ZARARLI YAZILIMLARIN ETKİSİNDE DİJİTAL ADLİ DELİLLERİN GÜVENİLİRLİĞİ

Emin ÇALIŞKAN
111692015

İSTANBUL BİLGİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
HUKUK YÜKSEK LİSANS PROGRAMI
(BİLİŞİM VE TEKNOLOJİ HUKUKU)

Yrd. Doç. Dr. Leyla Keser Berber

2013

ZARARLI YAZILIMLARIN ETKİSİNDE DİJİTAL ADLİ DELİLLERİN GÜVENİLİRLİĞİ

RELIABILITY OF DIGITAL EVIDENCES UNDER MALWARE INTERACTIONS

Emin ÇALIŞKAN
111692015

Yrd. Doç. Dr. Leyla Keser BERBER	:
Öğr. Gör. Dr. Hayretdin BAHŞİ	:
Yrd. Doç. Dr. Bülent ÖZEL	:
Tezin Onaylandığı Tarih	:
Toplam Sayfa Sayısı	:164

Anahtar Kelimeler	Keywords
1) Adli Analiz	1) Forensics
2) Adli Delil	2) Evidence
3) Zararlı Yazılım	3) Malware
4) Delil Karartma	4) Anti Forensics
5) Güvenilirlik	5) Reliability

ÖZ

Dijital adli analiz çalışmaları, adli bilişim disiplini kapsamında değerlendirilen ve dijital delillerin toplanmasıyla başlayıp, analiz edilmesiyle devam eden ve yetkili makamlara raporlanmasıyla son bulan bir süreç olarak incelenebilir. Günümüzde bilişim teknolojilerinin yaygınlaşması ile adli soruşturmalarda dijital delillere daha sık karşılaşılmaktadır. Bu durum, beraberinde bir takım soru ve sorunları da tartışmaya açmaktadır. Bunlardan belki de en önemlisinin dijital adli delillerin güvenirliği ile ilgili konular olduğu söylenebilir.

Dijital adli delillerin güvenilirliği; zararlı yazılımların etkisi ve delil karartma şüphesiyle tartışılagelen bir konu başlığıdır. Adli soruşturmalarda gündeme gelen truva atı savunmaları ve delil karartma iddiası, delil güvenilirliğinin netlik kazanmasına olan ihtiyacı gözler önüne seren iki farklı kutuptur. Bu bağlamda tez çalışması kapsamında dijital adli delil güvenilirliğinin tesis edilmesine engel teşkil eden sorunlar ele alınmıştır. Sonrasında dijital adli delil güvenilirliğinin sağlanması için kullanılabilecek iki farklı model tartışılmıştır.

Bu modellerden ilki olan karmaşıklık tabanlı niceliksel değerlendirmede, delil oluşum sürecindeki bütün olası senaryolar sayısal olarak ifade edilip bilgisayarda rastlanan dijital verilerin bu senaryolara uyumu hesaplanmıştır. Elde edilen sayısal değer, delilin zararlı yazılımlarla veya kullanıcı iradesiyle oluşma ihtimalini vermektedir. İncelenen bir diğer model olan güven seviyesi sınıflandırmasında ise, dijital adli delilin oluşumuyla ilgili her bir önerme için bir değerlendirme havuzu referans alınarak bulgunun güvenilirliğine göre sınıflandırma yapılmaktadır. Zararlı yazılım etkisiyle veya kullanıcı iradesiyle oluşturulduğu iddia edilen her bir dijital delil için, delilin kullanıcı ilişkisinin varlığı ya da yokluğu durumlarını açıklayan önermeler hakkında güvenilirlik kategorilerine göre sınıflandırma yapılmaktadır. Bu modeller sayesinde dijital adli delillerin güvenilirliği bilimsel olarak değerlendirilmiş olmaktadır.

ABSTRACT

Digital forensic analysis studies are considered within the scope of the discipline of computer forensics and they can be examined as a process which starts with digital evidence collection, proceeds with analyzing the forensic evidence and ends with producing reports to the relevant authorities. Today, with the proliferation of information technologies, digital forensics evidences are frequently encountered in legal investigations. Thus, aforesaid situation causes lots of discussions about the digital evidences which are being investigated in lawsuits. As a matter of fact, the most important discussion topic should be the reliability of those digital forensic evidences.

The reliability of digital forensic evidences can be debated with considering the affects of malwares and evidence spoliation. In this context, the scope of the thesis focuses on digital forensic evidences and problems which impede the establishment of reliability for those evidences. Afterwards, two different models were discussed in order to ensure the reliability of digital forensic evidences.

The first of the models which were discussed was the complexity based quantitative evaluation of forensics evidences. In that model, all possible scenarios which may result the digital forensic evidence were calculated and those findings were compared the actual digital data found an investigated computer. As a result, a numerical probability was shown whether the digital evidence was incurred from a malware interaction or it was consciously created by the user of the computer. In the other model, namely the confidence level classification, a reference pool is suggested to place every statements and findings to an appropriate confidence level. The absence or presence of every digital evidence and related digital findings may result a different confidence level. Thus, the reliability of digital evidences could be classified. The studies mentioned in the thesis were reviewed and discussed to help clarifying the reliability issues of digital forensics evidences.

İÇİNDEKİLER

ÖZ iii
ABSTRACT iv
İÇİNDEKİLER v
KISALTMALAR x
KAYNAKÇA xii
ELEKTRONİK BAĞLANTI ADRESLERİ xiv
ŞEKİL LİSTESİ xviii
TABLO LİSTESİ xx
Zararlı Yazılımların Etkisinde Dijital Adli Delillerin Güvenilirliği 1
§1. Giriş 1
I. Analiz aşamasında dijital adli deliller 2
II. Bulguların raporlanması ve delil güvenilirliği 4
§2. Dijital adli analiz çalışmaları 6
I. Dijital adli analiz süreçleri 6
A- Taraflar 7
B- Süreç modelleri 7
1. Hazırlık 8
2. Tespit 8
3. Koruma 8
4. Analiz 9
5. Raporlama 9
II. Kullanılan araçlar 10
A- Lisanslı ürünler 10
1. Tableau 10
2. Encase 11
3. FTK 12
4. X-Ways Forensics 13
5. Oxygen Forensic Suite 14
B- Açık kaynak kodlu ürünler 14
1. SIFT Linux işletim sistemi 14
2. The Sleuth Kit (TSK) 14
3. Log2timeline 15
4. AnalyzeMFT 15
5. ExifTool 16
III. Analizde kullanılan temel kavramlar 16
A- Dosyalama sistemleri 16
1. FAT, FAT32 17
2. NTFS 17
3. HFS+ 18
4. Ext2, Ext3, Ext4 18
B- Sabit disklerin veri saklama birimleri 18
1. *Hat* (Track) 21
2. *Geometrik sektör* (Geometrik sector) 21
3. *Disk sektörü* (Disk sector) 21
4. *Yığın* (Cluster) 21
5. Paylaştırılmamış yığınlar (Unallocated clusters) 22
IV. İncelenebilecek kritik veriler 23
A- Dosya sistemi verileri 23
1. $MFT 24
2. $MFTMirr 31
3. $LogFile 32

4. $I30 dosyası 34
5. $INDX dosyası 34
6. *Fazlalık alan* (Slack space) verileri 35
7. $Volume 35
8. $AttrDef 36
9. $Bitmap 36
10. $Boot 36
11. $BadClus 36
12. $Secure 36
13. $Upcase 37
14. $Extend 37
B- İşletim sistemi verileri 37
1. Olay kayıt dosyaları (Eventlogs) 37
2. Uygulama kayıtları 38
3. Güvenlik kayıtları 38
4. Sistem kayıtları 39
5. Kayıt defteri (Registry) 39
6. Pagefile.sys dosyası 41
7. Hiberfil.sys dosyası 41
8. Prefetch dosyaları 42
9. Takas dosyaları (Swap files) 43
10. *Sistem geri yükleme noktası* (System restore point) verileri 43
11. *Hacim gölge servisi* (Volume Shadow Service) verileri 43
12. Geçmiş yakın zaman dosyaları (MRU dosyaları) 44
C- Uygulama verileri 45
1. Dosya üstverileri 45
2. Dosya durumu 46
3. Yazar verisi 46
4. Tarih-zaman verisi 48
5. İnternet uygulamaları 49
a) *Çerezler* (Cookie) 49
a. Ziyaret geçmişi verileri (History) 49
b. Sık ziyaret edilenler (Bookmark) 50
6. Elektronik postalar 50
7. Anti virüs uygulama kayıtları 52
8. Kişiden kişiye dosya aktarım uygulamaları (Peer to peer-P2P) 52
9. Sanal işletim sistemi uygulamaları 52
D- Harici veriler 54
1. İnternet servis sağlayıcı (ISP) verileri 54
2. Elektronik posta servis sağlayıcı verileri 55
3. Sosyal medya uygulamaları bilgileri 56
V. Dijital adli analizin tarafları ve karar verme 56
§3. Zararlı yazılımlar 58
I. Tanım 58
II. Zararlı yazılım üreticilerinin motivasyonları 60
A- Eğlence, hobi ve ideolojinin yayılması 60
B- Şaka ve korkutma 61
C- Bilgisayar bilgisini gösterme ve saygınlık kazanma 61
D- Endüstriyel casusluk 61
E- Araştırmalar ve deneysel çalışmalar 61
F- Dijital barbarlık 62
G- İntikam 62
III. Sınıflandırma 62
A- Virüs 62
B- Bilgisayar kurtçukları 63

C- Truva atları 64
D- Rootkitler ve botlar 65
E- Diğer zararlı yazılımlar 66
IV. Zararlı yazılımların dağılımı 66
A- Dağılım oranları 67
B- Dağılma teknikleri 68
1. Rastgele yayılan zararlı yazılımlar 68
2. Hedefli zararlı yazılımlar 69
§4. *Delil karartma* (anti-forensics) 71
I. Delillerin imha edilmesi 71
II. Delillerin temizlenmesi 73
A- Basit silme işlemleri 73
B- Dosya temizliği 75
1. Üzerine yazma 76
2. Kalıntı temizleme 79
III. Veri gizleme 79
A- Verinin tespit edilememesi 80
B- Verinin şifrelenmesi 80
IV. Veri manipülasyonu 82
A- Zaman tarih manipülasyonları 83
1. setMACE ile örnek çalışma 85
B- Dosya üstveri manipülasyonu 88
V. Delil niteliğinde verilerin oluşumunu engelleme 89
A- Kayıt tutma fonksiyonlarının kapatılması 89
1. İşletim sistemi kayıt tutma özelliklerinin devre dışı bırakılması 89
2. Uygulamaların kayıt tutma özelliklerinin devre dışı bırakılması 90
B- Kayıt tutulmasını engelleyecek sistemler kullanma 91
§5. Dijital adli delillerin güvenilirliği ve güven seviyeleri 94
I. Delillerin varlığı 95
II. Delillerin ele alınması 95
A- Tekniğin test edilebilirliği 96
B- Tekniğin bilim çevrelerine açıklanmış olması 96
C- Hata ihtimalinin bilinmesi 96
D- Tekniğin denetlenebildiği standartların bulunması 96
E- Bilim çevrelerince genel kabulü 96
III. Dijital adli delil kuralları 97
A- Delil geçerliliği 97
B- Delilin aslına uygunluğu 98
C- Delilin bütünlüğü 100
D- Delilin kaynağı 101
1. Dış kaynaklı veri türleri 101
2. Dış kaynaklı olmayan veri türleri 101
E- Delilin kullanıcı ilişkisi 102
1. Delillerin kullanıcı ile ilişkisine dair veriler 102
2. Delil bilgisayarının kullanıcı ile ilişkisi 103
3. Delil bilgisayarının zararlı yazılımlarla ilişkisi 104
F- Delil inandırıcılığı 106
G- Delil tekrar incelene bilirliği 106
IV. Delil güvenilirliği tespit modelleri 107
A- Karmaşıklık tabanlı niceliksel değerlendirme 107
1. Tanım 107
2. Vaka çalışması 110
a) Hipotezler 112
b) Deliller 112
c) Değerlendirme 113

d) Tartışma 115
B- Güven seviyesi sınıflandırma modeli 116
1. Tanım 116
2. Vaka çalışması 119
a) Hazırlık 119
b) Tespit 120
c) Koruma 120
d) Analiz 121
e) Raporlama 125
f) Tartışma 128
§6. Ulusal ve uluslararası hukukta dijital adli deliller 130
I. Mevzuat 130
A- ABD perspektifi 130
1. Delilin gerçekliği 131
2. Delilin ilgili olması 131
3. Delilin önyargı oluşturmaması 131
4. Delilin başka kaynaklardan elde edilmesi 131
5. En iyi delil niteliği 132
B- AB perspektifi 132
C- Türkiye perspektifi 134
1. Yürürlükte olan mevzuat 134
a) Ceza Muhakemeleri Kanunu 134
b) Adlî ve Önleme Aramaları Yönetmeliği 135
c) Suç Eşyası Yönetmeliği 136
2. Tasarılar 137
a) Mevzuatta yapılacak değişimler 137
b) Kanun tasarıları 137
3. Yaşanan sorunlar 138
II. Şüpheden sanığın yararlanması ilkesi 140
A- Geçerli durum 140
B- Dijital delillerin niteliği 140
III. Delillerin inkârı ve Truva atı savunmaları 141
A- Tanım 141
B- Savunmanın Truva atı savunması 142
1. Kabul edilebilir şüphe uyandırmak 143
2. Taammüden yapılan işlemlerde manipülasyon iddiası 143
3. SODDI savunması 144
C- Savcılığın Truva atı savunmasına cevabı 145
1. Zararlı yazılımın karakteri ve yeteneği 145
2. Kullanıcının bilgisayar bilgisi 147
3. Zararlı yazılımla kullanıcının ilişkisi 148
4. Kullanıcının itirafı 148
D- Örnek davalar 149
1. Aaron Caffrey davası 149
2. Julian Green davası 150
3. Samuel Crabtree davası 150
E- Tartışmaya açık kararlar 151
§7. Sonuç 152
§8. Ekler 154
I. Dijital adli analiz çalışmalarını etkileyen sorunlar ve çözüm önerileri 154
A- Mevzuat 154
B- Standartlaşma 156
C- İhtisaslaşma 157
D- Disiplinler arası çalışma 158
E- Kaynak ayrımı 159

F- Teknik yetkinlikler 160
§9. Özgeçmiş 162

KISALTMALAR

AB	:	Avrupa Birliği
ABD	:	Amerika Birleşik Devletleri
API	:	Application Programming Interface
BIOS	:	Basic Input Output System
Bkz./bkz.	:	Bakınız
BPB	:	BIOS parametre bloğu
BSD	:	Berkeley Software Distribution
BTK	:	Bilgi Teknolojileri ve İletişim Kurumu
CD	:	Compact Disk
CERT	:	Computer Emergency Response Team
CMK	:	Ceza Muhakemesi Kanunu
CSV	:	Comma Seperated Values
CTOSE	:	Cyber Tools Online Search for Evidence
DDOS	:	Distributed Denial of Service
DFRWS	:	Digital Forensic Research Workshop
DLL	:	Dynamic Link Library
DOS	:	Disk Operating System
DOS	:	Denial of Service
DVD	:	Digital Versatile Disk
EXT	:	Extended File System
FAT	:	File Allocation Table
FN	:	File Name
FRE	:	Federal Rules of Evidence
FTK	:	Forensic Toolkit
GB	:	Giga Byte
GMT	:	Greenwich Mean Time
HFS	:	Hierarchical File System
HKCC	:	Hkey Current Config
HKCR	:	Hkey Classes Root
HKCU	:	Hkey Current User
HKLM	:	Hkey Local Machine
HKU	:	Hkey Users
HTTP	:	Hypertext Transfer Protocol
IDE	:	Integrated Drive Electronics
IEEE	:	Institute of Electrical and Electronics Engineers
IFIP	:	International Federation for Information Processing
IM	:	Instant Messenger
IP	:	Internet Protocol
ISP	:	Internet Service Provider

JPEG	:	Joint Photographic Experts Group
KB	:	Kilo Byte
KLM	:	Keystroke Level Model
LEF	:	Logical Evidence File
MACE	:	Modified Accessed Created Entry Modified Dates
MB	:	Mega Byte
MD5	:	Message Digest 5 Algorithm
MFT	:	Master File Table
MRU	:	Most Recently Used
NIJ	:	National Institute of Justice
NTFS	:	New Technology File System
OS	:	Operating System
PDF	:	Portable Document Format
PF	:	Prefetch
PGP	:	Pretty Good Privacy
POSIX	:	Portable Operating System Interface for Unix
RPM	:	Revolutions Per Minute
SATA	:	Serial ATA
SCSI	:	Small Computer System Interface
sf.	:	Sayfa
SHA1	:	Secure Hashing Algorithm 1
SIFT	:	The SANS Investigative Forensic Toolkit
SODDI	:	Some Other Dude Did It
SSD	:	Solid State Drive
STD	:	Standard
TBMM	:	Türkiye Büyük Millet Meclisi
TDM	:	Target Disk Mode
TİB	:	Türkiye Büyük Millet Meclisi
TİB	:	Telekomünikasyon İletişim Başkanlığı
TL	:	Türk Lirası
TR	:	Türkiye
TSK	:	The Sleuth Kit
URL	:	Uniform Resource Locator
US	:	United States
USB	:	Universal Serial Bus
UTC	:	Coordinated Universal Time
UYAP	:	Ulusal Yargı Ağı Projesi
VS.	:	Vesaire
VSS	:	Volume Shadow Copy Service
WWW	:	World Wide Web

KAYNAKÇA

Banday : M. Tariq Banday, Techniques and Tools for Forensics Investigation of e-mail, Kashmir 2011

Berber : Leyla Keser Berber, Adli Bilişim (Computer Forensic), İstanbul 2004

Berber Ders Notları : Leyla Keser Berber, Dijital Adli Analiz Ders Notları, İstanbul 2012

Billo/Chang : Charles G. Billo, Wellton Chang, Cyber warfare an analysis of the means and motivations of selected nation states, Hanover 2004

Blount : Walker C. Blount, Why 7200 RPM Mobile Hard Disk Drives, USA 2007

Bovet/Cesati : Daniel P. Bovet ve Marco Cesati, Understanding the Linux Kernel Second Edition, Sebastopol CA 2003

Brenner/Carrier/Henninger : Susan W. Brenner, Brian Carrier, Jef Henninger, The trojan horse defense in cybercrime cases, Indiana 2005

Capriotti : Jason Capriotti, FAT32 vs. NTFS, USA 2000

Casey : Eoghan Casey, Digital Evidence and Computer Crime, Maryland 2011

Conway : Maura Conway, What is Cyberterrorism?, Dublin 2002

Ćosić/Ćosić/Bača : Jasmin Ćosić, Zoran Ćosić, Miroslav Bača, Legal Aspects of Digital Antiforensic, Zagreb 2010

Craiger : Dr. Philip Craiger, Mac Forensics: Mac OS X and the HFS+ File System, Florida 2005

Denning : Dorothy E. Denning, "Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy", ABD 2001

Egele/Scholte/Kırda/Kruegel : Manuel Egele, Thedoor Scholte, Engin Kırda, Christopher Kruegel, A Survey on Automated Dynamic Malware Analysis Techniques and Tools, ABD 2010

Erdely : Robert Erdely, Shadow Copy Forensics, Indianapolis 2011

Farmer : Derrick J. Farmer, A Forensic Analysis of the Windows Registry, Vermont 2008

Harris : Ryan Harris, Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, Indiana 2006

Hosmer : Chet Hosmer, Proving the Integrity of Digital Evidence with Time, New York 2002

Iqbal : Hameed Iqbal, Forensic Analysis of Physical Memory and Page File, Gjøvik 2009

Kahvedžić/Kechadi : Damir Kahvedžić, Tahar Kechadi, Extraction of User Activity through Comparison of Windows Restore Points, Dublin 2008

Khanikekar : Sandeep Kumar Khanikekar, Web Forensics, Texas 2010

Krone : Tony Krone, A Typology of Online Child Pornography Offending, Avustralya 2004

Kwan/Chow/Lai : M Kwan, K P Chow, F Law, P Lai, Reasoning About Evidence using Bayesian Network, Advances in Digital Forensics IV, International Federation for Information Processing (IFIP), Tokyo 2008

Lloyd : S Lloyd, Measures of Complexity: a Non-exhaustive List, IEEE 2001

Maclean : Nicholas Paul Maclean, Acquisition and Analysis of Windows Memory, ABD 2006

Murdock : Everett Errol Murdock, DOS the Easy Way: A Complete Guide to

Microsoft's MS DOS, San Pedro CA 1988

Oh/Lee/Lee : Junghoon Oh, Seungbong Lee, Sangjin Lee, Advanced evidence collection and analysis of web browser activity, Republic of Korea 2011

Overill/Silomon/Chow : Richard E. Overill, Jantje A.M. Silomon, Kam-Pui Chow, A Complexity Based Model for Quantifying Forensic Evidential Probabilities, Polonya 2010

Öztürk : Özgür Öztürk, "E-posta'larda Spam Sorunu ve Çözüm Önerileri", Ankara 2009

Peron/Legary : Christian S.J. Peron, Michael Legary, Digital anti-forensics: Emerging trends in data transformation techniques, USA 2002

Richard/Yuval : Russon Richard ve Fledel Yuval, NTFS Documentation, Boston 2000

Rogers : Dr. Marcus K. Rogers, Anti-forensics, San Diego 2005

Sherman : Susan E.E.B. Sherman, Esq., Hearsay and Evidence in the Computer Emergency Response Team (CERT), ABD 2004

Thabet : Amr Thabet, Stuxnet Malware Analysis Paper, Alexandria 2011

Ünver/Canbay/Günaydın : Mustafa Ünver, Cafer Canbay, Yüksel Günaydın, Köle Bilgisayar ve Köle Bilgisayar Ağları (Zombi ve Botnetler), Ankara 2010

Wright/Kleiman/Sundhar : Craig Wright, Dave Kleiman, and Shyaam Sundhar R.S., Overwriting Hard Drive Data: The Great Wiping Controversy, USA 2008

Wu/Yu/Liu : Min Wu, Heather Yu, Bede Liu, Data Hiding in Image and Video: Part II—Designs and Applications, Çin 2003

ELEKTRONİK BAĞLANTI ADRESLERİ

A technical description of the BitTorrent protocol	:	http://www.cse.chalmers.se/~tsigas/Courses/DCDSeminar/Files/BitTorrent.pdf.
Admissibility of Digital Evidence	:	http://www.tmcec.com/public/files/File/Course%20Materials/FY09/Prosecutors/Moss%20-%20Digital%20Evidence.pdf.
AnalyzeMFT	:	http://www.integriography.com/
Anayasa	:	http://www.tbmm.gov.tr/anayasa/anayasa_2011.pdf
Application Programming Interface	:	http://en.wikipedia.org/wiki/Application_programming_interface.
Avrupa İnsan Hakları Sözleşmesi	:	http://www.echr.coe.int/NR/rdonlyres/3BAA147F-29C9-48CE-AF64FB85A86B2433/0/Convention_TUR.pdf.
Backtrack	:	http://www.backtrack-linux.org
BartPE	:	http://www.nu2.nu/pebuilder.
Bellek Analizi	:	http://computer-forensics.sans.org/blog/2011/07/21/live-mem-forensic-analysis.
Bilgisayar kullanım oranı	:	http://www.invest.gov.tr/trTR/infocenter/publications/Documents/BILGI.ILETISIM.SEKTORU.PDF
Bitlocker	:	http://windows.microsoft.com/is-IS/windows-vista/BitLocker-Drive-Encryption-Overview.
BPB	:	http://en.wikipedia.org/wiki/BIOS_parameter_block.
BTK	:	http://www.tk.gov.tr.
Catch me if you can	:	http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-foster-liu-update.pdf.
Ccleaner	:	http://www.piriform.com/ccleaner.
Ceza Muhakemesi Kanunu Madde 127	:	http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.5271&MevzuatIliski=0&sourceXmlSearch=
Cleaner After Me	:	http://www.nirsoft.net/utils/clean_after_me.html.
CMK 134 ve Düşündürdükleri	:	http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html.
Computer Forensic Artifacts: Windows 7 Shellbags	:	http://computer-forensics.sans.org/blog/2011/07/05/shellbags.
Computer Forensics: Finding "hidden" data	:	http://www.techrepublic.com/blog/security/computer-forensics-finding-hidden-data/232.
Computer Incident Response	:	http://www.sans.org/course/advanced-computer-forensic-analysis-incident-response.
CSV (comma seperated values) formatı	:	http://en.wikipedia.org/wiki/Comma-separated_values.
Cyber Tools On-Line Search for Evidence	:	http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=5319458.
Data Erasure	:	http://en.wikipedia.org/wiki/Data_erasure.
Delil çeşitleri	:	http://besiktas.iem.gov.tr/web_18467_1/entitialfocus.aspx?primary_id=1921&type=1075&target=productialdbl&detail=double&sp_table=&sp_primary=&sp_table_extra=&openfrom=sortial.
DFRWS	:	http://www.dfrws.org/index.shtml.

* Bu bölümde yer alan elektronik ağ adreslerinin tamamının güncelliği 7 Ocak 2013 tarihinde tekrar erişilmek suretiyle teyit edilmiştir.

Digital Evidence	:	http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Presentations/DigitalEvidence.pdf.
DOS	:	http://www.writeblocked.org/resources/ntfs_cheat_sheets.pdf.
Emule	:	http://www.emule.com.
Encase	:	http://www.guidancesoftware.com/encase-forensic.htm.
Event viewer	:	http://support.microsoft.com/kb/308427.
ExifTool	:	http://www.sno.phy.queensu.ca/~phil/exiftool.
Facebook	:	https://facebook.com
Faraday Kafesi	:	http://tr.wikipedia.org/wiki/Faraday_kafesi.
Faraday kafesi	:	http://tr.wikipedia.org/wiki/Faraday_kafesi
FAT	:	http://en.wikipedia.org/wiki/File_Allocation_Table.
Federal Rules of Evidence	:	http://www.law.cornell.edu/rules/fre.
Federal Rules of Evidence	:	http://federalevidence.com
Filevault	:	http://support.apple.com/kb/HT4790.
Firewire bağlantısı olan bilgisayarlarda TDM (Target Disk Mode) modu	:	http://en.wikipedia.org/wiki/Target_Disk_Mode
Fiziksel veri kurtarma	:	http://www.pc3000.com
Flame virus, most sophisticated malicious code	:	http://lighthousechurchinc.org/fire/newsnprophetic_pdf/FlameVirusDevelopedByUS.pdf.
FTK	:	http://www.accessdata.com/products/digital-forensics/ftk.
Gmail	:	https://mail.google.com/mail.
Haberi incelemek bkz. The case of the Trojan Wookiee	:	http://www.zdnet.com/the-case-of-the-trojan-wookiee-3039117240.
Hanehalkı bilişim teknolojileri kullanım araştırması	:	http://www.tuik.gov.tr/PreHaberBultenleri.do?id=10880.
Hard Drive Types	:	http://www.buzzle.com/articles/hard-drive-types.html.
HFS	:	http://en.wikipedia.org/wiki/Hierarchical_File_System.
Hiren's	:	http://www.hiren.info/pages/bootcd.
HKEY_USERS	:	http://pcsupport.about.com/od/termshm/g/hkey_users.htm.
Hotmail	:	https://login.live.com.
I30 Index Attributes	:	http://computer-forensics.sans.org/blog/2011/09/20/ntfs-i30-index-attributes-evidence-of-deleted-and-overwritten-files.
Incident Response Poster	:	http://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf.
Information Assurance Applied to Authentication of Digital Evidence	:	http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2004/research/2004_10_research01.htm.
Inspect documents	:	http://office.microsoft.com/en-us/help/inspect-documents-for-hidden-data-and-personal-information-HA010074435.aspx.
iMesh	:	http://www.imesh.com.
Kişisel bilgisayar	:	http://tr.wikipedia.org/wiki/Ki%C5%9Fisel_bilgisayar.
Klavye Vuruşu Seviye Modeli (Keystore Level Model-KLM)	:	http://en.wikipedia.org/wiki/Keystroke-level_model.
Knoppix	:	http://www.knoppix.net.
Limewire	:	http://www.limewire.com.
Linux	:	http://en.wikipedia.org/wiki/Linux.

Locard's exchange prinsible	:	http://en.wikipedia.org/wiki/Locard%27s_exchange_principle.
Log2timeline	:	http://code.google.com/p/log2timeline.
Lorraine v. Markel: Electronik Evidence 101	:	http://www.lexisnexis.com/applieddiscovery/LawLibrary/white Papers/ADI_WP_LorraineVMarkel.pdf
MACE	:	http://whereismydata.wordpress.com/2009/02/14/dates-ntfs-created-modified-accessed-written
Master File Table	:	http://msdn.microsoft.com/en-us/library/bb470206%28v=vs.85%29.aspx.
MFT Sequence number	:	http://jmharkness.wordpress.com/2011/01/27/mft-file-reference-number.
MFTRCRD	:	http://code.google.com/p/mft2csv/wiki/MFTRCRD.
Minnesota court takes dim view of encryption	:	http://news.cnet.com/Minnesota-court-takes-dim-view-of-encryption/2100-1030_3-5718978.html.
MRU (Most Recently Used)	:	http://msdn.microsoft.com/en-us/library/aa376960%28v=VS.85%29.aspx.
MSRT Observations – Online Game Password Stealers	:	http://blogs.technet.com/b/mmpc/archive/2009/02/19/msrt-observations-online-game-password-stealers.aspx
NFTS documentation and MFT Sequence numbers	:	http://integriography.wordpress.com/2010/02/10/updated-analyzemft-mft-sequence-numbers-and-ntfs-documentation.
NIJ	:	http://www.nij.gov/topics/forensics/welcome.htm.
Outlook	:	http://office.microsoft.com/tr-tr/outlook.
Oxygen Forensic	:	http://www.oxygen-forensic.com/en.
PandaLabs Quarterly Report	:	http://press.pandasecurity.com/wp-content/uploads/2012/08/Quarterly-Report-PandaLabs-April-June-2012.pdf.
POSIX	:	http://inform.pucp.edu.pe/~inf232/Ntfs/ntfs_doc_v0.5/help/glossary.html
RAW imaj formatı	:	http://www.forensicswiki.org/wiki/Raw_Image_Format.
SANS	:	https://computer-forensics.sans.org.
SANS Digital Forensic and Incident Response Poster	:	http://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf.
setMACE	:	http://reboot.pro/files/file/91-setmace.
setMACE	:	http://reboot.pro/files/file/91-setmace.
setMACE ve timestompt bu tür programlara örnek olarak verilebilir.	:	http://www.forensicswiki.org/wiki/Timestompvehttp://reboot.pro/files/file/91-setmace.
Shellbag	:	http://computer-forensics.sans.org/blog/2008/10/31/shellbags-registry-forensics.
Shred uygulaması	:	http://linux.about.com/library/cmd/blcmdl1_shred.htm
SODDI savunması örneği	:	http://www.salon.com/2005/11/19/libby_12.
Spam e-posta	:	http://tr.wikipedia.org/wiki/Y%C4%B1%C4%9F%C4%B1n_mesaj
Steganography	:	http://en.wikipedia.org/wiki/Steganography.
Superonline	:	http://www.superonline.net.
Şüphe Tür ve Dereceleri	:	http://cankattaskin.av.tr/?p=11.
Şüpheden sanık yararlanır ilkesi	:	http://www.turkhukuksitesi.com/showthread.php?t=12004.
Şüpheden sanık yararlanır ilkesi anayasa yorumu	:	http://www.anayasa.gov.tr/index.php?l=manage_karar&ref=show&action=karar&id=2416&content=.2007.
Tableau	:	http://www.tableau.com/index.php?pageid=products.

The Admissibility of Electronic Evidence In Court	:	http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf.
The Secure Hash Algorithm Directory MD5	:	http://www.secure-hash-algorithm-md5-sha-1.co.uk/.
Thunderbird	:	http://www.mozilla.org/en-US/thunderbird.
TİB	:	http://www.tib.gov.tr/tr.
Timestompt	:	http://www.forensicswiki.org/wiki/Timestomp
Truecrypt	:	http://www.truecrypt.org.
Truva atı savunması	:	http://en.wikipedia.org/wiki/Trojan_Horse_Defense.
Truva atı savunması	:	http://en.wikipedia.org/wiki/Trojan_Horse_Defense.
Truva atı savunması örneği, DDOS	:	http://www.zdnet.com/the-case-of-the-trojan-wookiee-3039117240.
Truva atı savunması örneği, Pedofili 1	:	http://www.out-law.com/page-3783.
Truva atı savunması örneği, Pedofili 2	:	http://cyb3rcrim3.blogspot.com/2012/08/the-thumbcache-malware-and-child.html
Truva Savaşı	:	http://tr.wikipedia.org/wiki/Truva_Savaşı.
TSK	:	http://sleuthkit.org.
TTNet	:	http://www.ttnet.com.tr/Sayfalar/Ana-Sayfa.aspx.
Twitter	:	https://twitter.com
Ultimate Boot CD for Windows	:	http://www.ubcd4win.com.
Unetbootin	:	http://unetbootin.sourceforge.net.
Unicode karakter listesi	:	bkz.http://unicode-table.com/en/#spacing-modifier-letters
Virtualbox	:	https://www.virtualbox.org.
VMware	:	http://www.vmware.com.
Vodafone	:	http://www.vodafone.com.tr.
What Are Rootkits?	:	http://www.5starsupport.com/tutorial/rootkits.htm.
What Is the Difference: Viruses Worms Trojans and Bots?	:	http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html.
WinBuilder	:	http://winbuilder.net/.
Wipe işlemi yapabilen başlıca ürünler -1	:	http://www.jetico.com/wiping-bcwipe
Wipe işlemi yapabilen başlıca ürünler -2	:	http://eraser.heidi.ie/vePGPWipeolarakbilinmektedir.
X-Ways Forensics	:	http://www.x-ways.net/forensics.
Yahoo	:	https://login.yahoo.com.
Yazılım	:	http://tr.wikipedia.org/wiki/Yaz%C4%B1l%C4%B1m
Yeni Nesil DDoS Saldırıları ve Savunma Yöntemleri	:	http://www.bilgiguvenligi.gov.tr/ag-guvenligi/yeni-nesil-ddos-saldirilari-ve-savunma-yontemleri-i.html.
Zimbra	:	http://www.zimbra.com/products/desktop.html
$I30 dosyası	:	http://computer-forensics.sans.org/blog/2011/09/20/ntfs-i30-index-attributes-evidence-of-deleted-and-overwritten-files.

ŞEKİL LİSTESİ

Şekil 1 - TÜİK İnternet ve Bilgisayar Kullanım Oranları. 1
Şekil 2 - Tableau Forensic Duplicator TD2 cihazı. 11
Şekil 3 - Örnek Encase ekran kopyası 12
Şekil 4 - FTK arayüzü. 13
Şekil 5 - 2,5" ve 3,5" sabit diskler. 20
Şekil 6 - Sabit diskin bölümleri;A: Hat, B: Geometrik Sektör, C: Hat Sektörü, D: Yığın. 20
Şekil 7 - $MFT dosyası. 25
Şekil 8 - AnalyzeMFT yardım komutları 25
Şekil 9 - $MFT dosyasının ayrıştırılması. 26
Şekil 10- $MFT dosyası içeriği. 27
Şekil 11 - $MFTMirr dosyası içeriği. 32
Şekil 12 - Fazlalık alan verileri. 35
Şekil 13 - Olay kayıt dosyaları. 38
Şekil 14 - Kayıt defteri giriş ekranı. 39
Şekil 15- Prefetch dosyaları. 42
Şekil 16 – Hacim gölge servisi verilerine ulaşma. 44
Şekil 17 - "Recent" klasörü ve içindekiler. 45
Şekil 18 - Office kurulumu kullanıcı metaverileri. 47
Şekil 19 - Office ilk açıldığında istenen veriler. 48
Şekil 20 - E-postaların kayıtlı olduğu *.pst dosyası. 51
Şekil 21 - Sanal işletim sistemi ekran kopyası. 53
Şekil 22 - Flame Zararlı Yazılımından Etkilenen Bölgeler. 60
Şekil 23 - Zararlı yazılım türlerine göre yaygınlık oranları. 67
Şekil 24 - Ülkelere göre zararlı yazılımların dağılımı. 68
Şekil 25 - Sahte e-posta örneği. 70
Şekil 26 - Parçalanmış bir sabit disk. 72
Şekil 27 - Geri dönüşüm kutusuna atarak dosya silme işlemi. 74
Şekil 28 - Dosyanın geri dönüşüm kutusundan silinmesi. 75
Şekil 29 - Silinmiş verinin geri döndürülebilmesi. 77
Şekil 30 - Dosya.txt dosyanın temizlenmesi 77
Şekil 31 - Temizlik sornası Dosya.txt'ya ait iz kalmaması. 78
Şekil 32 - Truecrypt ile şifrelenmiş alan. 82
Şekil 33 - Windows NTFS Zaman Değişim Kuralları. 84
Şekil 34 - MFTRCRD ile zaman verilerinin elde edilmesi. 86

Şekil 35 - SetMACE ile tarihin geriye çekilmesi. 86
Şekil 36 - Manipüle edilmiş tarih verilerinin kıyaslanması. 87
Şekil 37 - Windows kayıt dosyalarının devre dışı bırakılması. 90
Şekil 38 - Gizli gezinme özelliği. 91
Şekil 39 - MD5 ve SHA1 hash değeri hesaplatılmış sabit disk imajı. 99
Şekil 40 - P2P ile yayılan bir filmin modellemesi. 111
Şekil 41 - İmaj TD1 logu. 122

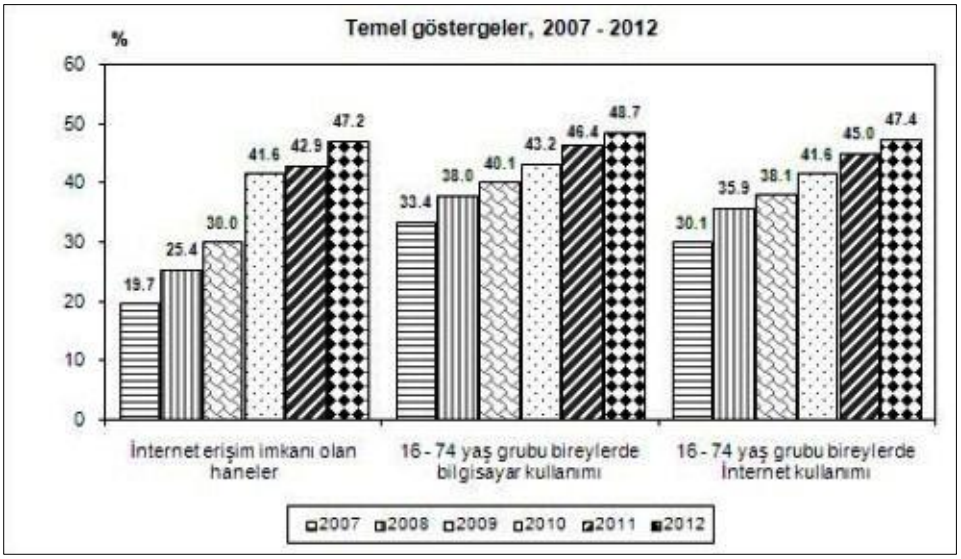
TABLO LİSTESİ

Tablo 1 - $MFT dosyasında bulunan üstveriler 28
Tablo 2 - Kayıt defteri veri grupları 40
Tablo 3 - İnternet geçmişi kullanılarak elde edilen e-posta kayıt örneği..... 50
Tablo 4 - KLM operatörleri ve normalize edilmiş değerler 114
Tablo 5 - KLM işlem değerleri 114
Tablo 6 – Dijital adli delillerin güven seviyeleri sınıflandırması 117
Tablo 7 - Sonuçların güven seviyesi sınıflandırmasıyla açıklanması..... 125
Tablo 8 - Güven seviyesi sınıflandırmasında avantaj ve dezavantajlar..... 128

Zararlı Yazılımların Etkisinde Dijital Adli Delillerin Güvenilirliği

§1. Giriş

Kişisel bilgisayarlar ve akıllı telefonların yaygınlaşması, fiber internet ile son kullanıcılara 100 Mbps ve daha hızlı internet erişim imkânlarının sunulması ve 3G ile hemen her yerden kablosuz internet erişimin makul fiyatlara inmesiyle, zaten genç olan ülke nüfusunun bilişim teknolojileri imkânlarından faydalanma oranı gün geçtikçe yükselmektedir. TÜİK'in 2012 yılı verilerine bakıldığında, 16–74 yaş arası bireylerde bilgisayar kullanımının son 5 yılda %50'den fazla artış gösterdiği anlaşılmaktadır[1].



Şekil 1 - TÜİK İnternet ve Bilgisayar Kullanım Oranları.

Bilgisayar ve internet kullanımının bu derece hızla yaygınlaşması, toplumun yaşam alışkanlıkları ve iş yapış tarzlarında da ciddi değişikliklere neden olmaya başlamıştır. Gündelik hayatta not tutulan kâğıt defterler yerini Microsoft Word veya Onenote vb. metin işleme programlarına, akıllı telefonların kişisel not

[1] Hane halkı bilişim teknolojileri kullanım araştırması, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=10880, erişim tarihi: 07.01.2013.

uygulamalarına ve hatta internet üzerinden erişilebilen çeşitli servislere bırakmaktadır.

Kimlik kartlarının yerini elektronik imza vb. teknolojilerin, baskı fotoğrafların yerini dijital resim dosyalarının ve not kâğıtlarının yerini çeşitli bilgisayar uygulamalarının almasıyla birlikte kritik bir soru gündeme gelecektir.

Bu dijital delillere ne kadar güvenilebilir?

I. Analiz aşamasında dijital adli deliller

Özel inceleme ve analiz teknikleri kullanılarak bilgisayarlar başta olmak üzere, tüm elektronik medya üzerinde yer alan potansiyel delillerin toplanması amacıyla, elektronik aygıtların incelenmesi sürecine kısaca *Dijital Adli Bilişim* (Computer Forensics) denilmektedir. Adli bilişim çalışmaları birkaç farklı adımdan oluşan bir süreçler bütünüdür. Toplama, inceleme, analiz ve raporlama adımları bu çalışmaların genel hatlarını teşkil etmektedir[2].

İnceleme ve analiz çalışmalarının temelinde, dijital adli delillerin ortaya çıkarılması işlemleri bulunmaktadır. Adli delillerin bulunması ve belirlenmesinin ardından analiz aşamasına geçilir ve konuya ilişkin olarak bilirkişiden talep edilen çalışmalar başlatılır.

Dijital adli delillerin tespiti sonrasında en sık gündeme gelen soru, bu delillerin kime ait olduğu bilgisidir. Örnek olarak ilgili dijital delil Windows ortamında tespit edilen bir yazı dosyasıysa, bu dosyanın;

- Hangi tarihte oluşturulduğu, değiştirildiği, erişildiği veya bilgisayara geldiği (MACE olarak kısaltılan bu veriler hakkında detaylı bilgi NTFS dosya sistemi kaynaklarında bulunabilir[3])
- Kim tarafından oluşturulduğu,
- Kim tarafından değiştirildiği,
- En son kim tarafından açıldığı veya kimlerin bilgisayarında bulunduğu,

[2] Adli Bilişim, CMK 134 ve Düşündürdükleri, http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html, erişim tarihi: 07.01.2013.
[3] MACE, http://whereismydata.wordpress.com/2009/02/14/dates-ntfs-created-modified-accessed-written, erişim tarihi: 07.01.2013.

- Analiz yapılan dijital deliller bir sabit diskte ise, bu sabit disk kullanıcısının bu dosyayla ilişkisi,
- Dijital adli delilin bulunduğu sabit diskte herhangi bir zararlı yazılım aktivitesi bulunup bulunmadığı,
- Zararlı yazılımların bu dosyayla herhangi bir ilişkisinin olup olmadığını tespiti,
- Dijital delillerin bulunduğu sabit diskte herhangi bir delil karartma işleminin (geri dönüşümsüz dosya silme (wipe[4]), dosya yazar ve tarih bilgilerinin manipülasyonu vb.) olup olmadığı,
- İlgili dosyanın $MFT, $LogFile, $INDX, $I30 [5] vb. gibi sistem dosyalarında izi olup olmadığı, bu izlerin hangi tarihlerde oluştuğu,
- Dijital delilin alındığı bilgisayar kullanıcısının teknik yeteneklerinin tespiti,
- İlgili bilgisayarda bulunan diğer yazılımlar ve dosyaların incelenen dijital delil ile ilişkisi,
- Dijital delilin toplandığı bilgisayarın antivirüs ve güvenlik duvarı kayıtları,
- Yukarda sıralanan bütün bilgilerin varlığının ve yokluğunun sorgulanması, şüpheli bir durum olup olmadığını tespiti

Gibi çeşitli bilgiler araştırılacaktır. Yapılacak tespitler neticesinde ilgili dijital delilin; isnat edilen iddiaları içerdiği/içermediği, delilin orijinalliği, delilin bulunduğu bilgisayar kullanıcısının bilgisi dâhilinde olup olmadığı, bilgisayar kullanıcısı tarafından herhangi bir işleme tabi tutulup tutulmadığı gibi neticeler ortaya çıkacaktır.

Görüldüğü üzere gerek delilin tespitine gerekse bulguların yorumlanmasına etki edecek çok sayıda unsur bulunmaktadır. Bu aşamada dijital adli analizi gerçekleştiren bilirkişinin teknik bilgisi ne kadar derin olursa olsun, raporlama ve mahkemeye sunma esnasında bazı noktalar dikkat etmek gerekecektir.

---

[4] Data Erasure, http://en.wikipedia.org/wiki/Data_erasure, erişim tarihi: 07.01.2013.

[5] I30, http://computer-forensics.sans.org/blog/2011/09/20/ntfs-i30-index-attributes-evidence-of-deleted-and-overwritten-files, erişim tarihi: 07.01.2013.

II. Bulguların raporlanması ve delil güvenilirliği

Teknik analiz yapıldıktan ve çalışma tamamlandıktan sonra geçilecek olan aşama, bulguların raporlanmasıdır.

Hazırlanacak rapor, bir dijital adli analiz çalışmasının sonucu olduğundan bazı noktalara dikkat edilmesi gerekecektir. Özet olarak;

- *Giriş Bölümü:* Çalışma hakkında genel bilgilerin bulunduğu; kapsamın, delillerin ve analizi istenen soruların belirtildiği,
- *Çalışma Özeti:* Gerçekleştirilen çalışmanın hangi dijital bulgulara yönelik olduğu, nasıl bir metodolojiyle çalışıldığı,
- *Detaylı Analiz Bulguları:* Çalışma hakkındaki tüm detaylar ve bulgular,
- *Sonuç:* Bulguların ne anlama geldiği, dijital delillerin incelemesi talep edilen bulguları içerip içermediği

Gibi ana başlıkların raporda yer alması gerekmektedir. Hazırlanacak raporun; bütün soruları cevaplandığından, tespit edilen bulgularla ilgili yeterli ekran kopyası, çıktı, fotoğraf vb. delilleri içerdiğinden ve mümkün olduğu ölçüde raporu okuyacak tarafın anlayabileceği dilde yazıldığından emin olunmalıdır. Raporlama aşamasının dijital adli analiz süreçlerindeki yeri ile ilgili detaylı bilgiler sonraki bölümlerde etraflıca ele alınacaktır.

Dijital adli analiz çalışmaları, birçok zaman gayet anlaşılır ve raporlanabilir sonuçlara ulaşmaktadır. Söz gelimi, bir kamera kayıt sisteminden özel bir alanın silinip silinmediği tespit edilebilirse bunu raporlamak zor olmayacaktır. Sonuç bilgisayar dilindeki 1 veya 0 kadar nettir. Ancak bazen dijital adli analiz çalışmaları oldukça karmaşık olayların incelenmesini gerektirir. Ayrıca dijital adli analiz çalışmalarında; işletim sistemi ve uygulamaların sürüm bilgisi, uygulama profili, işletim sisteminin bulunduğu zaman dilimi ve farklı yapılandırma ayarları gibi birçok nedenden ötürü çok yoğun şekilde istisnai durumlarla karşılaşılmaktadır. Bazı durumlarda dijital adli analiz çalışmalarında o kadar çok istisna yaşanabilir ki, genel geçer bir kurallar bile tanımlanamaz veya uygulanamaz.

Gerek dijital delilin sağlığını ve güvenilirliğini etkileyebilecek çok sayıda faktör, gerekse yukarda bahsedilen istisnai durumların tek tek ele alınması gerekliliği, analiz sonucundaki bulguları ve dolayısıyla hazırlanacak raporda kullanılacak ifadeleri doğrudan etkileyecektir.

Yukarıda bahsedilen istisnalara ve dijital adli analiz uzmanlarının düşebileceği muhtemel hatalara çeşitli örnekler verilebilir. İncelenen bilgisayarın sistem saati doğru olmayabilir, zaman-tarih verileri yanlış yorumlanmış olabilir, internet erişim kayıt bilgilerindeki IP adresi bir *vekil sunucu* (proxy) üzerinden geliyor olabilir ve böylece gerçek IP'yi göstermeyebilir, incelenen bir dijital dosyanın zaman tarih verileriyle oynanmış olabilir ve bu değişiklik kullanıcının kendisi tarafından yapılmış olabileceği gibi bilgisayarda bulunan bir zararlı yazılımla da yapılmış olabilir. Bu listeyi uzatmak mümkündür. Görüldüğü üzere herhangi bir dijital delilin doğru yorumlanmasına engel teşkil eden çok çeşitli durumlar bulunmaktadır.

Bu gibi nedenlerle dijital adli analiz çıktılarının belirli güven seviyelerine göre sınıflandırılması ihtiyacı gün geçtikçe kendini göstermektedir [6]. Bu çalışmanın sonunda, gerek zararlı yazılımların gerekse delil karartma işlemlerinin etkisine maruz kalmış dijital adli delillerin güvenilirliklerini sınıflandırmak için niceliksel bir yaklaşımla çözüm önerileri sunulacaktır. Ayrıca dijital adli çalışmalarında karşılaşılan çeşitli problemlere yönelik çözüm önerileri de tartışılmış olacaktır.

[6] Eoghan Casey, Digital Evidence and Computer Crime, Maryland 2011 ("Casey"), sf. 69.

§2. Dijital adli analiz çalışmaları

Bütün adli araştırmalar gibi dijital adli analiz araştırmalarının da temel hedefi gerçeği ortaya çıkarmaktır. Bu alandaki gerçeklik, "dijital verilerle ilişkili soruşturmalarda mahkemelerin öğrenmek istediği durumların net olarak tespiti ve karar vericilere sunulması" olarak belirtilebilir. Giriş bölümünde de değinildiği üzere, dijital adli deliller yargılama safhasında her geçen gün daha çok ihtiyaç duyulan bir bilgi kaynağı olmuştur. Kimi zaman masum insanların uzun yıllar mahkûmiyetine neden olabilecek tespitlerin yapıldığı bu analizler, kimi zaman gerçek suçluların arkasına saklanabildiği bir platform halini almaktadır. İşte bu nedenlerle dijital adli analiz, yargılama süreçlerini ve dolayısıyla verilecek kararları önemli ölçüde etkileyebilecek bir öneme haizdir.

Dijital adli analiz çalışmaları, analizi yapılan teknolojiye ve ortama göre ister istemez farklılık gösterecektir. Teknolojik çeşitlilik arasında masaüstü bilgisayarlar, tabletler, akıllı telefonlar ve bu cihazların üzerinde koşan farklı Windows, Linux, Unix, BSD gibi farklı işletim sistemleri sayılabilir. Bununla birlikte bir de incelemenin hangi kapsamda değerlendirileceği bulunmaktadır ki, bunlara da örnek olarak sivil, ticari, askeri ve organize suçlara ilişkin araştırmalar örnek verilebilir. Görüleceği üzere farklı ortamlarda ve farklı teknolojilerde çok sayıda örnekle karşılaşılabilmektedir. Sıralanan bu çeşitliliğe rağmen, çoğu inceleme birçok ortak özelliğe sahiptir. Bu nedenle dijital adli analiz çalışmalarında bir takım süreç modelleri ve yaklaşımlar geliştirilmiş bulunmaktadır.

I. Dijital adli analiz süreçleri

Son zamanlarda birçok kurum kuruluş, dijital adli analiz çalışmalarına yön verecek süreç tanımlama gayretleri göstermektedir. Çalışmanın geçirileceği safhaların tespiti, izlenecek metodolojinin teknik ve hukuki boyutlarının eşgüdümlü ilerlemesi ve bütün tarafların bu yaklaşımı benimsemesinin sağlanması, önerilen her bir yaklaşım için önemli isterlerdir. Bununla birlikte

tanımlanacak süreçlerde dijital adli analizin faydasının gözetilmesi, herhangi bir dayatma içermemesi temel hedeflerdendir. Dijital adli analizde her bir yeni çalışma, kendine has ve daha önce hiç karşılaşılmamış durumları inceleyebilir. Bu nedenle süreçler ancak bir ana çatı gibi algılanmalıdır.[7] Sınırları kesin olan ve çalışmayı katı kurallarla yönlendirerek bilirkişilere hareket imkanı tanımayan bir süreç, dijital adli analiz biliminde kendine yer bulamaz.

A- Taraflar

Dijital adli analiz bilimiyle uğraşan birçok kurum, kuruluş, dernek ve organizasyon bulunmaktadır. Kimi zaman konferanslar düzenleyerek bilgi paylaşımında bulunan, kimi zaman ise etkin katılımlı e-posta gruplarıyla faaliyetlerini sürdüren ve daha çok yurtdışı menşeli bu gibi topluluklar *dijital adli analiz* (digital forensics) ve *olay müdahalesi* (incident responce) çalışmalarında izlenebilecek metodolojiler hakkında çeşitli önerilerde bulunmaktadır.

