² yardımıyla bilgisayarda ya da belli cihazlarla¹³ kaynak veri depolama biriminden kopyanın alınacağı veri depolama birimine bilgisayar kullanmadan doğrudan yapılabilir. Kopyalama işleminden sonra da orijinal veri ile kopyalanan verinin birebir aynı olduğu gösterilmelidir. Bunun için orijinal delilin her "bit"¹⁴ inin, kopyalanmış olan veride de aynı olduğunun gösterilmesi gerekmektedir. Bu işlemi hızlandırabilmek ve dokümente edebilmek amacıyla özetleme fonksiyonları (hash fonksiyonları¹⁵) denilen fonksiyonlar kullanılmaktadır. Bu fonksiyonlar tek yönlü fonksiyonlardır ve girdinin (input) tek bir "bit"i bile değişse fonksiyonun çıktısı (output) farklı olmaktadır. Böylece, hem orijinal disk hem de kopyası (imajı) ayrı ayrı bu özetleme fonksiyonlarına girdi olarak verilmekte ve iki fonksiyonun sonucu karşılaştırılmaktadır. Sonuçlar aynı ise kopya ile orijinal aynıdır. Özetleme fonksiyonlarının en çok kullanılanları MD5 ve SHA1 fonksiyonlarıdır.

Delil toplama aşamasında kullanılan özetleme değerleri ilerleyen aşamalarda delil bütünlüğünün sağlanması amacıyla da kullanılmaktadır. Adli bilişimde delil bütünlüğünün sağlanabilmesi için delilin toplama aşamasından inceleme sonuçlanana kadar değişmediğinin gösterilmesi gerekmektedir. Bunun için de inceleme yapanlar, taraflarına iletilen kopyanın (inceleme safhasında yapılacak işlemlerin orijinal delil üzerinde değil, onun bir kopyası

¹² Digital Intelligence Ultrakit, www.digitalintelligence.com/forensicwriteblockers.php

¹³ Tableau Forensic Duplicators, www.tableau.com/index.php?pageid=products&category=duplicators

¹⁴ Bit sadece bir bilgi içeren 1 ya da 0 değerini alabilen birim

¹⁵ Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition, Albert Marcella, Jr., Doug Menendez

üzerinde yapılması mutlaka uyulması gereken bir kuraldır) incelemeye başlamadan özetleme fonksiyonları değerlerini hesaplatıp kopya ile orijinal delilin aynılığını tespit etmelidir.

Özetleme fonksiyonları bütün diskler ve kopyaları üzerinde çalışabildiği gibi tekil dosyalar üzerinde de çalışabilmektedir. Bir dosyanın özetleme fonksiyonuna girdi olarak verilmesi ile fonksiyondan alınan değer bu dosyanın özet değeridir. Bu değer yardımıyla bir dosyanın farklı dosya ya da dosyalar ile karşılaştırması yapılarak bu dosya ile tam olarak aynı olan dosyaların bulunması sağlanmaktadır. Bilinen sistem dosyalarının özet değerleri NIST tarafından yayınlanmakta ve bazı dijital adli analiz araçları¹⁶ da bu listeleri kullanarak bilinen dosyaları atlayarak inceleme yapabilmektedir. Bir dosyanın özetleme değeri ile dosya içeriği birebir ilintilidir. Birden çok dosyanın özetleme fonksiyonu değeri aynı ise dosyaların içeriği birbirinin tamamıyla aynısıdır. Bu tür özet değeri aynı dosyalar için dosya iç üst verileri (ileriki bölümlerde değinilecek) ve dosya içeriğinin farklı olmasının imkânı yoktur.

2.3.1.2.3 İnceleme

Adli bilişimde inceleme aşaması, diğer tüm aşamalardan daha önemli olan ve en fazla zamanın ayrıldığı kısımdır. İncelemeler ne tip bir bilişim sistemi ile uğraşıldığına, konunun ne olduğuna, istenilen incelemenin kapsamına göre değişiklik göstermektedir. İnceleme aşamasına gelindiğinde hazırlık safhasında yapılan plan çerçevesinde hareket edilip gerekli araçlar yardımıyla incelemeler gerçekleştirilmelidir. İncelemeler genelde bilişim sistemi içindeki veri depolama aygıtlarının incelemeleri, varsa bilişim sistemi üzerinde çalışan işletim sisteminin incelenmesi, veri depolama kabiliyetine göre dosya sistemi incelemeleri ve dosyaların içerikleri, dosya iç üst veri incelemelerini içermektedir. Bunun yanında canlı sistem incelemelerinde bilişim sisteminin bağlı olduğu ağ (network) ile haberleşmesi, çalışan işlemlerin neler olduğu ve bu işlemlerde neler yapıldığı, çalışan programların zararlı yazılım ihtiva edip etmediği gibi çok farklı analizler de yapılmaktadır.

Bir dijital verinin belli bilgisayar kullanıcısına aidiyeti konusunda; ilgili dijital verinin bilgisayarda oluşturduğu çeşitli izler, üst veriler, ilgili dijital veriyi çalıştıran bilgisayar programında oluşan kayıt verileri ve bu programın bilgisayarda yüklü olan diğer program ve uygulamalarla olan ilişkisine dair kayıt verileri analiz edilerek yorum yapılır. Ayrıca bazı doküman tiplerindeki bağlantılar (hyperlinks), dosya kaydedilme yollarındaki (path) dizinler ya da ağ adresleri, ağdaki yazıcı izleri gibi veriler de dosyaların kime ait olduğunun belirlenmesinde yardımcı faktörlerdendir. Buradan hareketle, dijital verilerin sahiplik bilgilerinin incelenmesinin çok farklı yollarının olduğu, incelenecek dijital veriye göre çeşitli yaklaşımlar ve farklı analiz tekniklerinin mümkün olduğu söylenebilir.

¹⁶ Encase, FTK NIST özetleme fonksiyonu veri tabanlarını kullanabilmektedir

Adli bilişim incelemelerinde kullanılan veri, genelde bilişim sistemlerinde depolanmış halde duran veri olmaktadır. Depolanmış veriler uçucu ve kalıcı veriler olarak iki sınıfta ele alınmaktadır. Çalışmakta olan (canlı) sistemlerde elektrik oldukça saklanan fakat elektrik olmadığı durumda kaybolan veriye uçucu (volatile) veri denilmektedir¹⁷. Uçucu veriye en güzel örnek bilişim sistemlerinde RAM (Random Access Memory – Rastgele Erişimli Hafıza) olarak adlandırılan birimde tutulan veridir. Elektriğe bağlı olmadan saklanan ve elektrik gitse de kaybolmayan veriye ise kalıcı (non-volatile) veri denilmektedir. Buna örnek olarak manyetik çalışma prensipli sabit diskler, dijital kartlar (SD, MicroSD, CF vb.), flash bellekler veya CD/DVD gibi optik veri depolama birimleri verilebilir.

2.3.1.2.4 Raporlama

Adli bilişim incelemelerinin sonuçlarının özetlendiği raporlarda, kavramların tanımlarının net bir şekilde yapılmış olması gerekmektedir. Raporlarda anlatılanların, olayın teknik kısmına vakıf kişiler tarafından okunduğunda kavram karmaşasına meydan vermeyecek şekilde anlaşılabilir olması gerekmektedir.

Ayrıca adli bilişim incelemeleri ve raporlarında önemli olan bir diğer kısım, teknik incelemelerin hangi araçlar ve metotlar kullanılarak yapıldığının açık bir şekilde anlatılmasıdır. İncelemelerin yapıldığı delil üzerinde farklı uzmanlar tarafından aynı araçlar kullanılıp, aynı prosedürler takip edildiğinde aynı sonuçlara ulaşılabilir olması gerekmektedir. İnceleme sonuçlarının neye dayanarak tespit edildiğinin söylenememesi, bulgunun başka bir uzman tarafından doğrulanmasını imkânsız hale getirebilir.

2.3.1.3 Adli Bilişimde Dijital Delil

Hayatımızın her alanında kullandığımız birçok dijital elektronik cihaz, bilgi çağı olgusu paralelinde gelişen bilişim sektörünün bir ürünüdür. Mobil cihazlardan akıllı arabalara, akıllı evlerden bilgisayarlara, akıllı televizyonlardan m2m (machine-to-machine, makineden makineye) cihazlarına kadar bilgi üreten, işleyen, transfer eden, saklayan ve yok eden sistemler ile iç içe bir yaşam sürülmektedir. Bu sistemlerde, belki ilk başta adli bilişim düşünülmeden tasarlanmış olmalarına rağmen, adli bilişim incelemelerinde kullanılabilen çok değerli bilgiler bulunmaktadır. Bu bilgiler dosya sistemi üst verileri, işletim sistemi izleri, dosya iç üst verileri, uygulama logları, uygulama ayar dosyaları ve uygulama veri tabanları gibi farklı bilgi kaynaklarından elde edilmektedir. Bu bilgiler sistemlerin doğru ve istenildiği gibi çalışabilmesi için çok önemlidir.

¹⁷ Computer System Architecture, 3rd Edition, M. Morris Mano

Ayrı bir bilim dalı olan adli bilişim dijital deliller üzerinde inceleme yapar^{18 19 20}. Bilişim sistemleri çalışmaları esnasında çok farklı tipte dijital verileri işlemektedir. Dijital deliller bilişim sistemlerinde dijital olarak saklanan ya da işlenen verilerden elde edilmektedir. Dijital deliller dava ve soruşturmalarda destekleyici delil olarak kabul görmektedir^{21 22}. 5271 sayılı Ceza Muhakemeleri Kanunu 134. maddede belirtildiği gibi hâkim kararına bağlı olarak bilişim sistemlerine el koyulmakta ve içlerindeki verilerden dijital deliller elde edilmektedir. Dijital veriler tüm dünyada delil olarak kabul edilmektedir^{23 24 25 26}.

¹⁸ Digital Evidence, www.nist.gov/oles/forensics/digital_evidence.cfm

¹⁹ Digital Evidence, www.ncfs.org/digital_evd.html

²⁰ Digital Evidence By Stuart Cameron, www.fbi.gov/stats-services/publications/law-enforcement-bulletin/august-2011/digital-evidence

²¹ Online Social Networks As Supporting Evidence: A Digital Forensic Investigation Model and Its Application Design, Norulzahrah Mohd Zainudin, Madjid Merabti, David Llewellyn-Jones

²² Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Eoghan Casey

²³ Using Log Record Analysis to Show Internet and Computer Activity in Criminal Cases, Mark L. Krotoski, Jason Passwaters, 2011

²⁴ Using Historical Cell Site Analysis Evidence in Criminal Trials, Thomas A. O'Malley, 2011

²⁵ Compelling Online Providers to Produce Evidence Under ECPA, Josh Goldfoot, 2011

²⁶ Admissibility of Forensic Cell Phone Evidence, Timothy M. O'Shea, James Darnell, 2011

2.3.2 5 NUMARALI DİSKE AİT GENEL BİLGİLER

2.3.2.1 Sabit diskin fiziksel bilgileri

Tarafımıza iletilip incelenmesi istenen sabit disk imajından (dava dilekçelerinde 5 numaralı sabit disk olarak adlandırılan diskin imajı) tespit edilen özellikler şunlardır²⁷:

- **Marka/Model:** SAMSUNG SP0802N
- **Seri Numarası:** 0637J2FWA19210
- **Firmware Sürümü:** TK100-23
- **Kapasite (in sectors reported Pwr-ON):** 156,368,016 (80.0 GB)
- **Kapasite (in sectors reported by HPA):** 156,368,016 (80.0 GB)
- **Kapasite (in sectors reported by DCO):** 156,368,016 (80.0 GB)
- **HPA kullanımda mı:** Hayır
- **DCO kullanımda mı:** Hayır
- **ATA Şifreleme kullanımda mı:** Hayır
- **Arayüz:** IDE
- **ATA PIO mode:** PIO 4
- **ATA DMA mode:** UDMA 5
- **MD5 hash value:** cb063b2c013a53cab2c8ed2afe091ff0
- **SHA1 hash value:** 3b745642d7c24856adc0ef0dfecf206bf37f91ec
- **Sector size:** 512 byte

Sabit diskin seri numarasından üretim tarihi tespit edilmeye çalışılmıştır. Samsung marka disk için Samsung şirketinden ve internet sitesinden direk olarak üretim tarihi bulunamamıştır. Seagate şirketinin internet sitesinde bulunan Samsung disklerle ilgili bir bilgi notuna bakılarak bu disk için tespit edilen üretim tarihi 2003 yılı Ekim ayıdır²⁸.

2.3.2.2 Sabit disk bölüm tablosu

İncelenen sabit disk imajında iki bölüm (partition) bulunmaktadır. Bölüm tablosundan elde edilen bilgiler şunlardır²⁹:

²⁷ İmajı alan Tableau TD2 Cihazının logları

²⁸ Interpreting Samsung Hard Drive Serial Numbers,

http://knowledge.seagate.com/articles/en_US/FAQ/221439en (Seagate firması Samsung sabit disk birimini 2011 yılında satın almıştır.)