Bu kuruluşlara örnek olarak DFRWS[8], National Institute of Justice[9] (NIJ) ve SANS[10] verilebilir. Bu otoritelerin önerdikleri süreç modellerinde bazı ufak farklılıklar olmakla beraber, ana başlıklarının oldukça benzer olduğu söylenebilir.

B- Süreç modelleri

Dijital adli analiz çalışmaları ve olay müdahalesinde takip edilen evreler; hazırlık, inceleme/tespit, koruma/saklama, analiz ve raporlama olarak 5 başlıkta incelenebilir[11].

---

[7] *Casey*, sf. 69.
[8] DFRWS, http://www.dfrws.org/index.shtml, erişim tarihi: 07.01.2013.
[9] NIJ, http://www.nij.gov/topics/forensics/welcome.htm, erişim tarihi: 07.01.2013.
[10] Computer Incident Response, http://www.sans.org/course/advanced-computer-forensic-analysis-incident-response, erişim tarihi: 07.01.2013.
[11] *Casey*, sf. 189.

1. Hazırlık

Başarılı bir dijital adli analiz çalışması için plan oluşturma safhasıdır. Gerekli materyaller ve kaynaklar bu evrede hazırlanır, olaya özgü nasıl bir yaklaşım sergileneceği bu aşamada kararlaştırılır.

2. Tespit

İlk tetkiklerin yapılacağı, delillerin kaynağı ve tipine göre ilk araştırmaların vuku bulacağı evredir. Dijital delilin hangi kaynaktan geldiği öğrenilir ve türüne göre yapılacak çalışma için ihtiyaç duyulan detaylar netleştirilir. Örnek vermek gerekirse delilin Internet üzerinden gelmesi, suç organizasyonun tespit edilmesi veya tekil bir suç mahallinin bulunuyor olmasına göre farklı yaklaşımlar sergilenecektir. Tespit aşamasında dikkat edilmesi gereken bir diğer konu, delillerin ihtiyaç analizinin yapılmasıdır. Arama esnasında tespit edilen bütün bilgisayarlar, taşınabilir bellekler, CD-DVD vb. elektronik kayıt ortamlarının el konulmasından ziyade, sadece ilgili olan delillerin toplanması esastır. Hazırlık aşamasında yapılacak bir risk değerlendirmesi bu bağlamda çalışmaları kolaylaştıracaktır[12].

3. Koruma

Bu adım, dijital adli delillerin korunması ve saklanması adımlarını içinde barındırır. Delil toplama ve imaj alma gibi faaliyetler bu başlığın altında incelenmektedir. Örnek vermek gerekirse; olay mahallenin tespitinin ardından, hali hazırda açık olan bir bilgisayarın varlığı anlaşıldığında bu bilgisayarın açık halde imajının alınması gerekmektedir. Bunun nedeni *bellekte* (memory) bulunan delillerin kaybolması ihtimalinin engellenmesidir [13] . Açık olan bilgisayarı kapatmamak, kapalı olan bilgisayarı açmamak ve cep telefonu gibi sürekli

[12] Leyla Keser Berber, Adli Bilişim (Computer Forensic), İstanbul 2004 ("Berber"), sf. 188.
[13] Bellek Analizi, http://computer-forensics.sans.org/blog/2011/07/21/live-mem-forensic-analysis, erişim tarihi: 07.01.2013.

kablosuz iletişim halinde olan cihazları faraday kafesi[14] gibi ekstra koruma kalkanları kullanarak toplamak verilebilecek diğer örnekler arasındadır.

4. Analiz

Konuyla ilgili detaylı incelemenin yapıldığı evredir. Bir önceki adımda elde edilen dijital adli deliller, konuyla ilişkili olarak bu adımda incelenir. Bu adımda dikkat edilmesi gerek bir diğer husus; dijital adli analizin *tetkik* (examination) ve *analiz* (analysis) aşamalarının birbirinden farklı olmasıdır. Burada tetkik ifadesi dijital adli delillerin tespiti, ortaya çıkarılması ve analize uygun hale getirilmesi anlamında gelmektedir. Analiz ise elde edilen ve ortaya çıkarılan bu bulguların konuyla ilgili olarak çözümlenmesi anlamında gelmektedir. Analiz aşamasında kim, ne, nerede, neden, nasıl ve niçin gibi soruların cevapları aranmalıdır.

Tetkik ve analizin farklılığı noktasında bilirkişiler ile karar verici hâkimler arasındaki ilişki bir sonraki bölümde irdelenecektir.

5. Raporlama

Tespit edilen bulguların, araştırma yapılan konu hakkında bilgi verici ve konuyla ilgilenen teknik olmayan kişilerin de anlayabileceği bir dilde hazırlanıp sunulması adımıdır. Askeri davalar, ticari suçlara ilişkin davalar veya organize suç örgütleriyle ilişkili soruşturmalara göre farklı teknik yoğunlukta hazırlanabilecek raporların, temelde incelemeye konu edilen dijital adli delillerin talep edilen (müzekkere) sorulara yeterli ölçüde cevap verip vermediği esastır. Raporlamada önemli bir unsur da kullanılan dildir. Her ne kadar teknik bulguların teknik olmayacak içerikte yazılması zor olsa da, hedef olabildiğince sade yazmaktır. Ancak kısaltılamayacak kadar teknik karmaşıklık içeren dijital adli analiz çalışmaları, elbette herkesin anlayamayacağı bir içeriğe sahip olabilir. Bu noktada raporu inceleyecek kişilerin dijital adli analiz ve bilgisayar teknolojilerinden anlayacak şekilde kişisel gelişim göstermeleri en güzel çözüm olacaktır.

[14] Faraday Kafesi, http://tr.wikipedia.org/wiki/Faraday_kafesi, erişim tarihi: 07.01.2013.

Yukarıda sıralandığı üzere dijital adli analiz araştırmalarında kullanılan ve kullanılması gereken süreç modelleri 5 ana başlıkta toplanmaktadır. İncelemesi yapılan duruma göre bir takım farklılıklar göstermekle birlikte, dünyada kabul gören metodoloji bu şekildedir.

II. Kullanılan araçlar

Dijital adli analiz araştırmalarında çalışmayı yapan uzmanın işini kolaylaştıracak ve kısa zamanda sonuç almasını sağlayacak çeşitli araçlar bulunmaktadır. Bazı yazılımların ücretli, bazılarınınsa ücretsiz olarak kullanılabildiği bu araçlar sayesinde hem dijital adli analiz alanında ortak bir yaklaşım sergilenebilmekte, hem de incelemeyi yapan uzmanın gerçekleştirmekte zorlanacağı işlemler kolaylaşmaktadır.

Dijital adli analiz araçlarını kullanabilmek ile dijital adli analiz uzmanı olmak arasında ciddi farklar bulunmaktadır. Bir uygulamayı ve özelliklerini öğrenmek birkaç haftada tamamlanabilecek bir çalışma isterken, konusuna hâkim bir adli bilişim uzmanı olmak ise belki yıllar alır. Bu nedenle aşağıda belirtilen uygulamaları öğrenmek bir dijital adli analiz uzmanı için önemli olabilir, ancak salt bu yazılımlar ile bir sonuca varmak mümkün olmayacaktır.

A- Lisanslı ürünler

Dijital adli analiz incelemelerinde kullanılan ve uluslararası kabul gören çeşitli lisanslı ürünler bulunmaktadır. Bunlardan en sık karşılaşılan ve kabul gören ürünler ve genel özellikleri aşağıdaki gibidir.

1. Tableau

İmaj alma işlemlerinde sıklıkla kullanılan Tableau[15] ürünleri, donanım seviyesinde veri kopyalama yaparak dijital delillerin değişmezliğini sağlamak ve bilirkişilerin incelemesi esnasında kullandıkları disklerin, orijinaliyle birebir aynı olduğuna emin olmak için kullanılmaktadır. Kopyası alınan diskin, kopyası alınan

[15] Tableau, http://www.tableau.com/index.php?pageid=products, erişim tarihi: 07.01.2013.

diskle birebir aynı olması, cihazın *yazma koruma* (write blocker) özelliği sayesinde mümkün olur. Böylece orijinal diskte hiçbir değişiklik yapılmamış olacaktır. Donanım seviyesinde veri kopyalama, imajı alınacak orijinal sabit diskin cihazın *sadece okunabilir* (read only) tarafında takılması, verilerin kopyalandığı yeni diskin ise cihazın diğer ucuna takılması ile gerçekleştirilir[16]. ABD merkezli GuidanceSoftware şirketinin bir ürünü olan Tableu TD1 ve yeni versiyonu TD2, bu özellikleriyle dijital adli analiz aracı olarak imaj alma işlemleri için kullanılan, yazılım ve donanım halde komple bir üründür.

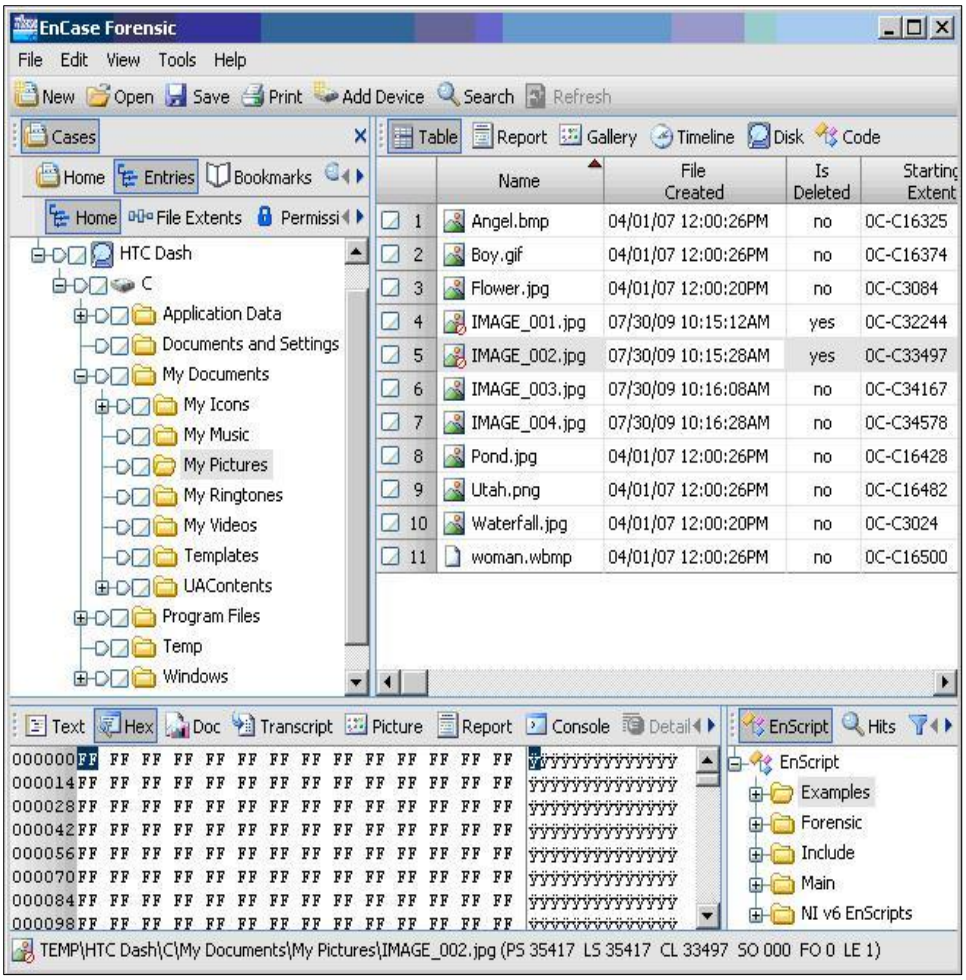
Şekil 2 - Tableau Forensic Duplicator TD2 cihazı.

2. Encase

Encase[17], dijital adli analiz alanında en popüler uygulamalardan biridir. Dijital adli analiz çalışmalarının omurgasını teşkil eden delillerin ortaya çıkarılması ve analiz edilmesi adımlarında, çalışmayı yapacak uzmanlara yardımcı

[16] Bkz. "Şekil 2 - Tableau Forensic Duplicator TD2 cihazı", sf. 21.
[17] Encase, http://www.guidancesoftware.com/encase-forensic.htm, erişim tarihi: 07.01.2013.

olur. Ürünün temel fonksiyonları arasında dijital delillerin imajının alınması, bulguların içinde derinlemesine arama yapılabilmesi, sık yapılan işlemlerin Enscript betikleriyle otomatize edilmesi ve yazılımın ürettiği delil imajlarının (LEF, E01) birçok ülkede yargı organları tarafından kabul görmesi sıralanabilir. Encase; kolay kullanımı ve orta ölçekli sistemlere yük getirmeden kullanılabilme özelliği ile sektörde en sık karşılaşılan ürün olma özelliğini taşır.



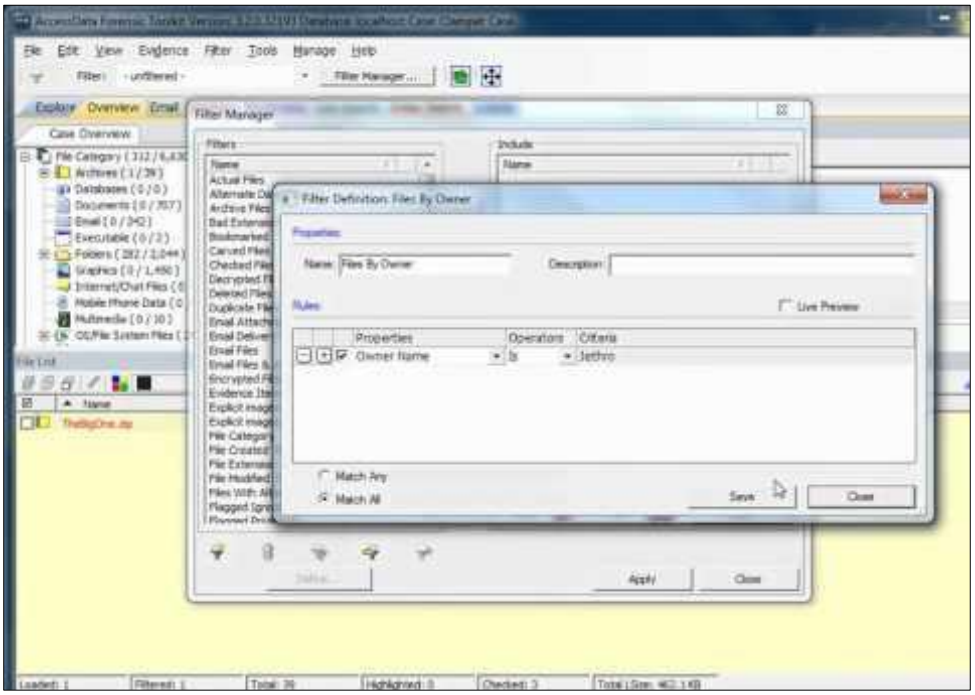
Şekil 3 - Örnek Encase ekran kopyası

3. FTK

Dijital adli analiz uzmanlarının faydalandığı bir diğer uygulama ise FTK[18] isimli programdır. Encase ile birçok konuda benzeşen bu ürün, delilleri

[18] FTK, http://www.accessdata.com/products/digital-forensics/ftk, erişim tarihi: 07.01.2013.

veritabanına kaydetmesi ve otomatize işleri kolayca yönetilebilmesi nedeni ile adli bilişim uzmanları tarafından yaygın olarak kullanılmaktadır. FTK Imager alt uygulaması ile dijital delillerin hızlıca incelenebilir hale gelmesine yardımcı olmakta, aynı zamanda hash tespiti yapma ve *ham* (raw) imajların[19] kolayca okunabilmesini sağlamaktadır.



Şekil 4 - FTK arayüzü.

4. X-Ways Forensics

Bir diğer dijital adli analiz uygulaması olan X-Ways Forensics[20], daha az kaynak tüketen ve böylece daha düşük kapasiteli kişisel bilgisayarlarda da rahatlıkla çalışabilen bir uygulamadır. Rakiplerine nazaran uygun maliyet avantajına sahip olsa da, teknik yetkinlikler açısından gelişime açık bir üründür.

[19] RAW imaj formatı, http://www.forensicswiki.org/wiki/Raw_Image_Format, erişim tarihi: 07.01.2013.
[20] X-Ways Forensics, http://www.x-ways.net/forensics, erişim tarihi: 07.01.2013.

5. Oxygen Forensic Suite

Oxygen Forensic Suite[21], hızla yaygınlaşan akıllı telefonlar ve tablet bilgisayarların oluşturduğu ihtiyaca binaen, mobil cihazlarda delil imajı alma ve analiz çalışmaları için konusunda gelişmiş bir üründür. 6000'den fazla cep telefonu modeli desteğiyle öne çıkmaktadır.

B- Açık kaynak kodlu ürünler

Açık kaynak kodlu ürünler, gerek adli bilişim konusunda eğitim alan öğrenciler ve öğretmenleri tarafından, gerekse yüksek lisans bedelleri ödemek istemeyen ve bu alanda bilimsel araştırma yapan uzmanlar tarafından sıklıkla tercih edilmektedir. Adli analiz çalışmalarından karşılaşılabilecek birçok özel durum için pratik betikler sunan bu uygulamalar, veri sınıflandırması ve tarih sıralaması gibi işlemler için sıklıkla başvurulan programlar olmaktadır.

1. SIFT Linux işletim sistemi

Bir Linux işletim sistemi olan SIFT, SANS[22] uzmanları tarafından en gerekli dijital adli analiz araçlarının içinde bulunduğu ücretsiz bir dağıtımdır. SANS'ın adli bilişim eğitimlerinde de kullandığı bu işletim sistemi ile birçok adli analiz çalışması gerçekleştirilebilmektedir. İçerdiği uygulamalardan bazıları; The Sleuth Kit (TSK), log2timeline, Autopsy ve PyFLAG olarak sıralanabilir.

2. The Sleuth Kit (TSK)

Kısa adıyla TSK olarak anılan The Sleuth Kit[23], açık kaynak kodlu ve ücretsiz dağıtılan en bilinir dijital adli analiz uygulamasıdır. Temelde komut satırından çalışan TSK için Autopsy ve DFLabs PTK gibi farklı kullanıcı grafik ara yüzleri geliştirilmiş olup, araştırma yapan uzmanlar bu yazılımlardan rahatlıkla faydalanabilmektedir.

---

[21] Oxygen Forensic, http://www.oxygen-forensic.com/en, erişim tarihi: 07.01.2013.
[22] SANS, https://computer-forensics.sans.org, erişim tarihi: 07.01.2013.
[23] TSK, http://sleuthkit.org, erişim tarihi: 07.01.2013.

3. Log2timeline

Adli bilişimde önemli adımlardan biri de, bulguların kronolojik olarak sıralanmasıdır. Lisanslı veya lisanssız ürünler bu ihtiyacı ancak bir nebze karşılayabilmektedir. Bir bilgisayardan elde edilen bütün verileri zaman tarih verilerine göre sıralamak için en sık kullanılan uygulama ise Log2timeline[24] olarak karşımıza çıkar.

Log2timeline, bir bilgisayarda bulunabilecek çok farklı kaynaklardan veri toplayıp bunları tarih sırasında göre listeler. Böylece, incelenen imajda herhangi bir anda gerçekten ne olduğuna dair fikir edinmek mümkün olabilmektedir. Log2timeline'ın kullandığı kaynaklar arasında olay kayıt defterleri, internet geçmişi dosyaları, dosya üstverileri gibi tarih bilgisi içeren birçok veri kaynağı sıralanabilir.

4. AnalyzeMFT

$MFT dosyası[25], sonraki bölümlerde daha etraflıca inceleneceği üzere, veri depolama ünitelerinde kullanılan dosya sistemlerinden NTFS'in (New Technology File System[26]) bütün dosyaların ve klasörlerin kayıtlarını tuttuğu ve verilere erişim için referans aldığı tabloyu içeren dosya sistemi meta veri dosyasıdır. Bir anlamda NTFS'in merkezidir.

AnalyzeMFT[27] uygulaması, işte bu $MFT dosyasının içindeki verileri okunabilir hale getirerek kullanıcıya sunmaktadır. Bu sayede, $MFT dosyası elde edilen bir sabit disk imajının, bahsi geçen $MFT dosyasında bulunan verileri açığa çıkmış olacaktır. Bu da bilgisayarda bulunan bütün dosyaların, oluşturma, değiştirme, bilgisayara geliş ve son erişim tarihleri de içinde olmak üzere birçok üstveri bilgisinin edinilmesi anlamına gelmektedir.

---

[24] Log2timeline, http://code.google.com/p/log2timeline, erişim tarihi: 07.01.2013.
[25] $MFT dosyası hakkında detaylı bilgi için bkz. "$MFT", sf.24.
[26] NTFS hakkında detaylı bilgi için bkz. "NTFS", sf. 27.
[27] AnalyzeMFT, http://www.integriography.com, erişim tarihi: 07.01.2013.

5. ExifTool

Dijital adli analizde en sık tartışılan ve bahsi geçen konulardan biri de üstveri bilgileri ve bu bilgilerin nasıl yorumlandığıdır. "Veri hakkında veri" olarak özetlenebilen bu bilgiler bilgisayarda bulunan dosyalar hakkında kullanıcı bilgileri, yazar isimleri, dosya versiyon bilgileri ve çok sayıda tarih verisini ihtiva edebilmektedir. DOC, DOCX, PDF, JPEG vb. çok sayıda dosya formatının türüne göre değişebilecek bu üstveriler dijital adli analiz kapsamında oldukça değerlidir. Bu verileri üst bölümde bahsi geçen Encase, FTK vb. lisanslı analiz araçlarıyla elde etmek mümkünse de, ExifTool[28] isimli ücretsiz uygulamayla hızlı ve pratik şekilde de görüntülenebilir. ExifTool, çok hızlı çalışması ve çalışma sonuçlarını CSV[29] ve Excel gibi formatlarda gösterebilme özellikleriyle sıkça kullanılan bir uygulamadır.

III. Analizde kullanılan temel kavramlar

Dijital adli analiz incelemelerinde kullanılan çok çeşitli teknolojiler bulunmaktadır. Adli bilişim, günümüzde bilgisayar dünyasının hemen her alanında kendine yer bulduğu için çok farklı sistemlerinin çalışma prensipleri de adli bilişimin ilgi alanına girmektedir. Adli bilişim incelemelerinde ve inceleme sonunda hazırlanan raporlarda en sık karşılaşılan terimler ve teknolojiler hakkında çeşitli özet bilgiler alttaki gibi sıralanabilir.

A- Dosyalama sistemleri

Farklı işletim sistemlerinin kullandığı farklı tipte dosyalama sistemleri bulunmaktadır. Kullanım alanına, işletim sisteminin performans yönetim yapısına ve *biçimlendirilebilecek* (format) alan boyutuna göre çeşitlenen bu dosyalama sistemleri, dijital adli analiz açısından incelemeyi yapacak uzmanın dikkat etmesi

[28] ExifTool, http://www.sno.phy.queensu.ca/~phil/exiftool, erişim tarihi: 07.01.2013.
[29] CSV, virgülle ayrılmış değerler (comma seperated values) anlamına gelmektedir. Günümüzde birçok metin editörü bu formatı desteklemektedir. Detaylı bilgi için bkz. http://en.wikipedia.org/wiki/Comma-separated_values, erişim tarihi: 07.01.2013.

gereken en önemli noktalardan biridir. Analizi yapılacak diskin dosyalama sisteminin tipine göre, elde edilebilecek veriler değişebilir, bazı veriler kurtarılabilirken bazıları kurtarılamaz durumda olabilir. En sık karşılaşılan dosyalama sistemleri alttaki gibidir.

1. FAT, FAT32

FAT ve FAT32[30], Microsoft Windows işletim sistemlerinin en temel ve ilkel dosyalama sistemleridir. FAT (File Allocation Table) dosyalama sistemi DOS [31] (Disk Operation System) dosyalama sisteminden türetilmiştir ve günümüzde daha çok taşınabilir belleklerde ve düşük hacimli harici disklerde kullanılmaktadır. FAT32 ise FAT tabanlı olmak üzere daha gelişmiş ve kapasite artırımı ile bir takım performans iyileştirmelerinin yapılmış olduğu dosyalama sistemidir. Windows işletim sistemlerinde FAT dosyalama sistemi en fazla 2GB hacimli disklerde kullanılabilirken, FAT32'de bu değer 32GB olmaktadır. Daha büyük sabit disklerin yaygınlaşması sonucu FAT ve FAT32 yetersiz kalmaya başlamış, bir sonraki bölümde açıklanan NTFS dosyalama sisteminin üretilmesi ihtiyacı doğmuştur.

2. NTFS

Yeni teknoloji dosya sistemi (New Technology File Sistem – NTFS[32]) Windows NT, 2000 ve XP işletim sistemleri ile kullanılmaya başlayan yeni nesil dosyalama sistemidir. Günümüzde kullanılan Vista ve Windows 7 işletim sistemleri de NTFS teknolojisini kullanmaktadır. İşletim sisteminin dosya yönetimini nasıl yapacağı, dosyaların nasıl kaydedileceği ve erişileceği gibi bilgiler dosyalama sisteminin temel görevleri arasında yer almaktadır. NTFS, giderek artan disk hacimleri ile ihtiyacı karşılamakta zorlanan FAT ve FAT32[33] gibi dosyalama sistemlerinin yerine gelmiştir.

---

[30] FAT, FAT32; http://en.wikipedia.org/wiki/File_Allocation_Table, erişim tarihi: 07.01.2013.
[31] Everett Errol Murdock, DOS the Easy Way: A Complete Guide to Microsoft's MS DOS, San Pedro CA 1988 ("Murdock"), sf. 54.
[32] Russon Richard ve Fledel Yuval, NTFS Documentation, Boston 2000 ("Richard/Yuval"), sf. 15.
[33] Jason Capriotti, FAT32 vs. NTFS, USA 2000 ("Capriotti"), sf. 6.

3. HFS+

Apple Mac işletim sistemlerinde kullanılmakta olan HFS+[34], HFS'in (Hierarchical File System[35]) yerini almış bir dosyalama sistemidir. Günümüzde Mac bilgisayarları, Iphone, Ipod, Ipad gibi çoğu Apple ürünlerinde HFS+ kullanılmaktadır. HFS+, NTFS dosyalama sisteminden özellikle "silme sonrası geri dönüşüm" konusunda ayrışan özelliklere sahiptir.

4. Ext2, Ext3, Ext4

Açık kaynak kodlu işletim sistemi Linux[36], doğumundan bu yana farklı sistemlerin oluşmasına ve teknolojik gelişmelere öncülük etmiştir. Linux işletim sistemlerinde kullanılan dosyalama sistemleri bu gelişime ayak uydurmuş ve farklı tip ve özelliklerde üretile gelmiştir. Bu işletim sistemlerinde kullanılan en temel ve yaygın dosyalama sistemleri Ext2, Ext3 ve Ext4[37] olarak görülmektedir.

B- Sabit disklerin veri saklama birimleri

Günümüz bilgisayarları bir önceki bölümde ifade edildiği üzere çeşitli dosyalama sistemleri kullanmaktadır. Bu dosyalama sistemleri verinin nasıl yönetileceğine ve erişileceğine dair yönergelerden oluşmaktadır. Bununla birlikte, dosyalama sistemlerinin üzerinde çalıştığı ve verilerin ilgili alanlarda saklanmasıyla ilgili çeşitli kavramlar bulunmaktadır.

Bilgisayarlarda verilerin saklandığı fiziksel ortamlara sabit disk (sabit disk) adı verilmektedir. Bir önceki bölümde değinilen "dosyalama sistemleri", sabit diskleri kendi biçimlerine uygun olacak şekilde kullanır. Dolayısıyla her sabit disk, kullanıldığı bilgisayarda bulunan işletim sisteminin dosyalama sistemine göre (NTFS, Ext2 vb.) verileri saklamaktadır.

---

[34] Dr. Philip Craiger, Mac Forensics: Mac OS X and the HFS+ File System, Florida 2005 ("Craiger"), sf. 8.
[35] HFS, http://en.wikipedia.org/wiki/Hierarchical_File_System, erişim tarihi: 07.01.2013.
[36] Linux, http://en.wikipedia.org/wiki/Linux, erişim tarihi: 07.01.2013.
[37] Daniel P. Bovet ve Marco Cesati, Understanding the Linux Kernel Second Edition, Sebastopol CA 2003 ("Bovet/Cesati"), sf 577.

Sabit diskler, boyutlarına göre 2,5" ve 3,5" (Şekil 5) olmak üzere ikiye ayrılmaktadır. 2,5" diskler Laptoplarda, 3,5" diskler ise masaüstü bilgisayarlarda kullanılmaktadır.

Bağlantı noktalarına (port) ve teknolojilerine göre ise farklı kategorilerde sabit disk türleri bulunmaktadır. En sık karşılaşılanlar;

- Integrated Drive Electronics (IDE)
- Serial ATA (SATA)
- Small Computer System Interface (SCSI)
- Solid State Drives (SSD)[38]

Olarak sıralanabilir. Bu disklerden en eski teknolojiye sahip ilkel diskler IDE, biraz daha performanslı ve verimli diskler SATA, dakikada daha fazla dönüş yaparak daha hızlı okunabilen (rpm[39]) SCSI ve dönüş yaparak çalışmayıp yarı iletken teknolojisiyle veri okuma-yazma yapabilen son teknolojiye sahip diskler SSD olarak ön plana çıkmaktadır.

Dijital adli analiz anlamında gerek imajın alınması[40], gerekse alınan imajın incelenmesi anlamında bu diskler arasında bir takım farklar bulunmaktadır. Özellikle SSD diskler, diğer sabit diskler gibi manyetik plakaların üzerine 0 ve 1 bitlerini yazarak işlem yapmadığı için fiziksel veri kurtarma anlamında farklılık göstermektedir. Bu farklılık dışında imajın alınması sonrasında diskler arasında bir farklılık kalmayacaktır.

---

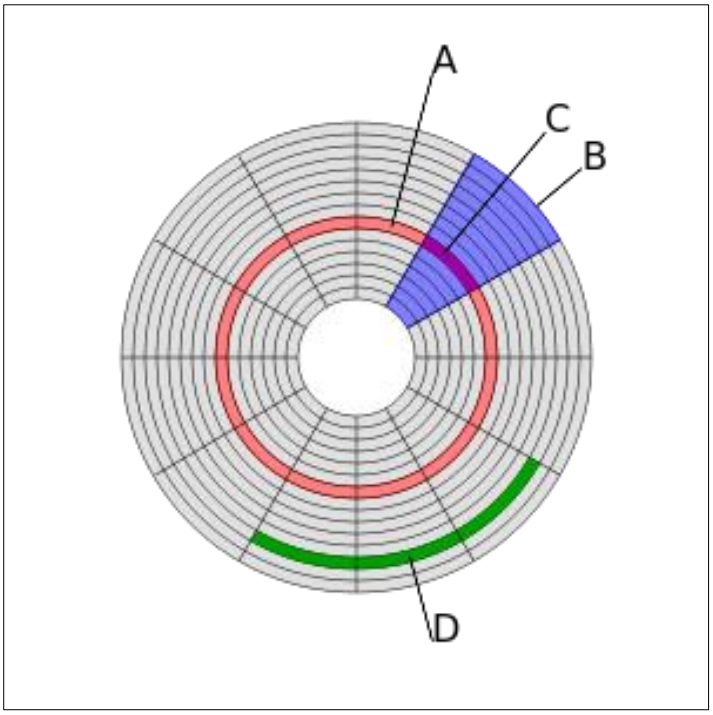
[38] Hard Drive Types, http://www.buzzle.com/articles/hard-drive-types.html, erişim tarihi: 07.01.2013.

[39] "Dakikada dönüş hızı" (Revolutions per minute) kelimelerin kısaltması olan bu ifadenin sabit diskler için yorumu hakkında bkz. Walker C. Blount, Why 7200 RPM Mobile Hard Disk Drives, USA 2007 ("Blount").

[40] İmaj alma işlemleri dijital adli analiz sürecinde "koruma" başlığı altında incelenmektedir. Detaylı bilgi için bkz. "Raporlama", sf. 24.

Şekil 5 - 2,5" ve 3,5" sabit diskler.

Verilerin saklanması ve biçimlendirilmesi anlamında geleneksel sabit disklerde bulunan plakaların detayı için alttaki şekil incelenebilir (Şekil 6). Bu terimlerle ilgili detay bilgiler sonraki başlıklarda incelenmiştir.



Şekil 6 - Sabit diskin bölümleri;A: Hat, B: Geometrik Sektör, C: Hat Sektörü, D: Yığın.

1. *Hat* (Track)

Diskin yüzeyi üzerinde bir turda okunabilecek çembersel iz anlamına gelmektedir. Sabit disklerde bulunan ve disk plakalarını okumayı sağlayan kafa, çembersel bir hareket yaparak bu hattın okunmasını sağlamaktadır. İçerdiği verinin hacminden ziyade sabit disklerin çalışma prensibinden kaynaklanan fiziksel bir tanımı ifade etmektedir.

2. *Geometrik sektör* (Geometrik sector)

Sabit diskin belirli bir açısından hat sektörlerinin bütününü ifade eder. Bu terim de bir önceki gibi verinin hacminden ziyade diskin bölümlendirilmesi amacıyla kullanılmaktadır.

3. *Disk sektörü* (Disk sector)

Disk sektörü, diğer bir ifadeyle sadece "sektör", hat (track) adı verilen disk bölümün en ufak ayrımıdır. Geleneksel biçimlendirmede her bir sektörde 512 byte veya 2048 byte veri bulunmaktadır. Yeni teknoloji sabit disklerde bu değer 4096 byte'a kadar çıkmıştır.

Dijital adli analiz anlamında disk sektörü ifadesi büyük önem taşır. Nedeni ise, diskte bütün verilerin bu alanlar kullanılarak yazılması veya okunmasıdır. Örnek vermek gerekirse, daha önce açıklanan NTFS dosya sisteminde kullanılan bütün dosyalar en ufak veri alanı olarak sektörlerde saklanır. Dijital adli analizde veri incelemesi ve silinmiş verilerin kurtarılması çalışmalarında bir sektörden önceki ve sonraki veriler anlam ifade edebilmektedir.

4. *Yığın* (Cluster)

Yığın(cluster), bir üst başlıkta açıklanan "sektör" terimi ile birlikte en sık kullanılan veri saklama birimidir. Dosya sistemi tarafından yazılabilen en ufak veri alanına işaret etmektedir. Dosya sistemi veri yazarken 1-2-4-8-16 gibi 2'nin

katları sayısında sektör kullanmaktadır.[41] Dolayısıyla dijital adli analizde veri incelemesi yaparken dikkat edilmesi gereken hususlarda biri, ilgili bilgisayarda bir yığının kaç sektörden oluştuğu ve her sektörün kaç byte veri ihtiva ettiğidir.

İşletim sistemleri, bilgisayarda bulunan dosyaları bu yığınlar içine belirli bir algoritmaya göre yerleştirmektedir. Bu algoritma, dosyaların *en uygun* (best-fit) yere yerleştirmesini ve sabit diskin olabildiğince verimli kullanılmasını amaçlamaktadır. Örnek vermek gerekirse, bilgisayarda yeni bir dosya oluşturulduğunda veya başka bir ortamdan yeni bir dosya kopyalandığında, işletim sistemi o dosya için sabit disk üzerinde en uygun yeri bulur ve dosyayı oraya yerleştirir. Büyük dosyalar için farklı yığınlar kullanılabileceği gibi, küçük dosyalar için art arda gelen yığınlar da kullanılabilmektedir. Bu tamamen bilgisayarda bulunan yığınların uygunluğuna ve işletim sisteminin o anda vereceği karara bağlıdır. Bir dosyanın hangi yığında bulunduğu, dosyanın oluşumu esnasında $MFT [42] dosyasına kaydedilmektedir. İlgili dosyaya erişilmesi gerektiğinde, işletim sistemi $MFT dosyasını okuyarak dosyanın hangi yığında tutulduğu bulur ve veriye erişir. Bu sayede yığınlar, işletim sistemi tarafından bilgisayar kullanıcısına içlerinde tutulan veriyi gösterebilmektedir.

5. Paylaştırılmamış yığınlar (Unallocated clusters)

Bir sabit disk ilk kullanımdan önce veya yeni biçimlendirildiğinde, üzerinde bulunan yığınların büyük bir bölümü kullanıma hazır haldedir ve boştur. Bu durumdaki sabit disklerdeki yığınlarda hiçbir veri bulunmamaktadır. Ancak daha önce kullanılmış olan bir sabit diskte, ilgili sabit diskteki veriler silinse veya biçimlendirilse bile eskiye dair veriler yığınlarda bulunmaya devam eder.

Konuyu bir örnek üzerinde açıklamak gerekirse; NTFS dosya sistemi kullanılan ve Windows işletim sistemi üzerinde çalışan bir bilgisayarda bulunan bir dosya silindiği zaman, dosyanın $MFT kaydına o dosyanın silindiğine dair bir işaret konur. Bunun dışında $Bitmap dosyasında saklanan ve o dosyaya ait verilerin hangi yığınlarda tutulduğunu gösteren veriler güncellenir. *Kullanılmakta*

[41] *Casey*, sf. 220.
[42] $MFT dosyası ile ilgili detaylı açıklamalar için bkz. "$MFT", sf. 39.

olan (allocated) yığınlar, *kullanıma hazır* (unallocated) yığınlar olarak işaretlenir. Sonuç olarak o dosyaya ait hem $MFT kaydında hem de dosyanın yığınlarında veri bulunmaya devam eder, ta ki dosyanın üzerine başkaca veri yazılana kadar. Bu nedenle bilgisayarlarda bulunan bir dosya silinse bile geri getirilme ihtimali bulunmaktadır. Bununla birlikte eğer dosya silindiyse ve verilerinin yazılı olduğu yığınların bazılarının üzerine başka veriler yazıldıysa, bu dosyaların bazılarının tamamen, bazılarının ise kısmen geri döndürülebilmesinin altında yatan neden budur.

Sonuç olarak paylaştırılmamış alanlar, işletim sistemi tarafından kullanılmaya hazır halde bekleyen alanları ifade eder. Bu alan boş olabileceği gibi, daha önceden kullanılmış da olabilir. Dolayısıyla paylaştırılmamış yığınların bulunduğu alanda herhangi bir veriye ait kalıntı bulunması, ilgili verinin daha önceden bilgisayarda bulunduğunu ancak silindiğini göstermektedir.

IV. İncelenebilecek kritik veriler

Bir önceki bölümde sıralandığı üzere incelemelerde kullanılabilecek lisanslı veya lisanssız çok sayıda ürün ve teknoloji bulunmaktadır. Bu yazılımlar incelemeyi yapacak uzmanın işini hızlandıran ve kolaylaştıran etmenler olmakla birlikte, elbette uzmanın bilgi birikimi neticesinde her olay için ayrı ayrı incelediği ve araştırdığı verilerle birlikte değerlendirilmelidir. Dijital adli analiz çalışmalarında, özellikle dijital delillerin güvenilirliği noktasında incelenmesi önem arz eden çeşitli sistemsel veriler ve dosyalar bulunmaktadır. Bu verilerde bulunan çeşitli kullanıcı isimleri, sistemsel tarihler ve dosyalara ait üstveriler, detayı ilerleyen bölümlerde tekrar yorumlanacak olan delil güvenilirliği noktasında değerli bilgiler ihtiva edecektir.

A- Dosya sistemi verileri

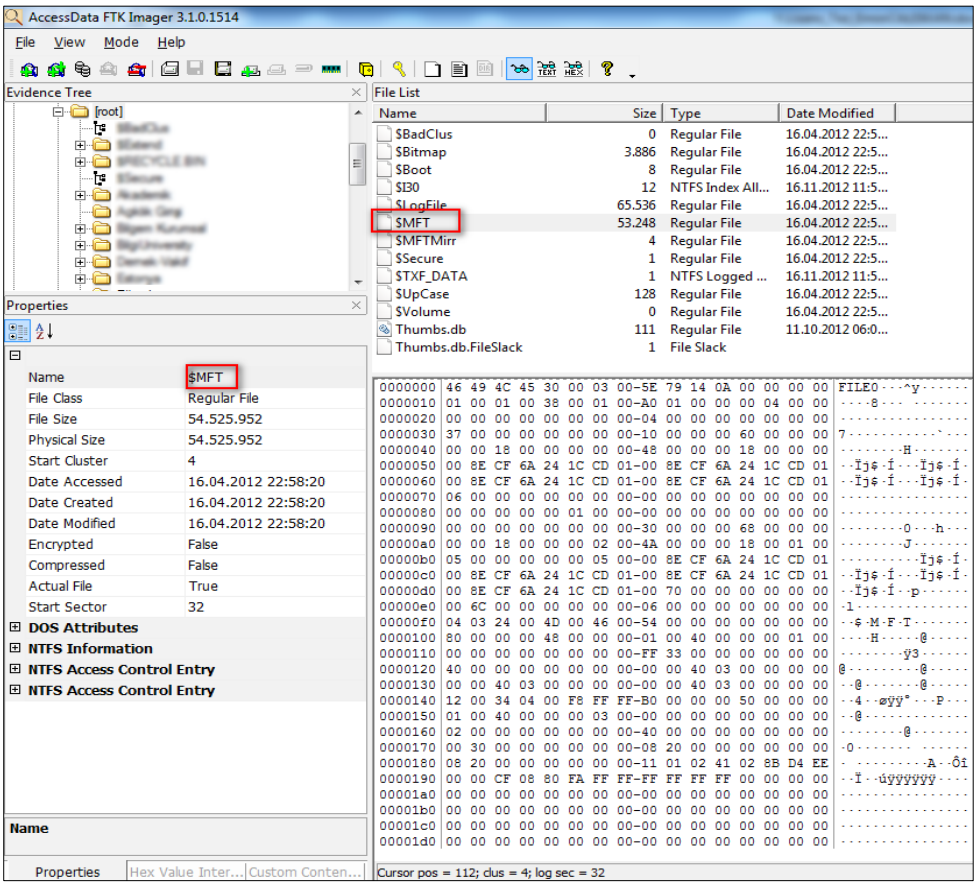
Kişisel bilgisayarlarda en sık karşılaşılan işletim sisteminin Windows olması nedeniyle, dijital adli analiz çalışmalarında da en çok NTFS dosyalama sistemi incelenmektedir. Bu nedenle aşağıdaki başlıklarda NTFS dosyalama

sisteminin temel özellikleri ve bu dosyalama sisteminin yönetiminde kullanılan dosyalar açıklanmış bulunmaktadır.

1. $MFT

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

$MFT tablosu, NTFS ile formatlanmış bir diskteki dosyalar için; dosya isimleri, dosya tarih-zaman bilgileri, dosyaların bulunduğu cluster numaraları, dosya değişken bilgileri (sıkıştırılmış dosya, sadece okunabilir dosya, şifreli dosya vb.) gibi bilgileri ihtiva eder. Dolayısıyla $MFT dosyası incelenerek diskteki bütün dosyalar hakkında yukarda sıralanan bilgiler elde edilebilir. $MFT dosyası, disklerin *kök* (root) dizinlerinde bulunur ve ön tanımlı olarak gizli durumdadır. Ancak bilgili bir kullanıcı tarafından, önceki bölümlerde bahsi geçen Encase, FTK Imager vb. uygulamalarla kolaylıkla görüntülenebilir ve kopyalanabilir. Sonrasında, AnalyzeMFT gibi betiklerle $MFT dosyası okunabilir hale getirilebilir.



Şekil 7 - $MFT dosyası.

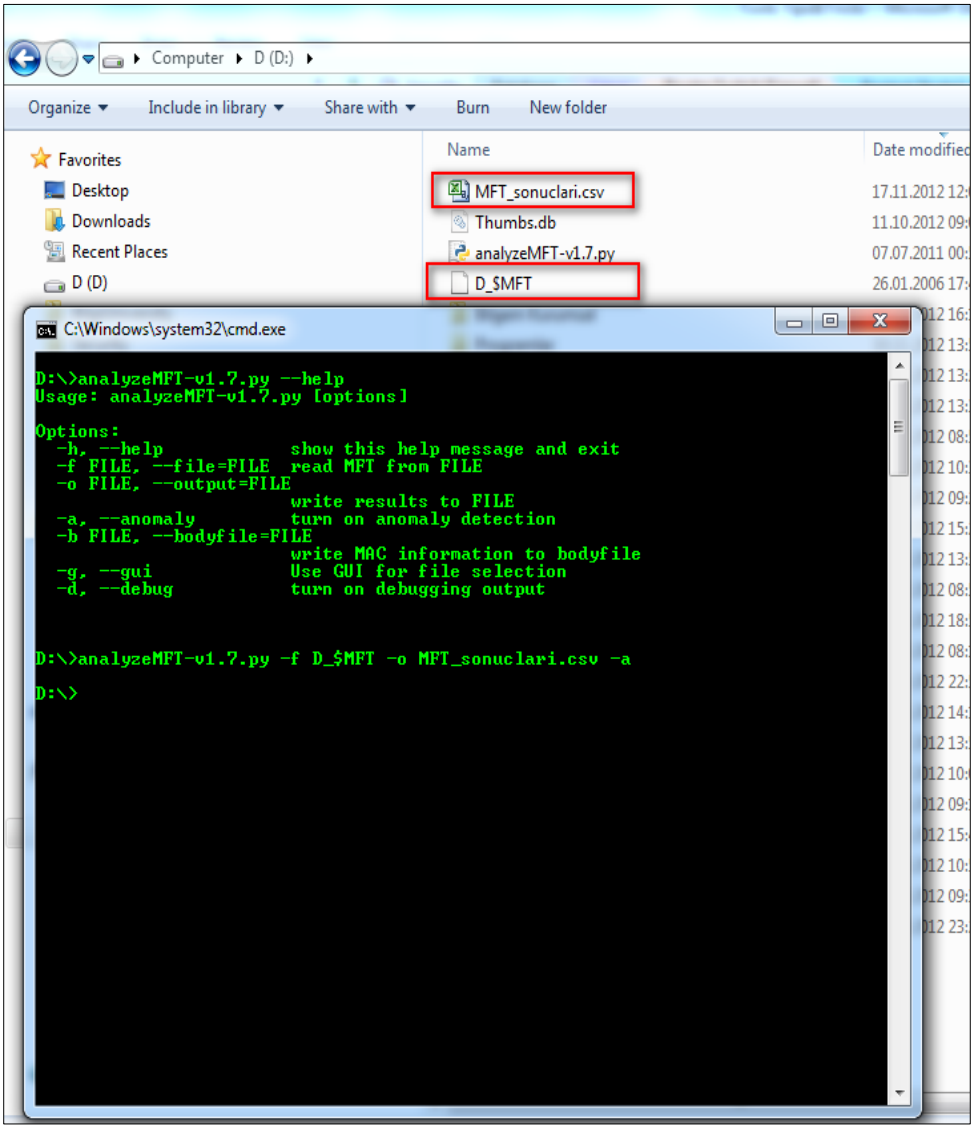
$MFT dosyası, dijital adli analiz araçlarının hemen hepsinde okunabilir şekilde *ayrıştırılabilmektedir* (parsing). Ayrıca bunun ilgili çeşitli pratik yazılımlar da açık kaynak kodlu olarak internette bulunabilmektedir. AnalyzMFT'nin komutlarıyla ilgili bilgi almak için alttaki komut kullanılabilir.

```
D:\>analyzeMFT-v1.7.py --help
Usage: analyzeMFT-v1.7.py [options]

Options:
  -h, --help            show this help message and exit
  -f FILE, --file=FILE  read MFT from FILE
  -o FILE, --output=FILE
                        write results to FILE
  -a, --anomaly         turn on anomaly detection
  -b FILE, --bodyfile=FILE
                        write MAC information to bodyfile
  -g, --gui             Use GUI for file selection
  -d, --debug           turn on debugging output
```

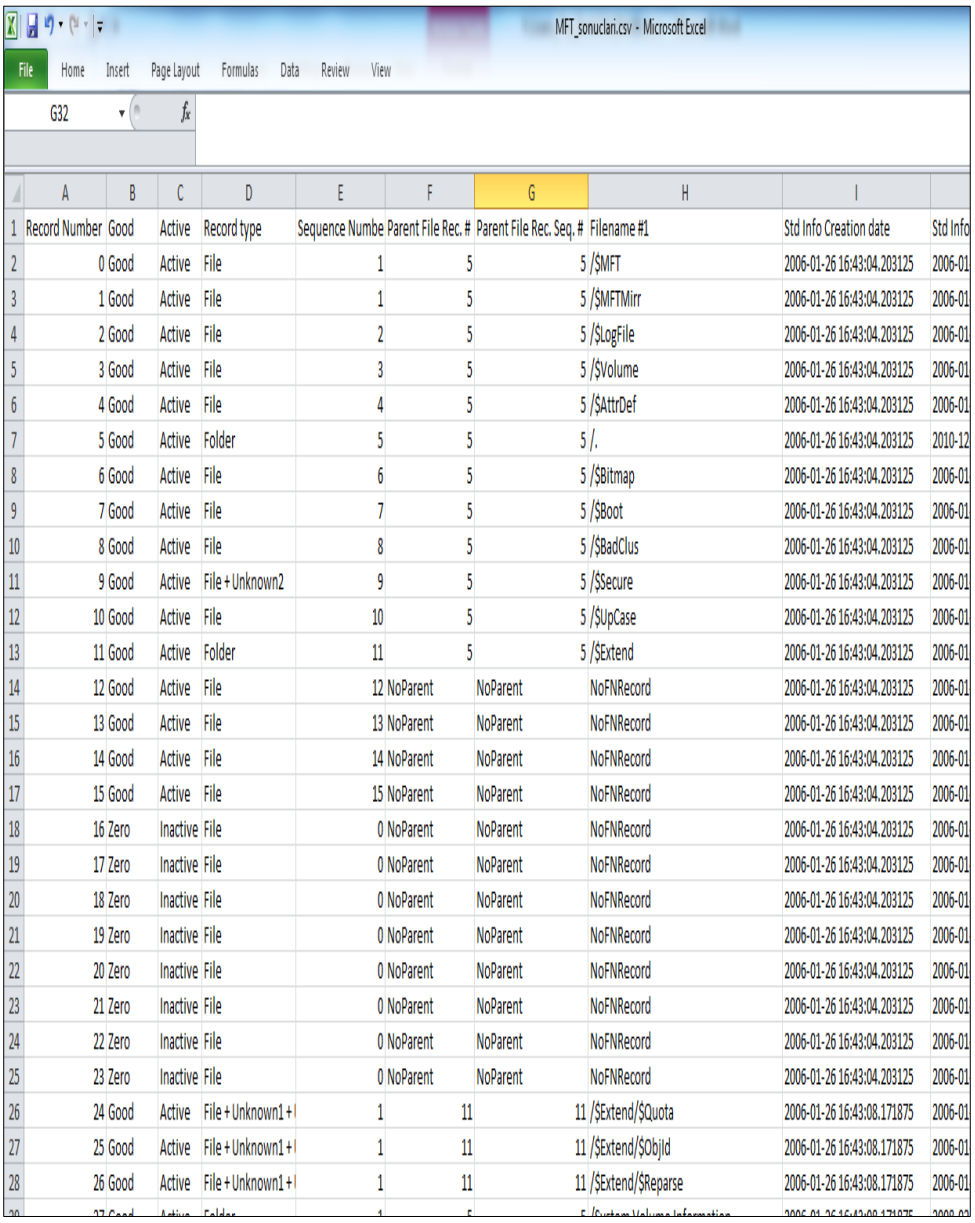
Şekil 8 - AnalyzeMFT yardım komutları

Bu komutlarla ayrıştırma işlemi alttaki gibi yapılabilir.



Şekil 9 - $MFT dosyasının ayrıştırılması.

Çalıştırılan betik sonucunda MFT_sonuclari.csv isimli bir dosya oluşturulmuş durumdadır.



MFT_sonuclari.csv - Microsoft Excel

File | Home | Insert | Page Layout | Formulas | Data | Review | View

G32

	A	B	C	D	E	F	G	H	I	
1	Record Number	Good	Active	Record type	Sequence Numbe	Parent File Rec. #	Parent File Rec. Seq. #	Filename #1	Std Info Creation date	Std Info
2	0	Good	Active	File	1	5	5	/$MFT	2006-01-26 16:43:04.203125	2006-01
3	1	Good	Active	File	1	5	5	/$MFTMirr	2006-01-26 16:43:04.203125	2006-01
4	2	Good	Active	File	2	5	5	/$LogFile	2006-01-26 16:43:04.203125	2006-01
5	3	Good	Active	File	3	5	5	/$Volume	2006-01-26 16:43:04.203125	2006-01
6	4	Good	Active	File	4	5	5	/$AttrDef	2006-01-26 16:43:04.203125	2006-01
7	5	Good	Active	Folder	5	5	5	/.	2006-01-26 16:43:04.203125	2010-12
8	6	Good	Active	File	6	5	5	/$Bitmap	2006-01-26 16:43:04.203125	2006-01
9	7	Good	Active	File	7	5	5	/$Boot	2006-01-26 16:43:04.203125	2006-01
10	8	Good	Active	File	8	5	5	/$BadClus	2006-01-26 16:43:04.203125	2006-01
11	9	Good	Active	File + Unknown2	9	5	5	/$Secure	2006-01-26 16:43:04.203125	2006-01
12	10	Good	Active	File	10	5	5	/$UpCase	2006-01-26 16:43:04.203125	2006-01
13	11	Good	Active	Folder	11	5	5	/$Extend	2006-01-26 16:43:04.203125	2006-01
14	12	Good	Active	File	12	NoParent	NoParent	NoFNRecord	2006-01-26 16:43:04.203125	2006-01
15	13	Good	Active	File	13	NoParent	NoParent	NoFNRecord	2006-01-26 16:43:04.203125	2006-01
16	14	Good	Active	File	14	NoParent	NoParent	NoFNRecord	2006-01-26 16:43:04.203125	2006-01
17	15	Good	Active	File	15	NoParent	NoParent	NoFNRecord	2006-01-26 16:43:04.203125	2006-01
18	16	Zero	Inactive	File	0	NoParent	NoParent	NoFNRecord	2006-01-26 16:43:04.203125	2006-01
19	17	Zero	Inactive	File	0	NoParent	NoParent	NoFNRecord	2006-01-26 16:43:04.203125	2006-01
20	18	Zero	Inactive	File	0	NoParent	NoParent	NoFNRecord	2006-01-26 16:43:04.203125	2006-01
21	19	Zero	Inactive	File	0	NoParent	NoParent	NoFNRecord	2006-01-26 16:43:04.203125	2006-01
22	20	Zero	Inactive	File	0	NoParent	NoParent	NoFNRecord	2006-01-26 16:43:04.203125	2006-01
23	21	Zero	Inactive	File	0	NoParent	NoParent	NoFNRecord	2006-01-26 16:43:04.203125	2006-01
24	22	Zero	Inactive	File	0	NoParent	NoParent	NoFNRecord	2006-01-26 16:43:04.203125	2006-01
25	23	Zero	Inactive	File	0	NoParent	NoParent	NoFNRecord	2006-01-26 16:43:04.203125	2006-01
26	24	Good	Active	File + Unknown1 +	1	11	11	/$Extend/$Quota	2006-01-26 16:43:08.171875	2006-01
27	25	Good	Active	File + Unknown1 +	1	11	11	/$Extend/$ObjId	2006-01-26 16:43:08.171875	2006-01
28	26	Good	Active	File + Unknown1 +	1	11	11	/$Extend/$Reparse	2006-01-26 16:43:08.171875	2006-01

Şekil 10- $MFT dosyası içeriği.

Bu dosya detaylı incelenerek imajdaki[43] bütün dosyalar hakkında bilgi sahibi olunabilecektir. Bu çalışma sonucunda $MFT dosyasında bulunan üstveri bilgileri elde edilebilmiştir.

MFT dosyasında bulunan üst veriler ve açıklamalar bir sonraki tabloda açıklanmıştır.

[43] İmaj (image), dijital adli analiz çalışmalarında delil toplama esnasında verilerin kopyalandığı yeni disk için kullanılan bir ifadedir.

Tablo 1 - $MFT dosyasında bulunan üstveriler

Orijinal Başlık Bilgisi	Türkçe Karşılığı	Tanımı
Record Number	Kayıt Numarası	Sıra numarası bilgisini verir
Good	Durum Bilgisi	Dosya durumu ve sağlığı hakkında bilgi verir (iyi veya kötü)
Active	Aktiflik Bilgisi	Aktiflik bilgisini verir. Eğer inaktif ise dosya silinmiş demektir
Record type	Kayıt Tipi	Veri tipini gösterir (dosya veya dizin)
Sequence Number	Sıra Numarası	MFT sıra numarasını verir.[44] Bu alan her bir dosya için kullanılabilecek MFT kayıt segmentinde sırayla çoğalmaktadır.[45] Kayıt segmentinin silinmesi durumunda ise sayaç sıfırdan başlamaktadır.
Parent File Rec. #	Bağlı olduğu dosyanın kayıt bilgisi	Bağlı oldu dosyanın kayıt bilgisinin verir
Parent File Rec. Seq. #	Bağlı olduğu dosyanın kayıt numarası	Bağlı olduğu dosyanın kayıt numarasını verir
Filename #1	Dosya Adı 1	Dosya adını kök dizinleriyle birlikte detaylı olarak gösterir. UNICODE karakter formatındadır. Büyük küçük harf desteği vardır.
Std Info Creation date	Std Info Oluşturma Tarihi	Dosyanın oluşturma tarihini verir
Std Info Modification date	Std Info Değiştirme Tarihi	Dosyanın değiştirme tarihini verir
Std Info Access date	Std Info Erişim Tarihi	Dosyanın en son erişim tarihini verir

[44] MFT Sequence number, http://jmharkness.wordpress.com/2011/01/27/mft-file-reference-number, erişim tarihi: 07.01.2013.

[45] NFTS documentation and MFT Sequence numbers, http://integriography.wordpress.com/2010/02/10/updated-analyzemft-mft-sequence-numbers-and-ntfs-documentation, erişim tarihi: 07.01.2013.

Std Info Entry date	Std Info Giriş Tarihi	Dosyanın MFT'ye yansıdığı tarihi verir. Bu tarih ilgili dosyanın bulunduğu lokasyona ilk geldiği tarihtir.
FN Info Creation date	POSIX Oluşturma Tarihi	Dosyanın oluşturma tarihini POSIX[46] sistemlerde destekleyecek şekilde gösterir.
FN Info Modification date	POSIX Değiştirme Tarihi	Dosyanın değiştirme tarihini POSIX sistemlerde destekleyecek şekilde gösterir
FN Info Access date	POSIX Erişim Tarihi	Dosyanın erişim tarihini POSIX sistemlerde destekleyecek şekilde gösterir
FN Info Entry date	POSIX Giriş Tarihi	Dosyanın MFT'ye geliş tarihini POSIX sistemlerde destekleyecek şekilde gösterir
Filename #2	Dosya Adı 2	Dosya adını kök dizinleri hariç olarak gösterir. UNICODE karakter formatındadır, büyük küçük harf desteği bulunmaz.
FN Info Creation date	Win32 Oluşturma Tarihi	Dosyanın oluşturma tarihini Win32 sistemlerde destekleyecek şekilde gösterir. Windows NT ve Win32 bu sistemlere örnek olarak verilebilir.
FN Info Modify date	Win32 Değiştirme Tarihi	Dosyanın değiştirme tarihini Win32 sistemlerde destekleyecek şekilde gösterir
FN Info Access date	Win32 Info Erişim Tarihi	Dosyanın oluşturma tarihini Win32 sistemlerde destekleyecek şekilde gösterir
FN Info Entry date	Win32 Info Giriş Tarihi	Dosyanın MFT'ye geliş tarihini Win32 sistemlerde destekleyecek şekilde gösterir
Filename #3	Dosya Adı 3	Dosya ismi DOS formatında desteklenecek şekilde görüntülenir. 8.3 ASCII[47] formatındadır, büyük küçük harf desteği bulunmaz.

[46] POSIX, http://inform.pucp.edu.pe/~inf232/Ntfs/ntfs_doc_v0.5/help/glossary.html, erişim tarihi: 07.01.2013.
[47] DOS, http://www.writeblocked.org/resources/ntfs_cheat_sheets.pdf, erişim tarihi: 07.01.2013.

FN Info Creation date	DOS Oluşturma Tarihi	Dosyanın oluşturma tarihini DOS sistemlerde destekleyecek şekilde gösterir.
FN Info Modify date	DOS Değiştirme Tarihi	Dosyanın değiştirme tarihini DOS sistemlerde destekleyecek şekilde gösterir
FN Info Access date	DOS Info Erişim Tarihi	Dosyanın oluşturma tarihini DOS sistemlerde destekleyecek şekilde gösterir
FN Info Entry date	DOS Info Giriş Tarihi	Dosyanın MFT'ye geliş tarihini DOS sistemlerde destekleyecek şekilde gösterir
Filename #4	Dosya Adı 4	Dosya ismi Win32'nin DOS alanını sığdığı durumlarda gösterildiği formattır. Büyük küçük harf desteği bulunmaz.
FN Info Creation date	Win32 7 DOS Oluşturma Tarihi	Dosyanın oluşturma tarihini Win 32 7 DOS sistemlerde destekleyecek şekilde gösterir.
FN Info Modify date	Win32 7 DOS Değiştirme Tarihi	Dosyanın değiştirme tarihini Win 32 7 DOS sistemlerde destekleyecek şekilde gösterir
FN Info Access date	Win32 7 DOS Info Erişim Tarihi	Dosyanın oluşturma tarihini Win 32 7 DOS sistemlerde destekleyecek şekilde gösterir
FN Info Entry date	Win32 7 DOS Info Giriş Tarihi	Dosyanın MFT'ye geliş tarihini Win 32 7 DOS sistemlerde destekleyecek şekilde gösterir

Görüleceği üzere $MFT dosyasında çok sayıda üstveri bulunmaktadır. Bunlardan en göze çarpanı ise tarih verileridir. Tarih verilerinin farklı formatlarda saklanıyor olması hem sistemler arası uyumluluk hem de işletim sistemlerinin geriye dönük desteği için gereklidir. Bununla birlikte, dijital adli analiz anlamında bu veriler oldukça kıymetlidir. Söz gelimi, tabloda geçen STD alanındaki tarih verileri çeşitli programlarla[48] kolaylıkla değiştirilebilirken, FN alanındaki veriler için bu daha zordur. Bununla birlikte, çeşitli delil karartma teknikleriyle bazı hallerde FN tarihlerinin manipülasyonu da mümkün olabilmektedir. Sonraki

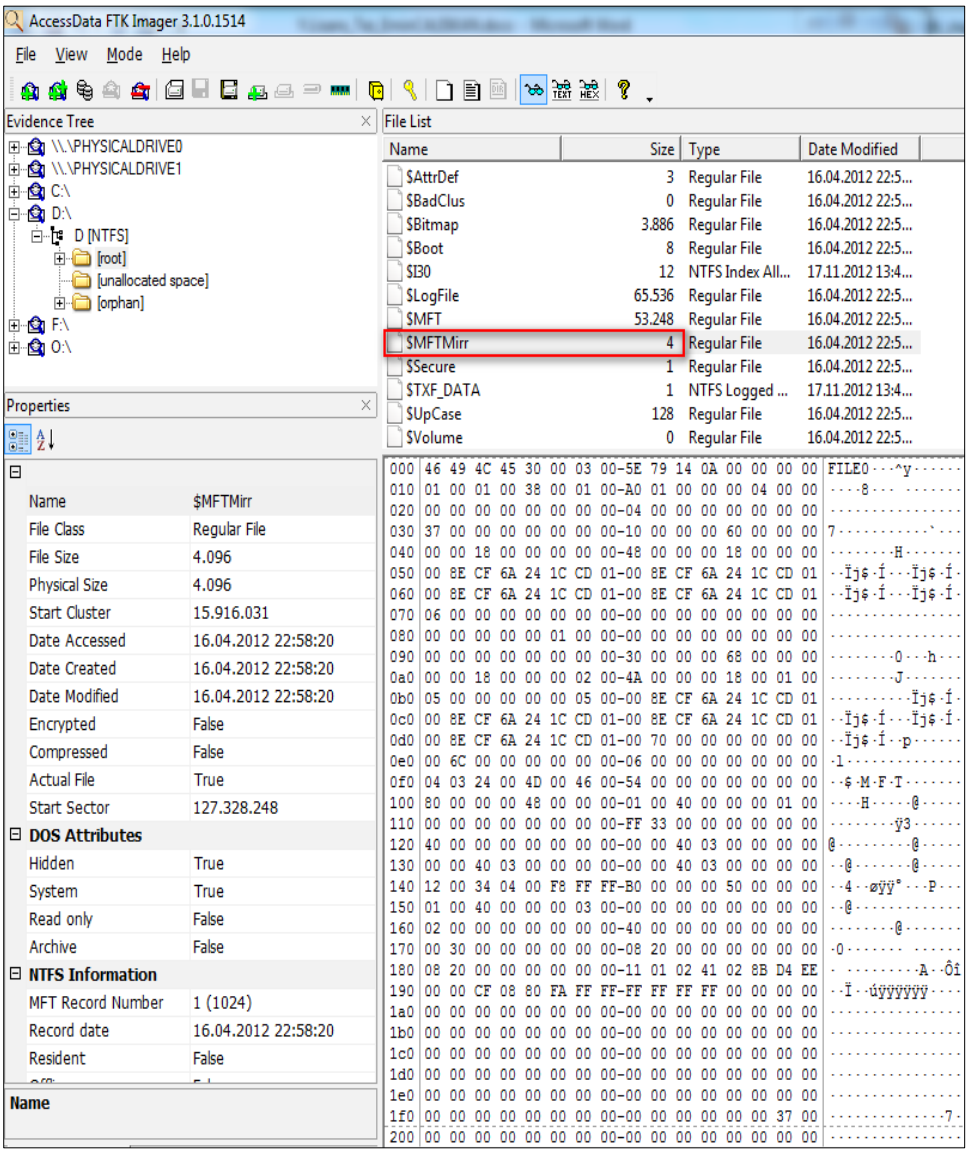
[48] setMACE ve timestompt bu tür programlara örnek olarak verilebilir. Detaylı bilgi için bkz. http://www.forensicswiki.org/wiki/Timestomp ve http://reboot.pro/files/file/91-setmace/, erişim tarihi: 07.01.2013.

bölümlerde incelenecek olan *delil karartma* (anti forensics) tekniklerinde bu konuyla ayrıntılı olarak ele alınacaktır.

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

2. $MFTMirr

$MFTMirr dosyası, $MFT dosyasında *bozuk sektör* (bad sector) oluştuğu durumda sistemin sorunsuz çalışmaya devam etmesi amacıyla tasarlanmıştır. $MFT dosyasının ilk dört kaydının kopyasını ihtiva etmektedir.



Şekil 11 - $MFTMirr dosyası içeriği.

3. $LogFile

NTFS dosyalama sistemi hakkında çeşitli bilgiler içermektedir. $LogFile, NTFS dosya sisteminde dosya veya klasör oluşturma, içeriğini veya ismini değiştirme ve MFT kaydındaki herhangi bir veriyi değiştirme vb. işlemlerin kayıtlarını tutmak için kullanılan dosya sistemi üst veri dosyasıdır. $MFT kaydının değişmesine sebep olacak bir işlemden önce halihazırdaki kaydın bilgileri ve yeni oluşacak kaydın bilgileri, işlemden sonra ise işlemin başarıyla tamamlandığına dair bir bilgi $Logfile dosyasına kaydedilir. Buradaki amaç

$MFT kayıtlarını değiştirecek olan işlemlerin gerçekleşmesi yarıda kalırsa veya bir şekilde tamamlanamazsa, $LogFile dosyasındaki bilgiler doğrultusunda bozulan $MFT kayıtlarının eski haline getirilebilmesidir. Bu şekilde dosya sisteminin bütünlüğünün korunması amaçlanmaktadır. Fakat $LogFile dosyasının boyutu işletim sisteminin kurulumuyla birlikte sabit olmakta ve dinamik olarak değişmemektedir. Bu yüzden dosyada yeni kayıtlar için yeterli yer kalmadığı takdirde bu kayıtlar sırayla en eski kayıtların üzerine yazılacaktır.

$LogFile dosyasının içeriği ve bu içeriğin nasıl ayrıştırılacağı konusunda $MFT'de olduğu gibi net bilgiler bulunmamaktadır. Windows'un bu konuda yayınladığı resmi bir API[49] olmadığı için, $LogFile'daki verilerin nasıl tutulduğu ve nasıl okunabileceği bilinmemektedir. Bununla birlikte piyasadaki bazı adli analiz araçları bu bilgiyi bir şekilde edinmiş ve $LogFile dosyasının çözümlenmiş halini ürünlerinde sunmuşlardır. Bunlardan öne çıkanı ise Encase yazılımıdır. Encase, $LogFile dosyasının çözümlenmiş halini göstererek adli analiz uzmanına yardımcı olmaktadır.

$LogFile dosyası yukarda izah edilen durumu itibariyle dijital adli analiz çalışmalarında büyük öneme sahiptir. $LogFile dosyasındaki verilere dışardan müdahalenin neredeyse imkansız derecesinde zor olması, $LogFile dosyasındaki verilerin sırayla oluşması ve bu nedenle dosyalar arasında olası ilişkiyi açığa çıkarması ile içerdiği tarih verilerinin güvenilirliği, delil inceleme esnasında bilirkişilere yol gösteren önemli özellikleri arasında sıralanabilir.

Sonuç olarak $LogFile dosyası, $MFT kaydı tamamen silinmiş olan ve üzerine yazılmış dosyalar için bilgi verebilecek önemli bir kaynaktır. Bir dosyanın $MFT kaydının bulunmamasına rağmen $LogFile kaydının olması, o dosyanın daha önce o diskte bulunduğu ancak silindiği ve daha sonra $MFT kaydı üzerine başka bir veri yazıldığı anlamına gelmektedir. Bununla beraber $LogFile'dan elde edilecek veriler kullanılarak o dosyanın veri kısmının yerine ulaşmak ve böylece verinin tamamını ya da bir kısmını geri döndürmek mümkün olabilmektedir.

---

[49] Application Programming Interface, http://en.wikipedia.org/wiki/Application_programming_interface, erişim tarihi: 07.01.2013.

4. $I30 dosyası

NTFS dosya sisteminde dijital adli analiz çalışmalarında kullanılabilecek başka bir önemli kaynak da $I30 dosyasıdır[50]. $I30, NTFS indeks verilerinden biri olarak, silinmiş ve hatta üzerinde yazılmış dosyalar için bile ciddi bir veri kaynağıdır.

$I30 dosyası, dizinler için tutulan dosya bilgilerine ilişkin bir indeks dosyasıdır. İlgili dizinde bulunan dosyalar için çeşitli veriler tutar. Bu klasörlerde bulunan dosyalar silinse ve üzerine başka veri yazılsa bile, $I30 dosyası içindeki veriler hemen değişmeyecektir. Bu nedenle silinmiş (unallocated space) veya silinmemiş olarak bulunan bir $I30 dosyası, dijital adli analiz uzmanı için incelenmesi gereken verilerden biridir.

$I30 dosyasında bulunan ve ilgili dizindeki dosyalar için saklanan veriler alttaki gibidir;

- Dosyanın tam adı,
- Bağlı bulunduğu klasör,
- Dosya boyutu,
- Dosya oluşturma zamanı,
- Dosya değiştirme zamanı,
- Dosya giriş zamanı,
- Dosya erişim zamanı.

5. $INDX dosyası

$INDX, NTFS dosya sisteminin kullandığı bir diğer veri merkezidir. $INDX dosyaları, bir klasörde bulunan dosyalarla ilişkili olarak çeşitli veriler tutar. Dosyanın adı, fiziksel ve mantıksal boyutu, dosyanın oluşturma değiştirme ve erişim tarihleri $INDX dosyasında bulunmaktadır.

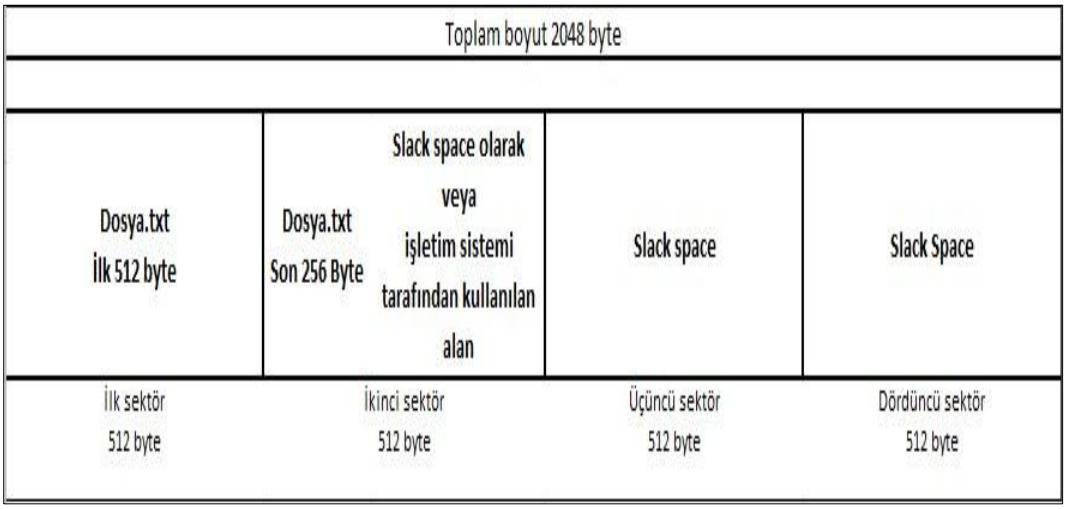
$INDX dosyasında tutulan bu veriler aracılığıyla silinmiş dosyaların geçmişi ve en son hangi tarihlerde işlem gördüğü tespit edilebilir.

---

[50] $I30 dosyası, http://computer-forensics.sans.org/blog/2011/09/20/ntfs-i30-index-attributes-evidence-of-deleted-and-overwritten-files, erişim tarihi: 07.01.2013.

6. *Fazlalık alan* (Slack space) verileri

Fazlalık alan (slack space) verileri, kullanıcı tarafından silinmiş bir verinin üzerine başka bir veri yazılması, ancak bu işlem esnasında verilerin tutulduğu yığınların [51] tamamının doldurulamaması nedeniyle oluşmaktadır. Önceki bölümlerde açıklandığı üzere, yığınlar birkaç disk sektörünün oluşturduğu veri kümeleridir. Örnek vermek gerekirse; 4 adet 512 byte disk sektörü barındıran bir yığında, toplam 2048 byte bir veri alanı oluşacaktır. Bir önceki dosya yazma işleminde bu yığında bulunan 2048 byte alanın tamamının doldurulduğu, ancak bu dosyanın silindikten sonra yerine gelen verinin 768 byte yer kaplayan bir dosya olması durumunda, bir önceki yazma işleminden arta kalan 1280 byte veri, yığının en son bölümünde bulunuyor olacaktır (Şekil 12).Çok küçük gibi görünen bu veri alanı, dijital adli analiz çalışmalarında büyük öneme sahip bilgileri açığa çıkarabilir. Bu nedenle fazlalık alan verilerinin de dikkatle incelenmesi tavsiye edilmektedir.



Şekil 12 - Fazlalık alan verileri.

7. $Volume

$Volume dosyası, diskteki *yığın* (volume) hakkında çeşitli bilgiler verir. Yığının etiketi ve versiyonu buna örnek olarak verilebilir.

[51] Detaylı için bkz. "*Yığın* (Cluster)", sf. 31.

8. $AttrDef

$AttrDef, NTFS dosyalama sisteminde kullanılan $STANDARD_INFORMATION, $FILE_NAME, $OBJECT_ID gibi özellik isimlerini, numaralarını ve tanımlarını içinde bulunduran dosyadır.

9. $Bitmap

$Bitmap dosyası, *küme bit haritası* (cluster bitmap) olarak da anılmaktadır. Diskte bulunan *kümelerde* (cluster) dolu ve boş olanları göstermektedir. Böylece yeni bir dosya oluşumu esnasında hangi yığınlara veri yazılabileceği bilgisi sistem tarafından edinilmiş olur.

10. $Boot

$Boot ismini taşıyan ve *başlatma sektörüyle* (boot sector) ilgili bilgiler veren bu dosya, BIOS parametre bloğu (BPB[52]) bilgilerini içinde barındırır. Bu sayede diskteki yığın, bilgisayarı başlatmak için gerekli bilgileri (bootstrap loader code gibi) kullanarak bilgisayarı açabilir. Bu dosyanın doğru okunamaması veya bozulması bilgisayarın açılamamasına neden olacaktır.

11. $BadClus

$BadClus dosyası, bozulmuş kümeleri işaretleyen bilgilerin olduğu dosyadır. Diskteki yığının hangi kümeleri bozuksa bu dosya sayesinde o kümeler devre dışı bırakılabilir.

12. $Secure

Yığındaki bütün dosyalarda kullanılan güvenlik özelliklerini ve yetkilendirmelerin tanımlandığı bir referans dosyasıdır.

[52] BPB, http://en.wikipedia.org/wiki/BIOS_parameter_block, erişim tarihi: 07.01.2013.

13. $Upcase

Bilgisayarda kullanılan unicode[53] karakterler için büyük-küçük harf eşlemesinin yapıldığı tanım dosyasıdır.

14. $Extend

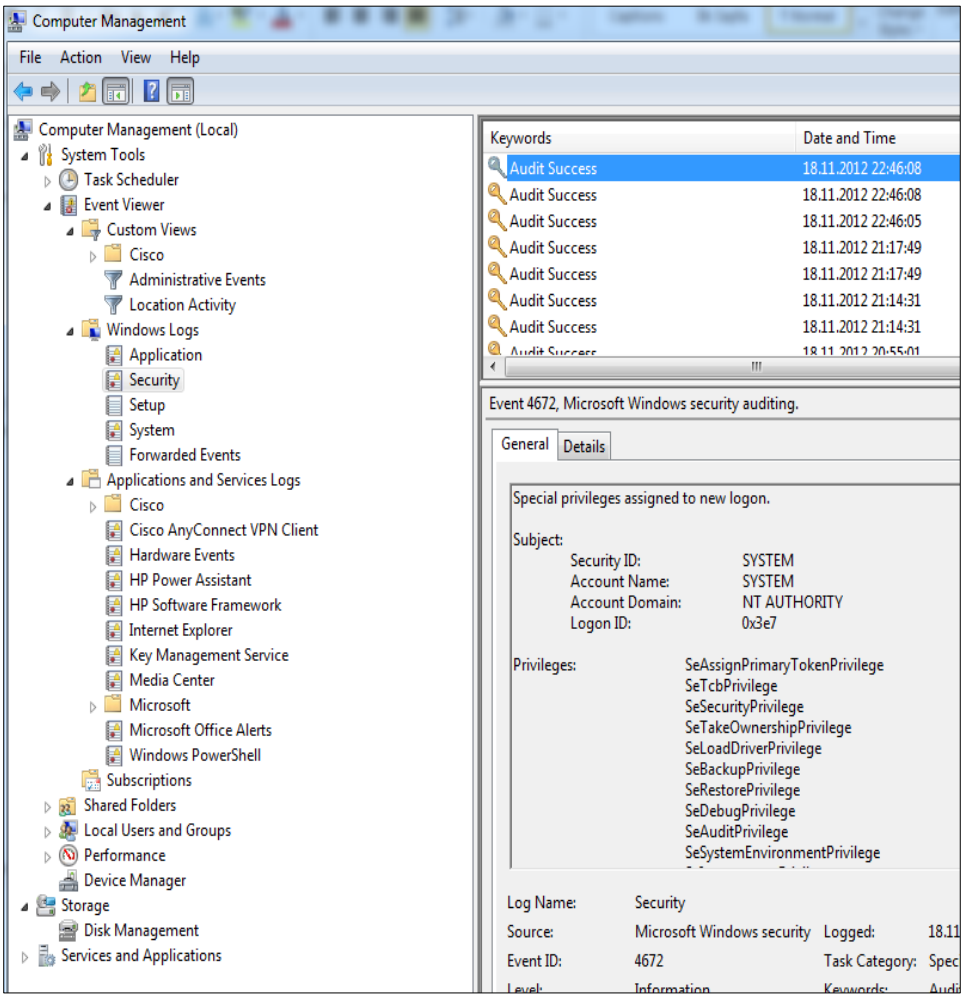
Kullanımı sistem tarafından zorunlu olmayan kota (quota) bilgileri ve nesne tanımlayıcıları gibi bilgileri içermektedir.

B- İşletim sistemi verileri

1. Olay kayıt dosyaları (Eventlogs)

Microsoft Windows işletim sistemlerinde 3 temel olay kayıt dosyası (Event log file) bulunmaktadır[54]. Bunlar uygulama, sistem ve güvenlik olmak üzere 3 ana başlıkta incelenmektedir. Windows 7 işletim sisteminde olay kayıtları daha alt başlıklarda ayrıca değerlendirilmekte ise de, sistemde toplanan olay kayıtlar yukarıda bahsedildiği gibi 3 ana başlıkta araştırılabilir.

[53] Unicode karakter listesi için bkz. http://unicode-table.com/en/#spacing-modifier-letters.
[54] Event viewer, http://support.microsoft.com/kb/308427, erişim tarihi: 07.01.2013.



Şekil 13 - Olay kayıt dosyaları.

2. Uygulama kayıtları

Uygulama kayıtlarında bilgisayardaki uygulamaların ürettiği çeşitli kayıtlar bulunmaktadır. Burada hangi uygulamanın ne tür kayıt üreteceği ve yazacağını *uygulama geliştirici* (software developer) belirlemektedir.

Dijital adli analiz konusunda uygulama kayıtları işe yarayabilmektedir. İncelene konuyla ilişkili bir uygulama varsa, burada bulunan uygulama kayıtları incelenebilir.

3. Güvenlik kayıtları

Güvenlik kayıtları, bilgisayara sızma girişimlerinden şüphelenildiğinde veya incelenen bilgisayara zararlı yazılım bulaşması durumu araştırıldığına

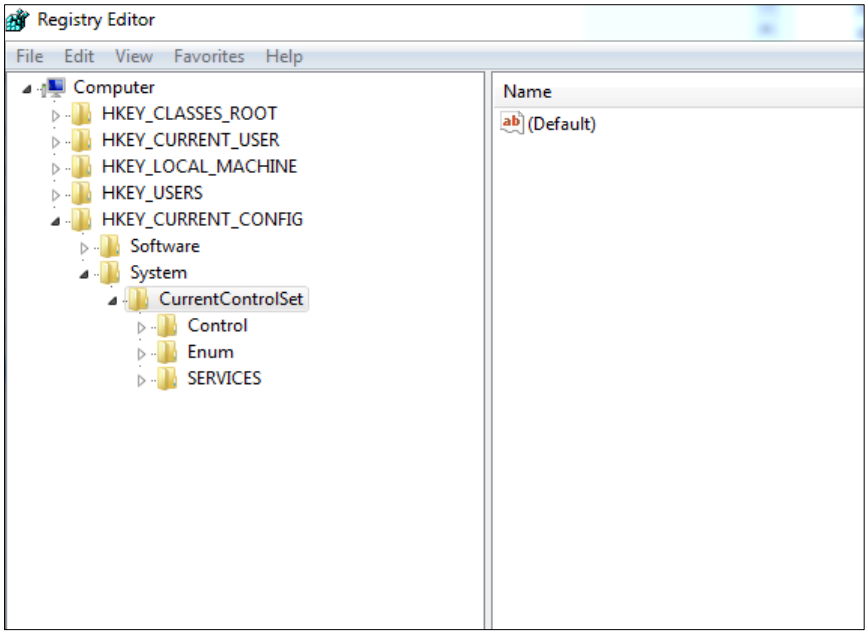
başvurula bilecek bir kaynaktır. Sisteme başarılı veya başarısız bütün *oturum açma denemeleri* (session) burada kaydedilecektir.

4. Sistem kayıtları

İşletim sistemindeki sistem uyarıları, hataları veya bildirimleri "sistem kayıtları" verilerinde bulunacaktır. Bu kayıtlar ilgili bilgisayarda hangi tür donanımların kurulduğu, sistemsel bir değişiklik yapılıp yapılmadığı veya *sürücü* (driver) kurulumunda karşılaşılan bir hatada oldukça bilgi verici olacaktır. Zararlı yazılımların işletim sisteminde oluşturacağı *anormallikler* (anomaly) bu sayede yakalanabilir.

5. Kayıt defteri (Registry)

Kayıt defteri, işletim sistemi dahil olmak üzere sistemde bulunan bütün programlar ve uygulamalar için çok sayıda yapılandırma ayarının tutulduğu bir kılavuzdur. Buradaki değerler, gerek bilgisayar kullanıcısının kimliği gerekse bilgisayardaki yazılımların hangi ayarlar ve özelliklerle çalıştırıldığını bilgileri gibi hassas verileri taşımaktadır. Bu nedenlerle dijital adli analiz incelemesinde bu veriler büyük öneme sahiptir.



Şekil 14 - Kayıt defteri giriş ekranı.

Kayıt defteri 5 ana *gruptan* (hive) oluşmaktadır[55].

Tablo 2 - Kayıt defteri veri grupları

İsim	Kısaltma	Tanım
HKEY_CLASSES_ROOT	HKCR	Dosya uzantı bilgileri, hangi tip dosyanın hangi programla açılması gerektiği ve dosya tipleriyle ilgili tanımlamaların yapıldığı gruptur.
HKEY_CURRENT_USER	HKCU	Bu grupta uygulamaların bilgisayar kullanıcılarına özgü ayarları saklanmaktadır. Ortam değişkenleri, masaüstü ayarları ve uygulama yapılandırmalarına buna örnek olarak verilebilir.
HKEY_LOCAL_MACHINE	HKLM	Bu grupta bilgisayara özgü yapılandırma bilgileri bulunmaktadır. Donanım, SAM, güvenlik, yazılım ve sistem olmak üzere 5 alt başlığa daha ayrılmıştır.
HKEY_USERS	HKU	Bilgisayarda hali hazırda açık olan kullanıcıların ayarları ve çalıştırdıkları uygulamalara özgü çeşitli verileri taşımaktadır.
HKEY_CURRENT_CONFIG	HKCC	Bilgisayardaki donanım profili hakkında saklanan veriler bu grupta bulunmaktadır[56].

Kayıt defterinde bulunan ve dijital adli analiz incelemesinde göz önünde bulundurulması gereken veriler vardır. Kullanıcının hesabı ve grubuyla ilgili veriler, *geçmiş yakın zaman verileri* (Most Recently Used), bilgisayara yüklenen çeşitli dosyalara ilişkin veriler, sistem saati bilgisi, taşınabilir disk kurulum verileri, dosya ve klasörlerin görüntülenmesiyle ilgili sınıflandırma bilgilerini

[55] Derrick J. Farmer, A Forensic Analysis of the Windows Registry, Vermont 2008 ("Farmer"), sf.2.

[56] HKEY_USERS, http://pcsupport.about.com/od/termshm/g/hkey_users.htm, erişim tarihi: 07.01.2013.

tutan *kabuk çantası* (shellbag) verileri, dosya ve klasörlerin görüntülenmesiyle ilgili sınıflandırma bilgilerini tutan *kabuk çantası* (shellbag) verileri [57] kayıt defterinde tutulan önemli bilgileri kısa birer örnektir[58].

6. Pagefile.sys dosyası

Pagefile.sys dosyası, bilgisayarda bulunan *belleğin* (memory) *sayfalama* (paging) işlemi esnasında yetersiz kaldığı durumlarda içinde bulunan verileri yazdığı ve sabit diskin *kök* (root) dizininde bulunan bir sistem dosyasıdır[59]. Dijital adli analiz incelemelerinde bellek oldukça önemli bir kaynağıdır. Bu nedenle belleğe ait verilerin bir kısmının bulunabildiği pagefile.sys dosyası da incelemeyi yapan uzman için önemlidir.

7. Hiberfil.sys dosyası

Yeni nesil bilgisayarlarda bulunan u*ykuda bekletme* (hibernation) özelliğinin kullandığı temel dosyadır[60]. Bu dosya sayesinde uykuda bekletilen bilgisayar yeniden başlatıldığı kaldığı yerden devam edecek, açık kalan programlar kapanmış olmayacaktır. Bunun yapılabilmesi için bilgisayar kapatılmadan önce bellekte bulunan bilgilerin sabit diskte bir dosyaya kaydedilmiş olması gerekir. İşte bu noktada devreye Hiberfil.sys dosyası girer. Bellekte bulunan veriler, uykuda bekletme öncesi bu dosyaya kaydolur. Bu özelliği nedeniyle dijital adli analiz uzmanı açısından Hiberfil.sys dosyası hassas bir yere sahiptir. Sabit diskte bulunamayacak birçok veri (çeşitli parola bilgiler, şifreli veriler, e-posta içerikleri vb.) Hiberfil.sys dosyasında bulunabilir.

---

[57] Shellbag, http://computer-forensics.sans.org/blog/2008/10/31/shellbags-registry-forensics, erişim tarihi: 07.01.2013.

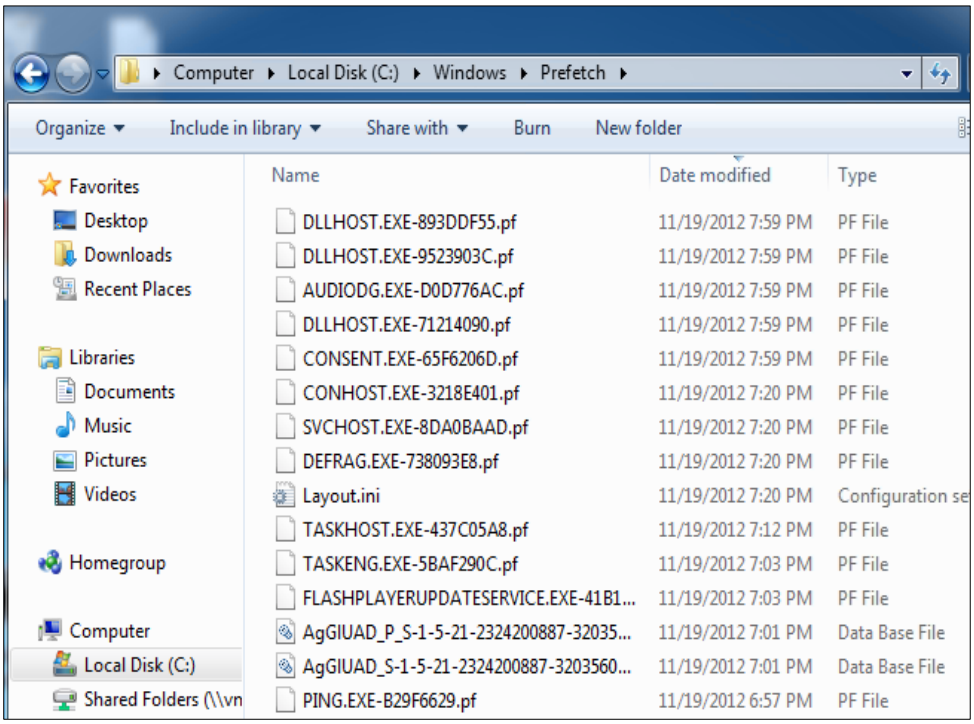
[58] Computer Forensic Artifacts: Windows 7 Shellbags, http://computer-forensics.sans.org/blog/2011/07/05/shellbags, erişim tarihi: 07.01.2013.

[59] Nicholas Paul Maclean, Acquisition and Analysis of Windows Memory, ABD 2006 ("Maclean"), sf. 12.

[60] Hameed Iqbal, Forensic Analysis of Physical Memory and Page File, Gjøvik 2009 ("Iqbal"), sf 27.

8. Prefetch dosyaları

Windows XP ile devreye alınan Prefetch dosyaları, uygulama başlangıç sürelerini düşürmek için tasarlanmıştır. Yakın zaman önce açılmış olan bir dosyaya ait prefetch kayıtları sistemin kök dizininde bulunan Prefetch dizinine kaydolur. Bu şekilde oluşan her bir ".pf" uzantılı için, dosyanın ilişkili olduğu *çalıştırılabilir* (executable) program, ilişkili DLL (Dynamic-link library) sistem dosyası, dosyanın kaç kez çağrıldığı ve en son çalıştırılma zamanı gibi bilgiler tutulmaktadır.



Şekil 15- Prefetch dosyaları.

Prefetch dosyaları, dijital adli analizde bir uygulamanın veya dosyanın açılıp açılmadığı ile en son ne zaman açıldığı gibi önemli verileri sunması bakımında incelenmesi gereken kaynaktır.

9. Takas dosyaları (Swap files)

Hiberfil.sys ve Pagefile.sys gibi *takas dosyaları* da (swap files), bilgisayarın belleğinden elde edilmiş bilgileri bulabileceğimiz bir kaynaktır[61]. Windows işletim sistemi, sistemdeki belleğin kapasite bakımından yetersiz kaldığı durumlarda disk üzerinde kendine bir alan oluşturur ve bu alanı bellek gibi kullanır. Bellekte çok çeşitli önemli bilgilere rastlanılabileceğinden takas dosyaları da bu nedenle dijital adli analiz anlamında önem taşır.

10. *Sistem geri yükleme noktası* (System restore point) verileri

Microsoft Windows, bilgisayarda yapılan değişiklikleri ön tanımlı bir zaman aralığında veya kullanıcının isteği doğrultusunda belirlenmiş bir zamanda daha sonra kullanılmak üzere kaydeder. "C:\System Volume Information_restore{GUID}" dizinin altındaki bu değerler, sistemin tutarsız haline gelmesi vb. problemlerde geri döndürülmekte ve problem giderilebilmektedir[62]. Bu dosyalarda saklanan veriler dijital adli analiz için geriye dönük inceleme yapılması ve sistemin eski durumu hakkında bilgi edinilmesi amacıyla kullanılabilmektedir.

11. *Hacim gölge servisi* (Volume Shadow Service) verileri

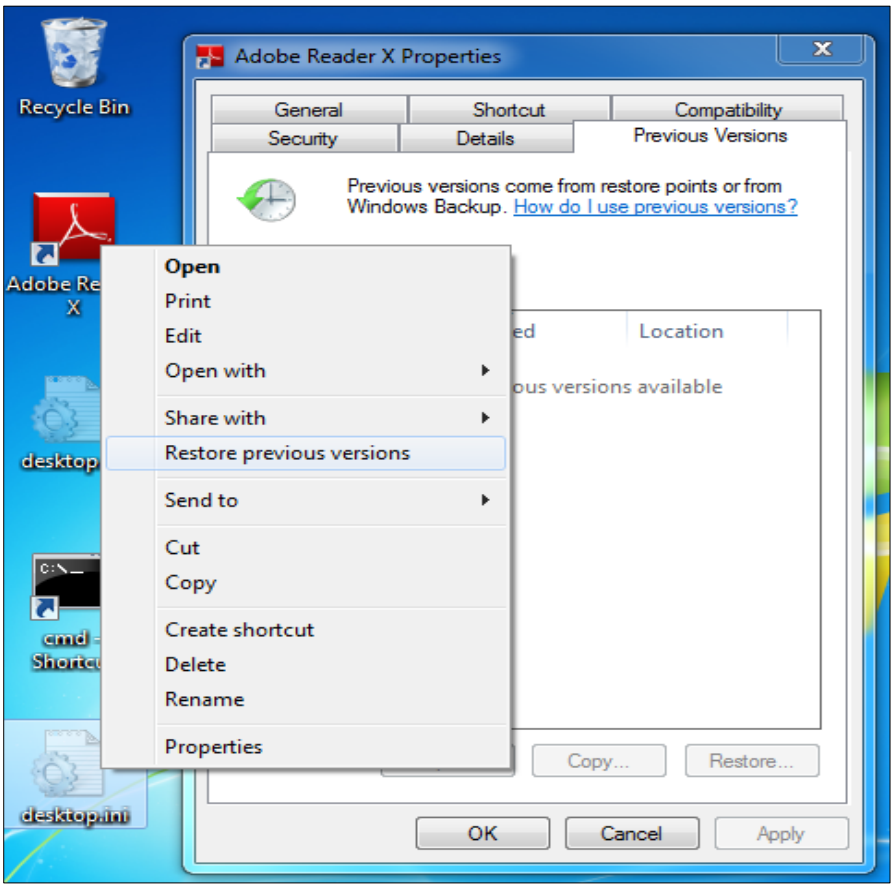
Bir önceki maddede açıklanan "sistem geri yükleme noktasına" benzer şekilde *hacim gölge servisi* (volume shadow service) verileri de bilgisayarda bulunan dosyaların önceki versiyonlarına dönülebilmesi amacıyla tasarlanmıştır[63]. Örnek vermek gerekirse, Microsoft Word uygulamasıyla yapılan bir çalışmanın önceki versiyonların dönebilmek için bu özellik kullanılabilir.

---

[61] Computer Forensics: Finding "hidden" data, http://www.techrepublic.com/blog/security/computer-forensics-finding-hidden-data/232, erişim tarihi: 07.01.2013.

[62] Damir Kahvedžić, Tahar Kechadi, Extraction of User Activity through Comparison of Windows Restore Points, Dublin 2008 ("Kahvedžić/Kechadi"), sf. 2.

[63] Robert Erdely, Shadow Copy Forensics, Indianapolis 2011 ("Erdely"), sf. 2.



Şekil 16 – Hacim gölge servisi verilerine ulaşma.

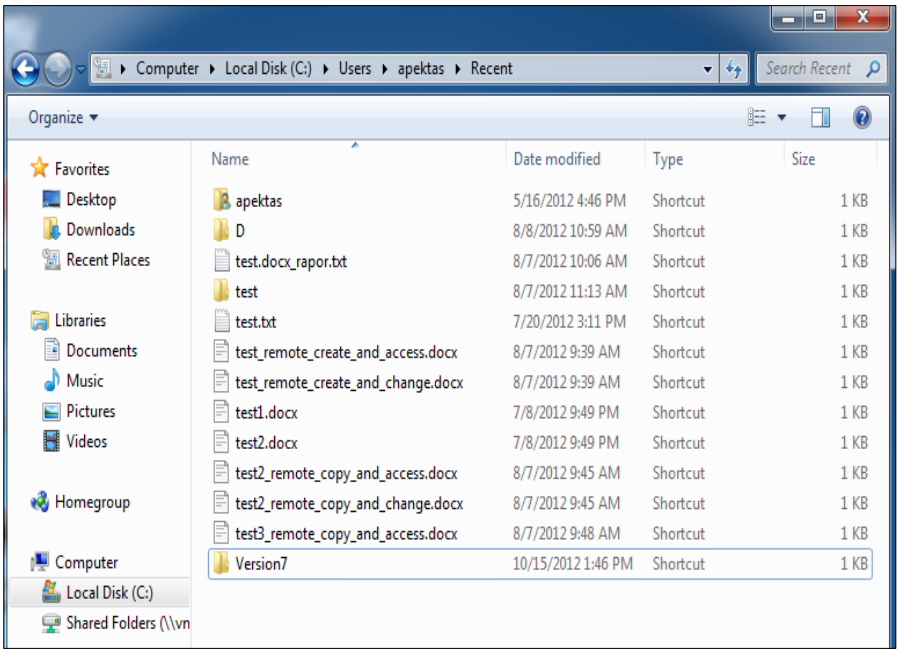
Hacim gölge servisi verileri, kısa adıyla VSS, dosyaların eski versiyonlarını NTFS dosyalama sisteminin desteğinden de faydalanarak özel bir alanda saklar. Sabit diskin %15'ine kadar büyüyebilen bu alan sayesinde dijital adli uzmanı, silinmiş veya üzerine yazılmış eski dosyaları açığa çıkarıp inceleyebilme imkanına sahiptir.

12. Geçmiş yakın zaman dosyaları (MRU dosyaları)

Geçmiş yakın zaman (Most recently used - MRU[64]) dosyaları, bilgisayar kullanıcısının yakın zaman önce açtığı dosyalar ve çalıştırdığı programlar gibi yapmış olduğu işlemler hakkında bilgiler verir. "Kayıt defteri verileri" başlığı altında incelenen verilerde bu şekilde MRU verilerine sıklıkla rastlanmaktadır.

[64] "Most Recently Used" kelimelerinin kısaltması olan MRU hakkında detay bilgi için: http://msdn.microsoft.com/en-us/library/aa376960%28v=VS.85%29.aspx, erişim tarihi: 07.01.2013.

Benzer şekilde Windows işletim sistemi de yakın zaman önce kullanılan dosyalara ait izleri, kullanıcının "Recent" dizini altında saklamaktadır(Şekil 17).



Şekil 17 - "Recent" klasörü ve içindekiler.

Kısayol (shortcut) olarak tutulan bu dosyalar, en son açılan dosyaların yakın zaman içinde tekrar açılması halinde işlemin hızlıca gerçekleşmesini sağlamaktadır. Dijital adli analiz uzmanı açısından ise, burada listelenmiş dosyaların bilgisayar kullanıcısı tarafından açıldığını gösteren değerli bir veri kaynağı olmaktadır.

C- Uygulama verileri

Dijital adli analiz çalışmalarında kullanılabilecek başka bir veri kaynağı da, bilgisayarda kurulu olan uygulamaların ürettiği verilerdir. İncelemenin konusuna göre, bilgisayarda tespit edilen dosyaların üstverileri, ilişkili olabilecek uygulamaların *kayıt dosyaları* (log) ve yapılandırmaları ayarları incelenebilir.

1. Dosya üstverileri

Dosya Üstverileri, incelenmek istenen dosyanın diskteki konumu tespit edilerek ortaya çıkarılabilmektedir. Bu alandaki veriler, dosyanın içerik bilgisiyle

birlikte tutulur ve dosya tipine özel olarak çeşitlenebilir. Örnek vermek gerekirse; Microsoft Office Word uygulamasına ait bir dosyanın üstverilerinde Yazar, Yönetici, Karakter sayısı vb. uygulamaya özgü veriler tutulurken, çalıştırılabilir exe tipinde bir dosya için Makine tipi ve Dosya işletim sistemi üstverileri tutulmaktadır. Benzer şekilde PDF tipinde bir dosya için de, PDF Oluşturma tarihi verisi ayrıca tutulmaktadır.

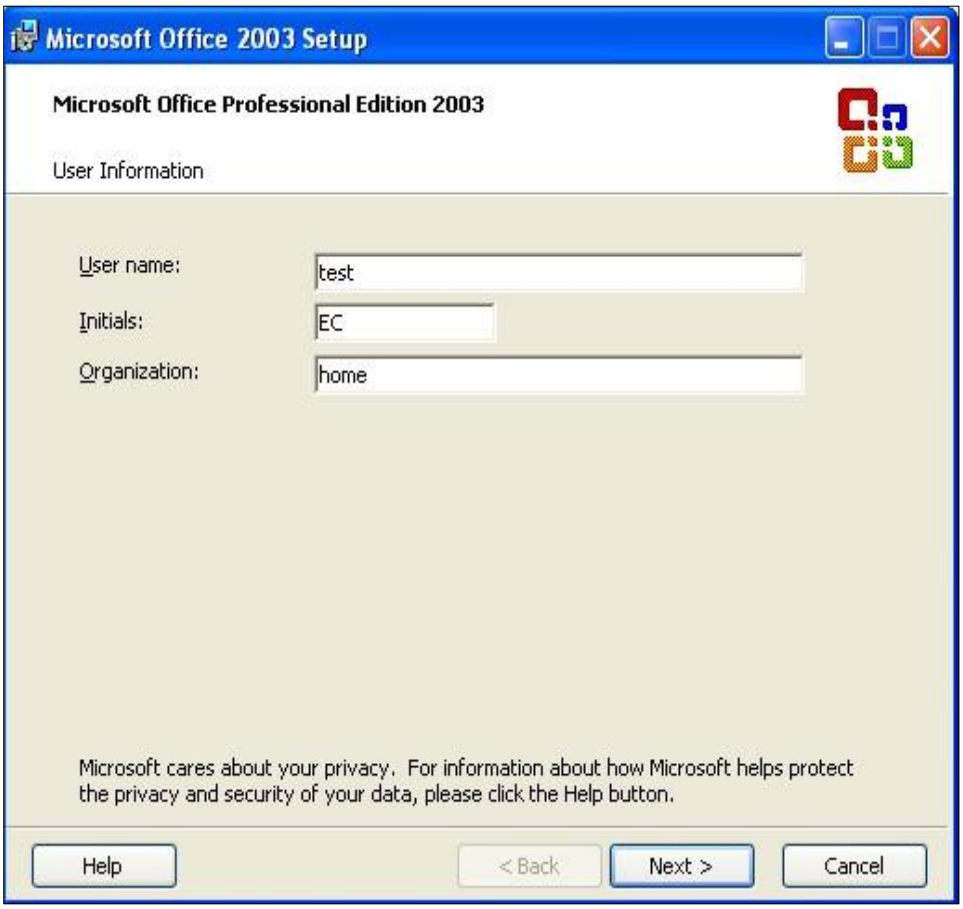
2. Dosya durumu

Dosya *durumu* (state), dosyanın kullanıcı tarafından silinip silinmediği bilgisini vermektedir. Bir dosyanın kullanıcı tarafından silinmiş olması, o dosyanın diskte bulunamayacağı veya ortaya çıkarılamayacağı anlamına gelmemektedir. Bu bilgilere çeşitli profesyonel araçlarla ulaşılabilir[65]. Ancak silinmiş olan dosyalar, sabit disk üzerinde zaman içinde tahrifata uğrayabilir. Bilgisayarda bulunan işletim sistemi, zaman içinde bu silinmiş verilerin olduğu disk bölümünün bir kısmının üzerine başka veriler yazabilir. Bu durumda dosyanın bir kısmı veya tamamı geri döndürülemez hale gelebilmektedir.

3. Yazar verisi

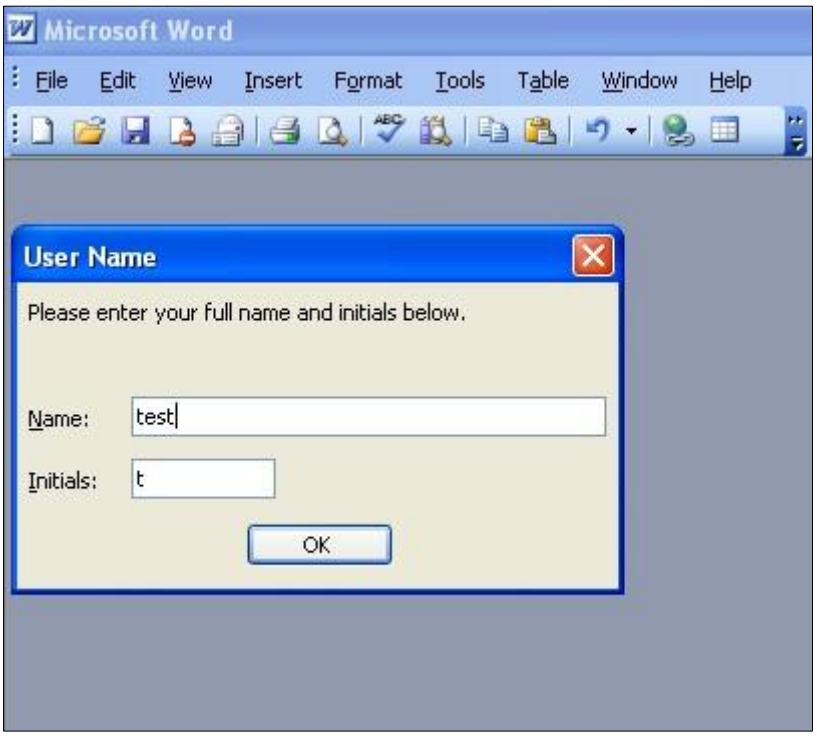
Yazar (author) verisi, Microsoft Office dokümanlarında saklanan ve dijital adli analiz çalışmalarında değerlendirilen en önemli üst verilerden biridir. Herhangi bir Word dosyasının ilk kez oluşturulduğunda, ilgili bilgisayardaki Office uygulamasının yazar bilgisi, oluşturulan dosyasının yazar bilgisi olarak kaydedilmektedir. 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 olmaktadır (Şekil 18). Şekilde İşletim sistemi kullanıcısı "test" olan kullanıcı için, "username" alanı da test olarak gelmiştir.