²⁹ The Sleuth Kit (TSK) kullanılarak

DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

Slot	Start	End	Length	Description
00: Meta	0000000000	0000000000	0000000001	Primary Table (#0)
01: ----	0000000000	0000000062	0000000063	Unallocated
02: 00:00	0000000063	0041945714	0041945652	NTFS (0x07)
03: 00:01	0041945715	0156360644	0114414930	NTFS (0x07)
04: ----	0156360645	0156368015	0000007371	Unallocated

Bölüm tablosundan (partition table) anlaşılan, disk üzerinde iki bölüm olduğu, bunların NTFS dosya sistemiyle formatlandığı, başlangıç sektörlerinin ilk bölüm için "63" ve ikinci bölüm için "41945715" olduğu ve bölümlerin uzunluklarının sektör sayısı olarak ilk bölüm için "41945652" ($41945652 \times 512 \text{ byte/sektör} = 21476173824 \text{ byte}$, yaklaşık olarak 20 GB), ikinci bölüm için "114414930" ($114414930 \times 512 \text{ byte/sektör} = 58580444160 \text{ byte}$, yaklaşık olarak 54 GB) dır.

2.3.2.3 Sabit disk dosya sistemleri

İncelenen sabit diskteki iki adet bölümde dosya sistemi olarak NTFS bulunmaktadır. NTFS dosya sistemi ile ilgili detaylı bilgi ilerleyen bölümlerde verilecektir.

Kapasitesi 80 GB olan bu sabit diskte iki ayrı bölüm olduğu (İşletim sistemi tarafından C: ve D: olarak adlandırılan) tespit edilmiştir.

İlk bölüm özellikleri:

- **Bölüm İsmi:** SİSTEM
- **Bölüm kapasitesi:** 20481 MB (yaklaşık 20 GB)
- **Sistem Diski:** Evet (Windows XP yüklü)
- **Dosya Sistemi:** NTFS
- **Dosya/Dizin Sayısı:** 22733
- **Boş Alan:** 15,9 GB

İkinci bölüm özellikleri:

- **Bölüm İsmi:** DATA
- **Bölüm kapasitesi:** 55866 MB (yaklaşık 54 GB)
- **Sistem Diski:** Hayır (İşletim sistemi yüklü değil)
- **Dosya Sistemi:** NTFS
- **Dosya/Dizin sayısı:** 4374
- **Boş Alan:** 52,1 GB

Detaylı dosya sistemi bilgileri için EK-4'e bakınız.

İncelenen 5 numaralı sabit diskteki iki bölümün formatlanma tarihleri için:

Bir disk NTFS ile formatlandığında **ilk oluşturulan dosya \$MFT** dosyasıdır. Disk içindeki iki bölümde de, \$MFT dosyasının oluşturulma tarihi 01.01.2001'i göstermektedir. Bu tarih disk formatlandığı sırada sistem saatinin tarihini göstermektedir veya disk direk formatlanmadan üzerine hazır bir disk imajından (bölüm tablosu, dosya sistemleri) kopyalanmıştır.

2.3.3 İŞLETİM SİSTEMİ

İncelenmek üzere tarafımıza iletilen sabit diskin ilk bölümünde Microsoft Windows XP işletim sistemi kurulu olduğu görülmüştür. Microsoft şirketi tarafından geliştirilen ve satılan Windows XP işletim sisteminin sabit diskin ilk bölümü (SİSTEM isimli) üzerinde kurulu bulunmaktadır. Sabit diskin diğer bölümünde (DATA isimli) işletim sistemi bulunmamaktadır. Windows XP işletim sistemi ilk defa bilgisayar üreticilerine 24.08.2001 tarihinde sunulmuştur³⁰. XP kısaltması eXPerience (deneyim) anlamına gelmektedir. 09.09.2002 tarihinde ilk servis paketi, 06.08.2004 tarihinde ise ikinci servis paketi yayınlanmıştır³¹.

Microsoft şirketi geliştirdiği işletim sistemlerine zamanla ortaya çıkan problemleri çözmek ya da güvenlik açıklarını kapatmak amacıyla yamalar yayınlamaktadır. Bu yamalar belli bir zaman sonra işletim sistemine entegre edilmekte ve aynı işletim sisteminin minör versiyonları şeklinde ilerlemektedir. Bu güncellemeleri alamayan bilgisayarlar için belli bir miktar güncelleme içinde olduğu servis paketleri yayınlanmaktadır. İncelenen sabit diskin ilk bölümünde kurulu olan Windows XP işletim sistemi bu servis paketlerinin ikincisine (Service Pack 2) sahiptir.

İncelenen 5 numaralı sabit diskin birinci bölümü (C: SİSTEM isimli) üzerinde kurulu olan işletim sistemi bilgileri şunlardır³²:

- **Ürün İsmi:** Microsoft Windows XP
- **Servis Paketi:** Service Pack 2
- **Ürün Kimlik Numarası:** 55896-642-7769785-23156
- **Güncel Versiyon:** 5.1
- **Güncel Derleme Versiyonu:** 2600
- **Derleme Versiyonu Detayı:** 2600.xpsp_sp2_rtm.040803-2158
- **Sistem Dizini:** C:\WINDOWS
- **Kurulum Zamanı:** 9 Nisan 2008, 11:50:40 (UTC)
- **Kayıt Eden Kurum:** DNK
- **Kayıt Eden Sahip:** DNK
- **Bilgisayar Adı:** IKK
- **TCP/IP Hostname:** ikk

Görüldüğü üzere incelenen sabit diske en son işletim sisteminin 9 Nisan 2008 tarihinde kurulduğu anlaşılmaktadır³³.

Bölüm 2.3.2.1'de belirtildiği gibi incelemeye konu olan sabit diskin üretim tarihi kesin olmamakla birlikte 2003 yılının Ekim ayı olduğu değerlendirilmektedir. Disk üzerinde görülen ilk dosyanın oluşturulma tarihi 01.01.2001 ve işletim sisteminin kurulma tarihi 09.04.2008

³⁰ Windows XP to Take the PC to New Heights, 2001, www.microsoft.com/en-us/news/press/2001/aug01/08-24winxp2mtr.aspx

³¹ Microsoft Releases Windows XP Service Pack 2 with Advanced Security Technologies to Computer Manufacturers, 2004, www.microsoft.com/en-us/news/press/2004/aug04/08-06winxpsp2launchpr.aspx

³² HKLM\Software\Microsoft\Windows NT\CurrentVersion "registry" anahtarı, forum.sysinternals.com/exact-windows-version-in-registry-key_topic1902.html

³³ Bu bilgi "C:\WINDOWS\setuplog.txt" dosyasından da doğrulanmıştır

olarak görülmüştür. Bu bilgiler ışığında diske imaj kopyalanmadıysa sistem saati 01.01.2001 olan bir bilgisayarda biçimlendirildiği, ardından Windows XP işletim sisteminin kurulması esnasında kullanıcıya sorulan tarih ve saatin kurulumu yapan kullanıcı tarafından düzenlendiği anlaşılmaktadır. Tarihin düzenlenmediği kurulumlarda işletim sisteminin o sırada sahip olduğu tarih ve saat değerlerini aldığı görülmektedir (Bölüm 2.3.3.6 laboratuvar testi MSWin-3 ve MSWin-4).

Ayrıca kurulum sırasında yapılanların kayıt altına alındığı "C:\windows\setuplog.txt" dosyasındaki bilgilere göre bilgisayarın sistem saati "ağ kurulumu başlangıcında otomatik olarak güncellenmeye ayarlı olduğunu" değil, işletim sistemi kurulumu sırasında kullanıcı tarafından belirlendiğini göstermektedir. Üzerinde Microsoft Windows XP işletim sistemi çalışan bir bilgisayarda çeşitli olayların kayıtları "Event Log" denilen dosyalarda tutulmaktadır³⁴. Ön tanımlı olarak belli tip olayların kayıtları tutulurken kullanıcı tarafından kaydı tutulan olayların neler olacağı da belirlenebilmektedir. Genelde bu kayıt dosyaları ile alakalı politikalar kullanıcılar tarafından değiştirilmemektedir. Bu kayıt dosyalarında oluşan kayıtlara bakarak sistem hakkında bazı bilgilere sahip olmak mümkündür. Diğer birçok olay yanında sistemdeki saat değişiklikleri de ön tanımlı olarak bu kayıt dosyalarında görülmektedir. Yapılan incelemede diskin ilk bölümünde bulunan işletim sisteminin sistem saatinin değiştirilmediği ve internet üzerinden de güncellenmediği tespit edilmiştir³⁵.

Windows işletim sistemleri dosya/dizin isimlendirmede uzun isimleri kabul etmekle birlikte önceki işletim sistemi versiyonlarına uyum için kısa isimlendirmeleri (short file name) de kabul etmektedir. Windows işletim sisteminin ilk versiyonlarında uzun dosya ya da dizin isimleri desteklenmemekte, dosyalar için 8-3 ve dizinler için de 8 karakter kuralı uygulanmaktaydı^{36 37}. Dosya isimlendirmede 8 karakter dosyanın ismine, 3 karakter de dosyanın uzantısına ayrılmaktaydı. Sonradan bu sınırlandırmalar genişletilerek dosya ve dizin isimleri daha çok karaktere (dosya ismi için 255 karakter³⁹) destek vermeye başlandı. Kullanıcılar tarafından eski Microsoft Windows işletim sistemlerinde komut satırından "dir" (dosya/dizin listeleme komutu) çalıştırıldığında komut çıktısındaki dosya ve dizin isimleri, uzun olanlarının ilk altı harfinden sonra "~" işareti ile devam etmekte ve bu işareten sonra birden başlamak üzere numara almaktadır. Microsoft Windows işletim sistemleri eskiye uyum (backward compatibility) için dosya ve dizin isimlendirmelerinde 8-3 kuralını (short file name) desteklemektedir. Sonuçta,

³⁴ C:\WINDOWS\system32\config dizininde bulunan "evt" uzantılı dosyalar

³⁵ İnternet üzerinden zaman güncellemelerinin başarısız olduğu System.evt dosyasındaki geçen şu hata mesajlarından anlaşılmaktadır: W32Time/17;Error;time.windows.com,0x1,Bir yuva işlemi erişilemeyen bir ana makine için denendi. (0x80072751)

³⁶ How Windows Generates 8.3 File Names from Long File Names, support.microsoft.com/kb/142982

³⁷ Naming Files, Paths, and Namespaces, msdn.microsoft.com/en-us/library/aa365247.aspx

³⁸ 8.3 filename, www.princeton.edu/~achaney/tmve/wiki100k/docs/8.3_filename.html

³⁹ How Windows Generates 8.3 File Names From Long File Names, https://support.microsoft.com/kb/142982

bir Windows işletim sisteminde içinde “~” işareti olan bir “yol” (path) bilgisi görmek normal bir durumdur.

2.3.3.1 Sabit diskte bulunan işletim sistemindeki kullanıcılar

5 numaralı diskin ilk bölümünde (SİSTEM isimli) kurulu bulunan işletim sisteminde mevcut kullanıcılar şunlardır:

- Administrator
- Guest
- HelpAssistant
- SUPPORT_388945a0
- İkk
- Kemal

Kullanıcıların detayları EK-3’de bulunmaktadır.

2.3.3.2 Sabit diskte bulunan işletim sistemindeki kurulmuş olan programlar

5 numaralı sabit diskin ilk bölümünde (SİSTEM isimli) bulunan işletim sisteminde kurulu olduğu belirlenen programlar şunlardır:

- McAfee VirusScan Enterprise v.8.6.0
- Microsoft Office 2000 Professional v.9.00.2720
- MPlayer2
- WebFldrs XP v.9.50.7523
- Adobe Acrobat 7.0 Professional v.7.0.0
- WinZip v. 10.0 (7245)
- WinRAR arşiv yöneticisi
- Intel(R) PRO Network Adapters and Drivers
- Intel(R) Extreme Graphics Driver
- SoundMAX

Kurulu programların detayları EK-3’de bulunmaktadır.

2.3.3.3 Sabit diskin ilk bölümü üzerinde (SİSTEM isimli) bulunan işletim sisteminin ağ ayarları

İncelenen Microsoft Windows XP işletim sisteminin ağ ayarları şu şekildedir⁴⁰:

- Adapter: {8C8A8213-EF5C-4784-98FE-F41CEEFC7CEE}
 EnableDHCP: 0
 IPAddress: 10.5.1.2
 SubnetMask: 255.255.255.0
 DefaultGateway: <BOŞ>

⁴⁰ “HKLM\ControlSet001\Services\{8C8A8213-EF5C-4784-98FE-F41CEEFC7CEE}\Parameters\Tcpip

DhcpIPAddress: 0.0.0.0
DhcpSubnetMask: 255.0.0.0
DhcpServer: 255.255.255.255

İşletim sisteminde bu bilgilerin bulunduğu ağ adaptörünün kayıt defteri (registry) anahtarı ayarlarındaki en son değişiklik 01.05.2008 15:19:37 tarihinde yapılmıştır⁴¹. Yani 01.05.2008 15:19:37 tarihinden sonra bağlantı ayarlarında değişiklik yapılmamıştır. Bu ayarlara göre sistemin kullandığı IP adresi 10.5.1.2'dir ve herhangi bir ağ geçidi adresi (DefaultGateway) veya DNS adresi tanımlanmamıştır. Ağ geçidi adresinin ayarlanmadığı bir sistemin kendi yerel ağı dışındaki bir ağdan veri alması veya kendi yerel ağı dışındaki bir ağa veri göndermesi mümkün değildir.