[65] Detaylı bilgi için bkz. "Kullanılan araçlar" sf. 10.



Şekil 18 - Office kurulumu kullanıcı metaverileri.

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



Şekil 19 - Office ilk açıldığında istenen veriler.

Yazar bilgisi ve diğer Office üstverileriyle ilgili üretici firma Microsoft'un kaynak verileri incelenerek konu hakkında detaylı bilgi elde edilebilir.[66]

4. Tarih-zaman verisi

Dosya sistemi üstverileri ve bu verilerin tutulduğu $MFT (Master File Table); bir bilgisayarda bulunan bütün dosyaların o bilgisayardaki ilgili diskin hangi bölümünde yer aldığını, boyutunun ne kadar olduğunu, dosyanın oluşturulma, değiştirilme, erişim ve kayıt değiştirme zamanlarının ne olduğunu verisini ihtiva etmektedir. Tutulan bu üstverilerin, işletim sistemi üreticisi Microsoft firması tarafından nasıl tanımlandığına dair çeşitli makaleler incelenebilir.[67] $MFT dosyasından edinilebilecek belli başlı zaman üstverileri "Dosya sistemi üstverileri" bölümünde etraflıca ele alınmış durumdadır[68].

[66] Inspect documents, http://office.microsoft.com/en-us/help/inspect-documents-for-hidden-data-and-personal-information-HA010074435.aspx, erişim tarihi: 07.01.2013.
[67] Master File Table, http://msdn.microsoft.com/en-us/library/bb470206%28v=vs.85%29.aspx.
[68] Detaylı bilgi için bkz. "$MFT", sf.24.

5. İnternet uygulamaları

Günümüzde İnternetin hızla yaygınlaşmaya devam etmesi, İnternete erişen veya İnternet üzerinden çalışan uygulamaların sayısını da artırmaktadır. Bunlardan en sık incelenen ve kullanıcı açısından kişisel bilgileri ihtiva etmesi bakımından en değerli olanın *tarayıcılar* (browser) olduğu düşünülebilir. Tarayıcılar, kullanıcıların kişisel bilgilerini, e-posta hesaplarını, hangi İnternet sayfasına ne zaman eriştiği, hangi uygulama veya dosyayı bilgisayarına indirdiği ve hatta kullanıcının kendi bilgisayarındaki dosyaları ne zaman açtığı veya kaydettiğine kadar çeşitli bilgiler barındırmaktadır[69].

a) *Çerezler* (Cookie)

Çerezler, kullanıcının işlem yaptığı tarayıcıdan, bağlandığı web sunucusuna özel olarak kaydettiği ve daha sonra okuyarak kullandığı küçük boyutlu yazı dosyalarıdır. Çerezlerin amacı, bilgisayar kullanıcısını web sunucusuna tanıtmak ve böylece o kullanıcıya özel sayfaların açılması, kimlik doğrulama ile giriş yapılması gerekiyorsa bu işlemin otomatik olarak yapılmasını sağlamaktır. Dijital adli analiz açısında çerezler, kullanıcının hangi İnternet sayfalarının ziyaret ettiği, ne sıklıkla giriş çıkış yaptığı ve ilgili web sunucunda sakladığı kişisel verilerin içeriği bakımından önem arz eder. İnternet Explorer, Firefox, Safari ve Chrome gibi tarayıcılarda farklı dizinlerde kayıtlı olan bu bilgiler, incelemeyi yapan uzman tarafından değerlendirilmektedir.

a. Ziyaret geçmişi verileri (History)

İnternet geçmişi (history) verileri, bilgisayar kullanıcısının geçmişte hangi sayfaları ziyaret ettiğini göstermektedir. Kullanıcının tercihine bağlı olarak çok eski zamanlarda girilmiş web sayfalarına ait izler bile internet geçmişi kayıtlarında bulunabilir. İnternet geçmişi incelenirken, kullanıcının görüntülediği

[69] Junghoon Oh, Seungbong Lee, Sangjin Lee, Advanced evidence collection and analysis of web browser activity, Republic of Korea 2011 ("Oh/Lee/Lee"), sf. 3.

bağlantı adresleri (Uniform Resource Locator – URL[70]) bilgileri de çok detaylı olarak tespit edilebilecektir.

Tablo 3 - İnternet geçmişi kullanılarak elde edilen e-posta kayıt örneği

Tarih	Saat	Kaynak	Bağlantı	Açıklama
01.09.2010	12:15:29	Firefox 3 history	URL: https://mail.google.com/mail/?shva=1#inbox/12d7414h7a4d20e3e0	Gmail - Buluşma mekânı - emincliskan@gmail.com

Yukarıdaki örnekte, kullanıcının 01.09.2010 tarihinde buluşma "Buluşma mekânı" içerikli bir e-posta görüntülediği tespit edilmiştir. İncelenen adli vakalarda böyle bir dijital adli delil oldukça önemli olabilir. İnternet geçmişi kullanarak bu ve buna benzer çok sayıda bilgi etmek mümkündür.

b. Sık ziyaret edilenler (Bookmark)

Bir önceki başlıkta incelenen "İnternet geçmişi" verilerinin yanı sıra, kullanıcının yoğun kullandığı ve *sık ziyaret edilenler* (bookmark) listesine eklediği web adresleri de önemli bir yere sahiptir. Bu alandaki veriler kullanılarak kullanıcının profili ve kişiliği hakkında çeşitli bilgiler edinilebilir.

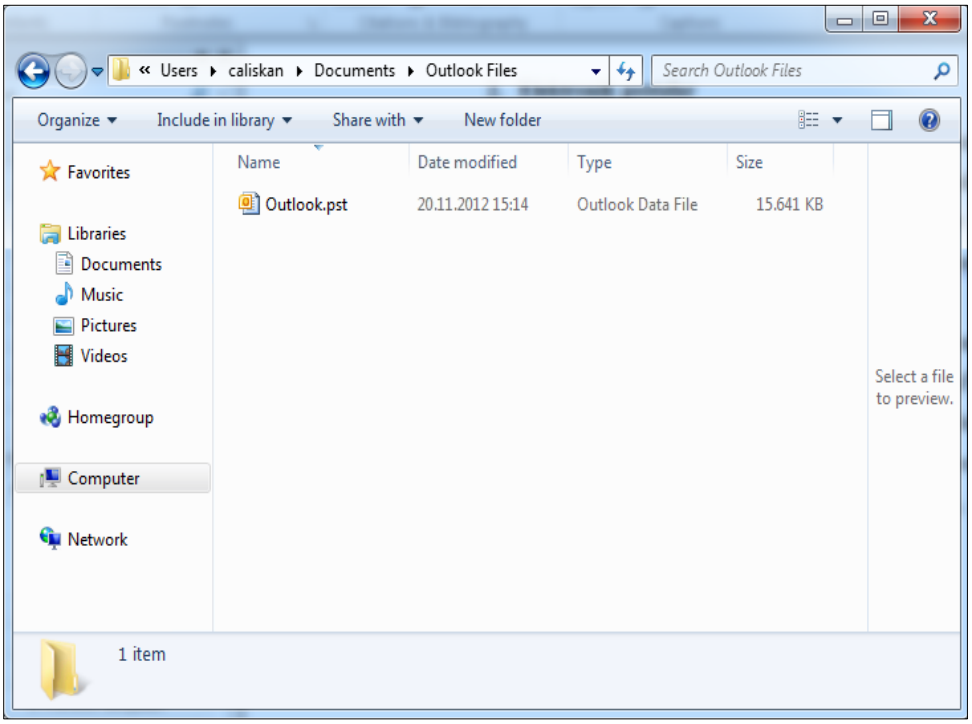
6. Elektronik postalar

Elektronik postalar (e-mail) , günümüzde iletişimin vazgeçilmez bir unsuru halini almıştır. Zaman ve maliyet tasarrufu sayesinde imkânlarıyla e-posta kullanımı gerek kurumsal gerekse bireysel alanda son derece yaygınlaşmış durumdadır. Hal böyleyken e-postaların dijital adli analiz konusunda da sağlam bir veri kaynağı olacağı şüphesizdir.

Uygulama tabanlı e-posta servisleri, işletim sistemine kurulan e-posta istemci uygulamasıyla birlikte çalışmaktadır. Outlook[71], Thundbird[72] ve Zimbra[73]

[70] Sandeep Kumar Khanikekar, Web Forensics, Texas 2010 ("Khanikekar"), sf. 47.
[71] Outlook, http://office.microsoft.com/tr-tr/outlook, erişim tarihi: 07.01.2013.
[72] Thunderbird, http://www.mozilla.org/en-US/thunderbird, erişim tarihi: 07.01.2013.

vb. çeşitli uygulamalar ile e-posta sunucularına bağlanan ve kullanıcının e-postalarını görüntüleyen servisler, dijital adli analizde kullanılabilecek çok sayıda veriyi bilgisayarda bırakmaktadır. Kullanıcının kayıtlı e-postaları, *kontak listesi* (contact list) ve *takvim* (calendar) gibi veri kaynakları, e-posta istemci uygulamaları sayesinde incelenen bilgisayarda bulunabilmektedir.



Şekil 20 - E-postaların kayıtlı olduğu *.pst dosyası.

Farklı işletim sistemi ve uygulamalarda farklı dizinlerde yer alan e-posta istemci uygulamalarının veri dosyaları, dijital adli incelemeyi yapan uzman için göz önünde bulundurması gereken bir kaynaktır. Bu tip analizleri kolaylaştırmak için çeşitli adli analiz yazılımları da piyasada mevcuttur[74]. Bu veriler bu yazılımlar ile, kullanıcının bilgisayarında bulunan ve suç unsuru içeren bir dosyanın, bilgisayara hangi yolla geldiğine dair çeşitli analizler yapılabilir.

[73] Zimbra, http://www.zimbra.com/products/desktop.html, erişim tarihi: 07.01.2013.
[74] M. Tariq Banday, Techniques and Tools for Forensics Investigation of e-mail, Kashmir 2011 ("Banday"), sf. 11.

7. Anti virüs uygulama kayıtları

Anti virüs programları, virüs, truva atı ve kurtçuk gibi zararlı yazılımlarla ilişkili olan dijital adli analiz incelemelerde atlanmaması gereken bir veri kaynağıdır. Anti virüs program kayıtları ile, ilgili bilgisayara herhangi bir zararlı yazılım bulaşıp bulaşmadığı, bilgisayarda tespit edilen ve suç isnadı yapılan dosyaların bu zararlı yazılımlar ilişkili olup olmadığı ve anti virüs programının ne sıklıkla güncellendiği vb. önemli bilgiler elde edilebilir.

8. Kişiden kişiye dosya aktarım uygulamaları (Peer to peer-P2P)

Kişiden kişiye dosya aktarım uygulamaları (P2P), günümüzde yasal olmayan içerikler için büyük bir dosya paylaşım havuzu oluşturmuştur. "Torrent" ismi verilen tanım dosyaları kılavuzluğunda çalışan bu programlara, eMule[75], iMesh[76] ve artık kurulumuna yasal yollardan izin verilmeyen Limewire[77] örnek olarak verilebilir.

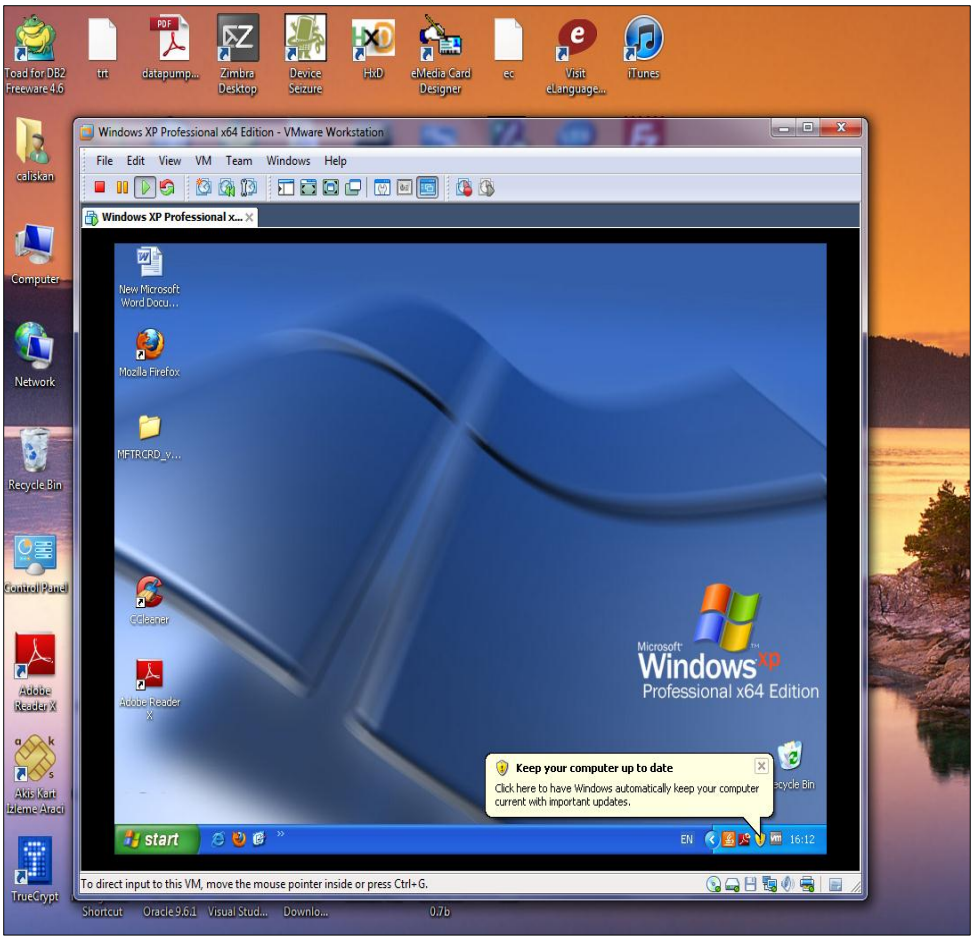
Çeşitli örgütlerin dosya paylaşmak için kullanabildiği bu tip yazılımlar, dijital adli analizde birbiriyle ilişkili delil bilgisayarlarının incelendiği durumlarda daha da önemli hale gelmektedir. Kullanıcıların hangi dosyaları paylaştığı, P2P programlar aracılığıyla herhangi bir veri alışverişi yapıp yapmadığı gibi konular adli mercilere yardımcı olması bakımından faydalı olmaktadır.

9. Sanal işletim sistemi uygulamaları

Daha çok teknik bilgisi yüksek kullanıcılar tarafından tercih edilen *sanal işletim sistemleri* (virtual operating systems), dijital adli analiz incelemelerinde çok farklı bir inceleme alanıdır. Sıradan kişisel bilgisayarlarda tek bir işletim sistemi bulunurken, VMware[78] ve VirtualBox[79] gibi farklı yazılımlar kurarak bir bilgisayarda birden fazla işletim sistemi kullanmak da mümkündür. Bu sayede ilgili işletim sisteminde iz bırakmadan veya daha az iz bırakarak çeşitli işlemler

[75] Emule, http://www.emule.com, erişim tarihi: 07.01.2013.
[76] iMesh, http://www.imesh.com, erişim tarihi: 07.01.2013.
[77] Limewire, http://www.limewire.com, erişim tarihi: 07.01.2013.
[78] VMware, http://www.vmware.com, erişim tarihi: 07.01.2013.
[79] Virtualbox, https://www.virtualbox.org, erişim tarihi: 07.01.2013.

yapılabilir. CD, DVD, USB gibi taşınabilir araçlarla işletim sistemi çalıştırmak ve bilgisayarın asıl işletim sistemine bu sayede dışardan erişmek mümkün olabilmektedir. Bu duruma bir örnek vermek gerekirse, taşınabilir bir veri kaynağı kullanılarak işletim sistemi açıldığında, o işletim sisteminde bulunan dosyalara iz bırakmadan erişilebilir. Normalde mümkün olmayan böyle bir müdahale sonrası, dijital adli analiz çalışmalarında delil etmenin güçleşeceği bazı durumlar oluşabilmektedir.



Şekil 21 - Sanal işletim sistemi ekran kopyası.

Dijital adli analiz çalışmaları esnasında bu tip bir durumla karşılaşılırsa, araştırmanın sanal işletim sistemlerinin yetkinlikleri düşünülerek gerçekleştirilmesi yerinde olacaktır.

D- Harici veriler

Önceki bölümlerde de değinildiği üzere dijital adli analiz, elde edilen bir bilgisayar sabit diski veya belleği üzerinden yapılan inceleme ve araştırmaları kapsamaktadır. Ancak bu durum incelemenin yapılmasındaki temel hedef olan dijital adli deliller kullanılarak gerçeğin açığa çıkarılması için yeterli olmayabilmektedir. Dijital deliller, özellikle de sadece tek bir sabit disk üzerinden yapılan çalışmalar neticesinde sağlam ve güvenilir bir veri kaynağı olmayabilir. Dijital delillerin değiştirile bilirliği, manipülasyona açık doğası, kişi kimlik bilgileriyle ilgili her zaman net bilgiler sunamaması gibi durumlar, bu güvenilmezliğin sebepleri arasında gösterilebilir.

Dijital delillerin şüphe barındırabilen özellikleri nedeniyle gerçeğin açığa çıkması noktasında karar vericilere yardımcı olabilecek başkaca veri kaynakları da kullanılabilir. Bu tip veri kaynaklarına ilişkin örnekler alt başlıklarda incelenmiş durumdadır.

1. İnternet servis sağlayıcı (ISP) verileri

İnternet servis sağlayıcılar (ISP); bilgisayar, akıllı telefon veya tablet gibi elektronik cihazların İnternete erişimi için hizmet veren, sundukları hizmeti almadan İnternete bağlanmanın mümkün olmadığı yapılardır. Türkiye'deki belli başlı internet servis sağlayıcıları Superonline[80], TTNet[81] ve Borusan'ı satın alarak internet altyapısı alanında faaliyetini genişleten Vodafone[82] olarak sıralanabilir.

İnternet servis sağlayıcı verileri, dijital adli analizle birebir ilişkili olmasa da, sahip oldukları veriler bakımından dijital adli delilleri destekleyebilmektedir. Salt sabit disk incelemesiyle elde edilmeyecek veriler, söz gelimi kullanıcının hangi tarihte hangi web sitesini ziyaret ettiği bilgisi, ancak ISP'ler tarafından sağlanacak bilgilerle ortaya çıkarılabilir. Bu nedenle ISP'lerden veri temini, mahkemelerin üzerinde durabileceği sağlam bir bilgi kaynağı olarak görünmektedir. Bu noktada kişisel verilerin mahremiyeti gibi unsurlar da doğal

[80] Superonline, http://www.superonline.net, erişim tarihi: 07.01.2013.
[81] TTNet, http://www.ttnet.com.tr/Sayfalar/Ana-Sayfa.aspx, erişim tarihi: 07.01.2013.
[82] Vodafone, http://www.vodafone.com.tr, erişim tarihi: 07.01.2013.

olarak önem kazanmaktadır. Mahkeme kararı olmadan veya kuvvetli suç şüphesi bulunmadan kişinin İnternet trafiğini dinlemek kuşkusuz tartışmalara açık bir yaklaşım olacaktır.

İnternet trafiğinin izlenmesi ve kaydedilmesi, ISP'lerin teknik imkânlarının bu iş için yeterli olmasıyla beraber, yetki bakımından Bilgi Teknolojileri ve İletişim Kurumu'na[83] bağlı olarak Telekomünikasyon İletişim Başkanlığı[84] tarafından yürütülmektedir.

Dijital adli deliller, soruşturma veya mahkeme aşamasına gelmiş incelemelerde giderek artan oranlarda başvurulan kaynaklardır. Bununla beraber gerçeğin ortaya çıkarılması ve adil karar verilebilmesi için, özellikle İnternet üzerinden işlem yapıldığından şüphelenilen araştırmalarda TİB'e başvurmak ve ilgili verileri talep etmek faydalı bir yaklaşım olarak görünmektedir.

2. Elektronik posta servis sağlayıcı verileri

Elektronik posta (e-mail) verilerin, dijital adli delillerin kaynak olarak yeterli olmadığı durumlarda başvurulabilecek bir bilgi kaynağıdır. Bilirkişilerin yaptığı çalışmalarda, sabit diskler üzerinde bir takım veriler elde edilebilir, bilgisayar kullanıcısının bazı e-postaları görüntülenebilir. Ancak bütün verilere erişmek her zaman mümkün olmamaktadır.

Gmail[85], Hotmail[86], Yahoo[87] vb. e-posta servisleri, kullanıcılarının hangi e-postaları kime ve ne zaman attığı gibi çok önemli verilere sahip durumdadır. Zararlı yazılımla ilişkilendirilen veya organize işlendiğinden şüphelenilen suç unsurları için bu verilere ulaşmak, soruşturmaların sağlığı açısından faydalı olabilmektedir. Kullanıcıların bilgisayarlarından alınan sabit disklerde bu verilerin bir çoğuna ulaşılamayacağından, e-posta servis sağlayıcılarıyla yasal yollardan iletişime geçmek ve soruşturma kapsamında bilgisine ihtiyaç duyulan e-posta hesaplarıyla ilgili ayrıntılı veriler almak faydalı olacaktır.

---

[83] BTK, http://www.tk.gov.tr, erişim tarihi: 07.01.2013.
[84] TİB, http://www.tib.gov.tr/tr, erişim tarihi: 07.01.2013.
[85] Gmail, https://mail.google.com/mail, erişim tarihi: 07.01.2013.
[86] Hotmail, https://login.live.com, erişim tarihi: 07.01.2013.
[87] Yahoo, https://login.yahoo.com, erişim tarihi: 07.01.2013.

3. Sosyal medya uygulamaları bilgileri

Dijital adli delillerin yetersiz kaldığı durumlardan bir diğeri de, kullanıcının İnternet üzerinde ve özellikle de sosyal medyada gerçekleştirdiği faaliyetlerin tespit edilememesidir. Twitter[88], Facebook[89] gibi son derece yaygın sosyal medya uygulamaları üzerinden paylaşılan resim, video veya yazılı iletiler, soruşturmalara yön verici nitelikte değerli veriler içerebilmektedir. Bu kaynaklardan veri elde edebilmek ve ilgili kullanıcıların hangi tarihlerde hangi IP'lerden erişim sağladığı gibi önemli bilgileri tespit etmek için, servis sağlayıcılarla iletişime geçmek yerinde bir davranış olacaktır.

V. Dijital adli analizin tarafları ve karar verme

Dijital adli analiz çalışmaları, gerek inceleme gerekse raporlama sonrası etkileri bakımında birden çok kişiyi etkilemektedir. Teknik analizi yapacak uzman (bilirkişi) haricinde; sonuçları yorumlayacak karar verici bir mercii (hakim), analizi yapılan dijital delillerin sahibi (sanık), dijital delillere el koyan ve saklayan otorite (emniyet mensupları), sanık avukatları ve savcılık tarafları olayın içinde yer almaktadır.

Bilirkişi uzmanları, dijital adli analizin belkemiği niteliğinde olan tetkik görevini ifa etmektedir. Bununla birlikte bu tetkik ve analizler soruşturmaların nihai bir karara bağlanması için elbette yeterli olmayacaktır. Haddi zatında karar verici merci zaten dijital adli analiz uzmanı da değildir. Özellikle ceza davalarında temel amaç, karar verici hâkimin konuyu anlaması ve yorumlaması, takdir hakkını kullanması ve neticede bir karar vermesidir.

Bir önceki bölümde detayı izah edilen dijital adli analizin 4. aşaması olan analiz; tetkik ve nihai analiz olmak üzere iki bölümden müteşekkildir. Dijital adli analiz uzmanının yapacağı tetkikler, bir sonraki aşamada hâkimin yorumlayacağı ve diğer delillerle birleştirerek bir analiz yapacağı veri kaynağı olacaktır. Ancak çalışmanın teknik detaylarına karar verici merciinin vakıf olmaması, ki bu çok sık

[88] Twitter, https://twitter.com, erişim tarihi: 07.01.2013.
[89] Facebook, https://facebook.com, erişim tarihi: 07.01.2013.

karşılaşılan doğal bir durumdur, bir takım sıkıntıları beraberinde getirmektedir. Mahkemeye "0" ve "1" rakamlarından oluşan bir bellek kopyasını sunmanın fayda getirmeyeceği açıktır. Bununla birlikte, dijital adli analiz çalışmalarının sonuçları, kimi zaman basite indirgenemeyecek seviyede kalabilir. Bu gibi durumlarda ise karar verici makamların bilgisayar teknolojisi ve adli analizin teknik boyutuyla ilgili bilgi sahibi olması gerekliliği ortaya çıkacaktır.

Dijital adli analiz uzmanları, çalışmalara teknik açıdan yaklaşır bilgi ve tecrübelerini işlerine yansıtır. Oluşturdukları rapor, tespit ettikleri bulguların yazıya dökülmüş halidir. Ancak dijital adli analiz bilimin belki en önemli halkası bundan sonra başlar. O da tespit edilen bu bulguların yorumlanmasıdır**.** Burada sıra karar verici mercilere gelir. Dolayısıyla herhangi bir çalışma kapsamında, dijital adli analiz uzmanının bilemeyeceği ve davaya konu taraflarla ilgili dijital olmayan bir takım bilgilerin de hesaba katılarak yorumlanması gerekmektedir. Türk hukuk sisteminden örnek verecek olursak, bilgisayarında suç unsuru tespit edilen bir sanığa ilişkin dijital adli analiz raporları, savcılığın hazırladığı iddianamedeki diğer unsurlarla birlikte değerlendirilmelidir. Bilirkişinin dijital adli analiz aşamasında elde ettiği bir takım teknik veriler, ancak karar vericilerin (hâkimlerin) bilebileceği bir takım başka verilerle kıyaslanmalıdır. Bilgisayarda tespit edilen suç unsurunun oluştuğu tarihlerde sanığın başkaca bir faaliyeti var mıdır? ISP ve telefon dinleme kayıtları ne göstermektedir? Sanık yurtdışına çıkmış mıdır? Teknik takibe takılmış mıdır? Bu ve benzeri sorular konuyu netleştirecektir. Bu nedenle dijital adli analiz, analiz aşamasının 2. adımından itibaren teknik olmayan ancak konu hakkında daha detaylı bilgiye sahip şahısların etki alanına girmektedir.

Sonuç olarak dijital adli analiz, birçok tarafın etkileşimi ile sürdürülen bir çalışmadır. Delillerin güvenilirliği, zararlı yazılımlar ve delil etkisinde bulguların güven seviyeleri, sonuçta bilirkişinin ortaya çıkaracağı tespitlerdir. Son aşamada ise bütün bu verileri derleyip toplayan, ilişkisini sorgulayan ve karar veren taraf ise hakim olacaktır.

§3. Zararlı yazılımlar

I. Tanım

Günümüzde hayatın hemen her alanında kullanmakta olduğumuz bilgisayarlar, akıllı telefonlar, tablet bilgisayarlar hatta televizyonlar ve oyun konsolları; üzerinde çalışan uygulamalar aracılığıyla işlem yapmaktadır. İletişim, bilgi edinme ve hatta eğlence ihtiyaçlarımız bile bu yazılım-donanım teknolojileriyle karşılanmaktadır. Bütün bu cihazların altyapısı, her geçen gün daha hızlı, daha küçük ve daha az enerji tüketen donanımlardan müteşekkilse de; ihtiyaçlarımıza uygun çözümler bu donanımları kullanan yazılımlar aracılığıyla sunulmaktadır.

Yazılım, "bir bilgisayarda donanıma hayat veren ve bilgi işlemde kullanılan programlarda; yordamlar, programlama dillerinin oluşturduğu *betikler* (script) ve belgelemelerin tümü"[90] olarak ifade edilebilir. Bu tanımdan hareketle her türlü bilgisayar programının ve çalıştırılabilir kod parçacığının bir yazılım olduğu söyleyebilir.

Yazılımlar her ne kadar ihtiyaçlarımızı karşılayan yararlı bilişim teknolojisi ürünleri olarak görülse de, tanım ne yazık ki bununla sınırlı değildir. Yaşamın her alanında olduğu gibi bilgisayar teknolojilerinde de kötüye kullanım sıklıkla karşılaşılabilen bir durum halini almıştır.

Zararlı yazılımlar (malware), bilgisayar sistemlerine ve bu sistemlerin kullanıcılarına zarar vermek, bilgi çalmak, rahatsız etmek ve bu sayede maddi manevi menfaat elde etmek için hazırlanmış kötücül yazılımlardır. Bu menfaatler arasında ilk akla gelenler para, şöhret, itibar ve kişisel tatmin gibi unsurlar olmakla beraber liste bununla sınırlı değildir. Yaygınlaşan bilgisayar kullanımı ile hemen her alana nüfuz eden sistemlerden ötürü devletlerin ve istihbarat örgütlerinin de ilgisini çeken zararlı yazılımlar; siber savaş[91], siber istihbarat,

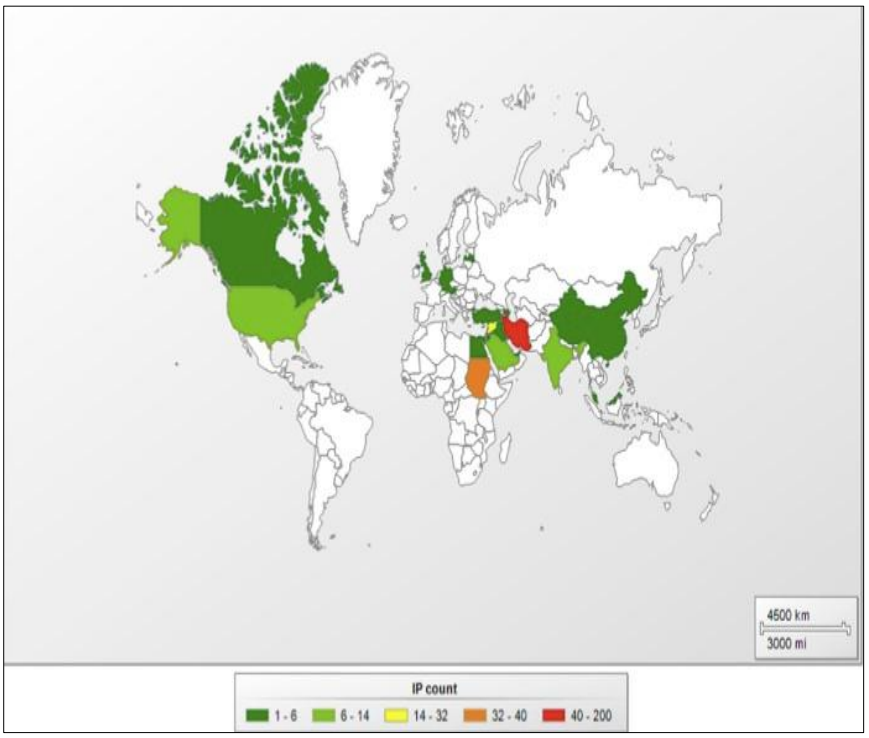
[90] Yazılım, http://tr.wikipedia.org/wiki/Yaz%C4%B1l%C4%B1, erişim tarihi: 07.01.2013.
[91] Charles G. Billo, Wellton Chang, Cyber warfare an analysis of the means and motivations of selected nation states, Hanover 2004 ("Billo/Chang"), sf. 27.

hacktivizm[92] ve siber terörizm[93] faaliyetlerinde de etkin şekilde kullanılmaya başlanmıştır. *Bilişim sistemi saldırganlarının* (hacker) motivasyonlarıyla ilgili detaylı bilgiler bir sonraki bölümde daha detaylı ele alınacaktır.

Günümüzde zararlı yazılımlar aracılığıyla geleneksel savaş tekniklerinin ötesine geçen devletler, bilişim güvenliği uzmanlarınca hazırlanan bu gibi zararlı yazılımlar ile hedeflerine ciddi zararlar verebilmektedir. Bu çalışmalara örnek olarak yakın zaman önce varlığı tespit edilen Flame[94] ve selefi Stuxnet[95] zararlı yazılımları incelenebilir.

İran'ın nükleer araştırma faaliyetlerine yönelik hazırlandığı tespit edilen bu zararlı yazılımın dünyada en yoğun olarak İran'da görülmesi rastlantı değildir[96]. Amerika Birleşik Devletleri ve İsrail'in ortak projesi olduğu düşünülen Flame, geleneksel zararlı yazılımların oldukça dışında faaliyet göstermekte ve devletlerin kendi çıkarları doğrultusunda kullandıkları bir siber silah halini almaktadır.

[92] Dorothy E. Denning, "Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy", ABD 2001 ("Denning"), sf. 25.
[93] Maura Conway, What is Cyberterrorism?, Dublin 2002 ("Conway"), sf 5.
[94] Flame virus, most sophisticated malicious code ever seen, was developed by U.S. Government, http://lighthousechurchinc.org/fire/newsnprophetic_pdf/FlameVirusDevelopedByUS.pdf.
[95] Amr Thabet, Stuxnet Malware Analysis Paper, Alexandria 2011 ("Thabet"), sf 3.
[96] Detaylı bilgi için bkz. "Şekil 22 - Flame Zararlı Yazılımından Etkilenen Bölgeler", sf. 75.



Şekil 22 - Flame Zararlı Yazılımından Etkilenen Bölgeler.

II. Zararlı yazılım üreticilerinin motivasyonları

Zararlı yazılım üreticilerinin gün geçtikçe değişen farklı motivasyonları bulunmaktadır. Zararlı yazılımların üretilmesinde ve yayılmasında en sık karşılaşılan sebepler aşağıdaki gibi sıralanabilir.

A- Eğlence, hobi ve ideolojinin yayılması

Bazı malware üreticileri yaptıkları işi sanat olarak görmektedir. Dolayısıyla yeni zararlı yazılımlar geliştirmek, bunları yaymak ve her yeni zararlı yazılımda daha komplike ve başarılı saldırılar yapmak bu tip saldırganların temel hedefidir. Üretilen zararlı yazıılmları kendi ideolojisini yaymak için kullananlar da bu grupta değerlendirilebilir.

B- Şaka ve korkutma

Bu tip saldırılarda, bilgisayarına zararlı yazılım bulaşan kullanıcısı korkutularak veya kandırılarak şaka yapılması amaçlanır. Son derece kaba, tabiri caizse "eşek şakası" kabul edilen bu tip zararlı yazılımlar genellikle arkadaş-dost çevresinde eğlence konusu olması için yapılmaktadır. Açılan bir dosyanın normal yollarla kapatılamaması, bilgisayardaki bütün verilerin silindiğine dair ekrana çıkan uyarılar vb. örnekler verilebilir.

C- Bilgisayar bilgisini gösterme ve saygınlık kazanma

En sık görülen malware çeşitlerindendir. Bilgisayara bulaştığı anda, zararlı yazılım üreticisinin yön verdiği uygulamalar çalışmaya başlamaktadır. Web sayfalarına yönelik saldırılar ve bu amaçla tasarlanmış zararlı yazılımlar bu kategori değerlendirilebilir.

D- Endüstriyel casusluk

Saldırganların bir şirketin gizli verilerini çalmak ve bunu kendi menfaatlerine kullanmak amacıyla ürettikleri zararlı yazılımlar bu kategoride değerlendirilir. Genellikle kötü niyetli rakip firmalar tarafından el altından yapılan işlemlerdir.

E- Araştırmalar ve deneysel çalışmalar

Bu tip zararlı yazılımlar, genellikle araştırmacılar ve bilimsel kuruluşlar tarafından özel olarak hazırlanmaktadır ve aksi giden bir durum olmadığı sürece internette yayılmamaktadır. Anti-Virus üretici firmaları da bu kapsamda çeşitli faaliyetlerde bulunmaktadır. Zararlı yazılımların nasıl tehditler oluşturabileceği hakkında fikir edinmek ve hazırlık yapmak için bu tip çalışmalar önem arz etmektedir.

F- Dijital barbarlık

Sanal dünyada saldırganlık ve rastgele zarar verme anlamına gelir. Bu tip zararlı yazılımlar bulaştıkları bilgisayardaki bütün verileri silebilir, değiştirebilir ve sistemi kullanılamaz hale getirir. Kötü niyetli ve ruh hali bozuk kişilerce böyle zararlı yazılımlar hazırlanabilmektedir.

G- İntikam

Özellikle şirketlerin eski veya memnun olmayan çalışanları tarafından gerçekleştirilmektedir. Kuruma/kişiye özel olarak tasarlanır ve saldırganın amacına göre farklı hedefler içerebilir. Çalıştığı kuruma milyonlarca TL'lik zarar veren saldırılar geçmişte yaşanmıştır.

III. Sınıflandırma

Zararlı yazılım terimi, *malfunction* (işlev bozukluğu) ve *software* (yazılım) kelimelerinin birleşmesiyle oluşmuştur. İşlev bozukluğu olan yazılımlar ya da başka bir deyişle zararlı yazılımlar, bu fonksiyonlarını icra ederken kullandıkları teknikler ve sahip oldukları yetkinlikler itibariyle farklı başlıklar altında toplanabilir. Temel özelliklerine göre zararlı yazılımların sınıflandırılması aşağıdaki gibidir.

A- Virüs

En bilinen zararlı yazılım türü olan virüsler[97], genellikle *.exe uzantılı çalıştırılabilir dosyalar aracılığıyla internetten indirilen dosyaların içinde veya USB disk gibi taşınabilir bellekler ile bilgisayarlara bulaşmaktadır. Bulaştığı bilgisayarda kodlandığı işlevi yerine getiren virüs, başta internet olmak üzere veri alış verişi yapılabilen her tür yöntemi kullanabilmekte ve hızla çoğalmaktadır.

[97] What Is the Difference: Viruses, Worms, Trojans, and Bots?, http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html, erişim tarihi: 07.01.2013.

Virüslerin en ayırt edici özelliği işte bu bulaşma tekniği ve hızla yayılma eğilimidir.

Virüsler geneli itibariyle DOS (Denial of Service) etkisi göstermez ve bulaştıkları sistemde herhangi bir servis dışı bırakma durumuna yol açmaz. Ancak bazı virüsler sistem dosyalarına bulaşır, önemli dosyaların üzerine kendi verilerini yazarlar ve böylece sistem çalışmaz hale gelebilir.

Virüsler etkileri itibariyle çok çeşitli amaçlara yönelik işlem yapabilirler. Bazı virüsler sadece önemli verileri toplayarak yönetim merkezlerine iletirler. Bazıları ise tamamen zarar vermek için tasarlanmıştır, kullanıcının bütün bilgisayarına kullanılamaz hale getirmeye çalışır. İnternetten oynanan oyunların parolalarını toplamaya yönelik geliştirilen virüsler bile mevcuttur[98]. Sonuç olarak, virüsler, programcısının isteğine göre tasarladığı ve bulaştığı sistemlerde bu amaca yönelik faaliyet gösteren zararlı programlardır denilebilir. Virüslerin bu esnek tasarım olanağı, adli bilişim incelemelerinde dikkate değer bir husus olmaktadır.

B- Bilgisayar kurtçukları

Birçok açıdan virüslere benzeyen *kurtçuklar* (worm), bulaştığı sistemlerde kullanıcı verisini ele geçirebilir ve bilgisayara zarar verecek başkaca faaliyetlerde bulunabilir. Virüslerden ayrıştığı özellikler ise;

- Virüsler başka bir program veya dosyaya bulaşarak çoğalır ve yayılır. Buna karşın kurtçuklar tek başlarına çalışırlar, başka bir uygulamayla birlikte hareket etmek zorunda değildir.

- Virüsler bilgisayardan bilgisayara e-posta, dosya paylaşım ortamları veya taşınabilir bellekler vb. aracılarla yayılırken, kurtçuklar *ağ* (network) altyapısını kullanarak yayılır.

- Virüsler kullanıcını etkileşimine ve hatasına dayalı yayılma politikası takip ederken, kurtçuklar daha ziyade sistem açıklarına dayalı çalışırlar ve kullanıcı etkileşimine daha az ihtiyaç duyar.

---

[98] MSRT Observations – Online Game Password Stealers,, http://blogs.technet.com/b/mmpc/archive/2009/02/19/msrt-observations-online-game-password-stealers.aspx, erişim tarihi: 07.01.2013.

Bu açıklamalara paralel olarak belirtmekte fayda olan bir nokta da; virüsler ve kurtçuklar yayılma yaklaşımı olarak birbirlerinin alanına girebilirler. Bu zararlı yazılımları net bir çizgi ile ayırmak ve sınıflandırmak mümkün değildir.

Virüsler terminolojik olarak son yıllarda daha yoğun kullanılmaktadır. Hatta kurtçuk ifadesi artık yerini virüslere bırakıyor demek yanlış olmayacaktır.

C- Truva atları

Yunanların Truvalılarla yaptığı savaşta[99] kullanılan ahşap attan esinlenen truva atı zararlı yazılım türü, savaşta kullanılan taktiğe benzer bir yaklaşımla hareket eder. Saldırgan, uzaktan erişim sağlayacak zararlı bilgisayar kodlarını içine enjekte ettiği e-posta ve anlık mesajlaşma vb. araçlarını kurbanına gönderir. Truva atları hedefli saldırılara verilebilecek güzel bir örnektir. Virüslerin aksine belirli bir hedefe yönelik olarak önceden tanımlanmış işlevleri yerine getirir.

Truva atı ya da trojan kendisini olduğundan farklı ve tehlikesiz göstererek gizleyebilen zararlı bir programdır. Bu programlar kullanıcıya arzu edilen bir fonksiyonu yerine getirecek bir yazılım olarak görünen, aslında kullanıcının bilgisayarına izinsiz erişimleri kolaylaştıran bir kötücül yazılımdır. Truva atları kendilerini kopyalamaz.[100]

Truva atı zararlı yazılımları, virüs ve kurtçukların aksine kendi kendilerine çoğalmaz. Hedeflerine yönelik hazırlandıkları için sadece o amaç için programlanmışlardır. Bu özelliğinden dolayı adli analiz incelemelerinde üzerinde dikkatle çalışılması gereken bir zararlı yazılım türüdür. Truva atının hangi kanalla geldiği, davaya konu dijital delillerde ne gibi işlemler yaptığı ve kim tarafından gönderilmiş olabileceği mevzuları ayrıca detaylı olarak incelenecektir.

---

[99] Truva Savaşı, http://tr.wikipedia.org/wiki/Truva_Savaşı, erişim tarihi: 07.01.2013.

[100] Mustafa Ünver, Cafer Canbay, Yüksel Günaydın, Köle Bilgisayar ve Köle Bilgisayar Ağları (Zombi ve Botnetler), Ankara 2010 ("Ünver/Canbay/Günaydın"), sf 8.

D- Rootkitler ve botlar

Rootkit tanım olarak "Çalışan süreçleri, dosyaları veya sistem bilgilerini işletim sisteminden gizlemek suretiyle varlığını gizlice sürdüren bir program veya programlar grubudur".

Rootkitler tek bir program olabileceği gibi birden çok programın birleşmesiyle de oluşabilir. Temel amaçları hackerların[101] bir sistemi uzaktan ve tamamen yönetebilmesini sağlamaktır. Rootkit bulaşan bilgisayarlar, komuta merkezindeki bilgisayar korsanlarından aldığı komutları daha fazla bilgisayarı ele geçirmek için bir zıplama tahtası olarak kullanılabilmektedir. Rootkitleri virüslerden ve kurtçuklardan ayıran en temel özellikler; çok gizli çalışmaları, kendi kendine çoğalmaları ve kontrol merkezleriyle düzenli haberleşmeleridir.[102] Bu özellikleri sayesinde bulaştıkları sistemlerde yıllarca fark edilmeyebilirler.

Rootkitlerle ilişkilendirilebilecek bir terim de "bot" ifadesidir. Botlar, robot kelimesinden türetilmiştir ve otomatik çalışan, belirli görevleri insan müdahalesine ihtiyaç duymadan yapabilen sistemlerdir.

Botlar, iyi amaçlar için kullanılabileceği gibi zararlı yazılımların ve bilgisayar saldırılarının bir parçası olarak da kullanılabilmektedir. Rootkit bulaşan ve uzaktan yönetilmeye başlanan sistemler, bu noktada bot ismini almaktadır. Böylece saldırgan rootkitler aracılığıyla ele geçirdiği sistemleri (botları) istediği amaç için kullanabilir. Botların en sık kullanıldığı saldırı tipi DDOS atağıdır. DDOS, *Dağıtık Servis Dışı Bırakma* (Distributed Denial of Service) saldırısı anlamına gelmekte olup, günümüzde çok sayıda kurumu hedef alan ve bu kurumların internetten verdiği hizmetlerde kesintiye yol açan bir tekniktir. Çok sayıda botun katıldığı saldırının başarı yüzdesi de paralel olarak artacaktır[103].

---

[101] Hacker kelimesi "Çökertici, bilgisayar korsanı" anlamına gelmektedir. Türkçe'de kullanımı giderek yaygınlaşan bu İngilizce asıllı kelime, bilgisayar sistemlerine izinsiz giren kişileri ifade eden argo bir sözcüktür.

[102] What Are Rootkits?, http://www.5starsupport.com/tutorial/rootkits.htm, erişim tarihi: 07.01.2013.

[103] Yeni Nesil DDoS Saldırıları ve Savunma Yöntemleri - I, http://www.bilgiguvenligi.gov.tr/ag-guvenligi/yeni-nesil-ddos-saldirilari-ve-savunma-yontemleri-i.html, erişim tarihi: 07.01.2013.

E- Diğer zararlı yazılımlar

Virüs, kurtçuk, truva atı ve rootkitlerin dışında başka zararlı yazılım tipleri de mevcuttur. Bulaşma ve yayılma teknikleri benzer olmakla beraber farklı hedefler gözeten bu zararlı yazılımlar arasında; kullanıcıların bilgisayar hareketlerini izleyip raporlayan ve topladığı verileri analiz merkezlerine ileten *casus yazılımlar* (spyware); yüklenirken kullanıcının rızasını alan, ancak kullanıcının beklemediği ve istemediği ölçüde internet reklamı yayınlayan *reklam yazılımı* (adware), internete bağlı telefonlara yüksek fatura getirecek aramalar yapan ve bunu kullanıcıdan gizleyerek maddi menfaat elde etmeye yönelik *telefon programları* (dialers) sıralanabilir.

Zararlı yazılım olmasa da, kullanıcıyı rahatsız eden ve istem dışı çalışan uygulamalara bir örnek de *istem dışı postalardır* (spam). Uluslararası alanda kesin kabul görmüş, üzerinde mutabakat sağlanmış ve çerçevesi tam olarak belirlenmiş bir spam tanımı bulunmamaktadır. Bununla birlikte, aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere zorlayıcı nitelikte gönderilmesine spam denmektedir. İstek dışı haberleşme olarak da adlandırılmaktadır.[104]

IV. Zararlı yazılımların dağılımı

Zararlı yazılımlar çoğu zaman kullanıcı hatası ve gerekli teknik önlemlerin alınmamış olması nedeniyle bilgisayarlara bulaşır. Kullanıcı zaaflarından faydalanarak gerçekleştirilen sosyal mühendislik atakları, kullanıcının bir şekilde ikna edilerek zararlı yazılımı bilgisayarına bulaştırması ile gerçekleşir. Teknik önlemlerin alınmaması; güncel işletim sistemi kullanılmaması, anti-virüs anti-malware güvenlik duvarı vb. güvenlik önlemlerinin alınmaması durumlarında ise kullanıcı etkileşimi olmadan da bu tip zararlı yazılımlar bulaşabilir.

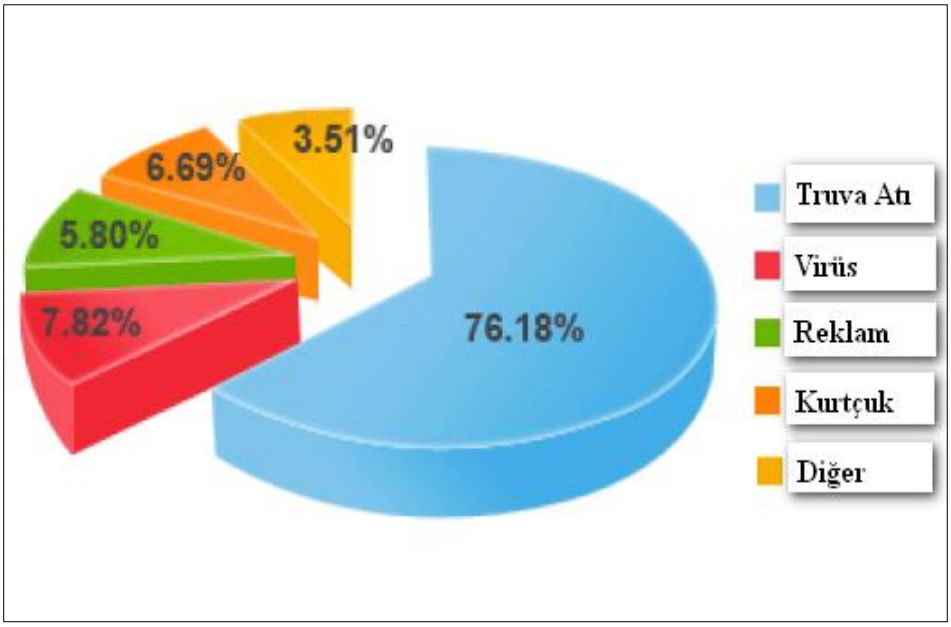
Zararlı yazılımlar, dijital adli analiz çalışmalarına etkisi bakımından iki başlıkta değerlendirilebilir. Bunlardan ilki genel amaçlı ve rastgele yayılan zararlı

[104] Özgür Öztürk, "E-posta'larda Spam Sorunu ve Çözüm Önerileri", Ankara 2009 ("Öztürk"), sf 27.

yazılımlar, diğer grup ise hedefli düzenlenen saldırılarla bulaştırılan zararlı yazılımlardır. Bunun dışında, zararlı yazılımların dünyada ve ülkemizde rastlanılma oranları da dikkate alınması gereken bir konudur.

A- Dağılım oranları

Zararlı yazılımların türlerine göre yapılan çalışmalarda, zararlı yazılımların rastlanma oranlarının dönem dönem veya ülkeden ülkeye değişiklik gösterdiği anlaşılmaktadır. İlk zararlı yazılımlar daha çok "kurtçuk" olarak hazırlanırken, günümüzde "truva atları" bayrağı devralmıştır. Gerçekleştirilen en son araştırmalara göre [105], Truva atları diğer bütün zararlı yazılım türlerinin toplamından daha sık rastlanır olmuştur (Şekil 23).

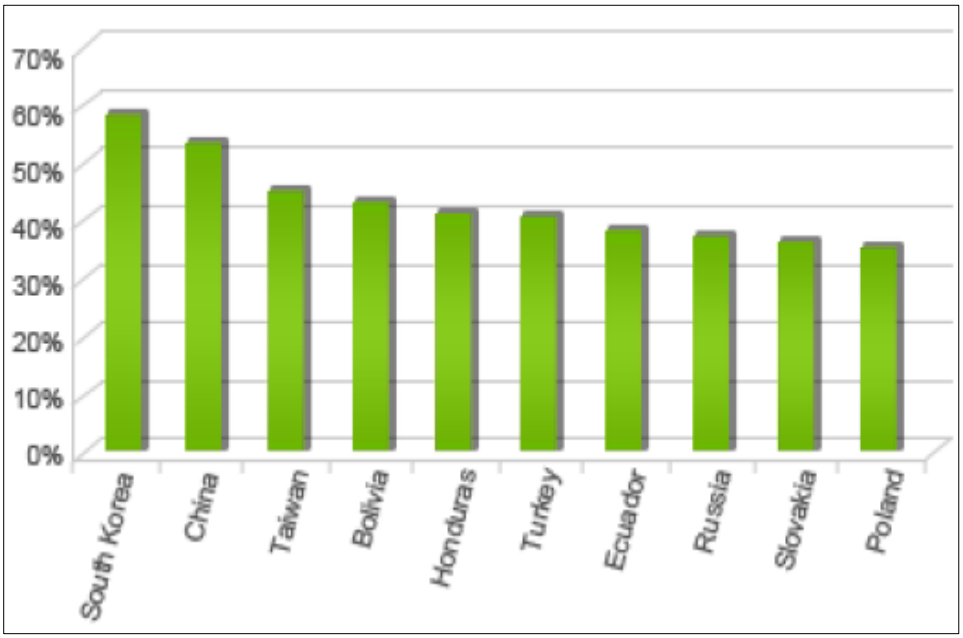


Şekil 23 - Zararlı yazılım türlerine göre yaygınlık oranları.