Bir işletim sistemi internete bağlandığında üzerinde birçok iz oluşmakta ve incelemeler sonucunda tespit edilebilmektedir. Fakat incelemeye konu olan sabit diskte bulunan işletim sisteminin kurulum tarihi olarak değerlendirilen 09.04.2008 tarihinden sonrasına ait herhangi bir internet bağlantı izine rastlanmamıştır.

Bu bulgular doğrultusunda, ilgili sabit diskte kurulu olan işletim sisteminin **internete hiç bağlanmadığı** değerlendirilmektedir.

2.3.3.4 Sabit diskin ilk bölümünde bulunan işletim sisteminde çalıştırılan programların izleri

İşletim sistemleri ve bu işletim sistemi üzerinde çalışan programlar çeşitli izler bırakabilmektedir. Microsoft Windows XP işletim sisteminde, çalışan uygulamalar ile ilgili birden fazla yerde izler kalmaktadır. Çeşitli izlere bakılarak tespit edilen çalıştırılmış programların listesi EK-3'de bulunmaktadır.

2.3.3.5 Sabit diskin ilk bölümünde bulunan işletim sisteminde açılan dokümanların izleri

Bir veri depolama aygıtında bulunan dokümanlar görüntülenirken ya da üzerlerinde değişiklik yapılırken işletim sisteminde ve sabit diskin üzerinde çeşitli izler bırakabilmektedir. İncelemeye konu olan 5 numaralı sabit diskin ilk bölümünde çalışan Microsoft Windows XP işletim sistemi üzerinde bu tip izler bulunmaktadır. Bunun yanında, bir sabit disk başka bir bilgisayara ister sabit disk olarak doğrudan ya da çeşitli aparatlar yardımıyla ekstra disk olarak takılabilir. Ekstra disk üzerindeki dokümanların açılmasıyla oluşan izler diskin o sırada takılı olduğu bilgisayarın işletim sistemi diskinde oluşmaktadır. Bu bağlamda, disk üzerinde bulunan işletim sisteminde bir dokümanın açıldığına dair iz bulunmaması o dokümanın hiç açılmadığını göstermez. Bu,

⁴¹ HKLM\ControlSet001\Services\{8C8A8213-EF5C-4784-98FE-F41CEEFC7CEE}\Parameters\Tcpip

B

Q

⚡

disk üzerindeki işletim sisteminin aktif olarak çalıştığı durumda o dokümanın açılmadığını gösterir.

İncelemeye konu olan 5 numaralı sabit diskte görüntülenmiş ofis dokümanlarına ait izler EK-3 de verilmiştir.

2.3.3.6 Laboratuvar Bulguları

Bu kısımda işletim sisteminin belli durumlarda nasıl davrandığına dair yapılmış laboratuvar sonuçları verilecektir.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSWin-1
Testin Üzerinde Koştuğu Sistem	Asus p4r800v Model Masaüstü PC (BIOS Phoenix Award BIOS v6.00PG)
İncelemeye Konu Olan Üstveri Alanları	Bilgisayar tarihi
Ön Koşullar	BIOS ayarlarını tutan pilin yeterince enerjiye sahip olmaması
Uygulama Adımları	➤ İşletim sistemi açıldıktan sonra saat tarih güncellendi ➤ Bilgisayar kapatıp açıldı ➤ Bilgisayarın saatinin aldığı değer tespit edildi
Bulgular	➤ İşletim sistemi ilk açıldığında 01.01.2003 tarihi gözlemlendi ➤ Tarih güncellenip kapatıp açıldıktan sonra tarihin 01.01.2003 olduğu gözlemlendi

LABORATUVAR BULGUSU	
Uygulama Kodu	MSWin-2
Testin Üzerinde Koştuğu Sistem	Farklı marka ve modelde bilgisayarlar (asus p5b, gigabyte ga8lg1000-g, hp 6000, hp 7900)
İncelemeye Konu Olan Üstveri Alanları	Bilgisayar tarihi
Ön Koşullar	BIOS ayarlarını tutan pilin arızalı olması ya da yeterince enerjiye sahip olmaması
Uygulama Adımları	➤ BIOS ayarlarını tutan pil anakarttan çıkarılır ➤ Bilgisayar yeniden başlatılarak bilgisayarın saatinin aldığı değer tespit edilir
Bulgular	➤ Bilgisayar saatinin marka ve modele (anakart ve BIOS sürüm modellerine göre) farklı zamanları gösterdiği tespit edilmiştir. ➤ Bu zaman bilgileri: ▪ 04.01.2009 (HP DC7900 Ultra Slim, PXE 2.1 Build 086) ▪ 01.01.2002 (ASUS P5B, American Megatrends v02.58) ▪ 01.01.2004 (GIGABYTE GA8IG1000G, Award BIOS v6.00PG) ▪ 26.02.2080 (HP Compaq 6000 Pro, HP Invent v1.09)

Bu bulgularla alakalı çeşitli kaynaklarda da bilgiler bulunmaktadır^{42 43}.

⁴² A damaged or insufficiently charged internal battery can corrupt CMOS or BIOS settings, support.microsoft.com/kb/308029

⁴³ What is the average lifespan of a cmos battery, answers.microsoft.com/en-us/windows/forum/windows_vista-system/what-is-the-average-lifespan-of-a-cmos-battery/e69e94cf-2f74-463a-bc54-f7b0fbcce5d1

LABORATUVAR BULGUSU	
Uygulama Kodu	MSWin-3
Testin Üzerinde Koştuğu Sistem	Asus Marka Masaüstü PC (Asus p4r800v, Phoenix Award BIOS v6.00PG)
İncelemeye Konu Olan Üstveri Alanları	Bilgisayar tarihi \$MFT dosyasının tarihi
Ön Koşullar	Bilgisayarın saatinin fabrika ayarlarında olması (Normale göre eski zaman bilgisine sahip olması – 13.2.1999)
Uygulama Adımları	➤ BIOS tarihi eski bir zamana ayarlanır (13.2.1999) ➤ Bilgisayara takılan boş bir diske Windows XP işletim sistemi kurulur ➤ Tarih ve saat manuel olarak değiştirilmeden kuruluma devam edilir ➤ Bilgisayar açıldıktan sonra tarih ve saati kontrol edilir
Bulgular	➤ Bilgisayarın tarih ve saatinin Windows XP kurulumu sonrasında değişmediği, BIOS daki ilk değerini muhafaza ettiği tespit edilmiştir ➤ \$MFT dosyasının oluşturulma tarihinin yine BIOS daki tarihe uyumlu olduğu görülmüştür

LABORATUVAR BULGUSU	
Uygulama Kodu	MSWin-4
Testin Üzerinde Koştuğu Sistem	Asus Marka Masaüstü PC (Asus p4r800v, Phoenix Award BIOS v6.00PG)
İncelemeye Konu Olan Üstveri Alanları	Bilgisayar tarihi
Ön Koşullar	Bilgisayarın tarihinin fabrika ayarlarında olması (Normale göre eski zaman bilgisine sahip olması – 15.8.2009)
Uygulama Adımları	➤ BIOS tarihi eski bir zamana ayarlanır (15.8.2009) ➤ Bilgisayara takılan boş bir diske Windows XP işletim sistemi kurulur ➤ Tarih ve saat manuel olarak değiştirilmeden kurulumu devam edilir ➤ Bilgisayar açıldıktan sonra tarih ve saati kontrol edilir
Bulgular	➤ Bilgisayarın tarihinin Windows XP kurulumu sonrasında değişmediği (15.8.2009 olarak kaldığı), BIOS daki ilk değerini muhafaza ettiği tespit edilmiştir. ➤ \$MFT dosyasının oluşturulma tarihinin yine BIOS daki tarihe uyumlu olduğu görülmüştür.

2.3.3.7 Bulgulara Dayalı Değerlendirmeler

Bilgisayarda kullanılan işletim sistemleri zaman ayarlarını BIOS'tan almaktadır. Bu zaman bilgisi, daha sonra gerçekleştirilen bütün işlemlerdeki zaman kayıt bilgisini belirlemektedir. Yukarıdaki laboratuvar çalışmalarında görüldüğü gibi bilgisayarların sistem saatleri güncel olmayabilmektedir. Bölüm 2.3.4.2 de açıklandığı üzere bazı dosyaların 28.07.2009 tarihinden sonra, sistem saati daha eski olan bilgisayarlardan aktarıldığı değerlendirilmektedir. Bu bilgiler ışığında, kullanıcının dosya alışverişi yaptığı bilgisayarlar arasında, yukarıdaki laboratuvar çalışmalarında gösterildiği gibi sistem saatleri güncel olmayan bilgisayarların olma ihtimali vardır.

2.3.4.2 bölümünde açıklandığı üzere "yasemin.ppt" dosyasının oluşturulduğu tarih, içeriğindeki verinin tarihinden öncedir. Bu durum, bu dosyanın sistem saati güncel olmayan bir bilgisayarda oluşturulmuş olduğunu göstermektedir. Ayrıca bu dosyanın 28.07.2009 tarihinden önce sabit

diske aktarılmış olması, kullanıcının dosya alışverişı yaptığı bilgisayarlar arasında sistem saati güncel olmayan bilgisayarların olma ihtimalini kuvvetlendirmektedir.

2.3.4 DOSYA SİSTEMİ

Bütün veri depolama birimleri içlerinde barındırdıkları veriyi organize edebilmek için dosya sistemlerine ihtiyaç duymaktadırlar. Dosya sistemleri bir kütüphanedeki kitap tasnif sistemi gibi çeşitli tipte ve içerikte dosyaların kullanıcı tarafından farklı farklı gruplandırılıp farklı dizinlerde tutulabilmesine olanak sağlamaktadır. Ayrıca, işletim sistemleri de bu dosya sistemlerini kullanarak gerekli ayarlarını saklamaktadır. Dosya sistemleri, birtakım ortak özelliklere sahip olsalar da her birinin farklı özellikleri vardır.

Bir dosya ile alakalı temelde iki grup üst veri tutulmaktadır:

- Dosya sistemi üst verisi
- Dosya iç üst verisi

Dosya sistemi üst verisi, bir dosyanın bir dosya sistemi içinde iken o dosya sistemi ile ilgili üst verileridir. Bu üst verilerin dosyanın bir dosya sisteminden diğerine aktarılırken korunması her durumda söz konusu değildir. Bu üst verilere örnek verilecek olursa; dosyanın ismi, büyüklüğü, sahibi, zaman bilgileri, dosyaya erişim hakları gibi bilgiler bu kategoridendir.

Dosya iç üst verisi ise dosyanın içinde bulunan ve farklı dosya tiplerinde farklı alanları olan veridir. Dosya iç üst verileri, dosya bir dosya sisteminden diğerine aktarılırken dosya ile birlikte hareket etmektedir. Farklı dosya tiplerinde farklı dosya iç üst verileri tutulmaktadır. Bu yüzden bir resim dosyasının dosya iç üst veri alanları ile bir doküman dosyasının dosya iç üst veri alanları birbirinden farklı olmaktadır. Bir resim dosyası için resmi çeken fotoğraf makinesinin markası, modeli, seri numarası, diyafram genişliği, çekim sırasında flaş kullanılıp kullanılmadığı, çekim anındaki GPS koordinatları vb. bilgiler saklanırken, bir doküman dosyasında dosyanın yazarı, son kaydedeni, ilk oluşturulma zamanı, son kaydedilme zamanı, son olarak çıktı alınma zamanı gibi bilgiler tutulmaktadır.

İncelenmek üzere tarafımıza iletilen diskte iki ayrı bölüm (partition) bulunduğu ve bu iki bölümün de NTFS (New Technology File System) ile formatlandığı tespit edilmiştir.

2.3.4.1 Sabit diskteki dosya sistemi (NTFS)

NTFS (New Technology File System – Yeni Teknoloji Dosya Sistemi) dosya sistemi Microsoft şirketi tarafından geliştirilmiş, Windows NT 3.1' den itibaren Microsoft Windows işletim sistemlerinde kullanılmaya başlanmıştır⁴⁴. NTFS dosya sistemi, kritik bilgilerini bir takım sistem

⁴⁴ A File System for the 21st Century: Previewing the Windows NT 5.0 File System, www.microsoft.com/msj/1198/ntfs/ntfs.aspx

dosyalarında tutmaktadır⁴⁵. Bu dosyaların isimleri "\$" karakteri ile başlamakta ve işletim sistemi tarafından korunmaktadır. Bu dosyalardan bazıları:

Sistem Dosyası	Dosya İsmi	MFT Kayıt Numarası	Dosyanın Kullanım Amacı
Master file table	\$MFT	0	Ana dosya tablosudur. Her bir dosya ve dizin için en az bir kayıt barındırmaktadır.
Master file table mirror	\$MFTMirr	1	\$MFT dosyasındaki ilk dört kaydın yedeğidir. \$MFT dosyasının ilk kayıtlarının bulunduğu sektörde bozulma durumunda bu yedekten geri dönme imkânı sağlar.
Log file	\$LogFile	2	Dosya sistemindeki işlemlerin kaydedildiği sistem dosyasıdır.
Volume	\$Volume	3	Bölüm bilgilerini (bölüm ismi ve bölüm versiyonu gibi) tutar.
Attribute definitions	\$AttrDef	4	"Attribute" isimlerini, numaralarını ve tanımlarını listeler.
Root file name index	.	5	Kök dizindir.
Cluster bitmap	\$Bitmap	6	Dosya sistemindeki "cluster" ların boş ya da dolu olduğu bilgisini tutar.
Boot sector	\$Boot	7	Boot edilebilir bölümler için boot kodunu barındırır.
Bad cluster file	\$BadClus	8	Bölümdeki çalışmayan "cluster" bilgilerini tutar.
Security file	\$Secure	9	Bölümdeki dosyalar için güvenlik bilgilerini tutar.
Uppercase table	\$UpCase	10	"Unicode" karakter eşleşmesi için küçük harfleri büyük harflere çevirir.
NTFS extension file	\$Extend	11	Opsiyonel özellikleri (kota bilgisi, "reparse point" bilgisi ve nesne tanımlayıcılar gibi) saklar.
-	-	12-15	Sonradan kullanım için tahsis edilmiş alandır.

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

MFT tablosunda ilgili disk bölümünün (partition) bütün dosya ve klasörleri için en az bir satır bulunmaktadır. Her bir MFT kaydında, ilgili klasör veya dosyanın ismi, silinip silinmediği, verilerinin disk bölümünde nerede tutulduğu ve dosya sistemi tarih-zaman bilgileri gibi birçok dosya sistemi üst verisi bulunmaktadır.

MFT kayıt sırası ve MFT kaydı güncellenme sayısı verileri de her bir MFT kaydında bulunan üst verilerdendir. MFT kayıt sırası, bir MFT kaydının, MFT dosyasında fiziksel olarak kaçınıcı sırada bulunduğunu göstermektedir. MFT kayıt sırası tek başına bir dosyanın diğer bir dosyadan önce veya sonra geldiği hakkında kesin bir bilgi vermemektedir. Çünkü bir dosya

⁴⁵ How NTFS Works, [technet.microsoft.com/en-us/library/cc781134\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc781134(v=ws.10).aspx)

veya klasör silindiğinde o dosyanın MFT kaydı yeni gelen başka bir dosya tarafından kullanılabilir. Böylelikle MFT kayıt numarası düşük fakat dosya sistemine sonradan gelen dosya veya klasörler oluşmaktadır.

Her bir MFT kaydında olan, diğer bir veri ise logfile sıra (sequence) numarasıdır. Özetle bu sıra numarası, ilgili MFT kaydında gerçekleştirilen en son işlemin \$LogFile dosyasındaki kayıt numarasıdır. \$LogFile dosyası, NTFS dosya sisteminde dosya veya klasör oluşturma, içeriğini veya ismini değiştirme ve MFT kaydındaki herhangi bir veriyi değiştirme vb. işlemlerin kayıtlarını tutmak için kullanılan dosya sistemi üst veri dosyasıdır. MFT kaydının değişmesine sebep olacak bir işlemten önce hâlihazırdaki kaydın bilgileri ve yeni oluşacak kaydın bilgileri, işlemten sonra ise işlemin başarıyla tamamlandığına dair bir bilgi \$LogFile dosyasına kaydedilir. Buradaki amaç MFT kayıtlarını değiştirecek olan işlemlerin gerçekleşmesi yarıda kalır veya bir şekilde tamamlanamazsa, \$LogFile dosyasındaki bilgiler doğrultusunda bozulan MFT kayıtlarının eski haline getirilebilmesidir. Bu şekilde dosya sisteminin bütünlüğünün korunması amaçlanmaktadır. \$LogFile dosyasının boyutu bölümün boyutuna göre otomatik olarak belirlenmekte fakat sonradan komutlar yardımıyla değiştirilebilmektedir⁴⁶. Bu dosyada tutulan kayıtlar dosyayı doldurduğunda eski kayıtların üzerine yazılmaktadır. Bu sebeple de \$LogFile dosyasına bakılarak sadece belli bir zaman aralığındaki dosya sistemi hareketleri anlaşılabilir.

\$MFTMirr dosyasında, \$MFT'deki bazı kritik sistem dosyalarının (\$MFT, \$MFTMirr, \$LogFile, \$Volume) yedek kayıtları tutulmaktadır. Eğer bu kritik sistem dosyalarının bilgileri \$MFT dosyasından okunamaz hale gelirse, \$MFTMirr dosyasında yapılan yedeklemeden geri dönülerek bu problem çözülür.

\$Bitmap dosyasında dosya sisteminin hangi kümesinin (cluster) dolu ya da boş olduğu bilgisi tutulmaktadır. Küme (cluster), dosya sistemi oluşturulurken (biçimlendirme) disk üzerindeki fiziksel kaç tane sektörün birlikte erişileceğini göstermektedir⁴⁷. Format işlemi sırasında kullanıcıya küme büyüklüğünün ne kadar olmasını istediği sorulmaktadır. Büyük kümeleme bir seferde daha çok bilgiye erişilebilmesi, küçük kümeleme ise boyutu küçük olan dosyaların disk üzerinde az yer kaplaması demektir⁴⁸.

NTFS dosya sisteminde FAT dosya sisteminden farklı olarak belli bir kullanıcının sabit disk üzerinde belli miktar alandan fazlasını kullanmamasını sağlayan sistem kota (quota) yönetim sistemidir⁴⁹.

⁴⁶ How NTFS Works, [technet.microsoft.com/en-us/library/cc781134\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc781134(v=ws.10).aspx)

⁴⁷ Cluster: A group of sectors on a disk, www.techterms.com/definition/cluster

⁴⁸ NTFS Optimization, http://www.ntfs.com/ntfs_optimization.htm

⁴⁹ Disk Quotas, [technet.microsoft.com/en-us/library/cc781134\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc781134(v=ws.10).aspx)

Ayrıca NTFS dosya sistemi dosyaları saklarken sıkıştırma yapabilmekte ve böylece daha fazla miktarda veriyi aynı alanda saklayabilmektedir.⁵⁰

NTFS dosya sisteminde dosyalar şifrelenerek de saklanabilmektedir. Bu da ekstra bir güvenlik özelliğidir⁵¹.

2.3.4.2 NTFS dosya sisteminde zaman bilgileri

NTFS dosya sisteminde temel olarak dört ayrı zaman bilgisi tutulmaktadır⁵².

- Dosya oluşturulma zamanı,
- Dosya son değiştirilme zamanı,
- Dosya son erişim zamanı,
- Dosya MFT girdisi son değiştirilme zamanı.

NTFS dosya sisteminde bir dosya ilk olarak oluşturulduğunda bu tarihlerin hepsi aynı olmaktadır. Dosyada bir değişiklik yapılmadığı ya da dosyaya erişilmediği sürece bu zaman bilgileri birbirinin aynısı olarak kalmaktadır.

NTFS dosya sistemi, dosyaların zaman bilgilerini çeşitli kurallara göre güncellemekte ve bu güncellemeler sonrasında dosya **oluşturma zamanı, değiştirme zamanı, erişim zamanı sıralaması değişebilmektedir**. Bu tarihler sıralı olmak zorunda değildir.

Bu nedenle bilgisayarda normal bir kullanıcı davranışıyla oluşturulan bir dosyanın **değiştirme zamanı, oluşturma zamanından eski olabilir**. Örnek vermek gerekirse, NTFS dosya sistemi bulunan bir bilgisayarda oluşturduğumuz bir dosya, bulunduğu klasörden başka bir klasöre kopyalandığında dosyanın oluşturma zamanı kopyalama işleminin yapıldığı zaman olacaktır. Ancak değiştirme zamanı, dosyanın mevcut değiştirme zamanı olarak korunmaktadır. Bu işlem dizisine göre değiştirme zamanı, oluşturma zamanından eski olacaktır.

Bir diskin üretilme ya da piyasaya sürülme zamanı ile içindeki dosyaların tarihleri arasında bir tarih ilişkisi olması beklenebilir. Fakat teknik olarak diskin içindeki dosyalar tarihlerini, işletim sisteminin tarihinden; işletim sistemi ise, BIOS zamanından alır. Bu bağlamda diskin üretim tarihi ile diske yazılan dosyaların tarihleri arasında direk bir ilişki yoktur.

Diskün üretim tarihinden daha eski tarihli bir dosya diskin içinde bulunabilmektedir. Bunun oluşma yollarından bazıları şunlardır:

⁵⁰ Compression of Files and Folders, [technet.microsoft.com/en-us/library/cc781134\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc781134(v=ws.10).aspx)

⁵¹ Encryption, technet.microsoft.com/en-us/library/cc976808.aspx

⁵² The Rules of Time on NTFS File System, K.P. Chow, Frank Y.W. Law, Michael Y.K. Kwan, Pierre K.Y. Lai, Univ. of Hong Kong, ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4155351

1. Dosya sistemi son deęiřtirme zamanı diskin üretim tarihinden eski dosyalar

Diskın üretim tarihinden önce oluşturulmuş bir dosya bulunduęu diskten (kaynak disk) bu diske (hedef disk) aktarıldığında, dosyanın hedef diskteki dosya sistemi "Son Deęiřtirilme" zamanı kaynak diskteki ile aynı olur. Bu dosyanın zaman bilgileri listelendiğinde, dosyanın diskin üretim tarihinden önce bir zaman bilgisine sahip olduęu görülür.

2. Diske imaj yüklenmesi

Kurumlarda, aynı özellikteki birden çok bilgisayara aynı işletim sistemi ve programları tekrar tekrar kurmamak için öncelikle bir bilgisayarda kurulum yapılmaktadır. İşletim sistemi kurulumu, sürücülerin tanıtılması, gerekli programların kurulması ve ayarların yapılması işlemleri tamamlandıktan sonra bu bilgisayarın sabit diskinin kopyası (imajı) alınmakta ve dięer bilgisayarların sabit disklerine bu kopya aktarılarak tüm işlemler tek bir adımda gerçekleştirilmiş olmaktadır. Bu işlemin amacı kurumlardaki biliřim teknolojisi (IT – Information Technology) bölümlerinin işlerini kolaylařtırmaktır. Burada dikkat edilmesi gereken husus, bu ilk imaj hazırlandığı zaman dosyaların sahip olduęu dosya sistemi zaman bilgileri kopya disklerin hepsine de aktarılmaktadır. Bu imajlar sabit disklerle ilk kurulum sırasında kullanıldığı gibi kullanım sırasında sabit diskin arızalanması durumunda da kullanılmaktadır. Bozuk disk yeni temin edilen diskle deęiřtirilmekte ve üzerine bu ilk hazırlanan kopya (imaj) yüklenmektedir. Bu durumda, yeni temin edilen diskin üzerinde eski dosya sistemi tarihli (oluřturma, deęiřtirme, son erişim gibi) dosyaların bulunması normal bir durumdur.

3. Yedekleme ve eşleme programları

Biliřim dünyasında bilginin kıymeti anlařıldıkça yedekleme sistemleri/uygulamaları sıkça kullanılmaya başlanmıştır. Kurumlar/kiřiler kendileri için deęerli olduęunu düşündükleri bilgilerin yedeklerini almaya özen göstermektedirler. Yedekleme (backup) ya da eşleme (synchronization) programları dosyaların içerikleri ile birlikte dosya sistemi üst verilerini de (dosya sistemi tarih bilgileri dâhil) saklayabilmektedir. Yedeęi alınan dosyaların yedekten geri dönüldükten sonra eski tarihlerine sahip oldukları görölmektedir.

4. Arřivleme programları

Arřivleme programları arřivledikleri dosyaların bazı zaman bilgilerini saklayabilmektedir⁵³. Bu arřivler sonrasında açıldığında dosyalar arřivlendikleri andaki zaman bilgileri ile görülebilirler (zip, rar, vb.).

5. Dięer programlar

Windows işletim sisteminde sürükle-bırak, kopyala-yapıştır ya da komut satırından yapılacak kopyalama işlemlerindeki dosya sistemi zaman kuralları ile kopyalama

⁵³ RAR 5.0 Archive Format, <http://www.rarlab.com/technote.htm#timerecord>

amaçlı kullanılabilen programların zaman güncelleme mantıkları aynı olmayabilmektedir. Bu programlar bazı durumlarda dosyaların kopyalandığı dosya sistemindeki zaman bilgilerini yeni dosya üzerine aktarmaktadır^{54 55}.

İncelemeye konu olan sabit diskin "DATA" etiketine sahip ikinci bölümü MFT kayıtlarındaki; MFT kayıt sırası, MFT güncelleme kayıt sırası, logfile sıra numarası ve MFT kayıtlarındaki zaman üst verileri incelenmiştir. Bu inceleme sonucunda, ilgili disk bölümüne, 28.07.2009 tarihinden sonra dosya aktarıldığı değerlendirilmektedir. SİSTEM isimli bölümün dosya sistemi üst verileri incelendiğinde ise diskteki Windows XP işletim sisteminin son olarak 28.07.2009 tarihinde kullanıldığı tespit edilmiştir. Bunlar, diskin işletim sisteminin son kullanılma tarihinden sonra başka bilgisayarlarda ikincil disk olarak kullanıldığını göstermektedir.

Bölüm 2.3.3.7 açıklandığı üzere kullanıcının veri alışverişi yaptığı bilgisayarlar arasında sistem tarihi güncel olmayan bilgisayarların bulunması muhtemeldir. Dosya sistemi üst verileri incelendiğinde de 28.07.2009 tarihinden sonra sabit diskin ikincil disk olarak kullanıldığı bilgisayarların sistem saatlerinin 28.07.2009 tarihinden geride olduğu tespit edilmiştir.