Zararlı yazılımların ülke bazlı dağılım oranlarında ise, ülkemiz açısından vahim bir tablo ile karşılaşılmaktadır (Şekil 24). Bu çalışmaya göre, ülkemizdeki bilgisayarların %40'ında yazılım bulunduğu tahmin edilmektedir. Bir üstteki zararlı yazılım türlerinin dağılım oranıyla birlikte değerlendirildiğinde, ülkemiz

[105] PandaLabs Quarterly Report, http://press.pandasecurity.com/wp-content/uploads/2012/08/Quarterly-Report-PandaLabs-April-June-2012.pdf, erişim tarihi: 07.01.2013.

bilgisayarlarının %30'una uzaktan erişim yapılabilmesine imkan tanıyan zararlı yazılımların varlığı görülmektedir. İşte bu rakamlar, dijital adli analiz çalışmalarında zararlı yazılım etkisinin üzerinde durulması gereken önemli bir konu olduğuna işaret etmektedir.



Şekil 24 - Ülkelere göre zararlı yazılımların dağılımı.

B- Dağılma teknikleri

Zararlı yazılımlar, hazırlanış amaçlarına uygun olarak farklı yöntemlerle dağılabilmektedir. Kesin bir sınır olmamakla birlikte bu durum, zararlı yazılımın hedef gözetmeksizin dağılması ve belirli bir hedefe göre dağılması olmak üzere iki başlıkta incelenebilir.

1. Rastgele yayılan zararlı yazılımlar

Genel amaçlı zararlı yazılımlardan; spam[106] e-posta gönderimi, internet bankacılık bilgilerinin çalınması, hizmet dışı bırakma saldırılarında (DDOS)

[106] "Yığın mesaj" olarak da anılan Spam e-postalar, "e-posta, telefon, faks gibi elektronik ortamlarda çok sayıda alıcıya aynı anda gönderilen gereksiz veya uygunsuz iletiler"in genel adıdır. Spam e-postalar hakkında detaylı bilgi için bkz. http://tr.wikipedia.org/wiki/Y%C4%B1%C4%9F%C4%B1n_mesaj, erişim tarihi: 07.01.2013.

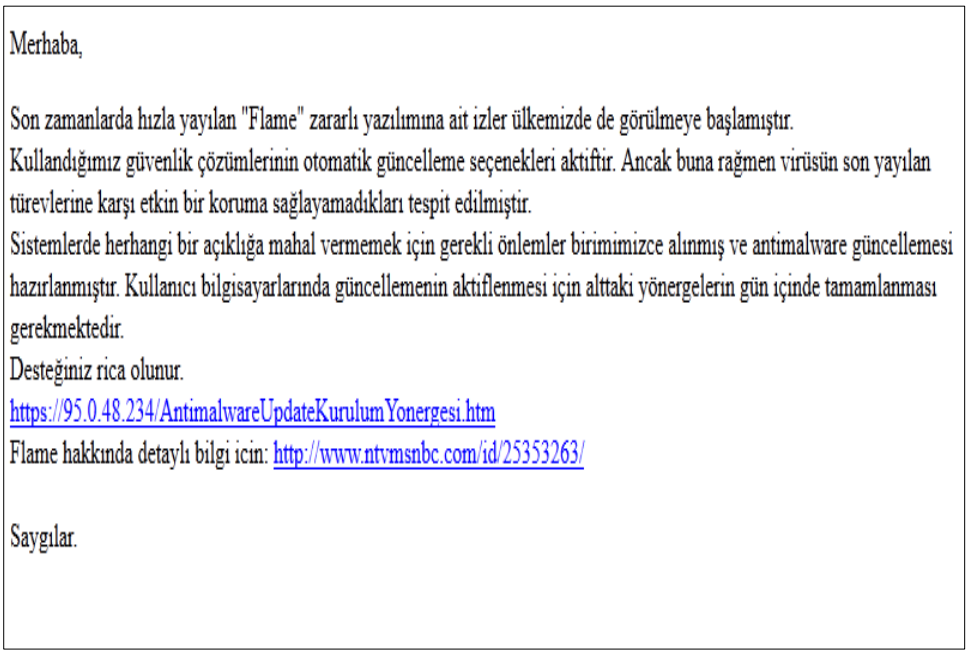
bulunulması, reklam yayınlanması gibi çeşitli faaliyetler yoluyla maddi çıkar sağlama amacıyla kullanılan zararlı yazılımlardır. Bu zararlı yazılımların birçoğu, dijital adli analiz çalışmalarını etkileyebilecek "bilgisayarı uzaktan kontrol etme" yetkinliklerine sahip olmamakla birlikte, kısıtlı birtakım işlemleri yapabilecek ve bilgisayar kullanıcılarından habersiz işlem yürütebilecek yetkinliklere erişebilir. Bu noktada kesin bir ayrım yapmak mümkün görünmemektedir. Bununla birlikte, zararlı yazılımın "hedefli" olarak gönderildiğine emin olunması durumunda analiz incelenmesi gereken noktalar farklılaşacaktır. Bununla ilgili değerlendirmeler bir sonraki başlıkta ele alınmıştır.

2. Hedefli zararlı yazılımlar

Zararlı yazılımların dijital adli analizi etkileyebilecek türleri daha çok "hedefli zararlı yazılımlar" olmaktadır. Bu tip hedefli zararlı yazılımlar, saldırı yapılan kullanıcıya özel olarak hazırlanmakta ve tuzağa düşen kullanıcının bilgisayarına zararlı yazılım bulaşmaktadır.

Hedefli zararlı yazılımlar, daha çok "sosyal mühendislik" teknikleriyle kullanıcıya bulaştırılmaktadır. Sosyal mühendislik, sosyal teknikler kullanılarak kişinin kaldırılması ve bilgisayarına zararlı yazılım bulaştırılması tekniğidir. Telefonla zararlı bir siteye yönlendirme, aldatıcı bir e-posta gönderip verilen *bağlantıyı* (link) tıklatma veya zararlı yazılım bulunan bir taşınabilir diski (veya CD, DVD vs.) kullanıcının bir şekilde çalıştırmasını sağlama buna örnek verilebilir.

Hedefli saldırılarda kullanılan sahte e-posta içerikleri, saldırganın hedefine göre değişkenlik göstermektedir. Kişisel ilgi alanları, beklediği bir haber veya parasal bir menfaat ile ilgili e-postalar daha başarılı olmaktadır. E-posta eklentisinde veya metin kısmında verilen bağlantı adresinde bulunan zararlı yazılım, kullanıcının bilgisayarında bu durumu engelleyebilecek bir zararlı yazılım olmadığı takdirde çalışacak ve bilgisayara uzaktan bağlantı kurulabilecektir. Örnek bir e-posta içeriği Şekil 25'de görülmektedir.


Merhaba,

Son zamanlarda hızla yayılan "Flame" zararlı yazılımına ait izler ülkemizde de görülmeye başlamıştır.
Kullandığımız güvenlik çözümlerinin otomatik güncelleme seçenekleri aktiftir. Ancak buna rağmen virüsün son yayılan türevlerine karşı etkin bir koruma sağlayamadıkları tespit edilmiştir.
Sistemlerde herhangi bir açıklığa mahal vermemek için gerekli önlemler birimimizce alınmış ve antimalware güncellemesi hazırlanmıştır. Kullanıcı bilgisayarlarında güncellemenin aktiflenmesi için alttaki yönergelerin gün içinde tamamlanması gerekmektedir.
Desteğiniz rica olunur.
https://95.0.48.234/AntimalwareUpdateKurulumYonergesi.htm
Flame hakkında detaylı bilgi icin: http://www.ntvmsnbc.com/id/25353263/

Saygılar.

Şekil 25 - Sahte e-posta örneği.

Bu zararlı yazılımların bulaştığı bilgisayarlar, dijital adli analiz uzmanlarının bu yönde inceleme yapmasını gerektiren unsurlar barındırır. Bilgisayarda bulunan zararlı yazılımın tesadüfen mi bulaştığı veya kasıtlı olarak ilgili bilgisayara bulaştırılıp uzaktan dosya aktarımı vb. gibi delil bütünlüğünü bozacak etkenlere mi maruz kaldığı, delil güvenilirliğini doğrudan etkilemektedir. Teknik inceleme ve analizler, bu gibi durumlarda çok detaylı araştırma yapılması gerektiğini göstermektedir. Hedefli saldırılarla bile bulaşmış olsa, sadece zararlı yazılımın varlığı tek başına bir anlam ifade etmeyecektir. Konunun hukuki boyutuyla ilgili detaylı analizler ilerleyen bölümlerde tekrar ele alınacaktır.

§4. *Delil karartma* (anti-forensics)

Delil karartma (anti-forensics), üzerinde hem fikir kalınan ve herkesçe kabul gören tek bir tanıma sahip bir kavram olarak yorumlanmamaktadır. Dijital delillerde delil karartma, bazı yaklaşımlara göre fark edilmenin önlenmesi ve takip edilmenin zorlaşması[107], bazı yorumlara göre ise sadece sistemlere yönelik sızma (hack) faaliyetlerinden sonra bırakılan izlerin silinmesi anlamına gelmektedir[108].

Adli bilişim" ve delil karartma alanında araştırma yapan akademisyenler ve teknik otoritelerin görüşleri bir araya getirildiğinde, delil karartma kavramı için "dijital adli delillerin toplanması, incelenmesi ve yorumlanması faaliyetlerini sekteye uğratarak bu delillerden anlamlı sonuçlar çıkarılmasının engellenmesi" tanımı yapılabilir.

Delil karartma işlemleri belli başlı kategoriler altında değerlendirilmektedir. Her bir teknik, bir şekilde dijital adli delillerin kullanılamaz hale gelmesini ve bırakılan izlerden faydalanılamamasını hedeflemekle birlikte, bu işlemler için farklı yöntemler izlenebilmektedir.

Peron ve *Legary'ye* göre delil karartma işlemleri; "temizlemek, gizlemek, manipüle etmek ve delilin oluşmasını engellemek" şeklinde dört ana başlıkta değerlendirilmelidir [109] . Benzer şekilde "gizlemek, kalıntı temizlemek, izleri karmaşıklaştırmak ve delilleri ortaya çıkaran araçları kullanılamaz hale getirmek" şeklinde farklı sınıflandırmalara da rastlanabilmektedir[110].

I. Delillerin imha edilmesi

Delil karartma tekniklerinin en başarılısı, delillerin bulunduğu sabit disk, taşınabilir disk, CD vb. materyalleri fiziksel olarak imha etmektir. Bir sonraki bölümünde değinilen *temizlik* (wipe) işlemlerinden sonra bile, bir takım verilerin

---

[107] Catch me if you can, http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-foster-liu-update.pdf, erişim tarihi: 07.01.2013.
[108] Ryan Harris, Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, Indiana 2006 ("Harris"), sf. 4.
[109] Christian S.J. Peron, Michael Legary, Digital anti-forensics: Emerging trends in data transformation techniques, USA 2002 ("Peron/Legary"), sf. 4.
[110] Dr. Marcus K. Rogers, Anti-forensics, San Diego 2005 ("Rogers"), sf 5.

silinememiş olması veya sistem dosyalarında bir takım artık verilerin kaldığı durumlar olduğu bilinmektedir. Bu nedenle çok hassas verilerin bulunduğu disklerin, ne şimdi ne de gelecekte hiç bir zaman tekrar elde edilememesi için bu yöntemler uygulanabilmektedir.

Şekil 26 - Parçalanmış bir sabit disk.

Günümüzde istihbarat dairelerinin ve çok hassas veri işleyen kurum kuruluşların, geçmişte kullandıkları sabit diskleri çok küçük parçalara ayırarak imha ettiği bilinmektedir. Bu yöntem kullanılarak işlem görmüş sabit disklerden veri kurtarılması pratikte mümkün olmamaktadır.

Diğer başarılı teknikler arasında sırasıyla; disklerin yüksek manyetik alanlara maruz bırakılarak bozulması (degaussing), cıva banyosuna batırılması veya terör örgütlerinin tercih ettiği gibi sabit diske kurşun sıkılması örnekleri verilebilir. Sabit disklerin bozulmuş olması, içindeki verinin hiçbir zaman geri döndürülemeyeceği anlamına gelmemekte, bir takım verilerin çeşitli tekniklerle kurtarılabildiği bilinmektedir[111].

[111] Bu tip çalışmalarla, 11 Eylül saldırılarından sonra fiziksel olarak hasar gören bazı sabit disklerden veri kurtarılabildiği söylenmektedir. Bu amaçla hizmet veren firmalar biri hakkında detaylı bilgi için bkz. http://www.pc3000.com, erişim tarihi: 07.01.2013.

II. Delillerin temizlenmesi

Delilerin temizlenmesi (wipe[112]), delil karartma işlemlerinde en sık karşılaşılan teknik olarak öne çıkmaktadır. Burada temizlik ifadesi, delilin orta düzey bilgiye sahip kullanıcıların bulamayacağı şekilde silinmesi anlamından ileri bir kavramdır. Bilgisayarda bulunan bir dosyanın sistem klasörleri altına taşınması, sonrasında silinmesi ve hatta geri dönüşüm kutusundan bile kaldırılması, delillerin tam manasıyla temizlendiği (wipe edildiği) anlamına gelmeyecektir. Bir örnekle açıklamak gerekirse; silahla işlenmiş bir suç sonrası faillerin tetikteki parmak izini bir bez parçasıyla silmesi, ancak daha sonra kriminoloji laboratuvarlarında parmak izinin bir şekilde görüntülenebilmesi örneği verilebilir.

"Silinmiş veride araştırma yapılması", "silinmiş verinin geri döndürülmesi" ve "silinmiş dosyaların bir kısmının görüntülenmesi" vb. ifadeler teknik kökenli olmayan kişiler için karmaşık kavramlardır. Bu kavramların ne anlama geldiği, son kullanıcının başvurduğu basit silme işlemleri ve geri döndürülemeyecek şekilde *temizlik* (wipe) yapılması işlemleri alt bölümlerde etraflıca incelenmiştir.

A- Basit silme işlemleri

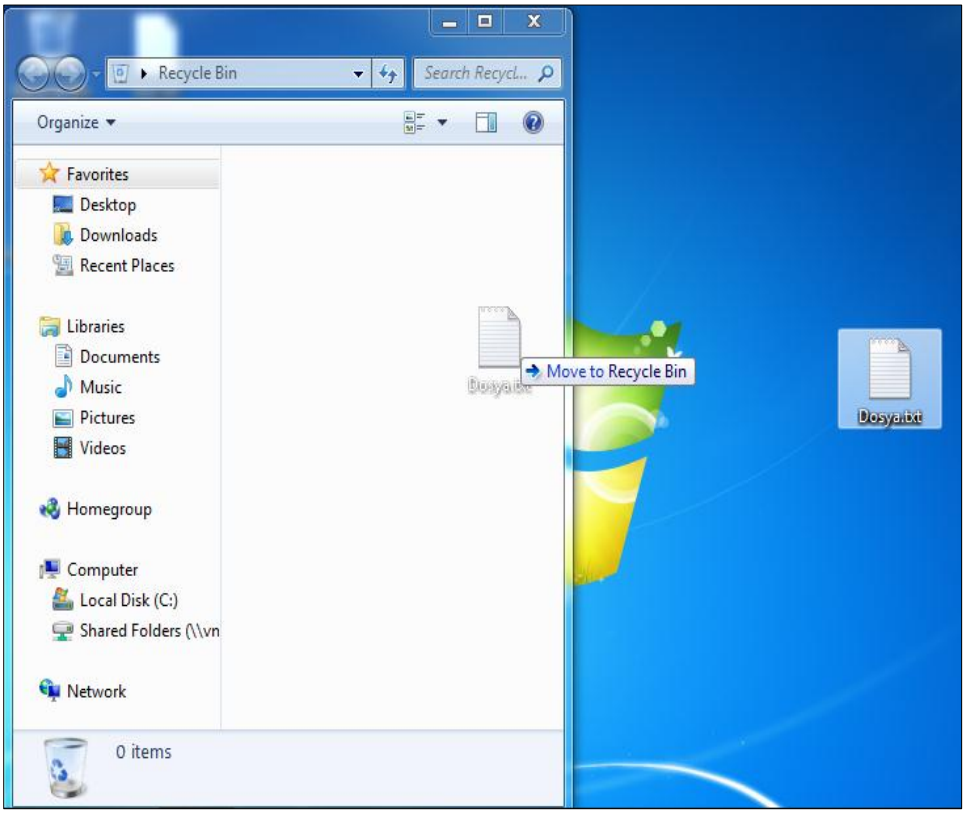
Dijital adli analiz çalışmalarında en sık karşılaşılan, son kullanıcıların en sık başvurduğu ancak kolaylıkla geri döndürülebilen silme işlemleri "basit silme işlemleri" olarak düşünebilir.

Kişisel bilgisayarda en çok tercih edilen işletim sistemi olan Windows'ta, son kullanıcının[113] uyguladığı iki çeşit silme işlemi bulunmaktadır. Bunlardan ilki herhangi bir dosyanın geri dönüşüm kutusuna taşınması işlemidir. Bu işlem aslında bir silme işlemi olmamakla birlikte, dosyanın kullanıcı tarafından önceden

[112] Wipe, Türkçeye "silmek" olarak çevrilen bir terimdir. Bu ifade, "wipe" kelimesinin anlamını tam olarak karşılayamamaktadır. "Wipe" işlemi, *geri döndürmenin çok zor veya imkansız olarak silme işleminin yapılması* olarak çevrilebilir.

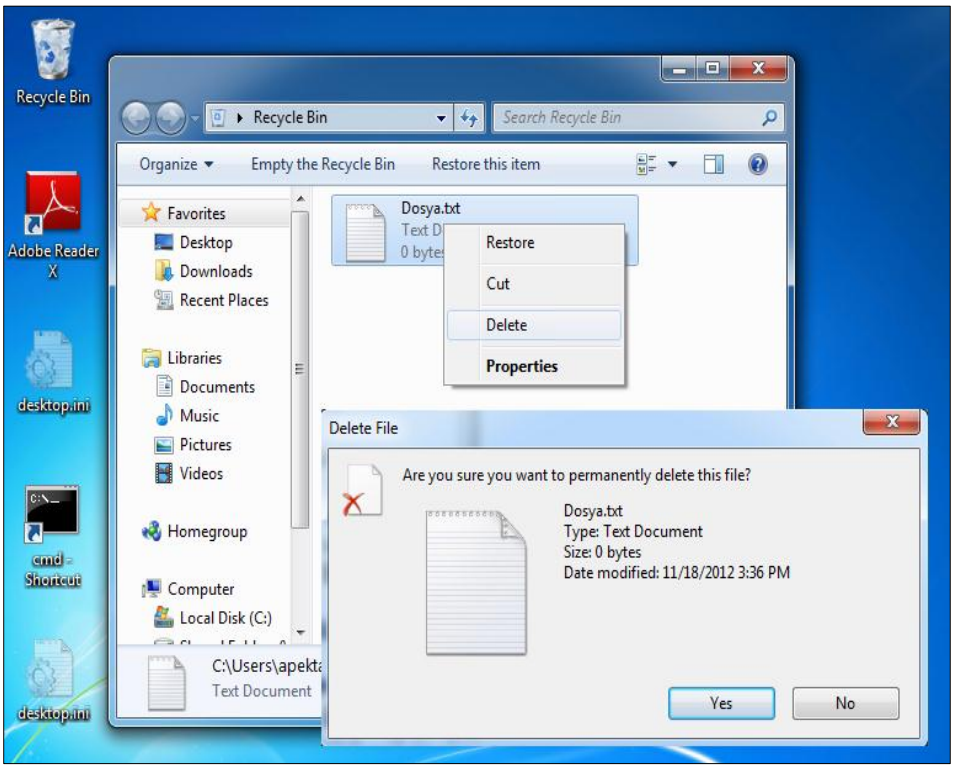
[113] "Son kullanıcı" ifadesi, herhangi bir sistem, ürün veya hizmeti kullanan, ilgili hizmetin üretimi veya geliştirilmesinde rol almayıp sadece üründen faydalanan kişileri ifade etmektedir.

bulunduğu dizinde görünmemesini sağlar. Dosya bunun yerine geri dönüşüm kutusunda bulunacaktır. Bu tür bir silme işlemi kullanıcı tarafından kolaylıkla geri alınabilmektedir (Şekil 27).



Şekil 27 - Geri dönüşüm kutusuna atarak dosya silme işlemi.

Son kullanıcıların uyguladığı bir sonraki adım ise, "Geri Dönüşüm Kutusunda" bulunan dosyaları silmektir(Şekil 28). Bu durumda dosyalar kullanıcının erişimine kapalı hale gelecekken, dijital adli analiz teknikleriyle geri döndürülme ihtimalini büyük oranda devam ettirecektir.



Şekil 28 - Dosyanın geri dönüşüm kutusundan silinmesi.

B- Dosya temizliği

Dosya temizliği (wipe) işlemleri, bilinçli kullanıcılar tarafından elle[114] veya hazır programlar kullanılarak yapılabilmektedir. Bu tip dosya temizliği yapabilecek araçlar ikiye kategoride değerlendirilmektedir. İlki, dosyaların, klasörlerin veya bütün sabit disklerin üzerine veri yazarak (00, FF veya rastgele 16'lık byte verileri) eski verinin okunmaz hale gelmesini sağlayan araçlardır. Bir diğer dosya temizliği araç grubunda ise, bir uygulama veya kullanıcı hareketi ile ilgili bütün verileri (registry, olay kayıt defterleri vb.) temizleyen araçlardır.

[114] Burada bilinçli kullanıcıların "elle" silmesinden kasıt, dosyanın bulunduğu yığın ve sektörlerin üzerine başka verilerin yazılması işlemidir. Bu işlem kullanıcının hazırlayacağı bir program vasıtasıyla yapılabilir.

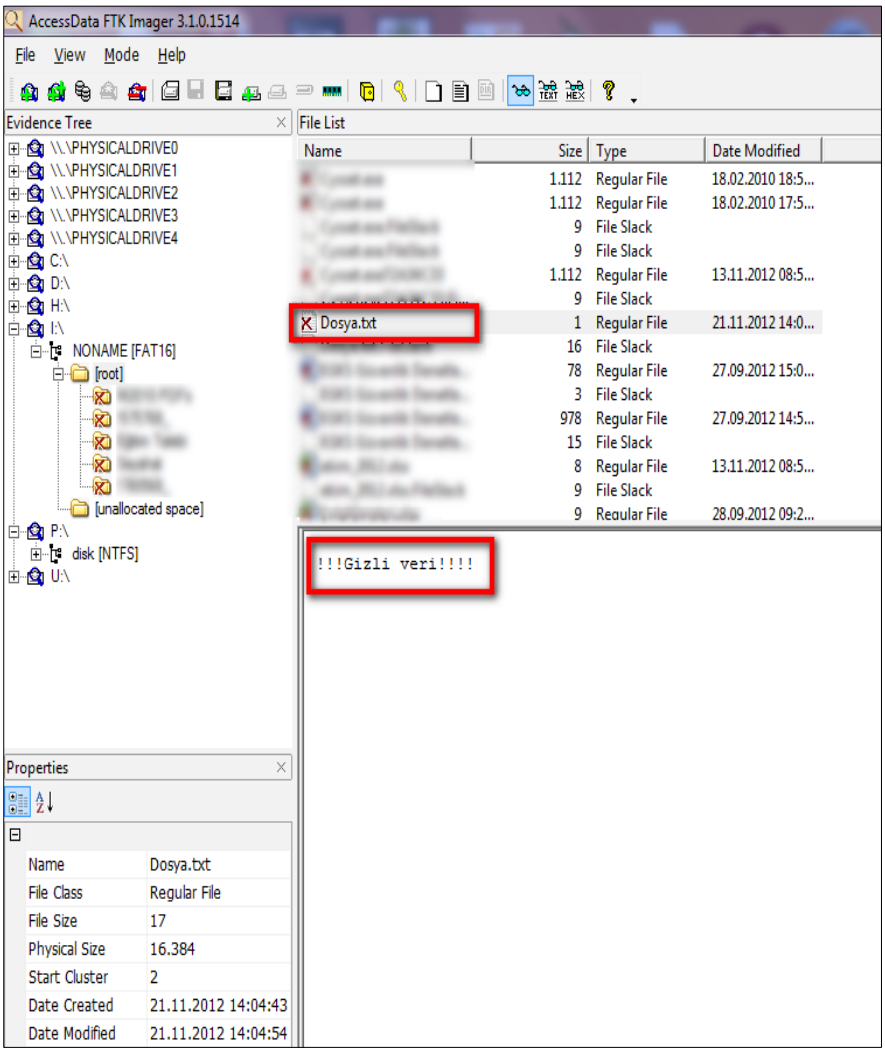
1. Üzerine yazma

Birinci yöntem, silinecek dosyanın verilerinin bulunduğu yığınların üzerine başka veriler yazmaktır. Bu işlemi özellikle Linux tabanlı sistemle kolayca yapılabilmesini sağlayan araçlar mevcuttur. Her bir sektörde bulunan verinin üzerine "00", "FF" veya rastgele başka verilerin yazılması ile işlem tamamlanmaktadır.

Bu yöntemle yapılan silme işleminin güvenilirliğine dair aşağıdaki örnekler incelenebilir:

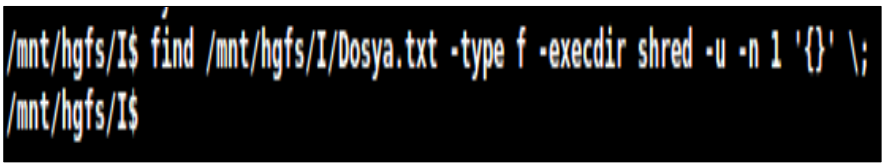
- Daha önce (Şekil 28) gösterildiği gibi Çöp Kutusundan silinerek kullanıcıların ulaşamaz hale gelen Dosya.txt, FTK Imager[115] (veya Encase vb.) uygulamalarla kolayca geri getirilebilmiştir.

[115] FTK Imager hakkında detaylı bilgi için bkz. FTK, sf. 22.



Şekil 29 - Silinmiş verinin geri döndürülebilmesi.

- Sonrasında aynı dosya (ve dosyanın bulunduğu taşınabilir bellek) Linux tabanlı shred [116] uygulaması ile üzerine yazılarak silinmiştir[117].

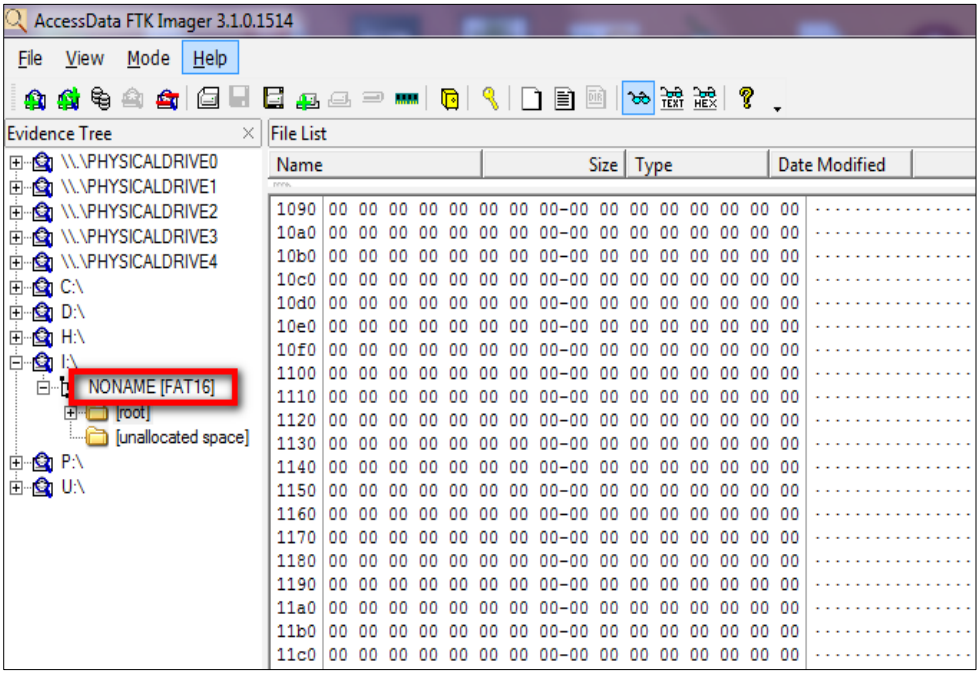


Şekil 30 - Dosya.txt dosyanın temizlenmesi

[116] Shred uygulaması hakkında detaylı bilgi için bkz. http://linux.about.com/library/cmd/blcmdl1_shred.htm, erişim tarihi: 07.01.2013.

[117] Wipe işlemi yapabilen diğer başlıca ürünler; Bcwipe "http://www.jetico.com/wiping-bcwipe/", Eraser http://eraser.heidi.ie/ ve PGPWipe olarak bilinmektedir. Erişim tarihi: 07.01.2013.

- Böylece “Dosya.txt” dosyasına ait veri yığınlarının üzerine başka veriler yazılmıştır. Taşınabilir disk FTK Imager ile tekrar incelendiğinde, Dosya.txt’ye ait hiçbir iz bulunamamıştır. (Şekil 31).



Şekil 31 - Temizlik sornası Dosya.txt'ya ait iz kalmaması.

Günümüzde kullanılan dijital adli analiz araçları, üzerine bir kez başka veri yazılan dosyaları kurtaramamaktadır. Bununla birlikte bu alanda yapılan çeşitli araştırmalar bulunmaktadır. Bunlarda biri, sabit disklerin verileri kaydediş biçimiyle ilgili “temizlik sonrası geri döndürülebilme” çalışması olarak öne çıkmaktadır.

Bu çalışmalardaki tespit neticesinde aşağıdaki yorumlar yapılabilmektedir. Sabit diskler, verileri ikili (*binary*) sistemde “0” ve “1” sembollerine indirgeyerek saklamaktadır. 0 çukurları, 1 ise yükseltileri göstermektedir. Oluşturulduktan sonra tekrar silinen veriler, sabit disklerin zaman içerisinde yıpranması nedeniyle “1” ve “0” olarak saklanamamakta, bunun yerine “0.9” ve “0.1” gibi değerlere kayabilmektedir. Bu nedenle verilerin ancak 35 kere üzerine yazılması gibi

durumlarda "kurtarılamaz" hale geldiği yönünde düşünceler bulunmaktadır[118]. Bununla beraber, günümüzde kullanılan adli analiz araçları, üzerine bir kez yazılan verileri bile kurtaramamaktadır. Bu nedenle bu yöndeki literatür çalışmaları henüz pratiğe dönme imkanı elde edememiştir.

2. Kalıntı temizleme

Günümüz bilgisayarlarından yapılan işlemler tek, bir dosyanın oluşturulması, okunması ve paylaşılmasından çoğu zaman daha komplekstir. Bu nedenle bir önceki maddeye yapılan *veri temizliği* (wiping), verilerin saklanması ve delillerin karartılması açısından yeterli olmayacaktır.

Detaylı veri temizliği ve kalıntı bırakılmaması amacıyla hazırlanmış çeşitli yazılımlar mevcuttur ve rahatlıkla edinilebilir. Bunlardan en bilinenleri Clean After Me[119] ve Ccleaner[120] uygulamalarıdır. Bu programların temel özelliği, bir çalışma esnasında bilgisayarda bırakılan bütün izleri temizlemektir. Web tarayıcı uygulamalarının geçici dosyaları, geçmiş verileri, çerezler ve kayıtlı parolaları başta olmak üzere bilgisayarda bulunan Çöp Kutusu, yakın zaman geçmiş dokümanları, geçici dosyaları ve kayıt defteri verileri bu araçlar sayesinde temizlenebilmektedir.

III. Veri gizleme

Veri gizleme (data hiding), bilgisayarda bulunan verilerin normalde olmayacak yerlerde saklanması veya şifreli, gizli bölümler oluşturarak ilgili verileri dijital adli incelemeyi yapan uzmanın tespit edememesini sağlamaya yönelik işlemlerdir. Veri gizleme, verinin tespit edilememesi ve verinin şifreli olarak saklanması alt başlıklarında incelenebilir.

---

[118] Craig Wright, Dave Kleiman, and Shyaam Sundhar R.S., Overwriting Hard Drive Data: The Great Wiping Controversy, USA 2008 ("Wright/Kleiman/Sundhar"), sf. 3.
[119] Cleaner After Me, http://www.nirsoft.net/utils/clean_after_me.html, erişim tarihi: 07.01.2013.
[120] Ccleaner, http://www.piriform.com/ccleaner, erişim tarihi: 07.01.2013.

A- Verinin tespit edilememesi

Verinin tespit edilememesi işlemleri, çoğu zaman saklanmak istenen dosyanın basit şekilde sistem dosyaları arasına kaydedilmesi veya ilgisi olmayan başka dizinlerin içine kopyalaması ile yapılmaktadır. Dikkatli uzmanların gözünden kaçmayacak ve bir şekilde elde edilebilecek bu tip veriler, ilk soruşturma aşamasında inceleme yapan uzmanların veya bilgisayara izinsiz şekilde giriş yapan bilgisayar korsanlarının hedefi olmaktan uzaklaşacaktır. Her ne kadar çok güvenilir bir teknik olmasa da, yine de ciddi bir delil karartma tekniği olarak düşünülebilir. Gerçek hayattan bir örnekle benzeştirmek gerekirse; Ankara'da işlenmiş bir suçla ilgili silahın İstanbul'da çok iyi bir şekilde saklanması, eğer yeterli başkaca ipucu yoksa bulunmasını oldukça zorlaştıracaktır. Veri gizleme teknikleri ile yapılan delil karartmalar bu örnek gibi düşünülebilir.

Bu alanda yapılan çalışmalar, günümüzde çeşitli verilerin resim veya video dosyalarının bile içine saklanabileceğini göstermektedir [121]. Bilgisayar sabit diskindeki paylaştırılmamış yığınlara [122] ve fazlalık alanlara [123] gizlenerek de yapılabilen, geçmişi 200 yıla dayanan steganografi [124] benzeri bu tür veri gizleme taktikleri "İleri düzey veri gizleme" olarak sınıflandırılabilir. Bu yöntemler, gizli şekilde haberleşmek isteyen kişi ve kurumlarca günümüzde kullanılabilmektedir.

B- Verinin şifrelenmesi

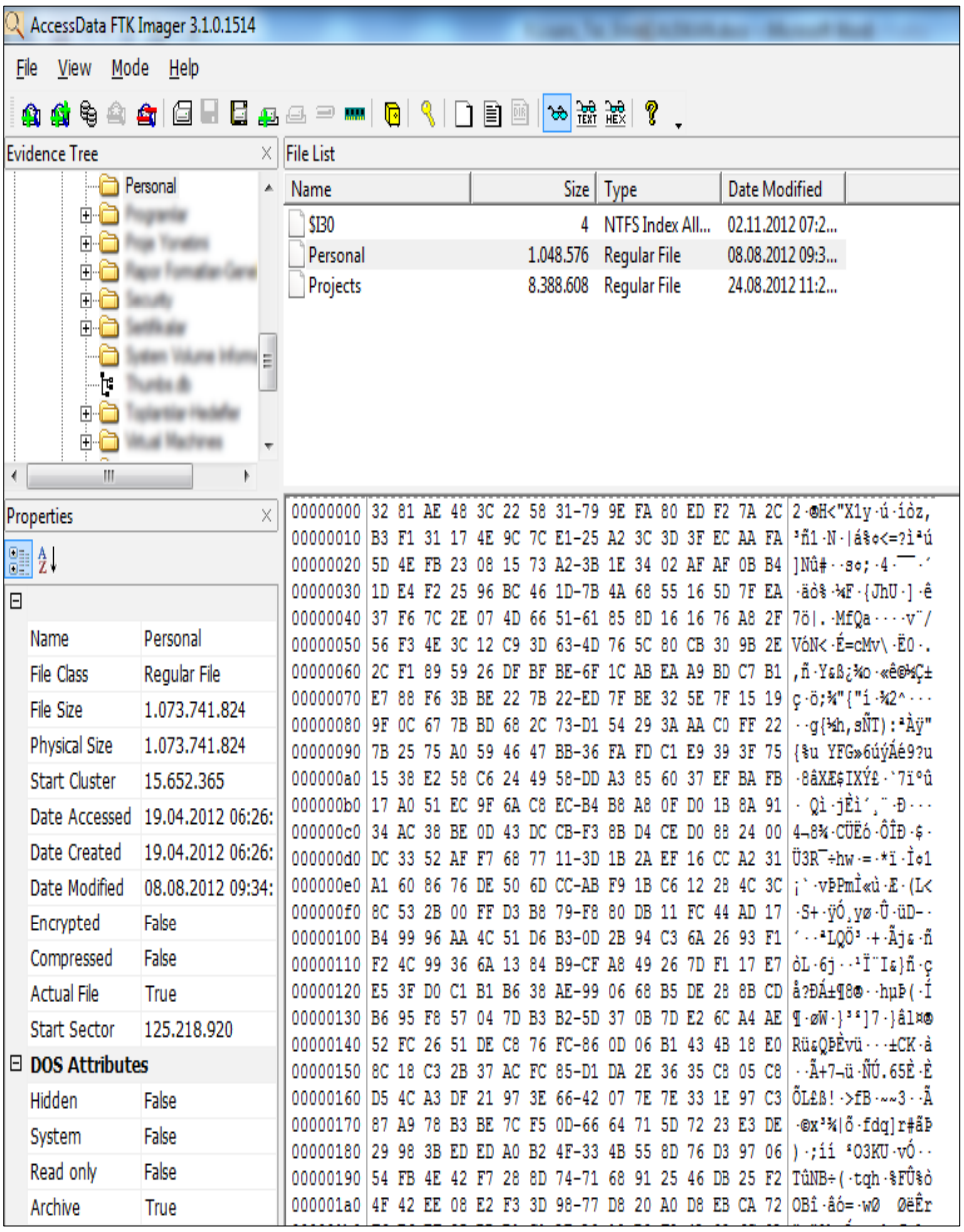
Veri gizleme tekniklerinden bir diğeri, verinin şifreli alanlarda saklanarak başkalarının erişememesini sağlamaya yönelik çalışmalardır. Son zamanlarda giderek yaygınlaşan ve kişisel verilerin mahremiyetini sağlamaya yönelik kişi ve kurumların dikkate aldığı bu tür teknikler, bazen de dijital adli delillerin analizinde karşılaşılabilen bir durum olmaktadır[125].

---

[121] Min Wu, Heather Yu, Bede Liu, Data Hiding in Image and Video: Part II—Designs and Applications, Çin 2003 ("Wu/Yu/Liu"), sf. 2.
[122] Detaylı bilgi için bkz. Paylaştırılmamış yığınlar (Unallocated clusters), sf. 32.
[123] Detaylı bilgi için bkz. *Fazlalık alan* (Slack space) verileri, sf. 43.
[124] Steganography, http://en.wikipedia.org/wiki/Steganography, erişim tarihi: 07.01.2013.
[125] Minnesota court takes dim view of encryption, http://news.cnet.com/Minnesota-court-takes-dim-view-of-encryption/2100-1030_3-5718978.html, erişim tarihi: 07.01.2013.

Günümüzde Truecrypt [126], Bitlocker [127] ve Filevault [128] gibi şifreleme yazılımları popüleritesini artırmaktadır. Bu uygulamalar kullanılarak şifrelenmiş verilere parola bilinmeksizin erişmek mümkün olmamaktadır. Bu nedenle şifrelenmiş alanlarda tutulan veriler, dijital adli analiz araçlarında anlamsız veri kümesi şeklinde görüntülenecektir(Şekil 32). Şekilde Truecrypt ile şifrelenmiş bir *veri alanı* (container) olan "Personel" dosyası ve bu dosyadaki verilerin şifreli hali görünmektedir.

[126] Truecrypt, http://www.truecrypt.org, erişim tarihi: 07.01.2013.
[127] Bitlocker, http://windows.microsoft.com/is-IS/windows-vista/BitLocker-Drive-Encryption-Overview, erişim tarihi: 07.01.2013.
[128] Filevault, http://support.apple.com/kb/HT4790, erişim tarihi: 07.01.2013.



Şekil 32 - Truecrypt ile şifrelenmiş alan.

IV. Veri manipülasyonu

Günümüzde adli bilişim çalışmalarında karşılaşılan ve çözüm aranan problemlerden biri de *veri manipülasyonudur* (data manipulation). Dijital adli delillerin manipüle edilmesi, ilgili delillerin kullanılıp kullanılamayacağına, eğer

kullanılacaksa bu delillere hangi seviyede güven duyulabileceğine ilişkin soruları beraberinde getirmektedir[129].

Dosya sistemi verileri[130], işletim sistemi verileri[131] ve uygulama bağımlı çok sayıda veri, çeşitli tekniklerle sonradan değiştirilebilir özelliğe sahiptir. Söz gelimi, Microsoft Word uygulaması kullanılarak oluşturulmuş bir metin dosyasında bulunan *yazar* (author) ve *oluşturulma zamanı* (create date) gibi *üstveri* (metadata) bilgilerinin bazıları kolaylıkla değiştirilebilmektedir. Bu verilerin bazıları çok kısıtlı şartlarda değiştirilebilirken bazılarının ise müdahaleye açık olduğu konusunda herhangi bir bilgi bulunmamaktadır.

A- Zaman tarih manipülasyonları

Dijital adli analizi yapılan bilgisayarda bulunan dosyaların zaman tarih verileriyle ilgili detay bilgiler, dosya üstverilerinin kayıtlı olduğu $MFT dosyasında bulunabilmektedir[132]. Bu veriler dosyanın ne zaman nasıl bir işlem gördüğüne dair önemli bir kaynak konumundadır. Bu nedenle delil karartma işlemlerinde bu tarih verileri önemli bir hedef haline gelmektedir.

Günümüzde birçok adli inceleme, incelenen delillerdeki tarih bilgileriyle doğrudan ilgilenmektedir. Suçun vasfı ve içeriği kadar hangi tarihte işlendiği konusu, karar vericiler için önemli bir bilgi olacaktır. Bu nedenle dosyalar üzerinde zaman tarih manipülasyonu konusu, üzerinde hassasiyetle durulması ve araştırılması gereken bir gündem olmaktadır.

$MFT dosyasında tutulan zaman-tarih verileriyle ilgili delil karartma analizi yapılmadan önce, buradaki verilerin NTFS dosya sistemi tarafından hangi hallerde değiştiriliyor olduğunu incelemek faydalı olacaktır.

NTFS dosya sistemi, dosyaların zaman tarih bilgilerini çeşitli kurallara göre günceller ve bu güncellemeler sonrasında dosya oluşturma tarihi, değiştirme

---

[129] Jasmin Ćosić, Zoran Ćosić, Miroslav Bača, Legal Aspects of Digital Antiforensic, Zagreb 2010 ("Ćosić/Ćosić/Bača"), sf 3.
[130] Detaylı bilgi için bkz. Dosya sistemi verileri, sf. 33
[131] Detaylı bilgi için bkz. İşletim sistemi verileri, sf.46
[132] MACE (Modified, Accessed, Created, Entry Modified) olarak kısaltılan bu tarih üstverileri ile detaylı bilgi için bkz. Tablo 1, sf. 38.

tarihi, erişim tarihi sıralaması değişebilir. Bu tarihler sıralı olmak zorunda değildir. İncelemelerde dikkat edilmesi gereken ilk husus bu olmaktadır.

Bu nedenle bilgisayarda normal bir kullanıcı davranışıyla oluşturulan bir dosyanın değiştirme tarihi, oluşturma tarihinden önce olabilir. Örnek vermek gerekirse, NTFS dosya sistemi kullanılan bir bilgisayarda oluşturulan bir dosya, başka bir klasöre kopyalandığında oluşturma tarihi, kopyalama işleminin yapıldığı tarih olacaktır. Ancak değiştirme tarihi ise, dosyanın ilk değiştirildiği tarih olarak kalacaktır. Bu işlem dizisine göre değiştirme tarihi, oluşturma tarihinden önce görünecektir. $MFT tablosunda dosyaların ne zaman ve ne şekilde güncellendiği konusunda aşağıdaki tablo yol gösterici olabilir.[133]

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

Şekil 33 - Windows NTFS Zaman Değişim Kuralları.

Dosyaların zaman tarih bilgileri yorumlanırken dikkat edilmesi gereken diğer bir konu zaman dilimleridir. Türkiye UTC/GMT +2 saat diliminde yer alır. Bu nedenle yerel saat UTC (Coordinated Universal Time)'ye göre 2 saat

[133] SANS Digital Forensic and Incident Response Poster, http://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf, erişim tarihi: 07.01.2013.

ileridedir. Yaz saati uygulaması nedeniyle yaz aylarında bu zaman farkı +3 saate çıkmaktadır. Kış aylarında tekrar +2 olmaktadır.

Bilgisayarlar yerel saatlerini bu hesaplamayla ayarlayarak kullanıcıya gösterir. Ancak dosya sistemi, saat bilgilerini UTC'ye göre tutmaktadır. Bazı adli analiz araçları UTC'ye göre rapor oluştururken, bazıları yerel saati hesaplayarak rapor oluşturur. Bu nedenle adli analiz araçlarından çıkan veriler yerel saat zaman farkı dikkate alınmadan yorumlanırsa, işlemin yapıldığı Türkiye saatine göre 2-3 saatlik bir farklılık oluşabilmektedir. Çalışmalarda bu konunun dikkatle ele alınmasında fayda görülmektedir.

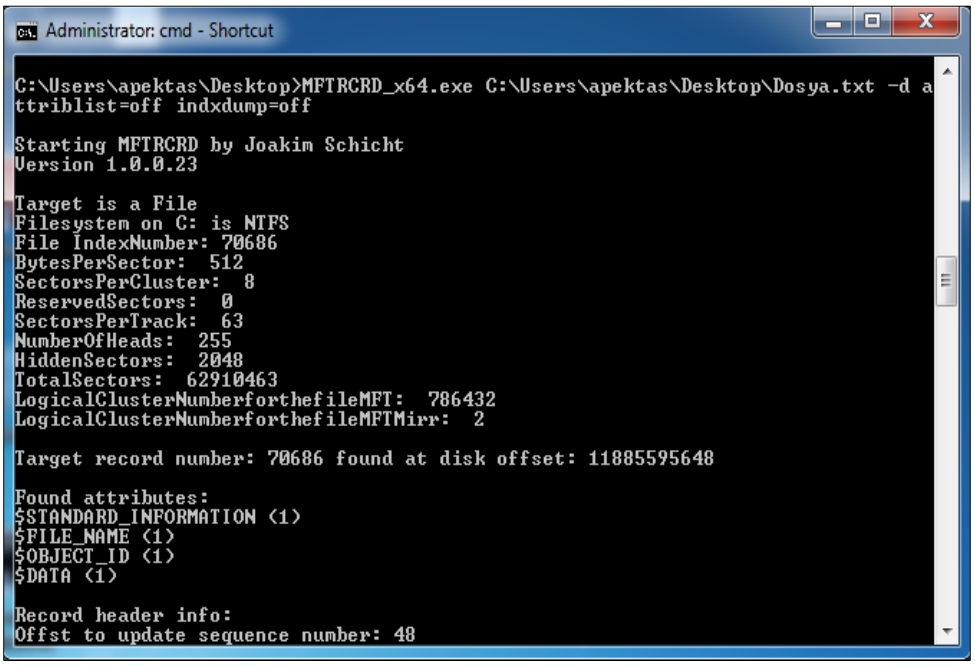
NTFS dosya sisteminin yönettiği $MFT dosyasında tutulan tarih verilerinin doğal işleyişi yukarıda açıklandığı gibi cereyan etmektedir. Ancak bu veriler çeşitli araçlar ile dışarıdan müdahaleye açık durumdadır[134].

1. setMACE ile örnek çalışma

Dosya sistemi ve tarih verilerinin saklanmasıyla ilgili gerek bu bölümde, gerekse daha önceki "Dosya sistemi verileri" bölümlerinde[135] yapılan yorumları bir örnekle açıklayabilmek adına dosya sistemi verisi üzerinde manipülasyon çalışması yapılmıştır.

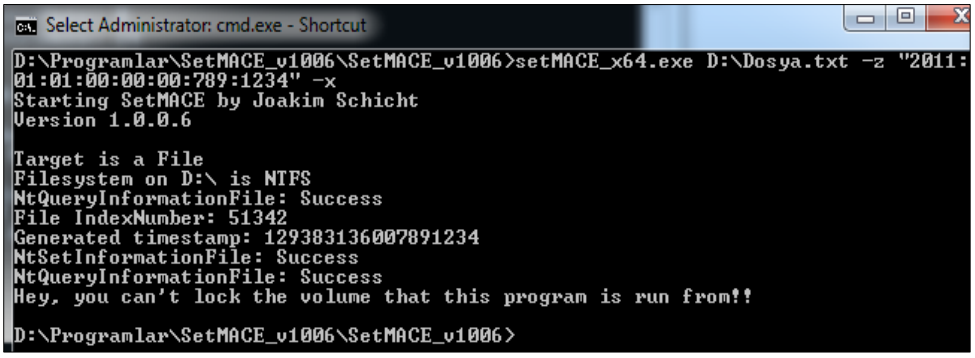
İlk adım olarak bilgisayarda örnek bir dosya seçilmiştir. İşlemlerden önce "Dosya.txt" dosyasının zaman tarih verileri MFTRCRD[136] aracı ile elde edilmiştir ve kaydedilmiştir.

[134] setMACE ve timestompt bu tür programlara örnek olarak verilebilir. Detaylı bilgi için bkz. http://www.forensicswiki.org/wiki/Timestomp ve http://reboot.pro/files/file/91-setmace/, erişim tarihi: 07.01.2013.
[135] NTFS ve $MFT dosyası ile ilgili bilgiler için bkz. Dosya sistemi verileri, sf. 33.
[136] MFTRCRD, http://code.google.com/p/mft2csv/wiki/MFTRCRD, erişim tarihi: 07.01.2013.



Şekil 34 - MFTRCRD ile zaman verilerinin elde edilmesi.

Sonrasında setMACE[137] kullanılarak tarih verileri eski bir tarihe alınmıştır.

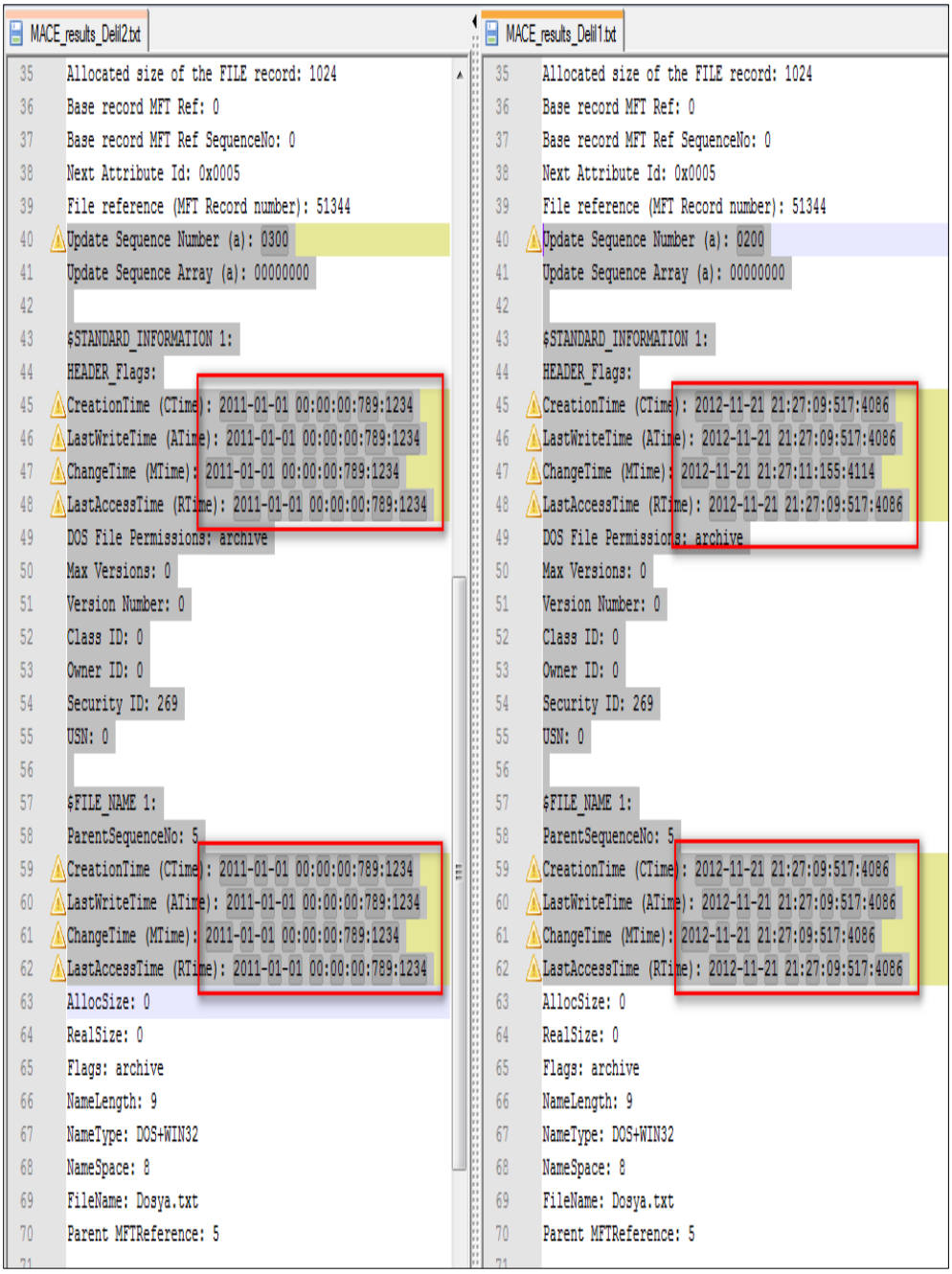


Şekil 35 - SetMACE ile tarihin geriye çekilmesi.