5 no'lu diskin DATA bölümündeki "masaüstü" dizininde bulunan "yasemin.ppt" dosyasının üst verileri incelendiğinde, son değiştirme zamanının 20.08.2003 10:00:28 olduğu, incelemeye konu olan diske 20.08.2008 10:27:39 da taşındığı, en son erişim zamanının ise 09.07.2009 09:39:05 olduğu görülmektedir. Dosyanın içeriğinde 18.08.2008 tarihine ait bir dekont bulunmaktadır. Bunlar, dosyanın sistem saati güncel olmayan bir bilgisayarda oluşturup, işletim sisteminin aktif olduğu tarihler arasında incelemeye konu olan sabit diske aktarıldığını ve yine bu tarihler arasında dosyaya erişildiğini göstermektedir. Kullanıcının veri alışverişi yaptığı bilgisayarlar arasında sistem tarihi güncel olmayan bilgisayarların bulunması kuvvetle muhtemeldir.

2.3.4.3 NTFS dosya sisteminde sahiplik bilgileri

NTFS dosya sistemi, dosyalara erişim hakları ile ilgili bilgileri barındırmaktadır⁵⁶. NTFS öncesinde Windows işletim sistemlerinde kullanılan FAT dosya sisteminde, her kullanıcı her dosyaya erişebilmekte ve bu dosyalar üzerinde değişiklik yapabilmekteydi. Yıllar geçtikçe hem bir bilgisayarı birden fazla kişinin kullanması hem de dijital dünyadaki güvenlik problemlerinin artması sonrasında dosyalara erişim kontrolünün gerekliliği ortaya çıkmıştır. NTFS dosya

⁵⁴ WinSCP Transfer Settings Dialog, http://winscp.net/eng/docs/ui_transfer_custom

⁵⁵ Code Sector Blog, Teracopy, <http://blog.codesector.com/category/code-sector-software/teracopy>

⁵⁶ NTFS Security Benefits, [msdn.microsoft.com/en-us/library/ms913208\(v=winembedded.5\).aspx](http://msdn.microsoft.com/en-us/library/ms913208(v=winembedded.5).aspx)

sistemi ile dosyaların sahipliklerinin belirlenmesi ve erişim kontrolü ile hangi kişilerin ya da gruplara üye olanların bir dosyaya erişebileceği, o dosyayı değiştirebileceği ya da bir programı çalıştırabileceği belli bir sistemle kontrol altına alınmıştır. Böylece izin verilmediği sürece aynı bilgisayarı kullanan farklı kişilere ait dosyalar - aynı sabit disk üzerinde bile olsalar - diğer kişiler tarafından erişilemez durumda olmaktadır.

2.3.4.4 Laboratuvar Bulguları

LABORATUVAR BULGUSU	
Uygulama Kodu	MSWin-5
Testin Üzerinde Koştuğu Sistem	HP 8200 Elite, Windows XP, Windows 2000 Server, Windows 2003 Server
İncelemeye Konu Olan Üst veri Alanları	Dosyaların Sahiplik Bilgisi
Ön Koşullar	Varsayılan ayarların geçerli olması
Uygulama Adımları	➤ Bilgisayarda yeni bir dosya oluşturulur ➤ Yeni oluşturulan dosyanın sahiplik bilgisi tespit edilir
Bulgular	➤ Bilgisayarda yeni oluşturulan dosyanın sahiplik bilgisinin Windows 2000 Server ve Windows 2003 Server' da Builtin\Administrators olduğu, Windows XP'de Builtin\Administrators olmadığı tespit edilmiştir

LABORATUVAR BULGUSU	
Uygulama Kodu	MSWin-6
Testin Üzerinde Koştuğu Sistem	HP 8200 Elite, Windows XP, Windows 2000 Server, Windows 2003 Server
İncelemeye Konu Olan Üst veri Alanları	Dosyaların Sahiplik Bilgisi
Ön Koşullar	Varsayılan ayarların geçerli olması
Uygulama Adımları	➤ Sahiplik bilgisi Builtin\Administrators olan bir dosya NTFS dosya sistemine sahip bir bölüme (volume) taşınır ➤ Yeni dosyanın sahiplik bilgilerine bakılır
Bulgular	➤ Windows XP hariç diğer işletim sistemlerinde yeni bölümde oluşturulan dosyanın sahiplik bilgisinin değişmediği tespit edilmiştir

İncelenen 5 no'lu sabit diskte dosyaların sahiplik bilgisi incelendiğinde bazı dosyaların Builtin\Administrators kullanıcısına ait olduğu görülmektedir. MSWin-5, MSWin-6 numaralı laboratuvar bulgularında görüldüğü üzere dosyalar oluşturulurken bazı işletim sistemlerinde Builtin\Administrators sahiplik bilgisine rastlanmaktadır.

2.3.5 MICROSOFT OFFICE PROGRAMI ÖZELLİKLERİ

Microsoft Office programı Microsoft şirketi tarafından geliştirilen, kapalı kaynak kodlu bir uygulamadır. Ticari olarak satışı yapılır ve alanında dünyadaki lider programlardan biridir. Uygulamanın oluşturduğu dosyanın formatı şirketin kendine has bir formattır. Bu formatın detayları ve ne gibi üst verileri tuttuğu Microsoft tarafından sunulan dokümantasyon haricinde "tersine mühendislik" yöntemleri ile tespit edilmektedir. Microsoft Office ailesi programlarının davranışı Microsoft şirketi tarafından açıkça dokümente edilip yayınlanmadıkça bu program içeriği ve nasıl çalıştığı ile alakalı yapılan yorumlar "tersine mühendislik" yöntemleri ile sınırlı olacaktır.

Microsoft Office yazılımı ile oluşturulmuş bir dijital dosyanın hangi bilgisayarda oluşturulduğunun tespiti için yalnızca üst verilerinin incelenmesi yeterli olmayacaktır. Bazı dijital dosyalar, oluşturuldukları bilgisayara ait *Bilgisayar Adı*, *MAC Adresi* gibi verileri saklarlar. Bu gibi üst verilerin kullanılıyor olması, incelemesi yapılan dijital dosyanın hangi bilgisayarda oluşturulduğuna dair fikir verecektir.

Ancak bununla birlikte, dijital dosyanın hangi bilgisayarda oluşturulduğunun tespiti hakkında incelenebilecek başka durumlar da söz konusudur. Bunun için o dijital dosyanın bilgisayara nasıl geldiği konusunda araştırma yapılabilir. Başka bilgisayarda oluşturulduğu düşünülen ya da analiz edilmek istenen dosyalar için, bu dosyaların içinde tutulan üst veri bölümlerinde bulunan bilgiler ile dosyanın transfer yoluyla gönderildiğinden şüphelenilen bilgisayarın kullanıcı bilgileri karşılaştırılır. Bu bilgiler, o dosyaların üst verilerinde bulunan *Yazar(Author)*, *Son Değiştiren Kullanıcı (LastModifiedBy)* gibi bilgilerdir. Bunun yanı sıra; elektronik imza ve mobil imza gibi ıslak imza yerine kullanılabilen teknolojilerle imzalanmış elektronik postaların kullanılmasının tespiti durumunda, dijital dosyaların hangi bilgisayarda oluşturulduğu ve iletildiği hakkında daha kesin sonuçlar elde edilmiş olur. Ancak elektronik imzalama ve mobil imzalama teknolojileri ülkemizde henüz yaygınlaşmaya başlamış ileri düzey teknolojilerdir. Birkaç sene öncesine kadar kurumlarımızda hiç kullanılmayan e-imza teknolojileri günümüzde sayılı kurumda nadiren kullanılmaktadır. Zaman içerisinde e-imza vb inkâr edilemezlik mekanizmalarının bireysel ve kurumsal kullanımda artması beklenmektedir.

Dijital dosyaların hangi bilgisayarda açıldığı ve düzenlendiği ile ilgili ilave bilgilere gerek duyulursa belgelerin düzenlendiği işletim sistemlerinde kurulu olan yazılımların sürümlerine ve yakın geçmişte açılmış dosya izlerine (recent documents) de bakılabilir.

Adli bilişim incelemelerinde özet (hash) değeri dijital verinin bütünlüğünü doğrulayan, değişikliğe uğramadığını garanti eden önemli bir parametredir. "2.3.1 ADLİ BİLİŞİM İNCELEME METODOLOJİSİ VE ADLİ BİLİŞİM RAPORLARI" bölümünde özet değerinin adli bilişim incelemelerinde ne şekilde kullanıldığı anlatılmaktadır.

Bir dosyanın farklı incelemelerde özet değerleri aynı ise tüm içerik ve dosya iç üst veri bilgileri de aynı olmak zorundadır. Bir dosya içeriğinde ya da üst verilerinin herhangi birinde yapılan bir karakterlik bir değişiklik bile hesaplanan özet değerinde kolaylıkla fark edilebilir büyük bir değişikliğe neden olacaktır. Bu nedenle farklı incelemelerde aynı hash değerine sahip bir dosyanın farklı içerik ya da üst veri barındırması imkânsızdır. Farklı incelemelerde bazı dosyaların tarih üst verilerinde görülen farklılıklar, inceleme yapan araştırmacının doğru saat dilimi kullanmamasından kaynaklanır. İnceleme yapan kişi olayın vuku bulduğu iddia edilen yerin saat dilimini inceleme yazılımına girdi olarak vermelidir. Ancak bu şekilde hesaplanan tarih verileri gerçeği yansıtacaktır. Aksi takdirde kendi bulunduğu yerin saat dilimini kullanan bir bilirkişi, incelemesinde verinin gerçek saat değerleri ile 24 saate kadar sapmalar görebilecektir.

İlerleyen bölümlerde T.C. İstanbul 12. Ağır Ceza Mahkemesi'nin 2010/34 sayılı davası kapsamında olay yerinde ele geçirilmiş 5 no'lu sabit disk üzerinde kurulu işletim sistemi üzerinde bulunan Microsoft Office uygulamasının detayları ve davranış biçimleri anlatılmaktadır.

Araştırılması istenen hususlarda öncelikle konu ile ilgili makaleler incelenmiş ve adli analiz programlarıyla dosyalar üzerinde çalışmalar yapılmıştır. Bununla beraber sorularda belirtilen durumlarla ilgili laboratuvar ortamı oluşturularak raporda belirtilen sonuçlar elde edilmiştir.

2.3.5.1 Sabit diskteki işletim sisteminde kurulu bulunan Microsoft Office programı

Microsoft Office uygulaması 1990 yılından günümüze kadar 13 büyük sürüm ve birçok alt sürüme sahip dünyanın en çok tercih edilen ofis yazılımıdır. İncelemeye konu olan Microsoft Office yazılımının sürümü 9.0 olarak tespit edilmiştir. Bu sürüm Microsoft Office 2000 olarak da bilinen sürümdür. Microsoft Office ailesinin bir üyesi olan ve kelime işlemci olarak kullanılan Microsoft Word yazılımı 9.0.2812 sürüm numarasına sahiptir. Office 9.0 altında yer alan bu sürüm Microsoft Word 2000 olarak da bilinmektedir. 1999 yılının haziran ayında piyasaya sürülen Microsoft Office 9.0 sürümüne Microsoft tarafından verilen destek 2004 yılının haziran ayında sona ermiştir ⁵⁷.

2.3.5.2 Sabit diskteki işletim sisteminde kurulu bulunan ofis programı ile oluşturulan dosyalarda bulunan dosya iç üst veri bilgileri

Microsoft Office programlarıyla oluşturulmuş dijital içerikler kendi içlerinde bir takım üst veriler tutmaktadır. Bu üst veriler dokümanların kimliği niteliğinde olup zaman, kullanıcı ya da içeriğe

⁵⁷ Microsoft Office 2000, an Essential Tool For All Knowledge Workers, Is Available This Week, www.microsoft.com/en-us/news/press/1999/jun99/offlaunchpr.aspx

ilişkin önemli bilgiler tutabilir. Dokümanın geçirdiği tarihsel süreç kısmen de olsa bu üst verilerden anlaşılabilir.

Office dokümanlarının üst verileri dosyayı işleyen yazılımın atayacağı değerlere sahip olur. Bir Office dosyası Microsoft Office yazılımları dışında başka bir uygulama ile de değiştirilebilir ve düzenlenebilir. Bu durumda kullanılan bu yazılımın üst verileri ne şekilde değiştireceği yazılımdan yazılıma değişebilmektedir. Microsoft Word haricinde kullanılan alternatif bir kelime işlemci dosya üst verilerini kendi belirlediği formatta yazar. Zaman zaman üst verileri tamamen sildiği görülen kelime işlemciler de mevcuttur⁵⁸. Bununla beraber Microsoft Office dokümanlarının üst verilerinin temizlenmesi de mümkündür. Üst verilerden arındırma işlemi, kurumsal şirketlerin ya da devlet kurumlarının bazılarında bulunan "İnternete koyulurken ya da başka bir kuruma/şirkete bir doküman gönderilirken üst verilerin temizlenmesi" politikası gereği olarak yıllardır yapılmaktadır. Bu işlem ya Microsoft Word programı içerisinde ya da başka uygulamalar yardımıyla yapılabilir.

Yazar (Author): Yazar verisi, Microsoft Office dokümanlarında saklanan üst verilerden biridir. Dosyanın ilk oluşturulduğu bilgisayarda, Office uygulamasının yazar bilgisini verir. Microsoft Office uygulaması, kurulum esnasında kullanıcıdan yazar bilgisi ister. Bu bilgi ön tanımlı olarak o bilgisayardaki işletim sistemi kullanıcısı olarak gelir. Kullanıcı başka bir veri girerek değiştirmezse yazar bilgisi kullanıcı adı ile aynı olur. Office uygulamasının kurulumu esnasında bu değerler girilmezse, kurulum sonrası açılacak ilk Office uygulamasında bu değerler tekrar sorulacaktır. Bilgisayarda yeni bir kullanıcı oluşturulduğunda, o kullanıcının açacağı ilk Office uygulamasında da aynı pencere gelecektir. Bu penceredeki veriler de silinse ve hiçbir kullanıcı adı girilme bile, Office uygulaması işletim sistemi kullanıcısını "Yazar" olarak kaydedecektir⁵⁹.

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

Şirket(Company): Dosyaya ilişkin şirket verisini gösterir. Bu bilgi Office uygulamasının kurulumu esnasında belirlenmektedir. Kullanıcının girdiği değer şirket verisi olmaktadır.

Uygulama (Application): Dosyanın oluşturulduğu uygulamanın sürümü hakkında bilgi verir. Microsoft Office XP öncesi tüm versiyonlarda majör sürüm numarası da bu alanda

⁵⁸ Abiword, www.abisource.com

⁵⁹ Inspect documents for hidden data and personal information, office.microsoft.com/en-us/help/inspect-documents-for-hidden-data-and-personal-information-HA010074435.aspx

belirtilmekteydi (örn. Microsoft Word 9.0). Ancak Microsoft Office XP sonrasında bu alanda yalnızca Microsoft Word yazmaktadır.

Uygulama Versiyonu (Version): Microsoft'un yazılıma verdiği detaylı sürüm numarası bu alanda bulunmaktadır. Yazılım üzerine geçilen yamalar ve güncellemeler bu sürüm numarasını etkilemektedir. Nokta ile ayrılan değerler majör ve minör sürüm olarak ifade edilmektedir (örn 9.0.2812).

Toplam Düzenlenme Süresi (Total Editing Time): Dosyanın ne kadar süre değişikliğe uğradığını gösterir. Kullanıcının dosyayı açık tuttuğu sürelerin toplamıyla hesaplanır. Her Microsoft Office uygulamasında tutulmayan bir üst veridir.

Revizyon Numarası (Revision Number): Dosyanın kaç kez açılıp değişiklik yapılarak kaydedildiğini gösterir. Her Microsoft Office uygulamasında tutulmayan bir üst veridir.

Belge Oluşturma Tarihi (Create Date): Belgenin oluşturulduğu tarihi gösterir.

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

Belge Çıktı Alınma Tarihi (Last Printed Date): Belgenin yazıcıya en son gönderildiği tarihi gösterir.

Belge Üzerinde Değişiklik Yapan Son On Kullanıcı (Last Ten Authors): Belgeler üzerinde düzenleme yapmış olan son on kullanıcı isimleri ve düzenleme yapılarak kaydedilen belgenin tam dosya yollarını içeren bir listedir.

Microsoft Office XP (Microsoft Office 10) sürümü ve sonrasında Microsoft'un bu bilgiyi artık Office belgeleri içerisinde tutmadığı bilinmektedir. Bu alan 2002 öncesi sürümlerde yazılımsal inceleme-izleme ve hata ayıklama amacıyla tutulmuş bir alan olduğu değerlendirilmektedir. Farklı Office sürümlerinde farklı davranışlar sergileyen alanın en genel özelliği, üzerinde değişiklik yapılan dosyanın kayıt yolu ve adını ve kaydeden kullanıcının bilgilerini tutmasıdır. Alan, Office XP ve sonrası Office sürümlerinde kaldırılmakta eski sürümde kaydedilince tekrardan oluşmaktadır.

Kullanıcılar bir değişiklik yaptıklarında dosya iç üst verilerinde son kaydeden alanı değişecek ve son on kullanıcı listesine kaydedilen dosyanın yolu ve kaydeden kullanıcı bilgisi girecektir. Bu itibarla son on kullanıcı listesindeki kullanıcı bilgisi ile son kaydeden kullanıcı bilgisinin aynı olması beklenir. Fakat Microsoft Office yazılımının farklı sürümlerinde farklı uygulamalar görülmektedir. Bu farklılıklarla ilgili testler laboratuvar bulguları bölümünde belirtilmiştir.

Bilgisayarın MAC Adresi (MAC Address): Bilgisayarlar ağ haberleşmelerini ağ kartları üzerinden yaparlar. Üretilen her ağ kartının üretim sırasında üzerine atanan biricik bir değeri vardır. Bu değer MAC adresi ya da fiziksel adres olarak adlandırılır. Aynı ağda olan

bilgisayarlar bu adresi dikkate alarak haberleşirler. Microsoft Office 2000 ve öncesi sürümlerde Office uygulaması MAC adresini iç haberleşmede kimlik tanımlama amacıyla kullanıyordu. Microsoft Office Word uygulaması ürettiği yeni dosyaların içerisine MAC adresi değerini koyuyordu.

Oluşturulan belgelerin içinde bulunan MAC adres değeri sayesinde, e-posta ekindeki Word belgeleri yoluyla yayılan Melissa virüsünün⁶⁰ kim tarafından oluşturulduğu tespit edilmiş ve virüsün yazarı Amerika Birleşik Devletleri mahkemelerince cezaya çarptırılmıştır⁶¹.

MAC adresi bilgisi Microsoft Word XP ve sonrası sürümlerde yer almamaktadır.

2.3.5.3 Laboratuvar Bulguları

Bu bölümde Microsoft Office uygulamalarının farklı kullanım durumlarında üst verilerde yaptığı değişiklikler test edilmiştir. Her laboratuvar bulgusu testin hangi koşullar altında gerçekleştirildiğini, test adımlarını, sonuçları ve bulguları içermektedir.

⁶⁰ Virus:W32/Melissa, www.f-secure.com/v-descs/melissa.shtml

⁶¹ Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison, www.usdoj.gov/criminal/cybercrime/melissaSent.htm

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-1
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son on kullanıcı listesi, yazar alanı
Ön Koşullar	İki farklı bilgisayar arası dosya aktarım imkânı
Uygulama Adımları	➤ Dosya Word ile düzenlenerek kaydedilir. Son on kullanıcı listesinde yazar ile ilgili kayıt oluşur. ➤ Dosya farklı bir kullanıcı ismine sahip bir bilgisayarda yeniden düzenlenerek kaydedilir. ➤ Düzenleme ve kaydetme son on kullanıcı listesi dolana ve hatta ilk kayıtlar kaybolup yerine en güncel kayıtlar gelene kadar devam ettirilir.
Bulgular	✓ Dosyanın ilk yazar bilgisi son on kullanıcı listesinde görünmemektedir.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-2
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son kaydeden alanı
Ön Koşullar	İki farklı bilgisayar arası dosya aktarım imkânı vardır. Yeni bir dosya oluşturulmuştur. Son on kullanıcı listesinde ilk kayıt şu şekilde oluşmuştur: Kullanıcı: kullanıcı1 Yol: C:\klasor1\abc.doc
Uygulama Adımları	➤ Dosya aynı sürüm Word yazılımını çalıştıran bir makineye taşınır. ➤ Dosya yeni makineye düzenlenerek tekrar ilk bilgisayara taşınır. Son on kullanıcı listesinde ikinci kayıt oluşur. Kullanıcı: kullanıcı2 Yol: C:\klasor2\abc.doc ➤ Dosya ilk kullanıcısının bilgisayarında yeni haliyle tekrardan açılarak düzenlenir ve kaydedilir.
Bulgular	✓ Son on kullanıcı listesindeki ilk kayıt, ilk oluşturan kişinin kayıdır. ✓ Son on kullanıcı listesindeki ikinci ve son kayıt ikinci bilgisayardaki düzenleme işlemi ile ilgilidir. ✓ İlk oluşturan kişinin yaptığı son düzenleme son on kullanıcı listesinde görülmemektedir.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-3
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerinden son kaydedilme tarihi ve son kaydeden alanları
Ön Koşullar	Otomatik kaydetme özelliği açıktır ve 1 dakika olarak seçilmiştir.
Uygulama Adımları	➤ Word dosyası açılır, üzerinde 30 dakika boyunca değişiklikler yapılır ve kaydedilmeden kapatılır.
Bulgular	✓ Dosya kaydedilmeden kapatıldığında son kaydeden ve son kaydedilme tarihi alanlarının değişmediği görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-4
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya özet (hash) değeri
Ön Koşullar	Dosya ilgili sürümde düzenlenmiş, kaydedilmiş, kapatılmış ve özet değeri hesaplanmış olmalıdır.
Uygulama Adımları	➤ Dosyanın özellikler menüsünden küçük bir değişiklik yapılır, kaydedilerek kapatılır.
Bulgular	✓ Üst veri değişir. ✓ Dosyanın hesaplanan yeni özet değerinin ilk değer ile aynı olmadığı görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-5
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Excel 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden revizyon sayısı ve toplam düzenlenme süresi alanları
Ön Koşullar	-
Uygulama Adımları	➤ Excel dosyası üzerinde uzun süre çalışılmış, defalarca düzenlenmiş ve kaydedilmiştir.
Bulgular	✓ Excel yazılımının ilgili sürümünde hiçbir şekilde bu alanların tutulmadığı görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-6
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden revizyon sayısı alanı
Ön Koşullar	Revizyon sayısı alanı 43 değerine sahiptir.
Uygulama Adımları	➤ Dosya "farklı kaydet" seçeneğiyle başka bir dizine kaydedilir.
Bulgular	✓ Oluşan yeni dosyanın revizyon sayısı 2 olmaktadır.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-7
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden revizyon sayısı alanı
Ön Koşullar	-
Uygulama Adımları	➤ Dosya hiçbir değişiklik yapılmadan defalarca "kaydet" seçeneğiyle kaydedilir.
Bulgular	✓ Dosyanın revizyon sayısının değişmediği gözlemlenmiştir.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-8
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden revizyon sayısı alanı
Ön Koşullar	Dosyanın revizyon sayısı alanı 17 değerine sahiptir.
Uygulama Adımları	➤ Dosya hiçbir değişiklik yapılmadan 20 defa "kaydet" seçeneğiyle kaydedilir. Dosya kapatılmaz. ➤ Dosya üzerinde değişiklik yapılarak "kaydet" seçeneğiyle kaydedilir ve kapatılır.
Bulgular	✓ Dosyanın revizyon sayısı, değişiklik yapılmadan yapılan kayıt işlemlerini de ekleyerek 38 olmaktadır (17 + 20 + 1).