SetMACE ile tarih verileri manipüle edildikten sonra, dosya üstverilerindeki tarih üst verileri tekrar alınmış ve ilk sonuçlarla kıyaslanmıştır (Şekil 36). Görüldüğü üzere hem $Standard_information hem de $File_name alanları manipüle edilen tarihi göstermektedir (sol taraf). Bu yöntemle yapılan bir üst veri manipülasyonu, $I30, $Logfile vb. farklı sistem dosyalarıyla karşılaştırılarak kontrol edilebilse de, bu kontrol her zaman mümkün olmayacaktır. Özellikle üzerinden bir miktar zaman geçtiği durumlarda, dosya

[137] setMACE, http://reboot.pro/files/file/91-setmace/, erişim tarihi: 07.01.2013.

sistemindeki farklı dosyalarda tutulan diğer kaynaklardaki veriler de kaybolabilir. Bu durumlarda gösterilen tarih manipülasyonunu tespit etmek daha da zorlaşacaktır.



Şekil 36 - Manipüle edilmiş tarih verilerinin kıyaslanması.

B- Dosya üstveri manipülasyonu

Günümüzde birçok dijital veri bir şekilde dışardan müdahale edilerek değiştirilebilmektedir. Özellikle ofis uygulamasına ait "yazar", "yönetici" ve "son değiştiren" verileri, dosyanın kim tarafından kullanıldığına dair önemli bir kaynak iken, bu verilerin çeşitli araçlarla kolaylıkla değiştirilebiliyor olması dijital adli analizi yapan uzmanın işini zorlaştırmaktadır[138].

Gerek zaman-tarih manipülasyonları, gerekse dosya üstveri manipülasyonlarıyla ilişkili dijital adli analizler, adli bilişim dünyasında zaman zaman karşılaşılabilen durumlardır. Bu verilerin bir şekilde değiştirilebiliyor olması, ilgili verilerin delil özelliğinin kaybolmasına neden olup olmadığı uzun bir tartışma konusudur. Bu şekildeki manipülasyonları gerçek hayattaki suç örnekleriyle kıyaslayarak durumu daha kolay anlaşılır hale getirmek de mümkündür. Söz gelimi, cinayet işlenen bir silahta parmak izi olmaması o silahın gerçekten kullanılmadığı göstermeyeceği gibi, cinayetin failleri hakkında da bir ipucu vermemektedir. Bununla birlikte cinayet sonrası tetiğe parmak izi bulaştırılan maktul hakkında detaylı araştırma yapılmadan "intihar ettiği" yargısı da peşin bir hüküm olacaktır. Dijital adli delillere de tıpkı bu örnekte olduğu gibi yaklaşılabilir. Zaman tarih manipülasyonundan şüpheleniliyorsa, bilgisayar kullanıcısının teknik bilgi seviyesinin araştırılması, bilgisayarda bu işlem için kullanılmış olabilecek bir yazılımın tespiti ve bilgisayarda bir zararlı yazılım olup olmadığı vb. gibi çok sayıda nokta detaylı olarak araştırılmalıdır. Bu nitelikteki karmaşık konularda özenle gerçekleştirilmiş bir dijital adli çalışması %100 netlikte bir sonuca her zaman varamasa bile, en azından yoğun şüphenin ne tarafta oluştuğu ve olasılık dağılımlarının nasıl şekillendiği konusunda bir sonuca varabilir. Bu konuyla ilgili detaylı yorumlara ilerleyen bölümlerde tekrar yer verilecektir.

[138] Dosya üstverilerini görüntüleyebilmesinin yanı sıra, bu verileri değiştirme yeteneğine de sahip olan ExifTool hakkında detaylı bilgi için bkz. ExifTool, sf. 25.

V. Delil niteliğinde verilerin oluşumunu engelleme

Delil karartmada kullanılan son teknik ise delillerin oluşumunun engellenmesidir. İşletim sisteminin kullanıcı tarafından değiştirilebilen yapılandırma ayarları, geriye dönük *kayıt* (log) tutabilen uygulamaların oluşturduğu günlükler veya İnternet geçmişinin kaydedilmesinin engellenmesi gibi farklı yollarla delillerin oluşması engellenebilir ve böylece deliller daha oluşmadan karartılmış olur.

A- Kayıt tutma fonksiyonlarının kapatılması

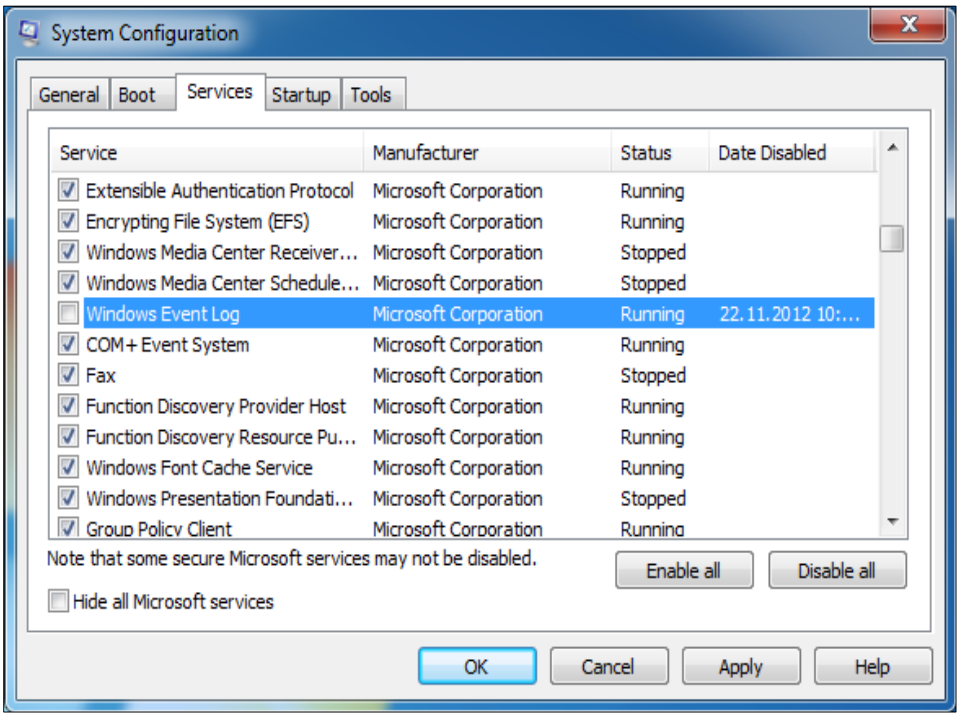
İşletim sisteminin kendi kayıtları veya uygulamaların tuttuğu özelleşmiş kayıt dosyaları delil karartma uygulanabilecek önemli veri kaynaklarıdır. Dolayısıyla bu verilerin sistem ayarlarının değiştirilerek hiç oluşmamasının sağlanması etkili bir yöntem olacaktır.

1. İşletim sistemi kayıt tutma özelliklerinin devre dışı bırakılması

İşletim sisteminde saklanan oturum açma zamanı, kullanıcı oluşturma zamanı, yeni bir kullanıcı ekleme vb. çok çeşitli hassas veriler *kayıt dosyalarında* (event log) saklanmaktadır[139].

Kayıt dosyalarını kapatmanın farklı yöntemleri olabilir. İşletim sisteminde tutulan bütün kayıt dosyalarını kapatmak için "C:\Windows\System32\msconfig" aracının kullanılabilmektedir. Bu sayede sistemdeki bütün kayıt dosyası üretici işlemleri *devre dışı* (disable) bırakılmış olacaktır.

[139] Kayıt dosyaları hakkında detaylı bilgi için bkz. "Olay kayıt dosyaları (Eventlogs)", sf.37.



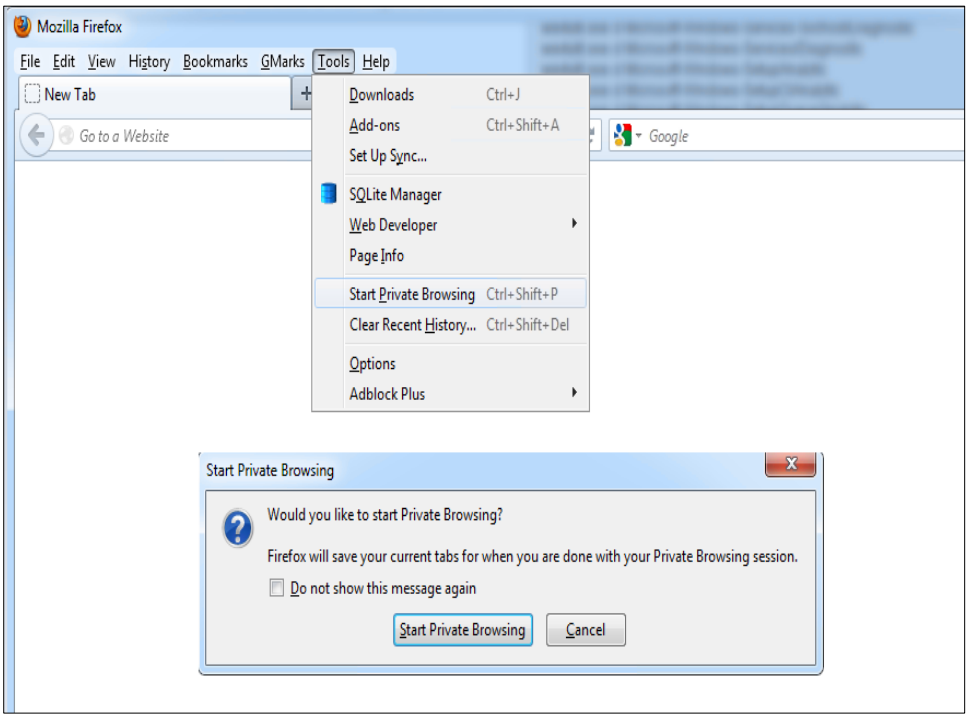
Şekil 37 - Windows kayıt dosyalarının devre dışı bırakılması.

2. Uygulamaların kayıt tutma özelliklerinin devre dışı bırakılması

Günümüzde birçok uygulama, kullanıcılarına esnek seçenekler sunmaktadır. Uygulama üzerinden yapılan işlemlerin kaydedilip kaydedilmeyeceğinin de seçilebildiği bu yapılandırmalar sayesinde, kullanıcılar ihtiyaçlarına göre farklı seçenekler uygulayabilirler.

En sık karşılaşılan örneklerden biri, İnternet geçmişinin kaydedilmemesi seçeneğini sağlayan *gizli gezinme* (private browsing) seçeneğidir. Bu özellik kullanıldığında, İnternette gezinme esnasında ziyaret edilen sayfaların kayıtlarının birçoğu tutulmayacaktır [140] . Bununla birlikte bazı gezinme verileri çeşitli tekniklerle elde edilebilir.

[140] Dijital adli analizde "hiçbir kayıt tutulmaması" ve "tamamen gizli işlem yürütme" gibi yaklaşımlar genelde mümkün olmamaktadır. Yukarıda verilen örneklerde, kayıt tutma fonksiyonlarının devre dışı bırakılması açıklanmıştır, ancak buna rağmen bir takım veriler analiz esnasında ortaya çıkarılabilir. Deliller ortaya çıkarılamasa bile, delil karartmanın uygulandığı çoğu zaman tespit edilebilecektir.



Şekil 38 - Gizli gezinme özelliği.

B- Kayıt tutulmasını engelleyecek sistemler kullanma

İşletim sistemi ve NTFS gibi dosya sistemleri, gerçekleştirilen işlemlere dair bir takım kayıtları gizli sistem dosyalarına kaydedebilmektedir. Bu durum, kullanıcının delil karartma için kullandığı tekniklerin yetersiz olabileceğine dair bi işarettir.

Örnek vermek gerekirse, Microsoft Windows ailesi işletim sistemlerinde bir ofis dokümanı açıldığında oluşan izler[141] şu şekilde kategorize edilebilir;

- İşletim sistemi izleri
  - Açılan dokümanlar için oluşturulan LNK uzantılı dosyalar
  - Kayıt defterinde (Registry) işletim sistemi tarafından oluşturulan kayıtlar
- Dokümanı açan programın izleri
  - *Kayıt defterinde* (Registry) dokümanı açan programlar tarafından oluşturulan kayıtlar

[141] Incident Response Poster, http://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf, erişim tarihi: 07.01.2013.

  - Dokümanı açan programın PF uzantılı "prefetch" dosyaları
  - Dokümanı açan programın kayıt girdileri
- Dosya sistemi üst verileri değişiklikleri
  - Dosya erişim tarihinin güncellenmesi
  - Dosya değiştirme tarihinin güncellenmesi

Delil kalıntılarını temizleyen araçlar yukardaki izlerin hepsini temizlemeyebilir. Bu durumda bir dosyanın hiç iz bırakmadan nasıl açılabileceği ve işlem yapılabileceği konusu gündeme gelmektedir.

Her hangi bir bilgisayarın işletim sistemini kullanmadan da o bilgisayardaki dosyalara erişmek mümkün olabilmektedir. Harici işletim sistemleri kullanılarak bilgisayar sabit diskinde bulunan verilere erişilebilir. Bunlardan en sık kullanılanları, CD ile *başlatılabilen* (boot) edilebilen sistemlerdir. Linux ve Windows işletim sistemlerine göre en sık kullanılan ürünler;

- Linux
  - Knoppix[142]
  - Hiren's[143]
  - Unetbootin[144]
- Windows
  - Bart PE[145]
  - Ultimate Boot CD for Windows[146]
  - WinBuilder[147]

Olarak sıralanabilir. Bu CD'ler ile bilgisayar başlatıldığında, sabit diskte kurulu olan işletim sistemi yerine CD'de bulunan işletim sistemi kullanılır. Böylece dosyanın açıldığına, oluşturulduğuna veya silindiğine dair izler oluşmayacaktır.

[142] Knoppix, http://www.knoppix.net, erişim tarihi: 07.01.2013.
[143] Hiren's, http://www.hiren.info/pages/bootcd, erişim tarihi: 07.01.2013.
[144] Unetbootin, http://unetbootin.sourceforge.net, erişim tarihi: 07.01.2013.
[145] BartPE, http://www.nu2.nu/pebuilder, erişim tarihi: 07.01.2013.
[146] Ultimate Boot CD for Windows, http://www.ubcd4win.com, erişim tarihi: 07.01.2013.
[147] WinBuilder, http://winbuilder.net/, erişim tarihi: 07.01.2013.

Delil karartma, dijital adli analiz çalışmalarını sekteye uğratan ciddi problemlerden biridir. Verilerin silinmesi, temizlenmesi ve manipüle edilmesi gibi yollarla karartılmış delillerin incelendiği araştırmalar, adli bilişiminde delillerin güvenilirliğini tehdit eden ve çözülmesi gereken önemli bir problem olarak karşımıza çıkmaktadır.

§5. Dijital adli delillerin güvenilirliği ve güven seviyeleri

Dijital adli delillerin güvenilirliği ve bu delillerin makul seviyede kabul edilebilirliği ve inandırıcılığı, hukuksal açıdan önem derecesi yüksek unsurlardır. Adli bilişim çalışmalarında değerlendirilen bütün veriler, tespitler ve nihai olarak deliller, hukuksal açıdan geçerliliği sorgulanabilen ve verilecek kararı etkileyebilecek olgulardır.

Dijital adli deliller, gerek bilişim teknolojilerinin durağan olmayan yapısı, gerekse delillere etki eden çok sayıda unsurun mevcudiyeti itibariyle belirsiz mahiyette olabilmektedir. Buradaki belirsizlik, "delil karartma", "zararlı yazılımlar" veya herkesçe bilinmeyen teknolojiler imkânlar nedeniyle oluşmaktadır.

Delil güvenilirliği; delillerin *akla yatkınlığı* (plausibility), *kabul edilebilirliği* (admissibility) ve *özgünlüğü* (authenticity) gibi özellikleriyle denetlenebilen ve *nicel tespitlerle*[148] (quantitative) ölçülebilen bir olgudur. Her ne kadar dijital adli deliller kesinlik ifade eden yargılara çoğu zaman kapalı da olsa, CMK'da "basit şüphe", "makul şüphe", "yeterli şüphe" ve "kuvvetli şüphe"[149] tanımlarına benzer şekilde dijital adli delillerde de bir takım şüphe seviyeleri oluşturulabileceği düşünülmektedir.

Dijital adli deliller de sonuç itibariyle birer "delil" olması nedeniyle öznitelikleri bakımından diğer delil gruplarıyla benzeşmektedir. Mahkemede bütün tarafların kabul edebileceği, iddianın geçerliliği veya geçersizliği noktasında belirleyici rol üstlenecek delillerin bir takım niteliklere sahip olması gerekmektedir. Genelde bütün delil türleri, özelde ise dijital adli delillerin kabul edilebilirliği ile ilgili tespitler aşağıdaki gibi ele alınabilir.

---

[148] Richard E. Overill, Jantje A.M. Silomon, Kam-Pui Chow, A Complexity Based Model for Quantifying Forensic Evidential Probabilities, Polonya 2010 ("Overill/Silomon/Chow"), sf. 4.
[149] Şüphe Tür ve Dereceleri, http://cankattaskin.av.tr/?p=11, erişim tarihi: 07.01.2013.

I. Delillerin varlığı

Dijital adli deliller doğası itibariyle diğer birçok adli delil türünden farklılıklar gösterse de, bilgisayarda oluşması beklenen izler bakımından bazı ortak noktaları da bulunmaktadır.

Adli delil incelemelerinde dünyaca kabul gören "Locard Prensibi", dijital adli delillerin analizi için de kullanılabilir[150]. Bu prensibe göre, "işlenen her suç, muhakkak surette ortamda bir iz bırakmaktadır". Bu delil, failin tamamen bilinçsiz olarak olay yerinde bırakabileceği bir iz olabilir. Dolayısıyla bu prensipten hareketle dijital adli analiz incelemelerinin neticesinde, bilgisayar teknolojisi kullanılarak işlenmiş her hangi bir suça ilişkin bir işaretin olay yerinde bırakılacağı düşünülebilir. Delilin mahkeme tarafından kabul edilebilir seviyede olup olmayacağı tartışmaya açık olsa da; sabit diski tamamen silme ve temizleme, hatta fiziksel olarak imha etme durumlarında bile bir takım izler kalacaktır. Bu izler suça kaynaklık eden delilleri ortaya çıkarmasa da, bir takım delillerin imha edildiğini ortaya koyabilir. Benzer şekilde, sabit diskteki bir verinin temizlenmesi işlemi, bu işlemin yapıldığı programın bırakacağı izler ile tespit edilebilir. Netice itibariyle adli bilişim alanındaki çalışmalar, detaylı incelemelerin yapılması neticesinde mahkemelerin gerçeği açığa çıkarma gayretlerine yardımcı olabilecektir.

II. Delillerin ele alınması

Dijital adli delillerin ele alınması sırasında izlenebilecek metodolojiyle ilgili yıllar içinde çeşitli görüşler ortaya atılmıştır. Delillerin bilimselliği ve kabul edilebilirliği bakımında en kabul gören yaklaşım *Daubert kurallarına uyumu* (Daubert Compliance) olarak isimlendirilmektedir[151].

Daubert'in yaklaşımına göre delillerin kabul edilebilmesi için bakılması gereken beş temel nokta bulunmaktadır. Bu kontrol maddeleri sonucunda,

---

[150] Locard's exchange prinsible, http://en.wikipedia.org/wiki/Locard%27s_exchange_principle, erişim tarihi: 07.01.2013.

[151] Suzanne Orofino, Daubert v. Merrell Dow Pharmaceuticals, Inc.: The Battle Over, Admissibility Standards for Scientific Evidence in Court, USA 1996, sf. 3.

incelemenin bilimsel olup olmadığı ve dolayısıyla mahkemede kabul edilip edilemeyeceği anlaşılmaktadır. *Dauber kurallarına uyum* listesi aşağıdaki gibidir.

A- Tekniğin test edilebilirliği

İncelemede kullanılan tekniklerin test edilebilir niteliklere sahip olması ve bu testin çalışma öncesi yapılmış olması beklenmektedir.

B- Tekniğin bilim çevrelerine açıklanmış olması

Teknikle ilgili ayrıntılar bilimsel bir yayınla bilim insanlarına açıklanmış olmalı ve fikir alışverişinde bulunulmuş olmalıdır.

C- Hata ihtimalinin bilinmesi

Çalışma sonucunda elde edilecek verilerin herhangi bir hata oranına sahip olup olmadığı, böyle bir durum varsa hata oranının bilinmesi gerekmektedir.

D- Tekniğin denetlenebildiği standartların bulunması

Çalışmada kullanılacak teknikle ilgili konunun uzmanları tarafından yapılan kontrollerin hangi standartlara uyumlu olduğu açıklanmalıdır.

E- Bilim çevrelerince genel kabulü

Tekniğin bilim çevrelerine açıklanması sonrasında bilim insanlarında oluşan genel kanının olumlu olması ve çoğunluk itibariyle kabul görmesi gerekmektedir. İhtilaflı görüşlerin yoğun tartışıldığı tekniklere şüpheyle yaklaşılmalıdır.

Dijital adli delillerin ortaya tespiti ve incelenmesinde kullanılacak teknikler, bilimsel olarak yukarıdaki listeye uyumlu olmalıdır. Adli bilişim disiplini çok yeni bir alan olduğu için bazı konular bilim çevrelerince henüz tartışılmamış olabilir. Buna rağmen dijital adli analizle ilgili birçok temel konuda

görüş birliğine varılabilmiş ve başta ABD olmak üzere birçok ülkede bu yöntemler aktif olarak kullanılmaya başlanmıştır. Genel kabul gören yaklaşımlar ve dijital adli delillerde aranan özellikler bir sonraki bölümde ele alınmıştır.

III. Dijital adli delil kuralları

Dijital adli delillerin mahkemede kabul edilebilmesi için çeşitli niteliklere sahip olması gerekmektedir [152] . Bu veriler sayesinde delillerin bilgisayar kullanıcısına aidiyeti hukuken kabul görebilecek ve bu delillere bağlı olarak isnat edilen suçlamaların sağlam dayanakları olacaktır[153].

A- Delil geçerliliği

Dijital adli delillerin elde edilmesi hukuki bütün kaidelere uygun olmak zorundadır. Arama emri, mahkeme kararı ve yürürlükte olan diğer yasal prosedürlere aykırı şekilde temin edilen dijital adli deliller kabul edilmeyecektir.

Delillerin soruşturma yapılan konuyla *ilgili* (relevant) olması da aranılacak bir diğer özelliktir. Dijital adli deliller, bilgisayarlar arasında kolay transfer edilebilir niteliklere sahip olması nedeniyle "ilgililik" yaklaşımı açısından çeşitli sorunları beraberinde getirir. İddia edilen bir suçlamaya ilişkin yapılan arama el koyma faaliyetlerinde, ortamdaki bütün bilgisayarlara el konulma ihtimali her zaman bulunmaktadır. İlgisiz dijital adli delillere el koymamak ve kapsam içine almamak hukuken daha doğru bir yaklaşım olarak görülmektedir[154].

Adli delillere el konulması, Ceza Muhakemesi Kanunu'nun (CMK) 127. maddesi uyarınca hâkim kararı veya gecikmesinde sakınca bulunan hallerde

---

[152] Dijital adli delillerin sahip olması gereken öznitelikler, Amerika Birleşik Devletleri (ABD) Federal Yasalarınca "Federal Rules of Evidence (FRE)" ile listelenen kurallar bütünüyle tanımlanmaktadır. Bilişim hukuku alanında ülkemizden ve Avrupa'dan oldukça ileride olduğu bütün otoritelerce kabul edilen ABD hukuk sistemi bu alanda referans alınabilir.

[153] Chet Hosmer, Proving the Integrity of Digital Evidence with Time, New York 2002 ("Hosmer"), sf 2.

[154] Lorraine v. Markel: Electronik Evidence 101, http:// www.lexisnexis.com/applieddiscovery/LawLibrary/whitePapers/ADI_WP_LorraineVMarkel.pdf, erişim tarihi: 07.01.2013.

Cumhuriyet savcısının yazılı emri ile gerçekleşmektedir[155]. Bununla birlikte dijital adli delillere ilişkin CMK'nın 134. maddesi düzenlenmiş ve "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" işlemleri mevzuatta yerini almıştır. Hukuk sistemimizde dijital adli delillere el konulmasıyla ilgili uygulanmakta olan kanunların detaylı incelemesi sonraki bölümlerde etraflıca ele alınacaktır.

B- Delilin aslına uygunluğu

Dijital adli delillerin *aslına uygunluğu* (authenticity), arama el koyma işlemlerinden dijital adli analiz uzmanına gelinceye kadar olan süreçte herhangi bir değişikliğe uğramamış olduğu anlamına gelmektedir. Bu "aslına uygunluk" garantisini vermenin ilk ve en önemli adımı *tek yönlü kriptografik özet* (hash) verilerinin kontrolüdür.

Arama-el koyma emrini yerini getiren kolluk kuvvetleri, tespit ettikleri bilgisayarların sabit disk imajlarını mümkün mertebe olay yerinde almaktadırlar[156]. İmajı alınan bilgisayar sabit diskinin, arama-el koyma esnasında işlemi yapılan bilgisayara ait olduğunu garanti altına almak için de *tek yönlü kriptografik özet* (hash) mekanizmaları kullanılmaktadır. Günümüzde güvensiz kabul edilen MD5, daha yaygın kullanılan ve daha güvenilir SHA1, bir üst versiyonu SHA2 ve yeni standart olarak kabul edilen en güvenilir SHA3 [157] algoritmalarıyla hesaplanabilen bu değerler, hem kopyası alınan orijinal sabit disk hem de verilerin kopyalandığı boş sabit disk için hesaplatılmakta ve değerlerin aynılığı garanti altına almaya çalışmaktadır[158] (Şekil 39).

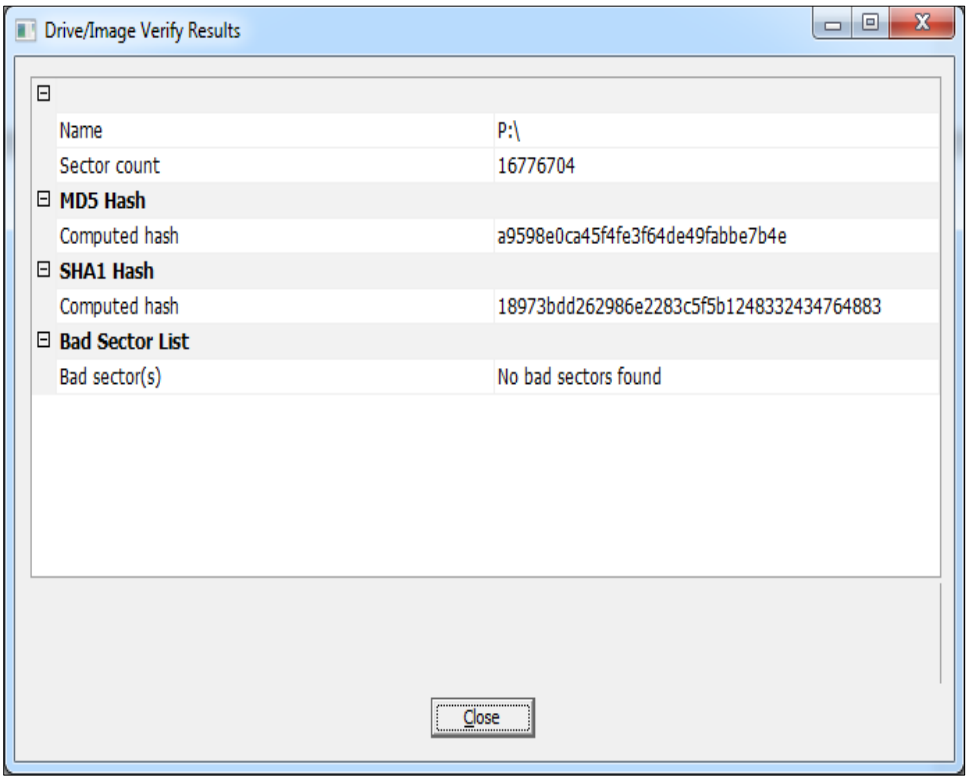
---

[155] Ceza Muhakemesi Kanunu Madde 127, http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.5271&MevzuatIliski=0&sourceXmlSearch=, erişim tarihi: 07.01.2013.

[156] Dijital adli analizde "imaj alma" işlemleri ve kullanılan araçlar hakkında detaylı bilgi için bkz. Tableau sf. 20.

[157] NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition, http://www.nist.gov/itl/csd/sha-100212.cfm, erişim tarihi 19.01.2013.

[158] The Secure Hash Algorithm Directory MD5, SHA-1 and HMAC Resources, http://www.secure-hash-algorithm-md5-sha-1.co.uk/, erişim tarihi: 07.01.2013.



Şekil 39 - MD5 ve SHA1 hash değeri hesaplatılmış sabit disk imajı.

Arama-el koyma işlemlerini yürüten görevlilerin yanı sıra, bu işlemlere nezaret eden sanık veya sanık vekillerinin imzasını da taşıyan "arama el koyma ve imaj alma" tutanağında, imajı alınan bilgisayarların MD5 ve/veya SHA1 hash değerleri bulunacaktır. Tutanaklara yansıyan bu değerler, orijinal diskten alınan kopyanın orijinalliği gösterecek ve bu delillerde daha sonra inceleme yapacak olan dijital adli analiz uzmanının referans alacağı kaynak olacaktır. Tutanaklarda yazan bu değerler, adli bilişim uzmanlarınca denetlendiğinde aynı değerin çıkması halinde kopya imajın gerçeğiyle aynı olduğu kabul edilecek ve analiz aşamasına geçilecektir.

Dijital adli delillerin *el koyma süresince* (chain of custody) herhangi bir değişikliğe uğramadığını garanti altına almak için dikkat edilmesi gereken hususlar bulunmaktadır. Bu konular başlıklar halinde;

- Delillerin bulunduğu fiziksel ortamların (imajların kaydedildiği sabit diskler, mobil cihazlar için faraday çantaları[159] vs.) özenle korunması ve delili olumsuz etkileyecek bütün faktörlerden uzak tutulması
- Delilin yetkisiz kişilerin erişiminden özenle korunması
- Delilin kim tarafından hangi araçlar ve tekniklerle elde edildiğinin yazılı tutanaklarda belirtilmesi
- Delille şu ana işlem yapmış (bilirkişiler, uzmanlar vs.) kişilerin listesi ve çalışmanın hangi tarihlerde yapıldığı bilgisinin kaydedilmesi
- Delilin hangi tarihlerde, hangi ortamlarda ve kimlerin mesuliyetinde saklandığı bilgisinin tutulması

Olarak sıralanabilir.

C- Delilin bütünlüğü

Dijital adli delillerin toplanmasında dikkat edilmesi gereken bir diğer husus *delil bütünlüğüdür* (completeness)[160]. Delil bütünlüğü, bir olay hakkında dijital adli delillerin toplanmasında sadece iddia makamının tespitlerine dayanarak kişinin suçluluğuna yönelik delillerin değil, aynı zamanda kişinin suçsuzluğunu gösterecek delillerin de toplanması anlamına gelmektedir. Örnek vermek gerekirse, bir bilgisayar sistemine saldırarak zarar verdiğinden şüphe duyulan kişi hakkında bilgi toplamak, sadece o kişinin suçlu ilan edilmesi için yeterli olmayabilir. Bunun yerine, sisteme o anda bağlı olan bütün kullanıcıların IP, kullanıcı adı vb. bilgilerinin tespit edilmesi ve saldırıyı yapanın neden diğer kullanıcılar olamayacağı araştırılmalıdır.

---

[159] "Faraday kafesi" hakkında detaylı bilgi için bkz. http://tr.wikipedia.org/wiki/Faraday_kafesi, erişim tarihi: 07.01.2013.

[160] Digital Evidence, http://infohost.nmt.edu/ ~sfs/Students/HarleyKozushko/ Presentations/DigitalEvidence.pdf, erişim tarihi: 07.01.2013.

D- Delilin kaynağı

Dijital adli delillerin bir kısmı, 2. veya 3. kişilerce öne sürülen deliller olabilmektedir. ABD yasalarında "Hearsay" olarak adlandırılan bu tür deliller, geneli itibariyle mahkemede kabul görmeyen adli deliller sınıfına girmektedir[161]. Dijital adli deliller bakımından ise bir delilin dış kaynaklı kabul edilip edilemeyeceği, o veri üzerinde kullanıcının etkileşimi olup olmadığı durumuna göre değişecektir. Bu nedenle deliller, kullanıcı müdahalesine açık veya kapalı olması durumuna göre değişen "dış kaynaklı" ve "iç kaynaklı" veriler olmak üzere iki grupta incelenebilir.

1. Dış kaynaklı veri türleri

Dijital adli delillerin bir kısmı kolay değiştirilebilir üstveriler ihtiva etmektedir. Söz gelimi, .DOC uzantılı bir yazı dosyasındaki *yazar* (author) verisi, bilgili kullanıcılar tarafından çeşitli tekniklerle değiştirilebilmektedir. Dolayısıyla sabit disk imajı alınan bir bilgisayardaki kullanıcının isminin geçtiği bir doküman, bu delilin kullanıcıyla ilişkisi olmadığı tahmin edilen herhangi birinin bilgisayarında tespit edilse, bu tür bir verinin delil olarak kabul edilebilirliği çok düşüktür. Nedeni, bu tip üstverilerin kolayca değiştirilebilmesidir. Bununla birlikte, ilgili dijital adli delilin kullanıcısıyla ilişkisi olduğu düşünülen birinin bilgisayarında bu tür bir veri tespiti olması, dosyaların ve yazarlarının ilişkili olabileceğini daha kuvvetli bir şüphe ile düşündürmektedir[162].

2. Dış kaynaklı olmayan veri türleri

Dijital adli delillerin bir diğer kısmı, kullanıcı etkileşimi çok düşük olan veya hiç olmayan verilerden oluşmaktadır. Sistem kayıtları, değiştirilemeyen dosya sistemi üstveri bilgileri, *yönlendirici* (router) ve *güvenlik duvarı* (firewall) cihaz kayıtları bu tip verilere örnek olarak verilebilir. Bilgisayar sistemlerinde

---

[161] Rule 401, Federal Rules of Evidence, Legal Information Institute, http://www.law.cornell.edu/rules/fre, erişim tarihi: 07.01.2013.

[162] Susan E.E.B. Sherman, Esq., Hearsay and Evidence in the Computer Emergency Response Team (CERT), ABD 2004 ("Sherman"), sf. 4.

"değiştirilmesi imkan dâhilinde olmayan veri" kavramı çok kısıtlı koşullarda geçerli olabilecek bir önermedir. Bununla birlikte, sistemlerin doğal işleyişine ve hayatın olağan akışına muhalif olarak, anormal bir durum oluşmadığı sürece bu tip sistemsel verilerin manipüle edilerek değiştirilmesi çok düşük ihtimaldir.

E- Delilin kullanıcı ilişkisi

Dijital adli delillerin tespit edildiği bilgisayarların kim tarafından kullanıldığı adli bilişim disiplini açısından büyük öneme sahiptir. Şüphelinin ismiyle oluşturulmuş bilgisayar hesapları ve isim soy isim verileriyle işlem yapılan dokümanlar gibi veriler önemli birer bulgu olsa da, bu gibi delillerin kesin olarak o kullanıcıya ait olduğu anlamına gelmeyebilir.

1. Delillerin kullanıcı ile ilişkisine dair veriler

Bir bilgisayar sabit diskinde dijital verinin bilgisayar kullanıcısına aidiyeti konusunda; ilgili dijital verinin bilgisayarda oluşturduğu çeşitli izler, üstveriler, ilgili dijital veriyi çalıştıran bilgisayar programında oluşan kayıt verileri ve bu programın bilgisayarda yüklü olan diğer program ve uygulamalarla olan ilişkisine dair kayıt verileri analiz edilerek bir yorum yapılabilir. Bütün bu inceleme ve analizler, dijital verilerin aidiyeti noktasında fikir oluşturmakla birlikte, kesinlik içeren ifadelerin kullanılması da mümkün olmamaktadır.

Örnek vermek gerekirse, incelenecek dijital veri word, excel vs. gibi bir Microsoft Office dosyası ise; Office uygulamalarının gerek kurulum gerekse kullanım esnasında kullanıcıdan istediği ve kaydettiği yazar ismi, şirket ismi vb. üstveriler ilgili bilgisayar kullanıcısına ait bilgi verebilir. İlgili dijital veriye ait *yazar* (author), *son kaydeden kullanıcı* (last saved by) gibi bilgiler incelenebilir. Bu bilgilerin girilmemiş olması halinde ise Microsoft Office uygulamasının verdiği *öntanımlı* (default) değerler görünecektir. Buna ek olarak bilgisayarların işletim sisteminin kurulumu esnasında kullanıcıdan girilmesini istediği *kullanıcı adı* (username) bilgisi kullanılabilir. Bu kullanıcı adı, o bilgisayarda yapılacak birçok işlem için referans olarak kullanılır. Bilgisayarda bulunan birçok dijital

veri de bu kullanıcı adını "dosya sahibi" olarak kendi üst verisine kaydeder. İşte bu işletim sisteminin kurulumu esnasında girilmiş ve çeşitli dijital verilerde iz bırakan kullanıcı adı bilgisi kullanılarak, dijital verilerin o bilgisayara ve bilgisayar kullanıcısına aidiyeti noktasında bilgi edinilebilir.

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

Dijital adli delil olarak kullanılabilen veriler, türlerine ve kullanım alanlarına göre bilgisayarlarda farklı izler ve üstveriler bırakabilir. Bir diğer örnek olarak, *pst* uzantılı bir dijital verinin, Microsoft firmasına ait Outlook ürününün kullandığı ve e-posta dosyalarını içeren bir veriyi işaret etmesi söylenebilir. Bu durumda, ilgili dosyada bulunan e-postaların incelenmesi ile dijital verinin aidiyeti noktasında fikir sahibi olunabilir. Buna benzer şekilde bilgisayarda kayıtlı olan *anında mesajlaşma* (IM) programlarının ürettiği veriler de analiz edilebilir. İncelenecek dijital veriye ait izlerin internet geçmişi, *çerez* (cookie) [163], arşivlenmiş bilgiler, kayıtlı kısayollar vb. yerlerde rastlanılması halinde ise analiz bu alanda yoğunlaştırılabilir ve o verinin ilgili bilgisayardaki geçmişi incelebilir. Bu ve buna benzer örnekler çoğaltılabilmektedir. Buradan hareketle, dijital verilerin sahiplik bilgilerinin incelenmesinin çok farklı yollarının olduğu, incelenecek dijital veriye göre çeşitli yaklaşımlar ve farklı analiz tekniklerinin mümkün olduğu söylenebilir.

2. Delil bilgisayarının kullanıcı ile ilişkisi

Dijital adli delillerin tespit edildiği bilgisayar ve o bilgisayarın kullanıcısı arasında ilişki kurmadan önce ise bazı kontroller yapılmalıdır. Bu durumu

[163] Çerezler hakkında detaylı bilgi için bkz. "*Çerezler* (Cookie)", sf. 57.

netleştirmek için ilgili delillerin tespit edildiği bilgisayarlara ait bazı özellikler sorgulanabilir[164];

- Bilgisayar İnternete veya yerel ağda başka bilgisayarlara bağlı mıdır?
- Bilgisayarın bulunduğu ağa kimler girebilmektedir?
- Bilgisayar ağına giren herkes, tespit edilen delilin bulunduğu bilgisayara ve ilgili klasörlere erişim yetkisine sahip midir?
- Yerel ağdan ve İnternetten gelecek saldırılara karşı yeterli koruma mevcut mudur?
- Bilgisayara mesai saatinde ve mesai dışında kimler erişebilmektedir?
- Ortamda yetkisiz işlem yürütmek imkan dahilinde midir?
- Bütün işlemler kayıt altına alınmakta mıdır?
- Erişim yetkilendirmeleri nasıl yapılmaktadır, bu konuda bir açıklık bulunmakta mıdır?

Bu ve buna benzer sorularla delilin tespit edildiği bilgisayarı kimin kullandığı ve delilin oluşmasında etkisi olabilecek muhtemelen şahıslar tespit edilebilir.

3. Delil bilgisayarının zararlı yazılımlarla ilişkisi

Delil elde edilen bilgisayarda "zararlı yazılım" tespit edilmesi durumunda incelemenin bu alana yoğunlaşmasında ve zararlı yazılımın bilgisayardaki olası etkileri üzerinde durulmasında fayda vardır[165]. Bu zararlı yazılım bir virüs olabileceği gibi, trojan da olabilir. Kullanıcıya özel olarak tasarlanması ve gönderilmesi bakımından "trojanlar", dijital adli analiz çalışmalarında daha ziyade üzerinde durulması gereken bir saldırı türüdür. Diğer zararlı yazılımlar gibi trojanlar da; elde edilmiş e-posta adres listeleri, kötücül yazılım dağıtımında kullanılan enfekte edilmiş web siteleri ve programlar gibi değişik yollar

[164] Information Assurance Applied to Authentication of Digital Evidence, http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2004 /research/2004_10_research01.htm, erişim tarihi: 07.01.2013.
[165] Zararlı yazılımlar hakkında detaylı bilgi için bkz. "Zararlı yazılımlar", sf. 68.

kullanılarak, en geniş kullanıcı sayısına ulaşma adına kullanıcı veya bilgisayar ayırt etmeden internet üzerinden dağıtılmaktadır. Bu zararlı yazılımlardan bazıları, bulaştıkları bilgisayarlar üzerinde yüklü antivirüs yazılımları tarafından engellenmesine rağmen, bu yazılımlara yakalanmadan da çalışabilmektedirler. Dolayısıyla, günümüz internet kullanıcılarının önemli bir kısmının bilgisayarlarında zararlı yazılımlar bulunmaktadır. Zararlı yazılımların büyük çoğunluğunun; spam gönderilmesi, internet bankacılık ve kredi kartı bilgilerinin çalınması, hizmet dışı bırakma saldırılarında kullanılması, reklam yayınlanması gibi genel olarak maddi çıkar sağlama amacıyla oluşturulup, merkezi bir şekilde yönetildiği bilinmektedir. Dijital adli analizi yapılan sabit disklerde bulunan zararlı yazılımların analizi yapılmadan, içinde trojan bulunan delil bilgisayarlarının güvenilmez olduğu iddia edilemez. Bir örnekle açıklamak gerekirse, delil bilgisayara zararlı yazılım aracılığıyla dosya gönderildiğinden şüpheleniliyorsa incelenmesi gereke hususlar;

- Zararlı yazılımın nasıl bulaştığının ortaya çıkarılması ve bu zararlı yazılımın hedefli bir saldırı ile gelip gelmediğinin tespiti,
- Zararlı yazılımın özel olarak yapılandırılan ve uzaktan yönetim olanağı sağlayabilen yetkinlikleri olup olmadığının anlaşılması,
- Delil bilgisayarlarında bulunan bu tür yazılımların aktif olarak devam ettirdiği faaliyetler,
- Zararlı yazılımın çalışmasını engelleyecek ayar ve programların durumu,
- Kullanıcının dosyalar ve zararlı yazılımlarla olan ilişkisine dair tespitler,
- İlgili bilgisayarda herhangi bir delil karartma çalışmasına dair izler,
- Geldiği tarihin, uzaktan atıldığı iddia edilen dosyalarla uyumluluk incelemesi veya bu dosyaların üstverilerinin değiştirildiğine dair bulguların varlığı,
- Kullanıcının bu dosyaların varlığından haberdar olduğuna dair bulguların, tespit edilen zararlı yazılımlar ve ilişkili dosyalara ait zaman-tarih üstverileriyle karşılaştırılması,

Olarak sıralanabilir.

Dijital adli delillerin kullanıcı ile ilişkisini tespit etmek açısından bakılabilecek birçok alan yukarıda sıralanmış olsa da, gerek teknolojik gelişmeler gerekse dijital adli analiz çalışmalarının hızla gelişmesi nedeniyle her geçen gün yeni bir tespit yapılmaktadır. Dijital adli analiz uzmanı, inceleyeceği her bir konu için mümkün olan bütün durumları ele almalı ve çalışmasını derinleştirmelidir.

F- Delil inandırıcılığı

Adli bilişim alanında en sık yaşanan problemlerde biri, iddia makamının sunduğu delillerin inandırıcılıktan uzak olmasıdır. İddiayı desteklemekle birlikte başka anlamlara da gelebilecek kavramlar ve net olmayan tespitler delilin inandırıcılığını zedeleyebilir. Söz gelimi, İnternet üzerinden *dağıtık servis dışı bırakma saldırısı* (DDOS) yapmakla suçlanan kişinin bilgisayarında, saldırı yapılan saatlerde İnternet erişimi kayıt bilgilerinin bulunması önemli bir veridir. Ancak sadece bu veriye dayanarak suçlama yapılması delil inandırıcılığını olumsuz etkiler. Sanık o saatlerde İnternette her hangi bir işlem yapıyor olabilir. Sadece bu duruma dayanarak saldırı faaliyetinden sorumlu tutulması inandırıcı olmayacaktır. Buna benzer karşılaşılabilen örnekler sunulan delillerin inandırıcılığının önemini göstermektedir.

G- Delil tekrar incelene bilirliği

Dijital adli deliller bilimsel tekniklerle ve her defasında aynı sonucu veren çalışmalarla ortaya çıkarılmalıdır. Rastgele oluşan değerlerle ve nasıl çalıştığı ispat edilemeyen tekniklerle ortaya çıkarılan delil niteliği kazanamayacaktır. Farklı uzmanlar tarafından aynı teknikler kullanıldığında yine sonucu veren dijital adli deliller mahkemede kabul görecektir. Bunun dışında kalan deliller, söz gelimi uluslararası geçerliliği olmayan ve bağımsız organizasyonlar tarafından desteklenmeyen ürünlerle elde edilmiş deliller, ilgili aracın her çalışmasında yanı sonucu veremeyebilir. Buna benzer hatalar barındıran ürünler piyasada bulunmaktadır. Bu nedenle dijital adli delillerin bilimsel hüviyet kazanması için

kabul görmüş tekniklerle ve uluslararası standartlara uygun araçlarla elde edilmesi gerekmektedir.

IV. Delil güvenilirliği tespit modelleri

Dijital delillerin ihtimallere açık doğası, adli bilişim disiplinini zorlayan ve karar verici makamların dijital adli delillerden tam anlamıyla yararlanmasını engelleyebilen bir durumdur. Günümüzde ceza yargılaması hukukunun temel prensiplerinden olan "şüpheden sanık yararlanır[166]" ilkesi ile çelişen bu durum, davaları çözümsüzlüğe götürebilecek, vicdanların tatmin olmasını engelleyebilecek, gerçekte suçlu olan insanların ceza almamasına ve daha vahimi suçsuz insanların ceza almasına neden olabilecektir. Bir sonraki bölümde detaylı olarak ele alınacak bu konu, günümüzde *Truva atı savunması*[167] (Trojan horse defense) olarak terminolojiye geçen ve ne yazık ki suçlu insanların ceza almamak için sağlam bir dayanak noktası haline dönüşen bir savunma mekanizması olarak kullanılabilmektedir.

Adli bilişim disiplini; dijital adli analiz çalışmaları, bilişim teknolojileri ve istatistik biliminden faydalanarak bu soruna çeşitli çözüm önerileri getirebilir. Bu alanda yapılan çalışmalar, dijital adli delillerin yorumlanmasında kullanılabilecek iki yaklaşımın ön plana çıktığını göstermektedir. Bunlardan ilki "karmaşıklık tabanlı niceliksel değerlendirme", diğeri ise "güven seviyesi" modeli olarak isimlendirilmektedir.

A- Karmaşıklık tabanlı niceliksel değerlendirme

1. Tanım

Karmaşıklık tabanlı niceliksel değerlendirme (complexity based quantitative models)[168], hâkimler kadar dijital adli analiz uzmanlarını da oldukça

166 Suçsuzluk karinesi:kavram hakkında genel bilgiler ve avrupa insan hakları sözleşmesi, acikarsiv.ankara.edu.tr/browse/1073/1652.pdf, erişim tarihi: 07.01.2013.
167 Truva atı savunması, http://en.wikipedia.org/wiki/Trojan_Horse_Defense, erişim tarihi: 07.01.2013.
168 *Overill/Silomon/Chow*, sf 3.

zorlayan *Truva atı savunmalarına* (Trojan horse defense)[169] ilişkin bir model olarak kullanılmaktadır.[170]

Truva atı savunmalarının dayanak noktası, incelenen bilgisayarda tespit edilen bir zararlı yazılımın varlığı ve bu nedenle o bilgisayardaki hiçbir veriden kullanıcının mesul olamayacağı iddiasına dayanır. İncelenen sabit diskte tespit edilen dijital deliller, soruşturmaya konu edilen içerikler, bu dosyalarla kullanıcının ilişkisini gösteren izler ve varsa zararlı yazılım aktiviteleri, incelemenin kompleksliğini artırmakta ve net bir sonuç çıkarılmasını engelleyebilmektedir. Bu gibi durumlarda karmaşıklık tabanlı niceliksel değerlendirme metodu sayesinde tespitler netleştirilerek hâkimlerin karar daha isabetli karar vermesi sağlanabilir.

Günümüzde karmaşıklığı tanımlayan farklı modeller bulunmaktadır. Sayısal karmaşıklık, bilgi tabanlı karmaşıklık, mantıksal derinlik karmaşıklığı, termodinamik derinlik karmaşıklığı ve şifreli karmaşıklık olmak üzere farklı sınıflarda incelenen modellerden, dijital adli analize en uygun türün "sayısal karmaşıklık" olduğu düşünülmektedir[171]. Bunun sebebi incelemeyi yapacak uzmanın elinde sayısal sabit disk imajından başkaca bir veri olmaması olarak açıklanabilir.

Karmaşıklık tabanlı niceliksel değerlendirme modelinin temelinde, tespit edilen dijital adli verinin oluşması için bilgisayarda çalıştırılması gereken bütün işlem süreçleri ve bu süreçlerdeki adımlar için gerekli olan işlemlerin yapılabilme ihtimalleri değerlendirilir. Modelleme adımları aşağıda sıralanmıştır.

- İlk adım olarak hipotez oluşturulur. Söz gelimi bu iddia "Kullanıcı kendi bilgisayarında orijinal sinema filmi DVD'sinin kopyasını oluşturdu ve internetten yaydı" olabilir.

169 Susan W. Brenner, Brian Carrier, Jef Henninger, The trojan horse defense in cybercrime cases, Indiana 2005 ("Brenner/Carrier/Henninger"), sf. 16.

171 S Lloyd, Measures of Complexity: a Non-exhaustive List, IEEE 2001 ("Lloyd"), sf. 7, erişim tarihi: 07.01.2013.

- Sonraki adımda bu iddianın gerçekleşebilmesinin hangi yollarla mümkün olduğu düşünülür. Orijinal CD-DVD'den bilgisayara filmi kopyalama, P2P yazılımı kullanarak torrent dosyası oluşturma, torrent dosyasını İnternette yayma vb. örnekler bu adımda incelenir.
- Her bir varsayım için bilgisayarda olması beklenen delillerin listesi çıkarılır. İnternet kayıtları, torrent dosyasının oluşturulduğuna ve açıldığına dair izler, Web tarayıcı geçmiş kayıt verileri vb. veriler ele alınır.
- Varsayımın gerçekleşebilmesi için oluşması gerektiği düşünülen her bir iz için komplekslik değeri hesaplanır ve elde edilen değerler toplanır. İşlem ne kadar kompleks ise, delilin zararlı yazılımla gönderilme ihtimali o kadar düşük olacaktır.
- Bir önceki adımda ifade edilen komplekslik değerinin hesaplanmasında, bilgisayarda komut verebilmek için yapılan hareketler değerlendirilmektedir. Örnek vermek gerekirse, tespit edilen delilin oluşumu için bilgisayar faresinin sürükleyip bırakma, sağ düğmesini kullanma, klavye ve farenin art arda kullanılması vb. örnekler düşünülebilir. Bu şekilde ne kadar çok işlem ihtiyacı varsa, işlem o kadar kompleks olacaktır.
- İşlem için gerekli olan İnternet bağlantısı, İnternetten indirilen veri varsa büyüklüğü, kullanıcının müdahale ve/veya fark etme durumları değerlendirilmektedir. Yapılan işlemin niteliğine göre skor ataması yapılır.
- Bütün değerler hesaplandıktan sonra her bir işlem sürecinin ihtimali Bayesian modeli ile hesaplanır[172]. Hesaplama sonunda işlemin bilgisayar kullanıcı tarafından mı yoksa başka bir şekilde

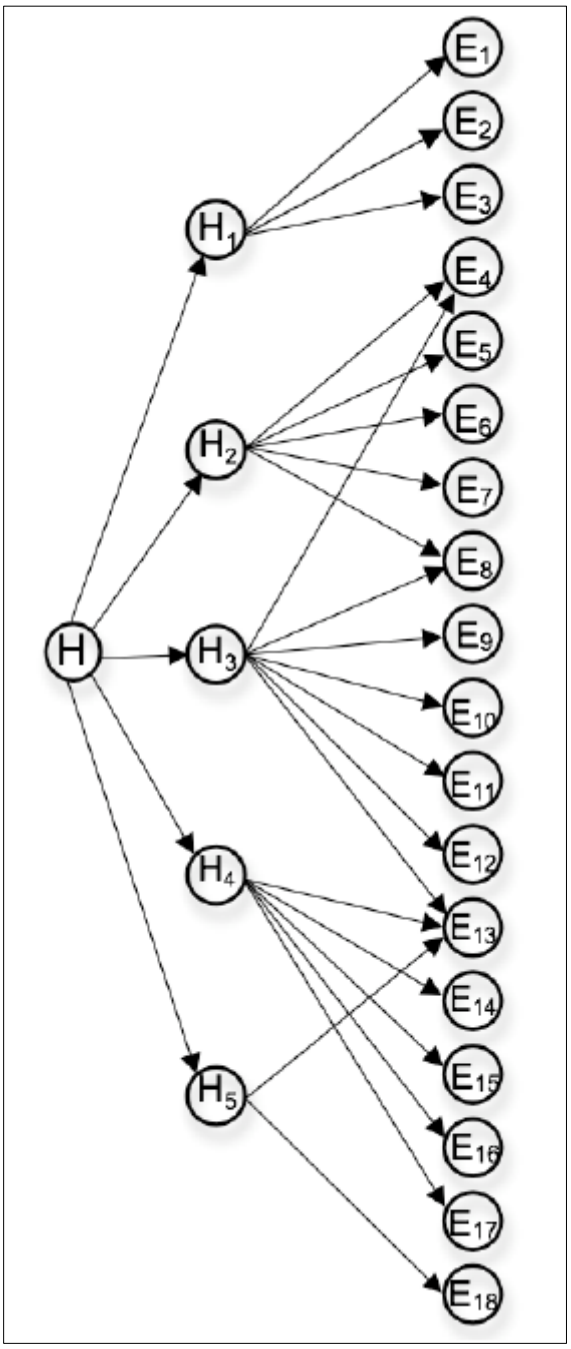
[172] M Kwan, K P Chow, F Law, P Lai, Reasoning About Evidence using Bayesian Network, Advances in Digital Forensics IV, International Federation for Information Processing (IFIP), Tokyo 2008 ("Kwan/Chow/Lai"), sf. 141.

kullanıcıdan habersiz mi gerçekleştiği ihtimallerinin oranı tespit edilir.