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-9
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden revizyon sayısı alanı
Ön Koşullar	Dosyanın revizyon sayısı alanı 17 değerine sahiptir.
Uygulama Adımları	➤ Dosya üzerine sağ tıklanarak özellikler menüsünden yazar bilgisi değiştirilir.
Bulgular	✓ Revizyon sayısının değişmediği görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-10
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden toplam düzenlenme süresi alanı
Ön Koşullar	Dosyanın inceleme öncesi toplam düzenlenme süresi 12 dakikadır.
Uygulama Adımları	➤ Word dosyası açılır. ➤ 20 dakika hiçbir değişiklik yapılmadan beklenir ve kapatılır.
Bulgular	✓ Dosyanın toplam düzenlenme süresinin değişmediği görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-11
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden toplam düzenlenme süresi alanı
Ön Koşullar	Dosyanın inceleme öncesi toplam düzenlenme süresi 12 dakikadır.
Uygulama Adımları	➤ Word dosyası açılır. ➤ 20 dakika hiçbir değişiklik yapılmadan beklenir. ➤ 20 dakikanın sonunda bir değişiklik yapılarak kaydedilir ve kapatılır.
Bulgular	✓ Dosyanın toplam düzenlenme süresi alanı 32 dakikadır.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-12
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son on kullanıcı listesi ve revizyon sayısı alanı
Ön Koşullar	Dosyanın son on kullanıcı listesinde on kayıt vardır. Revizyon sayısı 15 değerine sahiptir.
Uygulama Adımları	➤ Word dosyası açılır. ➤ Dosya "farklı kaydet" seçeneğiyle yeni bir dosya olarak kaydedilir.
Bulgular	✓ Son on kullanıcı listesinde on kayıt vardır. ✓ Dosyayı son kaydeden kullanıcı bilgisi son on kullanıcı listesinin en altında yer alır. ✓ Yeni oluşan dosyanın revizyon sayısı 2 olmaktadır.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-13
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son on kullanıcı listesi ve revizyon sayısı alanı
Ön Koşullar	Dosyanın son on kullanıcı listesinde 4 kayıt vardır. Dosyanın revizyon sayısı 4 değerindedir. İlk kayıta aşağıdaki değerler bulunmaktadır: Kullanıcı: kullanıcı1 Yol: "C:\klasor1\abc.doc" Diğer üç kayıta aşağıdaki değerler bulunmaktadır: Kullanıcı: kullanıcı1 Yol: "C:\klasor2\abc.doc"
Uygulama Adımları	➤ Dosya "C:\ klasor1\" klasörüne taşınır. ➤ Bu klasördeyken açılarak üzerinde 12 defa düzenleme ve kaydetme işlemi yapılır.
Bulgular	✓ Dosyanın son on kullanıcı listesinin değişmediği görülmüştür. ✓ Dosyanın revizyon sayısı alanı 16 değerindedir.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-14
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son on kullanıcı listesi ve revizyon sayısı alanı
Ön Koşullar	Dosyanın son on kullanıcı listesinde 2 kayıt vardır. Dosyanın revizyon sayısı 2 değerindedir. İlk kayıta aşağıdaki değerler bulunmaktadır: Kullanıcı: kullanıcı1 Yol: "C:\klasor1\abc.doc" Diğer kayıta aşağıdaki değer bulunmaktadır: Kullanıcı: kullanıcı2 Yol: "C:\klasor2\abc.doc"
Uygulama Adımları	➤ Dosya bir başka bilgisayarda düzenlenir ve kaydedilir. Son on kullanıcı listesine aşağıdaki kayıt düşer: Kullanıcı: kullanıcı3 Yol: "C:\klasor3\abc.doc" ➤ Dosya düzenlendiği bir önceki bilgisayara taşınır (kullanıcı2), tekrar düzenlenir ve kaydedilir
Bulgular	✓ Dosyanın son on kullanıcı listesinin değişmediği görülmüştür. ✓ Dosyanın son kaydeden alanı "kullanıcı2" değerine sahiptir.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-15
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son on kullanıcı listesi
Ön Koşullar	Dosyanın son on kullanıcı listesinde bir kayıt vardır: Kullanıcı: kullanıcı1 Yol: C:\klasor1\abc.doc
Uygulama Adımları	➤ Dosya "farklı kaydet" seçeneğiyle farklı bir klasöre kaydedilir. C:\klasor2\abc.doc
Bulgular	✓ Yeni oluşan dosyanın üst verilerinden son on kullanıcı listesinde iki kayıt olduğu görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-16
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son on kullanıcı listesi
Ön Koşullar	Dosyanın son on kullanıcı listesinde bir kayıt vardır: Kullanıcı: kullanıcı1 Yol: C:\klasor1\abc.doc
Uygulama Adımları	➤ Dosya "farklı kaydet" seçeneğiyle kaydedilir ve kapatılır. Yol: C:\klasor2\abc.doc ➤ Oluşan yeni dosyanın ismi, sağ tıklanarak "yeniden adlandır" seçeneğiyle değiştirilir. Yol: C:\klasor2\abc2.doc
Bulgular	✓ Yeni oluşan dosyanın son on kullanıcı listesinde iki kayıt vardır. 1. Kayıt: Kullanıcı: kullanıcı1 Yol: C:\klasor1\abc.doc 2. Kayıt: Kullanıcı: kullanıcı1 Yol: C:\klasor2\abc.doc

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-17
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9 Microsoft Word 11
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son on kullanıcı listesi
Ön Koşullar	Dosya Microsoft Word 9 sürümü ile defalarca düzenlenmiş ve kaydedilmiştir. Son on kullanıcı listesinde kayıtlar mevcuttur.
Uygulama Adımları	➤ Dosya Microsoft Word 11 sürümünü kullanan bir bilgisayara taşınır. ➤ Bu bilgisayarda açılarak değişiklik yapılır ve kaydedilir.
Bulgular	✓ Yeni oluşan dosyanın son on kullanıcı listesinin olmadığı görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-18
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9 Microsoft Word 11
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son on kullanıcı listesi
Ön Koşullar	Dosya Microsoft Word 9 sürümü ile defalarca düzenlenmiş ve kaydedilmiştir. Son on kullanıcı listesinde kayıtlar mevcuttur.
Uygulama Adımları	➤ Dosya Microsoft Word 11 sürümünü kullanan bir bilgisayara taşınır. ➤ Bu bilgisayarda açılarak değişiklik yapılır ve kaydedilir. ➤ Dosya tekrardan ilk bilgisayarda açılarak değişiklik yapılır ve kaydedilir.
Bulgular	✓ Yeni oluşan dosyanın son on kullanıcı listesinde en son işlemin kaydı görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-19
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son yazdırılma tarihi (Last Print Date) alanı.
Ön Koşullar	Dosyanın son yazdırılma tarihi alanı boş olmalıdır.
Uygulama Adımları	➤ Word dosyası açılır. ➤ Dosya yazdırılır. ➤ Dosyada hiçbir değişiklik yapılmadan dosya kapatılır.
Bulgular	✓ Son yazdırılma tarihi alanının boş kaldığı görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-20
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son yazdırılma tarihi alanı
Ön Koşullar	Dosyanın son yazdırılma tarihi alanı boştur.
Uygulama Adımları	➤ Word dosyası açılır. ➤ Dosya üzerinde değişiklikler yapılır ve kaydedilir. ➤ Ardından dosya yazdırılır. ➤ Dosyada yeni bir değişiklik yapılmadan dosya kapatılır.
Bulgular	✓ Son yazdırılma tarihi alanının değişmediği görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-21
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son yazdırılma tarihi alanı
Ön Koşullar	Dosyanın son yazdırılma tarihi alanı boştur.
Uygulama Adımları	➤ Word dosyası açılır. ➤ Dosya üzerinde değişiklikler yapılır ve kaydedilir. ➤ Ardından dosya yazdırılır. ➤ Dosyada değişiklik yapılır ve kaydedilir.
Bulgular	✓ Son yazdırılma tarihi alanı değişmiştir.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-22
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son yazdırılma tarihi alanı
Ön Koşullar	Dosyanın son yazdırılma tarihi alanı boştur.
Uygulama Adımları	➤ Word dosyası açılır. ➤ Dosya "dosyaya yazdır" seçeneğiyle prn uzantılı başka bir dosya olarak oluşturulur. Oluşan dosya "yenidosya.prn" ismindedir. ➤ Yenidosya.prn dosyası yazıcıya gönderilerek istenen sayıda çıktı alınır.
Bulgular	✓ Ana dosyanın son yazdırılma tarihi alanı değişmemiştir.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-23
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son yazdırılma tarihi alanı
Ön Koşullar	Dosyanın son yazdırılma tarihi alanı boştur.
Uygulama Adımları	➤ Word dosyası açılır. ➤ Dosya "pdf olarak yazdır" seçeneğiyle bir pdf dosyası olarak yazdırılır (pdf creator vb bir yazılım yardımıyla). Oluşan dosya "yenidosya.pdf" ismindedir. ➤ Yenidosya.pdf dosyası yazıcıya gönderilerek istenen sayıda çıktı alınır.
Bulgular	✓ Ana dosyanın son yazdırılma tarihi alanı değişmemiştir.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-24
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son yazdırılma tarihi alanı
Ön Koşullar	Dosyanın son yazdırılma tarihi alanı boştur.
Uygulama Adımları	➤ Word dosyası açılır. ➤ Dosya "pdf olarak yazdır" seçeneğiyle bir pdf dosyası olarak yazdırılır (pdf creator vb bir yazılım yardımıyla). Oluşan dosya "yenidosya.pdf" ismindedir. ➤ Ana dosya üzerinde bir değişiklik yapılır ve kaydedilerek kapatılır. ➤ Yenidosya.pdf dosyasından ileriki bir tarihte istenen sayıda çıktı alınır.
Bulgular	✓ Ana dosyanın son yazdırılma tarihi alanı pdf dosyasının oluşturulma tarihidir, pdf dosyasının yazdırılma tarihleri ana dosyanın üst verisini etkilememiştir.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-25
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9 Microsoft Word 12
İncelemeye Konu Olan Üst veri Alanları	Dosyanın özet (hash) değeri
Ön Koşullar	Microsoft Word 9 sürümüyle yeni bir dosya oluşturulmuştur. Otomatik kaydetme özelliği açıktır ve 1 dakika olarak seçilmiştir.
Uygulama Adımları	➤ Word dosyası Microsoft Word 12 yazılımı ile açılır, üzerinde 30 dakika boyunca değişiklikler yapılır ve kaydedilmeden kapatılır.
Bulgular	✓ Özet değerinin değişmediği görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-26
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Power Point 9 Microsoft Power Point 12
İncelemeye Konu Olan Üst veri Alanları	Dosyanın özet (hash) değeri
Ön Koşullar	Microsoft Power Point 9 sürümüyle yeni bir dosya oluşturulmuştur. Otomatik kaydetme özelliği açıktır ve 1 dakika olarak seçilmiştir.
Uygulama Adımları	➤ Word dosyası Microsoft Power Point 12 yazılımı ile açılır, üzerinde 30 dakika boyunca değişiklikler yapılır ve kaydedilmeden kapatılır.
Bulgular	✓ Özet değerinin değiştiği görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-27
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Excel 9 Microsoft Excel 12
İncelemeye Konu Olan Üst veri Alanları	Dosyanın özet (hash) değeri
Ön Koşullar	Microsoft Excel 9 sürümüyle yeni bir dosya oluşturulmuştur. Otomatik kaydetme özelliği açıktır ve 1 dakika olarak seçilmiştir.
Uygulama Adımları	➤ Word dosyası Microsoft Excel 12 yazılımı ile açılır, üzerinde 30 dakika boyunca değişiklikler yapılır ve kaydedilmeden kapatılır.
Bulgular	✓ Özet değerinin değiştiği görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-28
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son kaydedilme tarihi alanı ile dosya sistemi üst verilerinden son değişiklik tarihi alanı
Ön Koşullar	Dosya ilgili sürümde düzenlenmiş, kaydedilmiş, kapatılmış olmalıdır.
Uygulama Adımları	➤ Dosya açılmadan üzerine sağ tıklanarak adı değiştirilir.
Bulgular	✓ Üst veriler incelendiğinde dosya iç son kaydetme tarihi üst verisinin işletim sistemi son değişiklik tarihi üst verisinden geride kaldığı (küçük olduğu) görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-29
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerden son kaydedilme tarihi alanı ile işletim sistemi üst verilerinden değişiklik tarihi alanı
Ön Koşullar	Dosya ilgili sürümde düzenlenmiş, kaydedilmiş, kapatılmış olmalıdır. Testte kullanılan iki bilgisayarın sistem tarihleri birbirinden farklıdır.
Uygulama Adımları	➤ Dosya, sistem saati ileri bir bilgisayara kopyalanır. ➤ Yeni bilgisayarda dosya açılır ve düzenlenir. Kaydedilerek kapatılır. ➤ İlk bilgisayara geri aktarılır. İlk bilgisayarda açılmadan basit bir yeniden adlandırma değişikliği yapılır.
Bulgular	✓ Üst veriler incelendiğinde dosya iç son kaydetme tarihi üst verisinin ikinci bilgisayardaki sistem saatini aldığı için işletim sistemi son değişiklik tarihinden daha ileri bir tarihi gösterdiği görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-30
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerinden son kaydetme tarihi alanı
Ön Koşullar	Dosya içeriğine 2013 tarihli bir resmi yazı görüntüsü konmuştur. İkinci bilgisayarın sistem tarihi 2008 yılını göstermektedir.
Uygulama Adımları	➤ Dosya, ikinci bilgisayara alınır. ➤ Yeni bilgisayarda dosya açılır ve düzenlenir. Kaydedilerek kapatılır.
Bulgular	✓ Üst veriler incelendiğinde dosya iç son kaydetme tarihi üst verisinin dosya içinde bulunan resmi evrakın tarihinden daha geçmiş tarihli olduğu görülmüştür.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-31
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9
İncelemeye Konu Olan Üst veri Alanları	Dosya iç üst verilerinden son kaydedilme tarihi
Ön Koşullar	Dosya ilgili sürümde düzenlenmiş, kaydedilmiş, kapatılmış olmalıdır.
Uygulama Adımları	➤ Dosya açılmadan sağ tıklanarak özellikler menüsü görüntülenir. ➤ Buradan yazar, revizyon numarası, şirket, son kaydedilme tarihleri değiştirilir. Tamam düğmesiyle kaydedilir.
Bulgular	✓ Dosya üst verilerinin yeni değerleri taşıdığı görülmüştür. Dosyanın özet (hash) değeri değişmiştir.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-32
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9 Microsoft Word 12
İncelemeye Konu Olan İçerik	XML girdileri
Ön Koşullar	Dosya, Microsoft Word 9 sürümü ile oluşturulmuştur. Microsoft Word 9 çalıştıran bilgisayar ile Microsoft Word 12 çalıştıran bilgisayarın sistem saatleri birbirinden farklıdır. Microsoft Word 9 çalıştıran bilgisayar daha ileri bir tarihi göstermektedir.
Uygulama Adımları	➤ Dosya Microsoft Word 12 yazılımı ile açılır. ➤ Basit bir değişiklik ardından yeni bir dosya olarak farklı kaydedilir.
Bulgular	✓ Yeni oluşan dosya içeriğinde XML izlerine rastlanırken son oluşturma ve değişiklik tarihi ilk dosyanınkinden daha eski bir tarihi göstermektedir.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-33
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Word 9 Microsoft Word 12
İncelemeye Konu Olan İçerik	"Calibri" kelimesi
Ön Koşullar	Dosya, Microsoft Word 9 sürümü ile oluşturulmuştur. Microsoft Word 9 çalıştıran bilgisayar ile Microsoft Word 12 çalıştıran bilgisayarın sistem saatleri birbirinden farklıdır. Microsoft Word 9 çalıştıran bilgisayar daha ileri bir tarihi göstermektedir.
Uygulama Adımları	➤ Dosya Microsoft Word 12 yazılımı ile açılır. ➤ Basit bir değişiklik ardından yeni bir dosya olarak farklı kaydedilir.
Bulgular	✓ Yeni oluşan dosya içeriğinde "Calibri" kelimesine rastlanırken son oluşturma ve değişiklik tarihi ilk dosyanınkinden daha eski bir tarihi göstermektedir.

LABORATUVAR BULGUSU	
Uygulama Kodu	MSOFC-34
Testin Üzerinde Koştuğu İşletim Sistemi	Windows XP Professional Service Pack 2
Testin Uygulandığı Microsoft Office Uygulaması ve Sürümü	Microsoft Power Point 9 Microsoft Power Point 12
İncelemeye Konu Olan İçerik	Dosyanın özet değeri (hash değeri) ve son değişiklik tarihi
Ön Koşullar	Dosya, Microsoft Power Point 9 yazılımı ile oluşturulmuştur.
Uygulama Adımları	➤ Dosya Microsoft Power Point 12 yazılımı ile açılır. ➤ Hiçbir değişiklik yapılmadan ve kaydedilmeden kapatılır.
Bulgular	✓ Dosya iç üst verilerden son değişiklik tarihi değişmezken özet değerinin değiştiği görülmüştür

2.3.5.4 Bulgulara Dayalı Sonuçlar

Laboratuvar çalışmaları sonucunda Microsoft Office programı tarafından oluşturulan dosya iç üst verilerinin (düzenleme kaydı, belgenin revizyon sayısı, son on kullanıcının listesi, yazdırma tarihi vb.) farklı durumları incelenmiştir. Bu durumların normal kullanıcı davranışları ile oluşabileceği görülmüştür. İncelenen sabit diskteki Microsoft Office dokümanlarında da olan bu gibi dosya iç üst verilerinin normal kullanıcı davranışları çerçevesinde olduğu değerlendirilmektedir.

Microsoft Office dosyalarının dosya iç üst verileri ile dosya sistemi üst verileri arasında zamansal öncelik ya da sonralık durumları, normal bilgisayar kullanımlarının yanında farklı sistem saatlerinde çalışan bilgisayarlarda işlenmelerinden kaynaklanabilmektedir. Bölüm 2.3.3.7'de açıklandığı üzere kullanıcının dosya alışverişi yaptığı bilgisayarlar içinde sistem saatleri güncel olmayan bilgisayarların olduğu değerlendirilmektedir.

2.3.6 ZARARLI YAZILIM İNCELEMELERİ

5 no'lu sabit diskte güncel anti virüs yazılımları ile gerçekleştirilen virüs taraması sonucunda sabit diskte iki tür zararlı yazılımın olduğu tespit edilmiştir. Bu zararlı yazılımlar Microsoft tarafından Win32/Ahkarun.A⁶² ve Win32/Taterf⁶³ olarak adlandırılmaktadır.

2.3.6.1 Sabit diskte tespit edilen virüslerin durumu

Bu zararlı yazılımların sistemde uzun bir süre aktif olarak çalıştığı ve sistem kapatılana kadar da silinmediği anlaşılmaktadır. Bu sonuca aşağıdaki bulgular vasıtasıyla varılmıştır:

- Zararlı yazılım dosyalarının devamlı olarak sistem tarafından yedeğinin alınmış olduğu tespit edilmiştir.
- Zararlı yazılımların kayıt defterinde otomatik çalışma ayarlarına sahip olduğu tespit edilmiştir. Şekil 1'de Ahkarun zararlı yazılımına ait, "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" anahtarı altında "iexplore" girdisi ve Taterf zararlı yazılımına ait "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" anahtarı altında "amva" girdisi görülebilmektedir. Bu girdiler sayesinde her bilgisayar açılışında Ahkarun zararlı yazılımı, her oturum açılışında da Taterf zararlı yazılımı otomatik olarak işletim sistemi tarafından çalıştırılmaktadır.
- İşletim sistemi çalıştırdığı her uygulama için bir prefetch dosyası⁶⁴ oluşturmaktadır. İncelenen sistemde zararlı yazılım uygulamalarına ait prefetch dosyalarına da rastlanmıştır. Şekil 2'de listelenen bu dosyaların varlığı, ilgili zararlı yazılımların sistemde çalışmış olduğunu göstermektedir.

⁶² Worm:Win32/Ahkarun.A,
www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Worm%3AWin32%2FAhkarun.A#tab=2

⁶³ Win32/Taterf,
www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=Win32%2fTaterf#tab=2

⁶⁴ Windows XP: Kernel Improvements Create a More Robust, Powerful, and Scalable OS,
msdn.microsoft.com/en-us/magazine/cc302206.aspx

Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☒ Acrobat Assistant 7.0	AcroTray	Adobe Systems Inc.	c:\program files\adobe\acrobat 7.0\...
☒ HotKeysCmds	hkcmd Module	Intel Corporation	c:\windows\system32\hkcmd.exe
☒ iexplore			c:\windows\iexplore.exe
☒ IgfxTray	igfxTray Module	Intel Corporation	c:\windows\system32\igfxtray.exe
☒ McAfeeUpdaterUI	Common User Interface	McAfee, Inc.	c:\program files\mcafee\common fr...
☒ ShStatEXE	VirusScan tray icon	McAfee, Inc.	c:\program files\mcafee\virusscan e...
C:\Documents and Settings\All Users\Start Menu\Programlar\Başlangıç			
☒ Adobe Acrobat Speed Launcher.lnk			c:\windows\installer\{ac76ba86-10...
☒ Microsoft Office.lnk	Microsoft Office 2000 comp...	Microsoft Corporation	c:\program files\microsoft office\offi...
☒ Symantec Fax Starter Edition Bağlantı No...	Symantec Fax Starter Editio...	Microsoft Corporation	c:\program files\microsoft office\offi...
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
☒ Adres Defteri 6	Outlook Express Kurulum Ki...	Microsoft Corporation	c:\program files\outlook express\set...
☒ Microsoft Outlook Express 6	Outlook Express Kurulum Ki...	Microsoft Corporation	c:\program files\outlook express\set...
HKCU\Software\Microsoft\Windows\CurrentVersion\Run			
☒ amva			c:\windows\system32\amvo.exe

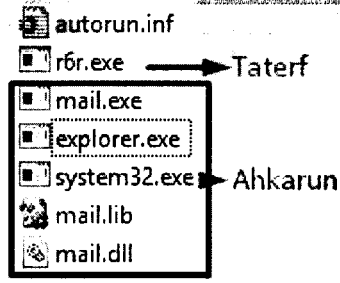
Şekil 1 Zararlı Yazılımların Otomatik Başlama Ayarları

AMVO.EXE-0410B3FF.pf	\DEVICE\HARDDISK\VOLUME1\WINDOWS\SYSTEM32\AMVO.EXE
R6R.EXE-03879216.pf	D:\R6R.EXE
R6R.EXE-04746948.pf	\DEVICE\HARDDISK\VOLUME1\R6R.EXE
R6R.EXE-03FDFDAF.pf	C:\R6R.EXE
R6R.EXE-28824532.pf	\DEVICE\HARDDISK2\DP(1)0-0+6\R6R.EXE
IEXPLORE.EXE-039C3063.pf	\DEVICE\HARDDISK\VOLUME1\WINDOWS\IEXPLORE.EXE

Şekil 2 Zararlı Yazılım Uygulamalarına ait Prefetch Dosyaları

2.3.6.2 Sabit diskte tespit edilen virüslerin özellikleri

Tespit edilen zararlı yazılımların, dikkate değer ortak bir özelliği, taşınabilir veri depolama cihazları (USB flash bellek, USB sabit disk, vb.) ile yayılabilmeleridir. Zararlı yazılımın başka sistemlere yayılabilmek için kullandığı bu yöntem şu şekilde çalışmaktadır: Zararlı yazılım, sisteme yeni bir taşınabilir veri depolama cihazı takılıp takılmadığını devamlı olarak kontrol etmektedir. Bu tür bir cihaz sisteme takıldığında, zararlı yazılım önce kendi dosyalarını ve sonra hazırladığı "autorun.inf" dosyasını bu cihaza atmaktadır. Güncellenmemiş sistemlerde "autorun.inf" dosyası, taşınabilir veri depolama cihazı bir sisteme takıldığında, zararlı yazılımın bu sistemde otomatik olarak çalışmasını sağlamaktadır. Böylelikle zararlı yazılımın bulaşmış olduğu taşınabilir veri depolama cihazı, her takıldığı sisteme, barındırdığı zararlı yazılımı bulaştırmaktadır. Şekil 3'de incelenen sabit disk üzerindeki işletim sistemine bir USB flash bellek tanıtıldığı takdirde, USB flash bellek üzerinde oluşan zararlı yazılım dosyaları gösterilmektedir.



Şekil 3 Taşınabilir Veri Depolama Cihazına Bulaşan Zararlı Yazılım Dosyaları

2.3.3.3 bölümünde açıklandığı üzere sabit diskteki kurulu olan işletim sisteminin internet erişimi bulunmamaktadır. Bu sebeple tespit edilen iki zararlı yazılımın da sisteme taşınabilir veri depolama cihazları ile bulaştığı değerlendirilmektedir. Aynı sebeple, bu zararlı yazılımlar vasıtası ile uzaktan sistemi yönetme, sisteme dosya atma veya sistemden dosya alma gibi işlemler mümkün değildir.

2.3.6.3 Sabit diskte tespit edilen virüslerin dosya sistemi üst verileri

Taterf zararlı yazılımına ait "C:\r6r.exe" ve "D:\r6r.exe" dosyalarının, dosya sistemi zaman üst verileri incelendiğinde, r6r.exe dosyasının sisteme 18.09.2008 tarihinde bulaşmış olduğu değerlendirilmektedir.

Taterf zararlı yazılımı her çalıştırıldığında mevcut disk bölümlerinde kendi kopyasını (r6r.exe) oluşturmaktadır. Dosya sistemi zaman üst verilerinde, MFT Değiştirme zamanı üst verisinin, diğer zaman üst verilerden eski olduğu görülmektedir. Bu sebeple, zararlı yazılımının 28.07.2009 tarihinden sonra takıldığı (bknz 2.3.4.2) sistem saati güncel olmayan bilgisayarlardan (bknz 2.3.3.7) birine de bulaştığı ve MFT Değiştirme zaman bilgisinin eski tarihi gösterecek şekilde değiştiği değerlendirilmektedir.

SONUÇ

İlk bölümde bilimsel adli analizin nasıl yapılması gerektiği açıklanmıştır. Dijital delillerin dünya çapında adli vakalarda kullanıldığından bahsedilmiştir. Yapılan tüm çalışmalarda, tekrar edilebilirlik göz önünde bulundurularak laboratuvar çalışmaları gerçekleştirilmiştir.

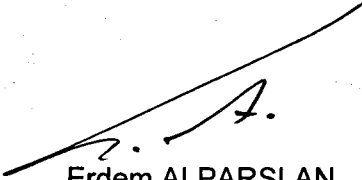
Sonrasında incelenen sabit diskin farklı açılardan analizleri yapılmıştır. İlk olarak sabit diskin fiziksel ve mantıksal özellikleri anlatılmış, içindeki dosya sistemlerine değinilmiştir. Diskin bölümleri, kullanım oranları, dosya sayıları gibi bilgiler verilmiştir.

Devamında, incelenen sabit diskin içinde kurulu bulunan işletim sistemi analiz edilmiştir. İşletim sistemi özellikleri, çalışan programlar ve açılan dokümanların izleri tespit edilmiştir. Yapılan laboratuvar çalışmaları ile işletim sistemi zamanlarının farklı durumları gözlenmiştir. İşletim sisteminin ayarları incelenerek internet ortamına erişiminin olup olmadığı anlaşılmıştır.

İşletim sistemi analizinden sonra incelenen sabit diskteki iki bölümün dosya sistemleri incelenmiştir. Diskte bulunan dosya sisteminin özellikleri hakkında bilgi verilmiştir. İncelenen diskin ne şekilde ve hangi tarihler arasında kullanıldığı analiz edilmiştir.

İncelenen sabit diskte bulunan Microsoft Office programı ve ofis dosyaları üzerinde yapılan analizlerde farklı üst veri durumları çeşitli laboratuvar çalışmaları ile modellenmiştir. Bu modelleme incelenen sabit diskin içindeki ofis dosyaları göz önünde bulundurularak yapılmıştır.

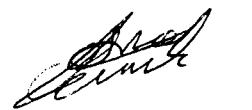
5 no'lu sabit diskte tespit edilen zararlı yazılımlar analiz edilmiş ve sisteme nasıl bulaştıkları anlaşılmaya çalışılmıştır. Zararlı yazılımların ilgili sabit disk üzerindeki etkileri çeşitli analiz metotları ile tespit edilmiş ve raporlanmıştır. (20.01.2014)



Erdem ALPARSLAN



Burak AKOĞUZ



Osman PAMUK