2. Vaka çalışması

Karmaşıklık tabanlı niceliksel değerlendirme modeli örnek bir vaka çalışması ile daha kolay anlaşılacaktır.

P2P paylaşım programı kullanılarak İnternette dağıtılmış yasadışı içerikte bir sinema filminin, incelemesi yapılan bilgisayarda oluşturulup oluşturulmadığı bu modelle çözülmeye çalışılabilir.



Şekil 40 - P2P ile yayılan bir filmin modellemesi.

Şekilde bulunan değerler, yukarıda belirtilen P2P film korsanlığı incelemesi için varsayılan alt hipotezleri ve bu hipotezlerin oluşabilmesi için gerekli delilleri ihtimallerini göstermektedir. Her bir maddenin açıklaması aşağıdaki gibidir.

a) Hipotezler

H:İncelenen bilgisayar korsan filmin dağıtılmaya başlandığı ilk bilgisayardır.

H_1:Korsan film, orijinal DVD'den kopyalanarak bilgisayara kaydedilmiştir.

H_2:Kopyalanan film dosyası için torrent[173] dosyası oluşturulmuştur.

H_3:Torrent dosyası haber gruplarına ve İnternet portallerine konulmuştur. Böylece insanlar dosyayı bulup indirmeye filmi indirmeye başlamıştır.

H_4**:**Oluşturulan torrent dosyası aktive edilmiştir. Aktive etme işlemi için dosyanın merkezi torrent sunucularıyla haberleşmesi gerekmektedir.

H_5:Merkezi torrent sunucusu ile incelenen bilgisayar iletişim kurmuştur.

b) Deliller

E_1:Kaynak dosya ile hedef dosyanın değiştirme zamanları aynıdır.

E_2:Hedef dosyanın oluşturma zamanı, değiştirme zamanından sonradır.

E_3:Hedef dosya ile kaynak dosyanın *kripto grafik özet* (hash) değerleri aynıdır.

E_4:BitTorrent istemci uygulaması bilgisayarda kurulmuş durumdadır.

E_5:Paylaşım dosyasına ait bağlantı dosyası (link) oluşmuştur.

E_6:Paylaşılan dosya sabit diskte bulunmaktadır.

E_7:Torrent dosyasının oluşturulduğuna dair kayıt bulunmuştur.

E_8:Torrent dosyası bilgisayarda bulunmaktadır.

E_9:Bilgisayarın başka bir kullanıcıya (peer) bağlandığı kaydı bulunmuştur.

E_{10}:Torrent sunucu bilgisayarına bağlantı bilgisi tespit edilmiştir.

E_{11}:Torrent dosyasının aktive olma zamanı, bağlantı dosyası (link) ve MACE[174] tarihleriyle uyumludur.

---

[173] A technical description of the BitTorrent protocol, http://www.cse.chalmers.se/~tsigas/Courses/DCDSeminar/Files/BitTorrent.pdf, erişim tarihi: 07.01.2013.

[174] MACE verileriyle ilgili detaylı bilgi için bkz. Tablo 1 - $MFT dosyasında bulunan üstveriler, sf. 43.

E_{12}:Torrent dosyasının dağıtım haberinin yüklendiği web sayfasına ait kayıtlar tespit edilmiştir.

E_{13}: Torrent dosyasının dağıtım haberinin yüklendiği web sayfasına ait çerez verisi bulunmuştur.

E_{14}: Torrent dosyasının dağıtım haberinin yüklendiği web sayfasına ait kayıtlar, sık ziyaret edilenler (bookmark) listesinde bulunmuştur.

E_{15}: Torrent dosyasının dağıtım haberinin yüklendiği web sayfasına ait kayıtlar, önbellek (cache) verileri arasında bulunmuştur.

E_{16}: Torrent sunucu bilgisayarına bağlantı bilgisi İnternet geçmişi kayıtlarında bulunmuştur.

E_{17}:İnternet bağlantısı bulunmaktadır.

E_{18}:Web tarayıcı yazılımı bulunmaktadır.

c) Değerlendirme

Tespit edilen hipotez ve varsayımlar, incelenen delil bilgisayarının detaylı analizi sonrasında ortaya çıkar verilerle modellenir. Bu yaklaşımda her bir hipoteze ulaştıran delil rotasına *k,* bu rotada uğranılan her bir delil setine ise $\{E_i\}$ denilerek hipotez karmaşıklığı aşağıdaki denklemle tespit edilir.

$$C_k = KLM_k + CC_k$$

Denklemdeki C_k karmaşıklığı işaret eden bileşendir. Her bir *k* rotası için hesaplanan rotanın oluşma ihtimali olan p_k, C_k ile ters orantılı olmaktadır.

$$\mathrm{Pk} \propto C_k{}^{-1}$$

Özetle karmaşıklık arttıkça, o rotanın kullanılmış olma ihtimali azalmaktadır. Denklemdeki KLM_k[175] değerleri ise, her bir delil rotasında işlenmesi yapılması gereken işlemler ve bunların karmaşıklığını verir.

[175] *Klavye Vuruşu Seviye Modeli* (Keystore Level Model-KLM) hakkında detaylı bilgi için bkz. http://en.wikipedia.org/wiki/Keystroke-level_model, erişim tarihi: 07.01.2013.

Tablo 4 - KLM operatörleri ve normalize edilmiş değerler

KLM Operatorü	Normalize Edilmiş Değer
K (Klavye tuşuna basıp bırakma)	2
P (Fare ile bir noktayı işaret etme)	11
B (fare tuşuna basıp bırakma)	1
H (klavyeden fareye el hareketi-veya tam tersi)	3
M (mantıksal hazırlık)	12

Bu değerler kullanılarak bilgisayarda yapılan işlemler için karmaşıklık puanı hesaplanabilir.

Tablo 5 - KLM işlem değerleri

İşlem	M	P	B	K	H	Toplam
1 Sürükle Bırak	2	2	2	0	0	48
2 Çift Tıklama	1	1	4	0	0	27
3 Tek Tıklama	1	1	2	0	0	25
4 Torrent Oluşturma	5	6	10	0	0	136
5 Torrent Yükleme	5	5	10	0	0	125
6 URL yazma	2	1	4	16	2	79
7 Giriş yapma (kullanıcı adı ve parola)	4	2	4	16	4	122

Hesaplanan bu değerler her bir delil rotası (E_i) için kullanıcı müdahalesinin değerini göstermektedir. Sayfa 112'de "Deliller" başlığı altında incelenen her bir değer için KLM değişkenleri kullanılarak bir karmaşıklık seviyesi atanır. KLM hesaplanan değerleri, iddia edilen işlemin kullanıcı tarafından yapıldığı gösteren işaretlerdir. Davaya konu işlemin zararlı yazılımlar etkisinde gerçekleştiğini gösteren durumlarda ise KLM değerleri 0 olur. Ancak bunun yerine diske erişim, dosya büyüklüğü ve erişim süresi gibi başka değerler kullanılarak delil rotası seviyeleri benzer şekilde tespit edilebilmektedir. Özetle her bir delilin (E_i)

kullanıcı tarafından veya zararlı yazılım tarafından yapıldığını destekleyen önermelerine ilişkin değerleri hesaplanır ve ihtimal ağırlıkları karşılaştırılır[176].

İncelenen bu örnekte delil ağırlıklarının kıyaslanması sonucu 4.6 değeri tespit edilmiştir. İşlemin *kullanıcı tarafından yapılma ihtimalinin, zararlı yazılımla yapılması ihtimaline* oranı olan bu değer, incelemenin %82 ihtimalle kullanıcı aleyhine neticelendiğini göstermektedir.

d) Tartışma

Karmaşıklık tabanlı niceliksel değerlendirme modeli, adli bilişim disiplinine matematiksel modelleme ve istatistik bilimlerini de katarak farklı bir yaklaşım sergilemektedir. Zararlı yazılımlar ve kullanıcıların davranış modellerini formüle etmeye çalışan bu modelleme, bir takım soruları da beraberinde getirmektedir.

- Modellemenin sonucunda elde ettiği değer, karar vericilerin işini gerçekten kolaylaştırmakta mıdır? Sayısal bilimlerle uğraşan insanlar için yüzdeli ifadeler anlamlı olsa da, bir hâkim için %51 ifadesi yeterli suç şüphesi anlamına gelmeyebilir. Böyle bir durumda %60, %70 bile yeterli olmayabilir. Bir suçun işlendiğine dair haklı olarak %100 emin olmak isteyen bir hakim, bu modelin çıktılarını yorumlarken zorlanacaktır.
- Her geçen gün değişen ve gelişen zararlı yazılımlar, bir bilgisayarın kontrolünü tamamen ele geçirdiği takdirde, yapacağı işlemleri tamamen kullanıcı yapmış gibi gösterebilir. Otomatize çalışmayan, kişiye özel hazırlanmış bu tip zararlı yazılımlarda klavye-fare hareketleri, kullanıcı davranışını gösteren kimlik doğrulama işlemleri vb. faaliyetler de yürütülebilir. Böyle durumlarda modelin sağlıklı uygulaması mümkün olmayabilir.

[176] Overill, Silomon ve Chow'un uyguladığı bu yöntemde ileri düzey istatistik ve matematiksel modellemeler kullanıldığı için daha fazla teknik ayrıntıya girilmemiştir. Ayrıntılı bilgi için yazarların ilgili makalesi incelenebilir. Bkz. *Overill/Silomon/Chow*.

- Modelde kullanılan değişkenler, modeli hazırlayan uzmanlarca atanmıştır. Ancak bu değer atamaları netice itibariyle görecelidir. Bir uzmanın klavye hareketine atadığı başka bir uzman tarafından kabul görmeyebilir. Bu durumda modelin uygulaması için bir standardın oluşması kolay olmayacaktır.

Her ne kadar eksik yanları ve tartışmaya açık noktaları bulunsa da, "karmaşıklık tabanlı niceliksel değerlendirme" modeli, dijital adli analiz çalışmalarında karşılaşılan "truva atı" savunmaları için bir çözüm olabilir. Adli bilişimin doğasında olan "ihtimalli" yorumlar, bu gibi matematiksel tespitlerle bir nebze olsun daha kolay anlaşılabilir. İçinde şüphe barındıran bütün durumların "%50 ihtimal" olarak kabul edilmesindense rakamların netleştirilmesi elbette faydalı olacaktır.

B- Güven seviyesi sınıflandırma modeli

1. Tanım

Güven seviyesi (confidence level) [177] yaklaşımı, dijital adli analiz çalışmalarında tespit edilen bulguları nitelik ve niceliklerine göre sınıflandıran, bu tespitlere göre bulguların "aslına uygunluğunu", "kaynağını" ve özellikle de "kullanıcı ilişkisini" yorumlayarak dijital adli delilin hangi güven seviyesi sınıfında olduğunu tespit eden bir çalışma modelidir[178].

Dijital adli analiz bulgularının yorumlanmasında ve bu yorumlar neticesinde karar vericilerin bir sonuca varmasında en büyük problemlerden biri, dijital adli analiz biliminin tanımlı bir matematiği olmamasıdır. Dijital delillerin hangi kriterlere göre hangi kategoride değerlendirileceği, bu delillerin güvenilirlik

[177] *Casey*, sf. 70.
[178] Dijital adli delil kurallarından "aslına uygunluk", "delil kaynağı" ve "kullanıcı ilişkisi" prensipleri hakkında detaylı bilgi için bkz. "Dijital adli delil kuralları" sf. 106.

seviyesinin tespit edilmesinde nesnel olmayan[179] sınıflandırılmaların yapılmasına neden olmaktadır. Bundan dolayı incelenen konu aynı bile olsa, farklı uzmanların tamamen farklı sonuçlara ulaşabilmesi muhtemeldir. Bu nedenle, dijital adli delillere güven seviyesi atanması ve karar aşamasında bu seviyelere göre değerlendirme yapılması faydalı olabilir.

Dijital adli analiz raporlarında karşılaşılabilen durumlara ilişkin daha tutarlı ve ölçeklenebilir yorumlar yapılabilmesi için alttaki tablo referans alınabilir

Tablo 6 – Dijital adli delillerin güven seviyeleri sınıflandırması

Güven Seviyesi	Tanım	Nitelik Sınıflandırması
G0	Bulgu bilinen doğrularla çelişiyor, tespit hiçbir şekilde kabul görmüyor.	Tamamen Yanlış
G1	Bulgu ciddi şekilde sorgulanıyor. Cevaplanamayan soru veya sorular bulunmakta.	Şüpheli
G2	Bulguların manipüle edilmesi zor, bununla birlikte açıklanamayan tutarsızlıklar ve delil bütünlüğünü etkileyen eksiklikler mevcut.	İhtimal Dâhilinde
G3	Bulgunun manipüle edilmesi imkânsız veya aynı sonuca ulaştıran çok sayıda manipüle edilebilme ihtimali düşük bulgu var.	Kuvvetle Muhtemel
G4	Birden çok bağımsız otorite tarafından manipüle edilmesinin imkânsız olduğu türde bulgular mevcut. Bununla birlikte geçici veri kaybı gibi çok ufak belirsizlik ihtimalleri var.	Neredeyse Kesin
G5	Bulgunun doğruluğu ve kesinliğine hiçbir şüphe	Kesin

[179] Nesnel olmayan değerlendirmeler, ”dijital adli analiz uzmanının tecrübe ve bilgisinden hareketle vardığı hissiyat” olarak tanımlanabilir.

	yok, bulgunun manipüle edilmesi imkansız.	

Örneklerle açıklamak gerekirse hayali bir "e-posta ile tehdit edilme" davasına bakacak olursak;

G5: Müzekkerede incelenmesi talep edilen dijital delillerin ilgili sabit disk imajında tespit edilmesi. Tespit edilen bu delillerdeki isimlerin, e-postalar ve benzeri diğer delillerin içeriklerinin ve resim/fotoğraf vb. materyallerin görsel inceleme sonucunda aynı delil olduğunun anlaşılması.

G4: Kullanıcı bilgisi, oturum bilgisi, e-posta hesabı veya IP adresi gibi verilerin, bilgisayarı incelenen şahsı işaret etmesi. Bağımsız otoritelerin bu gibi verilerde güven seviyesinin neredeyse kesin olduğuna dair tespitlerinin olması, bu alanda yayınlamış çeşitli makalelerin uluslararası camiada kabul görmesi.

G3: Sabit disk imajında tespit edilen ve tehdit içeren e-postaların, bilgisayarın kullanıcısı tarafından gönderildiğine dair olan gönderici adı, gönderenin e-posta sunucu IP'si gibi verilerin varlığı veya aynı tarihlerde oluşturulduğu tespit edilen ve e-posta içeriğiyle tutarlı birçok dosyanın sabit diskte bulunması.

G2: Sabit disk imajında ilgili tarihlerde hazırlandığı tespit edilen, üst verilerinin tarih ve kişi bilgileri ile tutarlı olduğu bir dosyanın tespiti. Bununla birlikte tehdit amaçlı gönderildiği iddia edilen e-posta kayıtlarının bulunmaması.

G1: İlgili imajda tehdit için kullanılmış olabilecek çeşitli internet sayfaları, bazı kişisel veriler ve sosyal medya araştırmalarına dair tespitlerin bulunması. Bununla birlikte tehdit için gönderildiği iddia edilen metin dosyasının veya e-postanın bulunmaması.

G0: Sabit disk imajında iddia edilen tehdit içeriğine veya öncesinde yapılmış olabilecek muhtemel araştırmalara dair hiçbir izin bulunmaması.

Bu sınıflandırma kullanılarak, dijital adli analiz uzmanının tespitleri hem daha kolay anlaşılır olacak, hem de belirli bir standarda sunulduğu için

mahkemeler ve bilirkişiler arasında yorum farklarını en düşük seviyelere indirilebilecektir.

2. Vaka çalışması

"Güven seviyesi" modelinin nasıl uygulanabileceğini görmek için örnek bir vaka çalışması yapılabilir. Bu çalışmada dijital adli analiz süreç modellerindeki sıralama esas alınarak elde edilen bulgular ve kesinlik dereceleri hesaplanacaktır. "Bilgisayarda tespit edilen dijital dosyalarla şahsın ilişkisini" araştıran bu örnek çalışmadaki unsurlar, günümüzde rastlanabilecek en karmaşık noktalara değinmektedir. Bununla birlikte, bir dijital adli analiz sürecinin bütün adımları detaylı olarak açıklanmamış, delil güvenilirliğini etkileyebilecek konuların üzerinde durulmaya çalışılmıştır.

a) Hazırlık

Senaryoya göre, terör örgütüne yardım ve yataklık ettiğinden şüphelenilen bir şahıs tespit edilmiştir. Sonrasında şahsın telefonları uzun süre dinlenmiş ve bağlandığı internet adresleri takip edilmiştir.

Bu çalışmalar sonucunda;

- Şahıs, örgütle bağlantılı olduğu bilinen başka bir kişiyle telefonda görüşmüş ve bunun üzerine teknik takip başlamıştır.
- Telefon dinlemeleri sonucunda ilgili şahsın finansal işlerden sorumlu örgüt üyesi olduğuna kanaat getirilmiştir.
- İnternet trafiği dinlenilmiş ancak sonuç alınamamıştır. Gündelik haber, oyun vb. web sitelerinin yanında, zaman zaman karmaşık e-posta hesaplarına giriş yapıldığı anlaşılmıştır.

Teknik takip ile daha fazla bilgi edinmenin mümkün olmadığı anlaşıldığından şahsın evine operasyon kararı alınmıştır. Gerekli teknik hazırlıklar başlatılmış, dijital adli analiz için imaj kopyalama araçları hazırlanmış, boş sabit diskler elde edilmiş ve şahsın evine baskın düzenlenmiştir.

b) Tespit

Operasyon esnasında evde 2 kişi olduğu görülmüştür. Şahısların talebi üzerinde avukatları olay mahalline çağrılmış ve inceleme başlatılmıştır. İncelemeler neticesinde;

- Evin salonunda bulunan masaüstü bilgisayarın sabit diski,
- Şahsın yatak odası olduğu tahmin edilen odada bulunan bir taşınabilir bilgisayar sabit diski,
- Başka bir odada bulunan taşınabilir bilgisayarın sabit diski,

İmajı alınmak üzere toplanmıştır. Salonda bulunan bilgisayarın baskın esnasında açık olduğu görülmüştür. Bununla birlikte parola ekranının aktif olması ve evde bulunan şahsıların ilgili parolayı söylememesi üzerine bilgisayar kapatılmıştır ve sabit diski o şekilde çıkarılmıştır.

Diğer odada bulunan taşınabilir bilgisayar da açık halde bulunmuş ve hemen imajı alınmıştır. İmaj alma işleminde sonra bilgisayar kapatıldığında tekrar açmak mümkün olmamıştır. Bütün sabit diskin şifrelendiği bilgisayarın imajı bu sayede alınabilmiştir.

Şahsın kendi odasındaki taşınabilir bilgisayar ise kapalı halde bulunmuştur, herhangi bir disk şifrelemeye maruz bırakılmadığı için imaj alma işlemi sorunsuz tamamlanmıştır.

Yapılan gözlemler neticesinde evde kablosuz İnternet bağlantısının bulunduğu görülmüştür. Salondaki masaüstü bilgisayarın evdeki modemle kablolu bağlantı yaptığı ve bu sayede İnternete çıktığı anlaşılmıştır.

c) Koruma

Toplanan delillerle ilgili işlem yapmak için imaj alma işlemine başlayan kolluk kuvvetleri taşınabilir bilgisayarların imajını almışlar, bu imajların *kripto grafik özet* (hash) değerlerini hesaplatarak tutanak hazırlamışlardır. Ancak masaüstü bilgisayarın imajı teknik bir problemden alınamamış, imaj alma işleminin büroda devam etmesine karar verilmiştir. Bunun üzerine şahsın avukatları, diğer kolluk kuvvetleri ve şahsın huzurunda imajı kopyalanan bütün

disklerle birlikte masaüstü bilgisayarın orijinal sabit diski çuvala konmuş ve ağzı mühürlenmiştir.

Emniyete götürülen deliller avukatlar huzurunda açılmıştır. Baskında yaşanan teknik problem nedeniyle imajı alınamayan sabit diskin kopyası alınmıştır. Kolluk kuvvetlerinde sabit disklerin ilk incelemesi yapılmış, bir takım örgütsel bilgilerin yer aldığı dosyalar tespit edilmiş ve bu bilgiler bir ön rapor hazırlanarak mahkemeye iletilmiştir.

Delilleri değerlendiren mahkeme, şahsın tutuklanmasına karar vermiş, evde bulunan diğer kişiyi ise tutuksuz yargılanmak üzere serbest bırakmıştır. Sanık ise suçsuz olduğunu ve dosyaların kendi bilgisi haricinde bilgisayarına konduğunu iddia etmiştir.

Bunun üzerine mahkeme heyeti detaylı bilirkişi raporu hazırlanmasını istemiştir. Mahkemenin kararı sonrasında, delillere ait tutanaklar ve sabit disk imajları hazır edilerek mahkemece atanmış bağımsız bilirkişilere teslim edilmiştir.

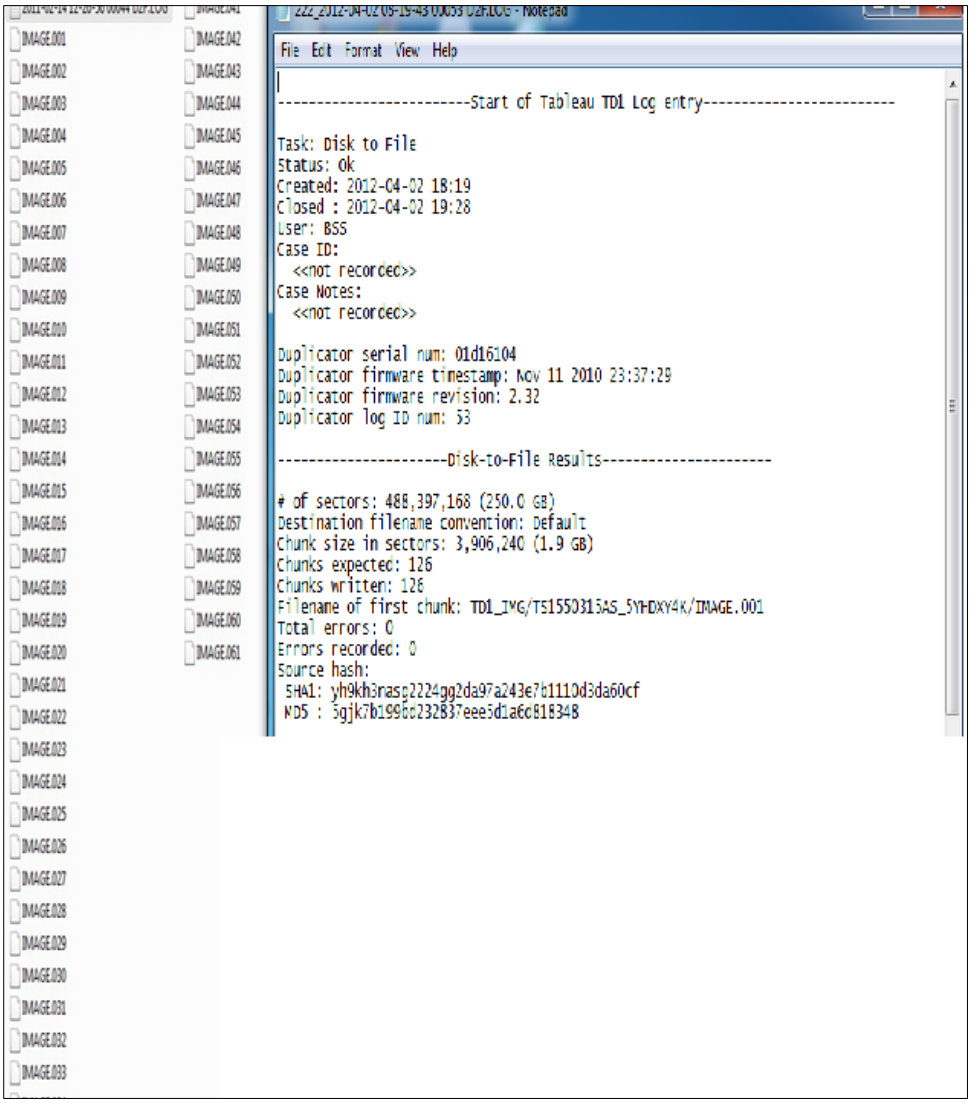
d) Analiz

Bilirkişiler teslim aldıkları diskleri incelemeye başlamadan önce, imaj alma işlemlerinin usulüne uygun olarak yapılıp yapılmadığına bakmışlardır. Yapılan inceleme sonucunda, imaj alma işlemleri için Tableau [180] ürününün kullanıldığı tespit edilmiştir. İmaj alma işlemlerinde sıklıkla kullanılan bu ürünün birçok uluslararası sertifikaya sahip olması ve "yazma korumalı" imaj alma desteğinin bulunması imaj dosyalarına güvenilebileceğini göstermiştir.

Sonraki adımda bilirkişiler disklerin *kripto grafik özet* (hash) değerlerine bakmıştır. Hesaplanan hash değerleri ile tutanaklardaki değerlerin arasında fark olup olmadığı kontrol edilmiştir. Arama-el koyma çalışmalarında evin salonundaki bilgisayardan alınan sabit diskin hash değeri, tutanaklarda silik çıktığı için bazı karakterler okunamamıştır. Bunun üzerine bilirkişiler imajın kayıtlı olduğu diskteki "imaj alma loglarına" bakmışlar ve değerleri karşılıklı tekrar kontrol etmişlerdir(Şekil 41). İlgili diskin imaj alma işleminin yarıda kalmış

[180] Ürün hakkında detaylı bilgi için bkz. "Tableau" sf. 20.

olması ve büroda sonra alınması tartışmalara neden olsa da, hash değerlerinin aynı olması sonucu delil geçerliliği sağlanmıştır.



Şekil 41 - İmaj TD1 logu.

Bütün imajların tutanaklardaki hash değerleri ile hesaplanan değerleri arasında fark olmadığı görülmüştür ve böylece delil imajlarının orijinal kopyalarıyla birebir aynı olduğu anlaşılmıştır[181].

Sonraki adımda diskler açılarak incelenmeye başlanmıştır. İlk incelenen disk, salonda ele geçirilen masaüstü bilgisayara ait olandır. Ancak bu noktada

[181] Kriptografik özet alınması ve hash değerlerinin önemiyle ilgili bkz. "Delilin aslına uygunluğu" sf. 107.

kötü bir sürprizle karşılaşılmış, diskin şifreli olduğu anlaşılmıştır[182]. Diskin tamamı şifreli olduğu için hiçbir veri incelenememiştir. El koyma işlemleri yapılırken açık olan bu bilgisayarın parolasının elde edilmesi veya bilgisayar açıkken imajın alınmasını sağlayan teknikler[183] kullanılsaydı, bu diskin incelenmesinde bir problem oluşmayacaktı.

İnceleme işlemlerine kullanıcının taşınabilir bilgisayarı (Delil A) ile devam edilmiştir. Dosya sistemi verileri, işletim sistemi verileri ve uygulama verilerinin Encase uygulaması ile yapılan detaylı tetkikleri neticesinde alttaki bulgular tespit edilmiştir.

- Kullanıcının okm112_mny@gmail.com isimli e-posta adresine sair defalar giriş yaptığı tespit edilmiştir.
- Şahsın bilgisayarında bu e-posta adresine giriş yapıldıktan birkaç dakika sonrasında oluştuğu tespit edilen bir Excel dosyası bulunmuştur. "Avrupadan_gelen.xlsx" isimli bu dosya silinmemiş halde bilgisayarda bulunmaktadır. İçinde çok sayıda örgütsel faaliyet kayıtları bulunmaktadır.
- İlgili bilgisayarda çok sayıda zararlı yazılım tespit edilmiştir. Bu zararlı yazılımların birçoğu rootkit[184] formatındadır.
- Zararlı yazılımların, bilgisayarın her açılışında çalışmasını sağlayacak şekilde *kayıt defterinde* (registry) girdi oluşturduğu görülmüştür.

İncelenen diğer taşınabilir bilgisayardan (Delil B) elde edilen bulgular aşağıdaki gibi olmuştur.

- Bilgisayar kullanıcısının e-posta hesaplarında okm112_mny@gmail.com adresine gönderilmiş birkaç ileti tespit edilmiştir. Ancak e-posta içeriklerinde suç unsuru olabilecek bir

[182] Bütün diskin şifrelenmesi tekniği (full disk encryption) kullanımı hızla yaygınlaşan bir güvenlik önlemidir. Truecrypt, bitlocker vb. araçlarla verilerin şifrelenmesi sonucunda deliller karartılarak dijital adli analiz çalışmalarından netice alınması engellenebilir. Detaylı bilgi için bkz. "Verinin şifrelenmesi" sf.80.

[183] Firewire bağlantısı olan bilgisayarlarda TDM (Target Disk Mode) desteğiyle bu tür imaj alma işlemleri yapılabilir. Detaylı bilgi için bkz. http://en.wikipedia.org/wiki/Target_Disk_Mode, erişim tarihi: 07.01.2013.

[184] Rootkitler hakkında detaylı bilgi için bkz. "Rootkitler ve botlar" sf. 75.

veriye rastlanmamıştır. Bununla birlikte e-posta eklerinde bazı *.exe uzantılı dosyaların olduğu görülmüştür.

- Delil A'da tespit edilen "Avrupadan_gelen.xlsx" dosyasına dair çeşitli izler Delil B'de de bulunmuştur. Dosyanın bu bilgisayarda işlem gördüğü $LogFile kayıtları incelenerek anlaşılmıştır. Ayrıca dosya içeriği *kazıma tekniği* (carving) ile çıkarılmaya çalışılmış ve üstverileriyle birlikte içeriğinin büyük bir bölümü kurtarılabilmiştir[185].
- Şahsın bilgisayarında "Diskwipe" isimli bir uygulama tespit edilmiştir. Uygulamanın kurulum tarihi birkaç yıl öncesinde dayanmaktadır. Diskwipe'ın son kullanıldığı tarih, "Avrupadan_gelen.xlsx" dosyasının $LogFile'a yansıdığı tarih ile çok yakındır. Aralarından bir kaç dakika fark vardır.
- Bu bilgisayarda bulunan bazı ofis dosyalarının üstverilerinde, diğer şahsın (Delil A kullanıcısı) adının bulunduğu görülmüştür. Suç niteliği taşıyan bu dosyaların zaman-tarih üstverilerine bakıldığında, dosyaların son oluşturma, değiştirme ve sistem giriş zamanlarının bu bilgisayardaki diğer zaman tarih verileriyle (Log2TimeLine çıktıları ve LNK dosyaları gibi) uyumlu olduğu görülmüştür.
- İnternet geçmişinde "reverse https", "undetectable payloads", "phishing e-mails" gibi ifadelerin geçtiği aramaların yapıldığı görülmüştür. Ayrıca bilgisayarda çeşitli programlama kitaplarının yanı sıra, metasploit ve backtrack uygulamalarının da kurulu olduğu görülmüştür[186].

[185] Bu inceleme için *kazıma tekniği* (carving) ile *paylaştırılmamış yığınlar* (unallocated clusters) üzerinde araştırma yapılmıştır. "Kazıma tekniği", dosyanın ismi yerine içeriğine dair kelimelerin araştırıldığı, içerik bazlı sorgulamaların yapıldığı araştırma tekniğidir.

[186] Backtrack, özelleşmiş bir Linux dağıtımıdır. Bu işletim sisteminde, "sızma testi" çalışmalarında kullanılan ve sistem açıklıklarını kullanarak başka bilgisayarları uzaktan yönetmeye yarayan araçlar bulunmaktadır. Metasploit de bunlardan biri ve en bilinenidir. Detaylı bilgi için bkz. http://www.backtrack-linux.org/, erişim tarihi: 07.01.2013.

e) Raporlama

Bilirkişiler incelemelerini tamamlayarak rapor hazırlama safhasına gelmişlerdir. Müzekkeredeki iddialar ve bu iddialara yönelik cevapların güven seviyeleri ile birlikte yorumu aşağıdaki gibi olmuştur.

Tablo 7 - Sonuçların güven seviyesi sınıflandırmasıyla açıklanması

Soru	Tespit	Nitelik İfadesi	Güven Seviyesi	Güven Seviye Açıklaması
Delil A'da suç unsuru içerdiği bilinen dosya bulunmakta mıdır?	İlgili dosya bir kısmı silinmiş alandan çıkarılarak görüntülenebilmiştir. Dosyanın tamamen ortaya çıkarılamasa bile, içeriği anlaşılacak kadar olan bir bölümü tespit edilmiştir. Dosyanın bir kısmının görüntülenmesi ve $LogFile'da isminin geçmesi dosyanın var olduğunu ispatlanmıştır.	Neredeyse Kesin	G4	Paylaştırılmamış yığınlar (unallocated clusters) alanından çıkarılan verilerin daha önce ilgili bilgisayarda bulunduğu düşünülür. Ancak dosyanın bir kısmı çıkarılamadığı için dosya bütünlüğü sorgulanmaktadır.
Delil A'da ilgili dosya silinmiş midir, delil karartma işlemine maruz bırakılmış mıdır?	İlgili dosya silinmemiş halde tespit edilmiştir. Dosya içeriği incelenebilmiştir.	Kesin	G5	Dosyanın ilgili bilgisayarda bulunduğundan hiçbir şüphe yoktur.

Delil B'da dosya silinmiş midir, delil karartma işlemine maruz bırakılmış mıdır? Dosyanın tamamen ortaya çıkarılamamasının sebebi nedir?	İlgili dosya silinmiş olarak elde edilmiştir. Aynı zamanda dosyanın silinme nedeni olarak delil karartma işleminde şüphelenilmektedir.	Kuvvetle Muhtemel	G3	Log2timeline analizi sonucunda $LogFile verilerinden hareketle dosyanın son erişim tarihi ile Diskwipe programının çalıştırılması tarihlerinin çok yakın olduğu anlaşılmaktadır. $LogFile verilerinin tekil kayıtlar bazında manipüle edilmesi zordur, ancak imkânsız değildir.
Delil A bilgisayarında zararlı yazılımlar var mıdır? Zararlı yazılımlar ile bilgisayara uzaktan bağlanılmış mıdır?	Bilgisayarda yapılan incelemeler sonucunda aktif olarak çalışan zararlı yazılımlar tespit edilmiştir.	Neredeyse Kesin	G4	Bilgisayarda aktif olarak çalışan zararlı yazılımlar bulunsa da, bilgisayara uzaktan bağlantı verileri bulunamamıştır. Bu nedenle delilin güven seviyesi azalmıştır.
Delil B bilgisayarında zararlı yazılımlar var mıdır? Zararlı yazılımlar ile bilgisayara uzaktan bağlanılmış mıdır?	Yapılan analizler neticesinde bilgisayarda bazı zararlı yazılım izlerine rastlanmıştır. Bununla birlikte ilgili zararlı yazılımların *kaynak kodları* (source code) da tespit edilmiştir.	İhtimal Dâhilinde	G2	Zararlı yazılımlar tespit edilse de, aktif olarak çalıştıklarına dair bir iz bulunmamıştır.

Delil A bilgisayarında bulunan dosya kullanıcı tarafından mı oluşturulmuş veya değiştirilmiştir?	Dosyaların üstveri bilgileri incelendiğinde bilgisayar kullanıcısının kendi verileriyle uyumsuzluklar tespit edilmiştir.	Şüpheli	G1	Dosyayı kullanıcı açsa ve değiştirseydi, dosyanın kendi üstverileri başta olmak üzere farklı noktalarda izler olması beklenirdi.
Delil B bilgisayarında bulunan dosya kullanıcı tarafından mı oluşturulmuş veya değiştirilmiştir?	Dosyaların üstveri bilgileri ve dosya sistemi verileri incelendiğinde, dosyanın bu bilgisayarda açıldığına dair çok kuvvetli izler bulunmuştur.	Neredeyse Kesin	G4	Kullanıcın dosyayı açması ve değiştirmesi neticesinde oluşabilecek izlere rastlanılmıştır. Bu izler geneli itibariyle manipülasyona kapalı izlerdir.

Oldukça karmaşık bu incelemenin neticesinde dijital deliller üzerinde delil karartma işlemleri yapıldığı anlaşılmıştır. İlgili dosya Delil A bilgisayarında açık halde ve silinmemiş olarak bulunsa da, dosyanın aslında ilk olarak Delil B bilgisayarında işlem gördüğü ve sonrasında Delil A bilgisayarına uzaktan bağlanılarak gönderildiği anlaşılmıştır. Bu sayede Delil A kullanıcısının dijital delillerin sorumluluğundan kurtulmaya çalıştığı, ancak Delil B'de çıkan veriler neticesinde organize bir çalışma yürütüldüğü tespit edilmiştir. Neticede Delil B kullanıcısı da olayda aktif rolü olduğu gerekçesiyle tutuklanmıştır.

Delil B bilgisayarının imajı alınamasaydı [187], Delil A kullanıcısının bilgisayarındaki zararlı yazılımlar zanlının suçsuzluğunu gösterebilecekti. Ancak Delil B ile birlikte bütüncül bir araştırma yapıldığında organize bir faaliyet yürütüldüğü anlaşılmıştır.

[187] İlgili delil bilgisayarının arama-el koyma işlemlerinde açık halde bulunmaması halinde, diskinin şifreli olması nedeniyle imajının alınamayacağı hatıra getirilebilir.

Teknik olarak karmaşık sayılabilecek bu gibi analizlerde, yukardaki tabloda verilen güven seviyesi sınıflandırması karar vericilerin olayı idrak etmesi açısından önem kazanmaktadır. Artı ve eksi yönleriyle detaylı tartışma bir sonraki bölümde ele alınmıştır.

f) Tartışma

Güven Seviyesi sınıflandırması, yukarıda açıklanan karmaşık senaryolara açıklık getirerek dijital adli analiz raporlarında çeşitli faydalar sunabilir. Karar verici makamların işini kolaylaştırabilir, olası anlaşılmazlıkları engelleyebilir. Ancak bununla birlikte çözülemeyen bazı noktalar da bulunmaktadır. Artıları ve eksileriyle "Güven Seviyesi" yaklaşımına dair tespitler aşağıdaki gibi özetlenebilir.

Tablo 8 - Güven seviyesi sınıflandırmasında avantaj ve dezavantajlar

Avantajları	Dezavantajları
Raporu yorumlaması gereken ancak teknik bilgiye haiz olmayan kişiler için kolay anlaşılabilir olması.	Her ne kadar yön gösterici olsa da, güven seviyelerinin atanmasında dijital adli analiz uzmanının öznel yorumunun devreye girmesi.
Raporlarda geçebilecek muğlak ifadelerin yerine daha anlaşılabilir ve kıyaslanabilir cümlelerin kurulabilmesi	Çok fazla etmenin sonucu değiştirebileceği, artı ve eksi yönde çok sayıda belirsizliğin olma ihtimali.

"Güven Seviyesi" sınıflandırmasının adli analiz uzmanının tespitlerine göre değişebilmesi ve esnek olması. Söz gelimi; incelenen imajda tespit edilen bir zararlı yazılımın güven seviyesini aşağıya çekebilmesi veya zararlı yazılımın, incelenmesi talep edilen delillerle ilişkisi olmadığında bu seviyenin tekrar yukarıya çekilebilmesi.	Esnekliğin uzmanlarca istismar edilebilmesi, bazı tespitlerin bilerek ve bilmeyerek atlanması neticesinde lehte ve aleyhte durum oluşturabilecek yorumların çıkması

Bu özellikleriyle güven seviyesi sınıflandırma yaklaşımı, dijital adli analiz raporlarında yardım alınabilecek bir referans olabilir. Bununla birlikte günümüzde dijital adli analiz uzmanının basite indirgemekte zorlanacağı kompleks analizler de bulunmaktadır. Bu analizlerin sınıflandırılması ve belli bir skor atanarak güven seviyesinin belirtilmesi mümkün olmayabilir. Bu nedenlerden dolayı dijital adli analiz bilimi, "güven seviyeleri sınıflandırması" gibi ceza hukukuna yardımcı olabilecek yeni metodolojiler geliştirse de, konuya kesin bir çözüm getirmek zordur. Bu nedenle dijital adli analiz konusunda ihtisaslaşan mahkemelerin kurulması ve karar verici makamların adli bilişim disiplinine yaklaşması, teknik uzmanların hazırlayacağı raporların daha isabetli yorumlanmasına yardımcı olabilecektir. Konuyla ilgili çözüm önerileri sonuç bölümünde etraflıca ele alınmıştır.

§6. Ulusal ve uluslararası hukukta dijital adli deliller

I. Mevzuat

Bir delil çeşidi olarak dijital adli delillerin mahkemede değerlendirilebilmesi için ilgili yasal düzenlemelerin yapılmış olması gerekmektedir. Bu düzenlemelerde dijital delillerin hangi durumlarda geçerli olabileceği ve nasıl işlenmesi gerektiği açıklanmış olmalıdır.

ABD başta olmak üzere gerek Avrupa ülkelerinde gerekse ülkemizde konuyla ilgili olarak bir takım kanunlar çıkarılmış durumdadır. Bu düzenlemeler ülkelerin teknolojik gelişmeleri ne oranda takip edebildiği ve hangi oranda yasalara yansıtılabildiği ile doğrudan ilişkili olup, dijital delillerin mahkemelerde kullanılabilmesini etkileyen faktörler olmaktadır.

Bu konuda mesafe kat etmiş ülkelerin ilgili düzenlemeleri ve bu konuda Türkiye'de uygulanmakta olan mevzuat alt başlıklar halinde incelenebilir.

A- ABD perspektifi

ABD, dijital adli delillerle ilgili düzenlemeleri yasalarına ilk entegre eden ülkelerdendir. Ülkenin teknolojik gelişmelere öncülük yapması beraberinde bu tür yasal düzenlemelere olan ihtiyacı gündeme getirmiş ve neticede ilgili kanunlarda ve yargı sisteminin bütününde "adli bilişim" disiplinin yaygınlaşmasına neden olmuştur.

ABD hukukunda dijital adli delillerin mahkemede kabul görmesi ve değerlendirilebilmesi için F*ederal Delil Kurallarında* (Federal Rules of Evidence[188]) bulunan ilgili maddelere uyumlu olması gerekmektedir[189]. Dijital delillerin ABD hukuk sisteminde değerlendirilmesine yön veren bu kurallar aşağıda sıralanmıştır.

---

[188] "Federal Rules of Evidence" hakkında detaylı bilgi ve sorgulamalar için bkz. http://federalevidence.com, erişim tarihi: 07.01.2013.

[189] Admissibility of Digital Evidence, http://www.tmcec.com/public/files/File/Course%20Materials/FY09/Prosecutors/Moss%20-%20Digital%20Evidence.pdf, erişim tarihi: 07.01.2013.

1. Delilin gerçekliği

Delilin gerçekliği (Authentication R. 901,902), delilin iddia edilen önermeyi desteklemesini veya delili sunan tarafın belirttiği durumun aynı şekilde delilde bulunup bulunmadığını sorgular. Sunulan dijital verinin delil niteliği kazanması için bu özelliklere haiz olması gerekmektedir.

2. Delilin ilgili olması

Delilin soruşturmayla *ilgili olması* (Relevance R. 401) kuralına göre, sunulan deliller konuyla ilgili olmalı, soruşturmanın dışında kalacak bir alanda yer almamalıdır.

3. Delilin önyargı oluşturmaması

Dijital delillerin geçerliliği için dikkate alınan bir diğer husus, ilgili delilin *önyargı oluşturmayacak* (Undue Prejudice (R. 403)) niteliğe sahip olması gerekliliğidir. Bu kurala göre sunulan delil soruşturmayla ilgili bile olsa; adil yargılamayı etkileyecek ağırlıkta ve yoğunlukta olması, yargılamayı geciktirme ihtimali bulunması, benzer nitelikteki başka delillerin varlığı nedeniyle zaman kaybı oluşturabilmesi ve jüriyi yanıltabilecek nitelikte olması gibi nedenlerle ilgili delil geçersiz sayılabilir.

4. Delilin başka kaynaklardan elde edilmesi

Dijital adli delil kurallarından bir diğeri delilin başkaca kaynaklardan elde edilmesi (Hearsay R. 801-804) halinde tabi tutulduğu değerlendirmedir.

Bu kurala göre soruşturmayla ilgili olabilecek başka kaynaktaki deliller dava kapsamında değerlendirilebilir. Karar vericilerde etki oluşturabilecek iş veya kamu düzeni kayıtları, ticari yayınlar ve tarafların ilgi alanlarını açıklayan deliller bu kural kapsamında yorumlanmaktadır.

5. En iyi delil niteliği

Dijital adli delillerde aranan son nitelik, delilin mümkün olan en iyi delil olmasıdır (Best Evidence Rule R.1001-1009).

Delilin orijinalliği, davanın taraflarına ait kimlik bilgilerine dair net veriler içermesi, soruşturmaya konu edilen olaya ilişkin en belirgin ve çözüme götürücü kanıtları sunması, "en iyi delil" nitelikleri arasında sayılmaktadır.

"En iyi delil" kavramı, bir delilin orijinalinin bulunduğu ve erişilebilir olduğu sürece soruşturmalarda bu delilin kullanılması gerektiğini belirtir. Örneğin, ıslak imzalı bir belgenin fotokopisi yerine aslının kullanılması esastır. Dijital deliller için de benzeri bir yaklaşım söz konusudur. Bunun için aranan temel nitelik, dijital adli delilin bulunduğu sabit diskin imajının kullanılmasıdır. Arama ve el koyma süreçlerinden sorunsuz geçmiş dijital adli delilin imajı üzerinden çalışmak, bu imajdan elde edilecek delillerin "en iyi delil" vasfını kazanmasını sağlar. Ayrıca imajı alınan diskteki verilerin de mümkünse kopya olmaması ve o bilgisayarın kullanıcısıyla birebir ilişkisi olması temel hedeflerdendir.

B- AB perspektifi

Avrupa ülkelerinde dijital delillerin değerlendirilmesine yönelik kapsamlı ve özel bir yasa bulunmasa da konuyla ilgili sivil, ticari ve diğer ceza hukuku yasalarında bir takım düzenlemeler yapılmış durumdadır[190]. Dijital delillere yönelik arama el koyma faaliyetlerine ilişkin bazı düzenlemeler ise birkaç Avrupa ülkesinde işletilmektedir. Birleşik Krallık'ta yürürlükte olan *Polis ve Suç Delili Kodu* (Police and Criminal Evidence Code) ve Belçika yasalarında bulunan *Bilgisayar Suçları Yasası (*Law on Computer Crimes) bu kapsamda örnek olarak verilebilir.

Avrupa ülkelerinde dijital delillerin kabul edilebilirliği ile ilgili doğrudan ilişkili düzenlemeler kısıtlı sayıda da olsa bulunmaktadır. Birleşik Krallık ve

[190] The Admissibility of Electronic Evidence In Court, http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf, erişim tarihi: 07.01.2013.

İrlanda yasalarında bulunan "dijital delillerin orijinal olması gerekliliği" bu bağlamda değerlendirilebilir. Bu ülkelerde dijital delilin orijinal olmasının yanı sıra delilin konuyla ilgili olması ve soruşturma kapsamında dışında kalan kaynaklardan elde edilmemiş olması gerekmektedir.

Dijital adli delillerin değerlendirilmesinde Avrupa yasalarında dikkate alınan temel kriterler; delilin *etkili olması* (effectiveness), *kullanışlılığı* (usefulness) ve *yasallığı* (legitimacy) olarak özetlenebilir. Bu şartlara haiz olan dijital adli deliller mahkemelerde "kabul edilebilir" delil olmak için ilk şartları yerine getirmiş olmaktadır. Takdir yetkisi hâkimlerde kalmak üzere dijital adli delillerde aranan bir takım diğer özellikler ise;

- Masumiyet varsayımı,
- Anayasal haklar,
- Mahkeme tebligatı,
- Sağduyu,
- Yasallık,
- Sadece suçla ilişkili olma,
- Çapraz değerlendirme,
- Güvenilirlik

Olarak sıralanabilir.

Dijital adli delillerin değerlendirilmesi bakımından ABD'ye göre geriden gelen Avrupa ülkeleri yasalarında derli toplu olmamakla birlikte bir takım düzenlemelerin olduğu görülmektedir.

AB ülkelerindeki mahkemelerde dijital adli delillerin kabul edilebilirliğini araştırarak hâkimlere yardımcı olmayı amaçlayan çeşitli projeler de yapılmıştır. Bunlardan en öne çıkanı AB Komisyonunun *"Delillerin Online Araştırılmasında Kullanılacak Siber Araçlar"* (CTOSE-Cyber Tools On-line Search for Evidence) projesidir. CTOSE bilişim suçları uyuşmazlıklarında veya davalarında, elektronik delillerin mevcut veya ileride açılacak bir davada kabule şayan deliller olarak

kabul edilebilmesini sağlayan doğrulama yöntemlerinin belirlenmesi amacıyla tasarlanan hukuki bir projedir[191].

Sonuç olarak dijital adli delillerin kabul edilebilirliğini tespit etmeye yönelik bazı çalışmalar yapılmasa da, konuyla ilgili mevzuata yansıyan bir standardın olmaması ve yetkinin çoğunlukla hâkimin takdirine bırakılması, Avrupa ülkelerindeki yasaların bu konuda çeşitli düzenlemelere ihtiyacı olduğunu göstermektedir.

C- Türkiye perspektifi

Türkiye, dijital adli delillerin elde edilmesinden mahkemelerde kabul edilmesine ve bu delillerin değerlendirilmesinin ardından verilen kararlarda kullanılabilmesine kadar geçen süreçte ciddi problemlerin yaşanabildiği bir ülkedir.

Ülkemizde ABD ve AB'den farklı olarak dijital adli delillerin etkisi ve bu delillerde aranacak temel özelliklerin tespiti bakımından bir takım eksiklikler bulunmaktadır. Hali hazırda yürürlükte olan düzenlemeler dijital delillerin daha ziyade nasıl elde edileceği ve saklanacağı yönünde direktifler içermektedir. Konuyla ilgili kanuni düzenlemeler ve yönetmelikler aşağıdaki gibi sıralanabilir.

1. Yürürlükte olan mevzuat

a) Ceza Muhakemeleri Kanunu

Dijital adli analiz çalışmalarının ilk safhası olan arama ve el koyma faaliyetlerine ilişkin düzenleme, Ceza Muhakemeleri Kanunu'nun (CMK) 134. maddesi olan "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" maddesidir [192] . İlgili düzenleme Resmi Gazete'de aşağıdaki şekilde yayınlanmıştır.

---

[191] Cyber Tools On-Line Search for Evidence, http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=5319458, erişim tarihi: 07.01.2013.

[192] Ceza Muhakemeleri Kanunu Madde 134, "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" Resmi Gazete , 17 Aralık 2004.

"MADDE 134 - (1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır."

b) Adlî ve Önleme Aramaları Yönetmeliği

Konuya ilişkin bir diğer düzenleme "Adlî ve Önleme Aramaları Yönetmeliği" madde 17'de yayımlanmıştır[193]. Yönetmelik, el koyma işlemini sadece bilgisayarlara münhasır kılmamış, aynı zamanda bilgisayar ağları, uzak bilgisayarlar ve çıkarılabilir donanımlar için de geçerli olduğunu belirtmiştir.

İlgili düzenleme Resmi Gazete'de aşağıdaki şekilde yayınlanmıştır.

"MADDE 17 - Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması hâlinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar

[193] Adlî ve Önleme Aramaları Yönetmeliği, Madde 17, "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" Resmi Gazete , 17 Aralık 2004.

kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması hâlinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır.

İstemesi hâlinde, bu yedekten elektronik ortamda bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir."

c) Suç Eşyası Yönetmeliği

Bir diğer düzenleme Suç Eşyası Yönetmeliğinin "Kıymetli eşya ve evrak ile bozulacak, değerini kaybedecek veya muhafazası zor olan suç eşyası hakkında yapılacak işlemler" hakkındaki 9. maddesinin 2. fıkrasıdır[194]. Bu madde el konulan bilgisayar malzemelerinin nasıl saklanması gerektiğini anlatmaktadır.

"MADDE 9, FIKRA 2 - Bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin asıl ya da kopyaları, ses ve görüntü kayıtlarının bulunduğu depolama aygıtları gibi eşya, bozulmalarını engelleyecek, nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak uygun ortamda muhafaza edilir."

[194] Suç Eşyası Yönetmeliği, Madde 9 Fıkra 2, "Kıymetli eşya ve evrak ile bozulacak, değerini kaybedecek veya muhafazası zor olan suç eşyası hakkında yapılacak işlemler" Resmi Gazete , 01 Haziran 2005.

2. Tasarılar

a) Mevzuatta yapılacak değişimler

Dijital adli analiz çalışmalarına girdi oluşturacak arama ve el koyma faaliyetlerine ilişkin CMK'nın 134. maddesinde bazı değişiklikler yapılacaktır[195].,

Mevcut 134. maddenin 2. fıkrasında el koymanın şartı, "şifrenin çözülememesi" olarak belirlenmiştir. Adli bilişim bilgisayar incelemelerinde işletim sistemi, kullanıcı adı ve şifreye gerek olmadığından dolayı bu ifade kaldırılacaktır. Ayrıca, el koyma şifrenin çözülememesinden dolayı değil, incelemenin uzun sürmesi durumunda gerekli olmaktadır.

Mevcut 134. maddenin 5. fıkrasında, "kopyası alınan veriler kağıda yazdırılarak.." ifadesi kaldırılacaktır. Bilgisayar çıktılarının hepsi kâğıda yazdırılamayacağı (video dosyası, müzik dosyası, çalıştırılabilir dosya, kütüphane dosyası, vb.) gibi yazdırılacak metinler çok fazla sayfa tutabilir. UYAP projesi göz ününde bulundurulduğunda artık her hâkim ve savcının kendisinde ve ofisinde bilgisayar sistemlerinin bulunması, incelemelerin mümkün mertebe bilgisayar ortamında yapılmasını sağlayacaktır. Bu ifade kaldırılması neticesinde, kâğıda yazdırılma durumu bir zorunluluk olmaktan çıkarılıp savcı veya hâkimin istemesi durumunda başvurulacak bir yöntem olarak belirlenmiştir.

b) Kanun tasarıları

Henüz hazırlık aşamasında olan ancak yürürlüğe girmesi halinde dijital adli analiz çalışmaları kapsamındaki arama el koyma faaliyetlerini etkileyecek yeni bir tasarı bulunmaktadır. "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı" bu alanda iyileşme sağlayacak düzenlemelerden biri olacaktır. Yürürlükte olan CMK 134. maddesini etkileyecek olan bu değişiklik, özellikle 2. fıkradaki "şifre çözülememesi" ifadesini kaldırarak el koyma tanımını daha mantıklı ve teknik açılardan geçerli bir zemine oturtacaktır.

---

[195] Leyla Keser Berber, Dijital Adli Analiz Ders Notları, İstanbul 2012 ("Berber Ders Notları"), sf. 16.

İlgili tasarının son hali aşağıdaki gibidir.

Bilgisayar, bilgisayar programları, bilgisayar ağları, uzak bilgisayarlar ile veri saklama ünitelerinde arama, kopyalama ve el koyma tasarısı:

(1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkanının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar, bilgisayar programları, bilgisayar ağları, uzak bilgisayarlar ile veri saklama ünitelerinde arama yapılmasına hakim tarafından karar verilir.

(2) Eğer arama işlemi uzun sürecekse veya detaylı arama yapılacaksa şüphelinin kullandığı bilgisayar, bilgisayar programları, bilgisayar ağları, uzak bilgisayarlar ile veri saklama ünitelerine el konabilir.

(3) Bilgisayar, bilgisayar programları, bilgisayar ağları, uzak bilgisayarlar ile veri saklama ünitelerine elkoyma işlemi sırasında, sistemdeki bütün verilerin kopyası alınır.

(4) Bilgisayar, bilgisayar programları, bilgisayar ağları, uzak bilgisayarlar ile veri saklama ünitelerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.

(5) İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

3. Yaşanan sorunlar

CMK'nın 134. maddesinin günümüz uygulamalarında bir takım sıkıntıların yaşandığı görülmektedir. Bunların başında kişisel verilerin mahremiyeti ile delil niteliğine ilişkin dengenin kurulamamış olması söylenebilir.

İlgili madde dijital delillerin toplanabilmesi için "başka surette delil elde etme imkânının bulunmaması halinde" şartını koymuştur. Kişisel verilerin gizliliği için pozitif bir tutum sergileyen bu yaklaşım, uygulama sahasında geçerli olmamakta, çoğu zaman dijital adli delillerin tamamına el konulmaktadır. Bütün dijital delillere el konulması sanık aleyhinde çeşitli durumlara neden olmakta, söz gelimi bilgisayarında porno içerikli bir materyal bulunan şahıs aynı zamanda

"yayıncılık" suçuyla da karşı karşıya kalabilmektedir. Benzer şekilde bilgisayarında başka bir suç unsuru bulunduğu tespit edilen sanık hakkında soruşturmayla ilgisi olmamasına rağmen bu delillerle ilgili başka bir iddianame hazırlanabilmektedir.

Konunun bir diğer boyutu dijital adli delillere ancak başka bir delil bulunmaması halinde başvurulmasının salık verilmesidir. Bu durum, günümüz dünyasında geçerliliğini hızla yitirecek bir olgu olarak karşımızdadır. Dijital delillerde el koyma işlemlerinin ayrım gözetmeksizin top yekûn yapılması kadar, dijital delillere sadece "başka bir surette delil etme imkânı olmadığında" başvurulması da sakıncalıdır. İlk durum kişisel verilerin gizliliğini tehdit ederken, ikinci durumda önemli delillerin göz ardı edilmesi ihtimali bulunmaktadır. Çalışmalarda "tutarlılık" ilkesinin ön planda tutulması ve el koyma işlemlerinde "gereklilik" ve "kapsam" durumlarının göz önünde bulundurulması çözüm olabilir.

Yürürlükte olan CMK 134, el koymanın şartı olarak "bilgisayarlarda şifrenin çözülememesi" gibi teknik açıdan geçersiz bir yaklaşımı öne sürmektedir. Dolayısıyla şu anki el koyma çalışmalarından bu durum dikkate alınmamaktadır. Yapılan iş doğru olsa da, kanunen sakıncalı bir durum ortaya çıkmaktadır. Bir önceki bölümde[196] belirtilen tasarıların yürürlüğe girmesiyle bu problemin ortadan kalkacağı düşünülmektedir.

Dijital adli delillerin değerlendirilmesi hususunda başka bir durum ise bu gibi delillerin dijital adli analiz bilimine uygun olarak değerlendirilmesi ve hâkimlerin hizmetine sunulması sürecinde yaşanan problemlerdir. Delillerin geçerliliği ve kabul gören tetkiklerle analizi, bu delillerin karar vericilerin yorumuna uygun hale getirilmesi ve hâkimlerin delillerle ilgili hazırlanan bilirkişi raporlarını inceleyebilecek teknik yeterliliğe haiz olması konuları çözüm bekleyen konular arasında sayılabilir. Bu durumlarla ilgili çözüm önerilerine sonuç kısmında tekrar değinilecektir.

[196] Detaylı bilgi için bkz. "Kanun tasarıları", sf. 147.

II. Şüpheden sanığın yararlanması ilkesi

A- Geçerli durum

Şüpheden sanık yararlanır (in dubio pro reo) ilkesi, ceza yargılaması hukukunda geçerli olan ve mevzuatımızda yazılı olarak hükme bağlanmamış bulunan bir ispat kuralıdır. Günümüzde bütün hukuk devlerinde tartışmasız kabul edilmiş bu ilke, masumiyet karinesi ile de doğrudan ilişkilidir[197].

İlkeye göre, suç işlediği iddiasıyla yargılanan kimse hakkında mahkûmiyet kararının verilebilmesi için, bu durumun şüpheye yer bırakmayacak şekilde ispatlanmış olması gerekmektedir.

Bu kuralın başka bir dayanağı da Anayasanın 38. maddesinin 4. fıkrası[198] ve Avrupa İnsan Hakları Sözleşmesinin 6. maddesinin 2. fıkrasında[199] belirtilen "suçsuzluk karinesidir". Buna göre suçsuz olduğu varsayılan kişinin suçlu kabul edilmesi için kesin hükümle mahkûm olması ve mahkûmiyetin de fiilen ispatlanması gerekmektedir. Sonuç olarak şahsın suçlu kabul edilebilmesi bütün deliller değerlendirilmeli ve suçsuzluk ihtimalinin ortadan kaybolduğu müşahede edilmelidir.

B- Dijital delillerin niteliği

Bilişim dünyası insanların yaşam alışkanlıklarını değiştirdiği gibi, hukuk sisteminde de birçok değişikliğe neden olabilecek yapıya sahiptir. Adli bilişimi etkileyen tarafı ise dijital adli delillerin manipülasyona açık yapısı ve kişinin kimliği hakkında şüphe barındırabilen niteliğidir[200].

---

[197] "Şüpheden sanık yararlanır" ilkesi hakkında yorumlar için bkz. http://www.turkhukuksitesi.com/showthread.php?t=12004, erişim tarihi: 07.01.2013.

[198] Anayasanın ilgili maddesi için bkz. http://www.tbmm.gov.tr/anayasa/anayasa_2011.pdf.

[199] Avrupa İnsan Hakları Sözleşmesinin ilgili maddesi için bkz. http://www.echr.coe.int/NR/rdonlyres/3BAA147F-29C9-48CE-AF64FB85A86B2433/0/Convention_TUR.pdf, erişim tarihi: 07.01.2013.

[200] Delilin kullanıcı ilişkisi hakkında detaylı bilgi için bkz. "Delilin kullanıcı ilişkisi", sf. 112.

Dijital adli deliller; kimyasal, biyolojik ve fiziksel delillerden bazı noktalarda ayrılabilmektedir[201]. Özellikle tek dayanağın dijital deliller olduğu soruşturmalarda, delilin kullanıcı ilişkisini ispatlamak imkânsız olabilmektedir. Daha basit bir tanımla, dijital adli delillerin bir sanığı işaret etmesi hiçbir zaman "kesin bir dille" ifadeyle edilemeyecektir. O zaman şöyle soruların gündeme gelmesi kaçınılmazdır: Dijital delillerin manipülasyona açık doğası bu tür delillerin hiçbir zaman kullanılmayacağını mı göstermektedir? Bu delillerin kanıt olarak kullanıldığı soruşturmalarda az ya da çok bir şekilde şüphenin barınıyor olması "şüpheden sanık yararlanır" ilkesiyle birlikte nasıl değerlendirilecektir?

Bütün bu sorular, günümüz hukuk sisteminin dijital delillerle ilgili yaşadığı problemlerin başında gelmektedir. Kesin bir çözüm olmamakla birlikte delillerin sınıflandırılması, şüphe seviyelerinin belirlenmesi ve dijital olmayan delillerle karşılaştırılması neticesinde hâkimlerin karar vermesinin kolaylaşacağı düşünülmektedir. Truva atı savunmalarının yapıldığı davalarda "şüpheden sanık yararlanır" ilkesinin nasıl değerlendirebileceği hakkında öneriler bir sonraki bölümde, "dijital adli delillerin güvenilirliği" hakkında genel çözüm önerileri ise çalışmanın son kısmında yer almaktadır.

III. Delillerin inkârı ve Truva atı savunmaları

A- Tanım

Son yıllarda gerek ülkemizde gerekse Avrupa ülkeleri ve ABD'de dijital delillerin kilit rol oynadığı birçok dava görüşülmektedir. Soruşturmaların ve iddianamesi hazırlanan davaların büyük çoğunluğunda bu dijital adli deliller kolayca tespit edilen, bilgisayar kullanıcıları tarafından inkâr edilmeyen ve kısa süreli çalışmalar neticesinde ortaya çıkarılabilen deliller olmuştur.

Dijital adli delillere başvurulan diğer bazı davalarda ise bu delillerin geçerliliği ciddi şekilde sorgulanmıştır. Delil ile delilin elde edildiği bilgisayarın

[201] Delil çeşitleri hakkında bkz. http://besiktas.iem.gov.tr/web_18467_1/entitialfocus.aspx?primary_id=1921&type=1075&target=productialdbl&detail=double&sp_table=&sp_primary=&sp_table_extra=&openfrom=sortial, erişim tarihi: 07.01.2013.

kullanıcısı arasındaki ilişkinin doğrulanamayacağı iddiası özellikle sanıklar tarafından sıkça kullanılmaya başlamıştır.

Bir bilgisayar kullanıcısının; bilgisayarında tespit edilen ve suç unsuru içeren durumlardan haberi olmadığı, suç unsuru içeren dosyanın oluşturulması ve üzerinde işlem yapılması veya başka bir yere aktarılması gibi herhangi bir faaliyetin kendi bilgisi dışında gerçekleştiği ve bütün bunlara sebep olan faktörün bilgisayarına uzaktan bağlanan bilgisayar korsanları (hacker) olduğu iddiasına *Truva atı savunması* (Trojan horse defense) denilmektedir[202].

Günümüzde Truva atı savunmalarına sıkça başvurulmasının bir diğer sebebi ise bilgisayar korsanlığı faaliyetlerinin her geçen gün artması ve "Truva atı" denilen zararlı yazılımlarla giderek daha sık karşılaşılıyor olmasıdır[203].

İlk bölümlerde tartışıldığı üzere zararlı yazılımların bilgisayarlar üzerinde ciddi etkileri olabilmektedir. Bunlar arasında bir bilgisayara tamamen uzaktan erişilmesi ve kontrol edilmesi bulunmaktadır. Bütün bu işlemlerin bilgisayar kullanıcısından habersiz gerçekleşebiliyor olması problemin ilk kaynağını oluşturmaktadır. Madalyonun öteki yüzünde ise, gerçekten suçlu insanların Truva atı savunmalarıyla ceza almaktan kurtulma çabası görülmektedir. Her iki durumda da hâkimlerin karşısına ciddi bir problem çıkmaktadır: Sanık bilgisayarındaki bütün faaliyetlerden habersiz ve gerçekten masum mu? Yoksa Truva atı savunması ile işlediği bütün suçlardan kurtulmaya çalışan bir düzenbaz mı? Sorunun cevabı basit olmamakla birlikte dijital adli analiz uzmanlarına ve hâkimlere yardımcı olacak çok sayıda unsur bulunmaktadır. "Savunmanın Truva atı savunması" ve "savcılığın cevabı" başlıklarında bu konular irdelenmektedir.

B- Savunmanın Truva atı savunması

Truva atı savunmalarında sanıkların öne sürdüğü iddiaların genelde üç temel dayanak noktası bulunmaktadır; kabul edilebilir şüphe uyandırılması, taammüden yapılan işlemlerin manipülasyonu ve "benim haberim yok başkası

---

[202] Truva atı savunması, http://en.wikipedia.org/wiki/Trojan_Horse_Defense, erişim tarihi: 07.01.2013.

[203] Bir zararlı yazılım çeşidi olan Truva atlarıyla ilgili detaylı bilgi için bkz. "Truva atları" sf. 74.

yaptı"[204] iddiasıdır. Her üç durumda da kişinin bilgisayarında iradesi dışında bir takım işlemler yapıldığı ve bu nedenle ilgili delillerden dolayı suçlanamayacağı iddiası gündeme getirilmektedir[205]. Bu üç dayanağın nasıl kullanıldığı ile ilgili detaylar aşağıda incelenmiştir.

1. Kabul edilebilir şüphe uyandırmak

Kabul edilebilir şüphe uyandırma (raise reasonable doubt) yaklaşımında, sanık olayla ilgili tamamen başka bir senaryo uydurur. Sanığın bilgisayarında bulunan ve soruşturmayla ilgili olabilecek diğer delilerle desteklenebilen bu tür savunmaların temel amacı, hâkimlerin "tam ve kesin olarak doğru" bir karara varmalarını engellemek ve akıllarında şüphe uyandırmaktır. Senaryoya göre suç unsuru bulunan delillerin bilgisayara nasıl gelmiş olabileceği ile ilgili farklı ihtimaller açıklanır. Diğer bazı deliller ve genel-geçer durumlarla desteklenir. "Bilgisayarda bulunan bir dosyanın üstverileri manipüle edilebileceğinden bu verilere güvenilemez", "Bilgisayarda bulunan herhangi bir virüs bunu yapmış olabilir" vb. söylemlerle şüphe duygusu uyandırılmaya çalışılır. Özellikle "şüpheden sanık yararlanır" ilkesine göre[206] sanığın suçlu olmadığına dair ufak bir şüphenin bile var olması sanık aleyhine karar vermeyi zorlaştıracakken, sanığın bu tarz bir savunma yapması hâkimleri zor duruma düşürmektedir.

2. Taammüden yapılan işlemlerde manipülasyon iddiası

Bir diğer savunma tarzı, *taammüden yapılan işlemlerde manipülasyon iddiası* (mens rea) olarak karşımıza çıkmaktadır. Bu tarz savunmalarda sanık olayla ilgisi olduğunu kabul eder, ancak yaptığı işlemlerin neticesinde kendi

---

[204] "Benim haberim yok başkası yaptı" savunması ingilizcede SODDI (some other dude did it) olarak isimlendirilen savunma tekniğidir. Oldukça eskiye dayanan bu tarz savunmalar Truva atı savunmalarının da dayanak noktasıdır.

[205] *Brenner/Carrier/Henninger,* sf. 18.

[206] "Şüpheden sanık yararlanır" ilkesi, Anayasanın 38/4, İHAS 6/2 madde ve fıkrasında dolaylı olarak "suçluluğu hükmen sabit oluncaya kadar, kimse suçlu sayılamaz" düzenlemesiyle anlatılmıştır.
Bu ilkenin değerlendirildiği örnek bir karar için bkz. http://www.anayasa.gov.tr/index.php?l=manage_karar&ref=show&action=karar&id=2416&content=, erişim tarihi: 07.01.2013.

niyetiyle oluşmayan ve hatta oluşması mümkün dahi olmayan sonuçlara varıldığını iddia eder.

Örnek vermek gerekirse, vergi iadesi formu dolduran bir muhasebeci bu işlemi kendi bilgisayarında yaptığını kabul eder. Ancak formda girilen değerlerin, söz gelimi iadesi istenen meblağın, kendi bilgisi dışında manipüle edildiğini savunur. Özetle "kısmı bir zararlı yazılım etkisi" bulunduğunu iddia eder. Bu tarz savunmaların da varmak istediği nokta "kendi iradesi dışında işlem yapıldığı" durumudur. Sanık kendisiyle ilişkili olan ve/veya ilişkili olma ihtimali bulunan durumları peşinen kabul eder, yalnızca suç teşkil eden faaliyetlerin sorumluluğundan kurtulmaya çalışır. Günümüzde bu tarz savunmalarla da karşılaşılabilmektedir.

3. SODDI savunması

Ben yapmadım başkası yaptı (some other dude did it-SODDI) savunması bütün Truva atı savunmalarının temel dayanağıdır. Sanık, kendi bilgisayarına dışarıdan bağlanıldığını ve suç unsuru teşkil eden durumların bu şekilde oluştuğunu savunur.

SODDI savunması Truva atı savunmalarından önce de bulunmaktaydı[207]. Bununla beraber Truva atı zararlı yazılımları ile "ben yapmadım başkası yaptı" iddiası birbiriyle tam olarak örtüştüğü için bu tarz savunmalarla günümüzde daha sık karşılaşılmaktadır.

Truva atı savunmalarına bir bütün olarak bakılırsa sanıkların 3 farklı olguyu öne sürdükleri görülmektedir;

- Bilgisayarlarında Truva atı veya benzeri zararlı yazılım bulunduklarını iddia ederler.
- Bu zararlı yazılımı kendilerinin yüklemediğini, bir başkası tarafından yapıldığını savunurlar.

[207] ABD üst düzey bürokratlarından Lewis Libby'nin aleyhine açılan bir davada SODDI savunması yapmasına dair bkz. http://www.salon.com/2005/11/19/libby_12, erişim tarihi: 07.01.2013.

- Bütün bu olaydan haberleri olmadığını, tamamen kendi bilgileri dışında cereyan ettiğini belirtirler.

Bilişim suçlarıyla ilgili bu 3 durumu sağlayan birçok davada Truva atı savunmasına başvurulabilmektedir. Bu savunmaları destekleyen bir diğer durum ise, işlenen suçun niteliğine göre sanığın bu yetkinlikte olmadığını iddia etmesidir[208].

Sonuç olarak Truva atı savunmalarına ilişkin teknik ve taktikler yukarıda sıralandığı gibi gerçekleşmektedir. Gerçekten suçlu olan kişilerin bu yaklaşımla aleyhlerinde karar çıkmasını engelleyebilecekleri düşünüldüğünde, iddia makamının konuya yaklaşımı daha bir önem kazanmaktadır. Benzer şekilde suçsuz insanların Truva atı savunmalarıyla temize çıkma gayretleri atıl kalmamalı ve bunun için oldukça dengeli bir yaklaşım sergilenmelidir. Gerçeğin ortaya çıkması için savcılığın olaya azami dikkat ve titizlikle yaklaşması gerekecektir.

İddia makamının Truva atı savunmalarına cevabı hakkında bir sonraki bölüm incelenebilir.

C- Savcılığın Truva atı savunmasına cevabı

Truva atı savunmasıyla karşılaşan iddia makamı, durumun adli bilişim teknikleriyle daha detaylı analizini isteyebilir. Karmaşık görünse de suçlu ile suçsuzun ayrıştırılmasını sağlayacak önemli bulgular elde edilebilir. Sorgulanabilecek ana başlıklar aşağıda sıralanmış durumdadır.

1. Zararlı yazılımın karakteri ve yeteneği

Zararlı yazılımların her geçen gün yeni bilgisayarlara bulaştığı ve uzaktan kontrol edilebildiği gerçeği yadsınamaz[209]. Kötü niyetli kişilerce başka insanları zan altında bırakacak ve bu kişilerin kimliklerini gizleyerek yasa dışı faaliyetlerde

[208] Konuyla ilgili yaşanan ilk örneklerden biri Aaron Caffrey isimli şahsın kendi bilgisayarından 11608 farklı IP'ye *dağıtık servis dışı bırakma saldırısı* (DDOS) yaptığına ilişkin görülen davadır. 2003 yılında karara bağlanan görüşmede sanık "böyle bir yetkinliğe sahip olmadığını" savunmuş, bilgisayarında zararlı yazılım bulunmamasına ve çok sayıda DDOS uygulaması bulunmasına rağmen hakkındaki iddialar kabul edilmemiş ve serbest kalmıştır. Detaylı bilgi için bkz. http://www.zdnet.com/the-case-of-the-trojan-wookiee-3039117240, erişim tarihi: 07.01.2013.

[209] Konuyla ilgili detaylı bilgi için bkz. "Dağılım oranları" sf. 77.

bulunmasını neden olacak zararlı yazılımlar, elbette sanığın kendi işlediği suçlardan kurtulması için de kullanılabilecektir.

Böyle bir durumla karşılaşıldığında iddia makamının inceleyebileceği ilk durum, konu edilen bilgisayarda gerçekten zararlı yazılım bulunup bulunmadığıdır. Eğer böyle bir zararlı yazılım tespit edildiyse sonraki aşamaya geçilerek ve zararlı yazılımın yetkinliği araştırılabilir.

- Zararlı yazılım bilgisayara hangi tarihte bulaşmıştır? Zararlı yazılım aktif midir? Eğer aktif değilse faaliyetine ne zamana kadar devam etmiştir?
- Zararlı yazılımın türü nedir? Bu tip zararlı yazılımların genel amaçları nedir? İncelenmekte olan soruşturmayla ilgili bir konuda etkisi olabilir mi?
- Zararlı yazılım bilgisayara nasıl bulaşmıştır? Bu zararlı yazılım özel hedefli bir saldırı sonucunda bulaşan bir Truva atı mıdır, yoksa internette rastgele dağılan bir virüs çeşidi midir?
- İlgili zararlı yazılımın etkisi nedir? Soruşturmaya konu edilen duruma net bir etkisi var mıdır? Adli bilişim araştırmaları neticesinde detaylı zaman analizi yapıldığında, zararlı yazılımın bulaştığı ve/veya çalıştığı tarihlerle suç unsuru teşkil eden dosya ve/veya faaliyetlerin mantıksal bir yakınlığı söz konusu mudur[210]?

Soru listesi uzatılabilir. Bu açıklamalarla varılmak istenen nokta, eğer gerçekten bir zararlı yazılım varsa bu zararlı yazılımın suç teşkil eden unsurlarla ilişkisi olup olmadığının ortaya çıkarılmasıdır. Ortada bir zararlı olmasına rağmen olayla ilişkisi kanıtlanamıyorsa, sanık aleyhine bir durum oluşacaktır.

Zararlı yazılım tespit edilemediği durumlarda ise, bilgisayarda bir delil karartma işleminin uygulanıp uygulanmadığı incelenebilir[211]. Böylece sanığın "Bilgisayarımda bulunan zararlı yazılım yasa dışı faaliyetlerden sonra kendini ve olabilecek bütün kanıtları sildi" iddiasına cevap verilebilecektir. Bilgisayarda

[210] Zaram analizi hakkında detaylı bilgi için bkz. "Log2timeline", sf. 24.

[211] Delil karartma teknikleri hakkında detaylı bilgi için bkz. "

", sf. 82.

delillerin geri döndürülmez şekilde silinmesine neden olan bir uygulama varsa, deliller silinse bile bu programın kendisi kalacaktır. Hatta sonraki aşamada programı kaldırılsa bile, bu sefer programı kaldıran uygulama veya işleme dair izler kalabilecektir. Detaylı adli bilişim incelemeleri sonucunda bu duruma ilişkin kanıtlar tespit edilebilir. Böylece "virüs kendini temizledi" iddiasına cevap aranabilecektir.

2. Kullanıcının bilgisayar bilgisi

İncelenebilecek bir diğer başlık ise kullanıcının bilgisayarlar hakkındaki bilgi seviyesidir. Bazı Truva atı savunmalarında sanıkların bilişim dünyasına uzak olduklarına dair savunmaları olabilmektedir. Kullanıcının bilgisayar bilgi seviyesinin ve olası zararlı yazılım faaliyetlerine karşı yaklaşımı tespit edilebilirse bu durum iddia makamının elini güçlendirebilir.

Bilgisayar bilgisi 2 şekilde etkisini gösterecektir. Bunlardan ilki kullanıcının zararlı yazılımlara karşı tedbir alıp almadığı noktasıdır. Kullanıcı anti virüs programı yüklemiş midir? Güvenlik duvarı ayarlarını yönetebilecek kapasiteye sahip midir? Akademik kariyerinde, iş yaşamında ve özel hayatında hangi bilgisayar yetkinliklerini kullanmaktadır? Zararlı yazılım saldırılarını tespit edebilecek kapasiteye sahip midir? Kullandığı anti virüs yazılımlarını düzenli olarak güncelleştirmekte midir? Bu ve benzeri sorularla kişinin kimliği ve kullanıcı profili çıkarılabilir.

Bilgisayar bilgisinin ikinci etkisi ise, kullanıcının bir savunma amacı olarak kasıtlı şekilde zararlı yazılımın çalışmasına izin verip vermediğidir. Kullanıcı zararlı yazılımı kendisi oluşturmuş olabilir mi? Kendisine ait başka bir bilgisayarda zararlı yazılım oluşturup suç faaliyetini yürüttüğü bilgisayara aktarmış olabilir mi? Kullanıcı bilerek ve isteyerek zararlı yazılım bulaşabilecek siteleri ziyaret etmiş olabilir mi? Aynı şekilde kendi bilgisi dâhilinde eski ve yamasız işletim sistemleri kullanarak bilgisayarını uzaktan erişime açmış olabilir mi? Bu tip sorularla kullanıcının bilgisayar bilgisi tahmin edilebilir ve yeni sorgulama başlıkları oluşturulabilir.

3. Zararlı yazılımla kullanıcının ilişkisi

Zararlı yazılımla kullanıcının ilişkisinin tespiti Truva atı savunması yapılan davalarda önemli bir gelişme olarak kabul edilir. Truva atı savunmalarının temelinde "ben yapmadım başkası yaptı" iddiası bulunmaktadır. Kanıt olarak zararlı yazılımla bilgisayarın ele geçirilmesinden bahsedilir. Zararlı yazılımın kullanıcıyla ilişkisinin tespiti halinde bütün bu iddialar çökebilir. Zararlı yazılımın kaynak kodları veya zararlı yazılıma dair *betikler* (script) bilgisayarda bulunmakta mıdır? Bu kaynak kodlarının içinde kullanıcının kimliğine dair izler var mıdır? Zararlı yazılımın dinamik analizi [212] yapıldığında hangi IPlerle iletişim kurulmaktadır? Bu IPlerin kullanıcı ile bir ilgisi var mıdır? Zararlı yazılım geliştirmede kullanılan araçlar bilgisayarda bulunmakta mıdır? Eğer varsa, zararlı yazılımın bu araçlarla ilişkisi tespit edilebilmekte midir? Bu ve benzeri sorularla zararlı yazılımın kullanıcı ile ilişkisi sorgulanarak Truva atı savunmasına cevap niteliğinde bulgular elde edilebilir.

4. Kullanıcının itirafı

Truva atı savunmalarında kullanılabilecek bir diğer yaklaşım ise sanığın itiraf etmesini sağlamak olabilir. Dijital adli analizin uzun sürmesi ve zahmetli bir iş olması, bazen sanığın uzun süre tutuklu kalmasına neden olabilmektedir. Bu durum kullanıcının daha sürecin başında böyle bir itirafta bulunmasını zorlaştırabilir. Ancak bununla beraber bilgisayar suçlarının birçoğunun çocuk pornosu ile ilgili olduğu bilinmektedir[213]. Çocuk pornosu suçu işleme profilinde ise ağırlıkla daha önce suça bulaşmamış ve eğitimli insanlar olduğu görülmektedir[214]. Bu durumdaki sanıkların dava ilerlemeden sorgulanması ve eldeki verilerle hüküm giyme ihtimalinin yüksek olduğunun belirtilmesi durumunda, iddia edilen suçu gerçekten işlemişlerse Truva atı savunması gibi

[212]Dinamik analiz, zararlı yazılımın bulaştığı ortamın birebir aynısının oluşturulması ve simüle edilen bu ortamda zararlı yazılım çalıştırılarak etkisinin anlık olarak incelenmesi anlamında gelmektedir. Detaylı bilgi için bkz. Manuel Egele, Thedoor Scholte, Engin Kırda, Christopher Kruegel, A Survey on Automated Dynamic Malware Analysis Techniques and Tools, ABD 2010 ("Egele/Scholte/Kırda/Kruegel").

[213] *Brenner/Carrier/Henninger*, sf. 27.

[214] Tony Krone, A Typology of Online Child Pornography Offending, Avustralya 2004 ("Krone").

yola gitmeyecekleri tahmin edilebilir. Truva atı savunmaları oldukça kompleks bir duruma sebebiyet verdiği için detaylı teknik analize başvurmadan konunun çözülebilmesi özellikle iddia makamı ve karar vericiler açısından faydalı olacaktır.

D- Örnek davalar

1. Aaron Caffrey davası

Truva atı savunmalarına ilişkin çarpıcı örneklerden biri 2003 yılında Southwark Crown mahkemesinde görülen ve Aaron Caffrey isimli şahsın sanık sandalyesinde oturduğu davada yaşanmıştır[215]. Görüşülen duruşmada Caffrey'nin bilgisayarının çok sayıda kritik sunucuya dağıtık servis dışı bırakma saldırısı (DDOS) yaptığı hem iddia hem savunma makamı tarafından belirtilmiş ve kabul edilmiştir. Aaron Caffrey'nin geçmişte çeşitli bilgisayar suçları işlemiş olması, bilgisayarında zararlı yazılım bulunmaması ve hatta saldırı yapılan 11608 IP'nin bilgisayarında tespit edilmiş olması bile Caffrey'nin suçlu bulunması için yeterli olmamıştır.

İlgili olayda Caffrey, "Bilgisayarına zararlı yazılım bulaştığı, DDOS saldırısının kendi bilgisi dışında gerçekleştiği, saldırı yapan kişinin kendi bilgisayarındaki zararlı yazılımı saldırı sonrası temizlediği ve bu nedenle iz bırakmadığı" iddiasını jüriye kabul ettirebilmiş ve ceza almamıştır.

İlgili olayda gerçeğin ne olduğunu bilmek şu anda mümkün olmadığı gibi, mahkemenin verdiği karara yorum yapmak da elbette doğru olmayacaktır. Ancak bu dava, Truva atı savunmalarının önünü açması ve bu savunmaların bilişim suçlarıyla ilişkili davalarda her geçen gün daha sık başvurulan bir yöntem haline gelmesi açısından oldukça önemlidir.

---

[215] Haberi incelemek bkz. The case of the Trojan Wookiee, http://www.zdnet.com/the-case-of-the-trojan-wookiee-3039117240, erişim tarihi: 07.01.2013.

2. Julian Green davası

İngiltere Torquay'da yaşayan Julian Green, 2002 yılı Kasım ayında evinde yapılan arama esnasında bilgisayarında tespit edilen 172 çocuk istismarı fotoğrafı nedeniyle gözaltına alınmıştır[216]. Yaklaşık 12 ay süren dava süresince tutuklu kalan Green, bilgisayarında yapılan detaylı adli analiz incelemesi neticesinde 11 Truva atı yazılımının bulunması nedeniyle serbest bırakılmıştır ve özgürlüğe kavuşmuştur.

Green'in bilgisayarında dijital adli analiz uzmanlarının tespit ettiği Truva atı uygulamaları, bilgisayara uzaktan bağlantı yapabilmekte ve şahıstan habersiz olarak işlem gerçekleştirebilmekteydi. Sanığın ilgili fotoğraflarla ilgisinin olmadığını ispat etmesi ve bilgisayarında bu yetkinliğe sahip Truva atı yazılımları bulunması neticesinde dava beraat ile sonuçlanmıştır.

3. Samuel Crabtree davası

2012 yılından karara bağlanan ve yine zararlı yazılım etkisinin tartışıldığı bir diğer davada, ABD Kentucky Eyaletinden Samuel Crabtree, "bilgisayarında çocuk istismarına ilişkin materyal bulunması nedeniyle" 5 yıl cezaya çarptırılmıştır[217].

2009 yılından Crabtree bir problem nedeniyle bilgisayarını servise bırakmıştı. Teknisyen, bilgisayarı tamir ederken sabit diskte bir takım çocuk pornosu fotoğrafları bulmuş ve durumu kolluk kuvvetlerine bildirmişti. Olayın ardından tutuklanan Crabtree, duruşmadaki savunmasında ilk olarak "bilgisayarında dosyalarla ilişkisi olmadığını" iddia etse de, devam eden süreçte detaylı dijital adli analiz raporları gelmiş ve bazı fotoğrafların özel olarak kaydedildiği ortaya çıkmıştı. Bununla birlikte bazı dosyaların zararlı yazılımla geldiğine dair izler de bulunuyordu. İlgili fotoğrafların Crabtree tarafından kasıtlı olarak mı kaydedildiği yoksa zararlı yazılımların mı bu işlemleri yaptığı ilk

---

[216] Detaylı bilgi için bkz. Porn charges dropped with Trojan horse defence, http://www.out-law.com/page-3783, erişim tarihi: 07.01.2013.

[217] Detaylı bilgi için bkz. The Thumbcache, Malware and Child Pornography, http://cyb3rcrim3.blogspot.com/2012/08/the-thumbcache-malware-and-child.html, erişim tarihi: 07.01.2013.

planda tam olarak tespit edilememişti. Devam edegelen süreçte bilgisayardaki zararlı yazılımlarının etkisinin oldukça düşük olduğu ve dosyaların kasıtlı olarak bilgisayarda bulundurulduğuna dair delillerin çoğalmasıyla Crabtree çaresiz kalmış ve durumu itiraf etmişti. "Limewire uygulaması ile internetten dosya transferi yaparken ilgili içerikte materyalle karşılaştığını, merakından ötürü indirdiğini ancak kasıtlı olarak saklayıp bu fotoğraflara bakmadığını" iddia etse de Crabtree ceza almaktan kurtulamamış ve dava şahsın suçlu bulunmasıyla neticelenmişti.

E- Tartışmaya açık kararlar

Truva atı savunmaları yapılan davalarda verilecek karar ne olursa olsun, hâkimlerin, savcıların, sanıkların, mağdurların ve hatta bazı davalarda bütün kamuoyunun aklında bir şüphe belirebilir. Verilen karar gerçekten doğru ve hakkaniyetli bir karar mıdır, yoksa sanık kanunların bu alandaki belirsizliklerinden faydalanıp kurtulmakta mıdır?

Önceki bölümlerde izah edilen yaklaşımlar sonuna kadar araştırıldığında, şüphe ve belirsizliklerin yarı yarıya kalması oldukça küçük bir ihtimaldir. Bununla birlikte can alıcı bir sorunun gündeme gelmesi kaçınılmazdır: "Suçlu birini suçsuz olma ihtimaline dayanarak salıvermek mi, suçsuz birine suçlu olma ihtimaline dayanarak ceza vermek mi daha kötüdür?"

İşte bu soruya cevap vermek zorunda kalmamak için dijital adli analiz tekniklerinin düzgün şekilde uygulanması ve Truva atı savunmalarına karşı doğru bir metodolojinin izlenmesi gerekmektedir. Kapsamlı çözüm önerileri çalışmanın sonuç bölümünde detaylı olarak yer almaktadır.

§7. Sonuç

Dijital adli deliller; karmaşık, çok etmenli ve çoğu zaman kimlik doğrulama imkanlarından mahrum doğası nedeniyle şüpheyle yaklaşılan ve güvenilirliği tartışılan deliller olarak değerlendirilmektedir.

Çalışma kapsamında dijital adli delillerin tanımı yapılarak bu tür delillere ilişkin analiz çalışmalarında takip edilen uluslararası metodolojilerin üzerinde durulmuştur. Dijital adli delillerin analizinde izlenen yol ve yöntemlerin, bu gibi delillerin güvenilirliğine olan etkisini inceleyebilmek için zararlı yazılımlar ve delil karartma başlıkları altında teknik ayrıntılara girilmiştir. Değinilen başlıklarda, özellikle zararlı yazılımların etkisi ile oluştuğu iddia edilebilecek dijital adli delillerin nitelikleri ortaya konmuştur.

Dijital adli delillerin güvenilirliğinin ölçülmesi ve güven seviyelerinin tespit edilebilmesi için iki yöntem üzerinde durulmuştur. Bu yöntemlerden ilki olan karmaşıklık tabanlı niceliksel değerlendirme modeline göre, her bir dijital delilin oluşumunda yaşanması gereken bütün süreçler göz önünde bulundurulmakta ve bu süreçlerin her biri için bilgisayarda oluşması beklenen izlere sayısal değer atanmaktadır. Sonrasında bu sayısal değerler ile bilgisayarda tespit edilen izler kıyaslanmakta ve elde edilen bulgulardan hareketle ilgili dijital adli delillerin kişinin kendi iradesiyle mi yoksa zararlı yazılımlar aracılığıyla mı oluştuğu tespit edilmeye çalışılmaktadır. Karmaşıklık tabanlı niceliksel değerlendirme modelinin çıktıları, yüzdesel bir ihtimalle sonucu belirlemekte ve dijital adli delilin kaynağını rakamsal olarak tespit etmeye çalışmaktadır.

Bir diğer model olan güven seviyesi sınıflandırma modelinde, her bir önermenin doğruluğunun tespiti için öntanımlı bir değerlendirme havuzu referans alınarak bulgunun güvenilirliğine göre sınıflandırma yapılmaktadır. Zararlı yazılım etkisinde oluşturulduğu iddia edilen bir dijital delil için; delilin varlığı, kullanıcıyla ilişkisi, oluşturulma tarihi gibi durumları açıklayan her bir önerme hakkında güvenilirlik kategorilerine göre sınıflandırma yapılmaktadır. Güven seviyelerine ilişkin havuzlarda birleştirilen bu tespitler, son adımda ağırlıklarına göre toplanarak oluşturulan nihai derecelendirmeyle raporlanabilmektedir.

Gerek karmaşıklık tabanlı niceliksel değerlendirme gerekse güven seviyesi sınıflandırma modelinde, dijital adli delillerin oluşum sürecinde etkisi olabilecek bütün işlemler net bir şekilde tespit edilmeye çalışılır. Sonrasında her bir bulgu, matematiksel modellemelerle veya sınıflandırma havuzlarıyla değerlendirilerek dijital adli delilin oluşumuna neden olan bütün etkenler hesaplanmış olur. Karmaşıklık tabanlı niceliksel değerlendirme modeli, dijital adli delilin oluşma sürecindeki işlemlerin kullanıcı veya zararlı yazılım etkisi altında oluşma oranlarını birbirine kıyaslarken; güven seviyesi sınıflandırma modeli, herhangi bir dijital delilin kullanıcı veya zararlı yazılım tarafından oluşturulma ihtimallerini kolay anlaşılabilir kategorilerde değerlendirerek raporlar. Her iki modelin de amacı, zararlı yazılım etkisi iddia edilen dijital adli delillerin güvenilirliğini tespit etmek ve karar vericilere anlaşılır raporlar sunarak yardımcı olmaktır.

Sonuç olarak günümüz bilgisayar çağında her tür bilginin sanal ortamda olması, dijital adli delillerin çok daha fazla gündeme geleceğine ilişkin bir gösterge olarak kabul edilebilir. Bu durumdan hareketle dijital adli delillerin, gerek özel hukuk gerekse ceza davalarında daha çok karşılaşılan bir delil türü olacağı düşünülebilir. Bu delillere dayanarak karar vermek ise her şeyden önce bu delillere güvenmeyi gerektirir. Dijital adli delillere güven duymak; konusuna hâkim ve motivasyon sahibi dijital adli analiz uzmanlarının zararlı yazılım ve delil karartma etkisini incelemesi ve bulgularını bu alanda ihtisaslaşan hukukçularla birlikte değerlendirmesi sayesinde mümkün olabilir. Tez çalışması kapsamında dijital adli delil güvenilirliğinin tespitine ilişkin tartışılan karmaşıklık tabanlı niceliksel değerlendirme ve güven seviyesi sınıflandırma modelleri ile, dijital adli analiz uzmanlarına yardımcı olunabileceği, karar verici makamlara daha faydalı ve anlaşılabilir raporlar sunulabileceği değerlendirilmektedir.

§8. Ekler

I. Dijital adli analiz çalışmalarını etkileyen sorunlar ve çözüm önerileri

A- Mevzuat

Dijital adli analiz çalışmaları, bu çalışmalarda kullanılan dijital kaynakların delil niteliği kazanması ve mahkemelerde her geçen gün daha çok dijital adli delilin hâkimlerin yorumuna sunulması, günümüz hukuk sisteminde sayısını ve önemini artıran bir süreç haline dönüşmüştür.

Sürecin bir tarafı tamamen sayısal bir disiplin olan bilişim teknolojilerinden müteşekkilken, diğer tarafta sosyal bir disiplin olan hukuk sistemi bulunmaktadır. Kökeni asırlar öncesinde dayanan "adaletin yerini bulması" gayretleri ve bu uzun yıllar boyunca oturmuş bir sistematiğe sahip hukuk disiplini ile mazisi ancak 50 yıl öncesine giden kişisel bilgisayarların[218] etkileşimi ve tek çatı altında bir sonuç üretebilmeleri elbette kolay olmayacaktır.

Dijital adli analiz, kişisel bilgisayarların ülkemizde yaygınlaşmasının ardından[219] hem kurumsal hem de kişisel verilerin işlendiği birincil ortam haline gelmiştir. Bu durum bilgiye erişim hızını ve üretkenliği son derece pozitif etkilerken, bilgisayarlarda saklanan verilerin de çeşitlenmesine neden olmuştur. Hemen her tür bilgi, defterler ve kitaplardan önce bilgisayarlara kaydedilmeye başlanmış, üzerine bir de tablet ve akıllı telefonların yaygınlaşması eklenince kâğıt üzerinde bilgi saklanması yerini giderek bilişim teknolojilerine bırakmıştır.

Bilişim teknolojilerindeki gelişmeleri tetikleyen bir diğer unsur internetin yaygınlaşması olmuştur. Erişilebilir fiyatlar, kablosuz teknolojilerin yaygınlaşmasıyla hemen her yerden ulaşım ve fiber optik bağlantı olanaklarıyla son derece hızlı internet imkânı her türlü bilgiye erişimi kolaylaştırmış, kurum ve

---

[218] İlk "kişisel bilgisayar" terimi 3 kasım 1962 tarihinde New York Times gazetesi tarafından kullanılmıştır. Bilgi için bkz. Kişisel Bilgisayar, http://tr.wikipedia.org/wiki/Ki%C5%9Fisel_bilgisayar, erişim tarihi: 07.01.2013.

[219] 2010 yılında kişisel bilgisayar sayısının nufüsun %29'una yükselmesine ilişkin rapor için bkz. http://www.invest.gov.tr/trTR/infocenter/publications/Documents/ BILGI.ILETISIM.SEKTORU. PDF, erişim tarihi: 07.01.2013.

kuruluşların ticari faaliyetlerini internet üzerinden yürütmesinden devletin kamu hizmetlerini internet aracılığıyla vatandaşlarına sunmasına kadar çok farklı alanlarda kullanılmaya başlanmıştır.

Bütün bu imkânlar ve teknolojilerin tahmin edileceği üzere sadece faydalı amaçlar için kullanılması beklenemez. Sürecin doğan sonucu olarak yasadışı faaliyetler ve suç unsuru içeren her tür bilgi ve belge de sanal ortama taşınmıştır. İşin içine bir de sanal dünyaya özgü yeni suç tanımları girince, bilişim teknolojileri yasa dışı faaliyetler için adeta yeni bir barınak haline gelmiştir.

Bahsedilen bütün bu unsurlar, adli bilişim disiplinin doğmasına ve hızla yaygınlaşmasına neden olmuştur. Bu disiplin kapsamında yer alan dijital adli analiz çalışmaları ise, bilgisayarlar başta olmak üzere her tür bilişim teknolojisi üzerinde analiz yapılması ve eğer varsa suç unsuru olan bilgi ve belgelerin ortaya çıkarılması anlamına gelmektedir. Dijital adli çalışmalarını diğer veri analizi çalışmalarından ayıran temel fark, durumun adli bir konu olmasından kaynaklanır. Özel bir şirketin bilgisayarlarında yapılan tetkik faaliyeti veya kişinin kendi bilgisayarındaki silinmiş verilerin kurtarılması bu bağlamda "dijital adli analiz" çalışması olarak değerlendirilmeyecektir.

Dijital adli analiz çalışmaları her geçen gün daha çok talep görse de, bu çalışmalardan elde edilen sonuçlar karar vericilerin faydasına aynı oranda etki etmeyebilmektedir. Bu durumun birçok sebebi olabilir. Disiplinlerin çok farklı olması nedeniyle taraflar arasındaki iletişim bozuklukları ve hukukun nadiren değişen yazılı mevzuatlara dayalı olmasına karşın bilişim teknolojilerinin dinamik ve her geçen gün değişen kural seti bu durumlara örnek olarak verilebilir.

Bu çalışma kapsamında dijital adli delillerin temel nitelikleri araştırılmış, bir dijital verinin adli delil olarak mahkemeye sunulmasına ve hâkimlerin vereceği karara yardımcı olmasına kadar geçen sürede delilin etkilenebildiği etmenler değerlendirilmiştir. Özel olarak dijital adli delillerin güvenilirliği sorgulanmış ve güvenilirliğe etki eden bütün unsurlar ele alınmıştır.

Çalışmanın sonucunda dijital adli delillerin temelde iki faktörden etkilendiği görülmüştür; zararlı yazılımlar ve delil karartma işlemleri. Zararlı yazılımlarla ilgili olarak; bu tür yazılımların tanımı yapılmış, sınıflandırılmasına

değinilmiş ve delil niteliğindeki dijital verilerde ne tür etkileri olabileceği araştırılmıştır. Delil karartma konusunda ise delil karartma türleri açıklanmış, türlerine göre delil karartma işlemlerinin dijital adli deliller üzerindeki etkisine ve verilecek kararlara nasıl yansıyabileceğine değinilmiştir.

Sonraki bölümlerde dijital adli delillerin güvenilirliğine etki eden diğer faktörler üzerinde durulmuştur. Uluslararası standartlara göre bir dijital delillerin kabul görmesi için dikkat edilmesi gereken noktalar araştırılmıştır. Güven problemi olan şüpheli delillere yönelik "güven seviyesi" ve "karmaşıklık tabanlı niceliksel değerlendirme" modelleri incelenmiş, modelleme çıktıları artı ve eksi yönleriyle tartışılmıştır. Dijital adli delillerin ulusal ve uluslararası hukuk sistemlerinde nasıl ele alındığı ve özellikle delil niteliğinin kesinlik arz etmediği hallerde hangi yaklaşımların sergilendiği araştırılmıştır.

Bütün bu çalışmaların sonunda dijital adli delillerin vasıflarıyla ilgili bir takım bulgular tespit edilmiş durumdadır. Özellikle sıkça yaşanan problemlere çözüm getirebilecek tavsiye niteliğinde öneriler aşağıda derlenmiştir.

B- Standartlaşma

Dijital adli analiz çalışmalarına yön verecek ve her çalışmanın sonunda aynı kalitede çıktı oluşmasına yardımcı olacak yasa, yönetmelik veya standartların bulunmaması önemli bir eksiklik olarak öne çıkmaktadır. Bu alandaki çalışmalar her geçen gün kendini yenilese ve yeni ürün, yazılım veya teknikleri hayata geçirse de, bütün bu çalışmalarda izlenmesi gereken temel yol haritasının belli olması sürece katkı sağlayacaktır[220]. Herhangi bir davada mahkemelerin dijital adli analiz çalışması talep etmesiyle başlayan ve hazırlanacak raporun hâkimlerin sunulmasıyla tamamlanan bütün iş akışı en azından ana hatlarıyla düzenlenebilir. Çalışmalarda görev alacak personelin seçimi ve yetkilendirilmesi, izlenmesi gereken metodoloji ve çalışmanın sonunda hazırlanacak raporun nitelikleri gibi çok temel alanlarda bir standardın oluşturulması halinde daha kaliteli çıktılar üretilebileceği düşünülmektedir. Dijital adli analizin belirli bir kaliteye ulaşması

[220] Bu standartların oluşmasında dikkate alınabilecek süreç modelleri hakkında bkz. "Süreç modelleri", sf. 22.

da neticede dijital adli delillerin güvenilirliğini artıracak, bu delillerin eksiksiz bir çalışmanın sonucunda ortaya çıktığından emin olunacaktır.

C- İhtisaslaşma

Adli bilişim disiplini, bilişim teknolojilerinin bir uzmanlık sahası gibi algılansa da çok farklı yetkinliklere ihtiyaç duyulan bir bilim dalıdır. Olayın hem hukuki boyutunda hem de teknik tarafta bu ayrıma duyulan ihtiyaç belirgin şekilde kendini göstermektedir.

Adli bilişim, "bilgisayar mühendisliği" alanı kapsamında değerlendirilebilse de, bir takım farklı yetkinliklere de ihtiyaç duyulan bir çalışma sahasıdır. Bilgisayar mühendisliği alanında farklı konularda uzun yıllardır süregelen akademik çalışmalar sayesinde ciddi bilimsel mesafeler katedilmiş durumdadır. Adli bilişim disiplini ve dijital adli analiz alanında yapılacak bilimsel çalışmalar ile bu alanlarda da ihtisaslaşma sağlanabilir.

Dijital adli analiz konusunda çalışan uzmanlarda aranabilecek bir diğer nitelik, konunun hukuki tarafına yaklaşmak olabilir. "Bilişim hukuku" alanında eğitim alan bilirkişiler, yapacakları çalışmaların hukukçulara daha faydalı olmasını sağlayabilir, hukuki açıdan süreci yorumlayarak incelenmesi gereken noktaları hâkimlere işaret edebilir.

Adli bilişim alanının hukuki boyutunda da gelişmeye açık konular bulunmaktadır. Dijital adli analizin çok yeni ve farklı bir disiplin olması, avukatların savcıların ve hâkimlerin konuya yabancı kalmasına neden olabilmektedir. Bazı davaların en önemli delilleri "dijital adli deliller" olmaya başlamışken, hukuk camiasının olaya uzak kalması ve salt "bilirkişi raporları" üzerinden karar vermeye çalışması sıkıntılı durumlar oluşturabilmektedir. Hâkimler başta olmak üzere adli bilişimle ilgili davalarda görev alan bütün hukukçuların adli bilişimi kavraması, iddia ve savunma makamlarının ve karar verici hâkimlerin bilimsel ve hakkaniyetli sonuçlara oluşmasını sağlayacaktır. Yargı mensupları bu alanda eğitim veren akademik programlara teşvik edilebilir, Ulusal Yargı Ağı Projesi (UYAP) platformu üzerinden çeşitli etkinliklerle bilinç

düzeyi artırılabilir. Adli bilişimi ilgilendiren soruşturma sayısının artmaya devam etmesi halinde kendini bu alanda özel olarak yetiştirmiş hukukçulara duyulan ihtiyaç da artacaktır. İlerde bu alanda ihtisaslaşan mahkemelerin kurulması bile gündeme gelebilir.

Hukukçuların bu alanda kendilerini yetiştirmesi, dijital adli delillerin kesinlik ifade etmeyebilen yapısından kaynaklanan hatalı yorumların önüne geçebilecek en önemli set olacaktır.

D- Disiplinler arası çalışma

Adli bilişim; bilgisayar mühendisliği, hukuk ve kriminoloji disiplinlerinden faydalanan "disiplinler arası" bir çalışma sahasıdır. Dijital delillerin toplanması ve değerlendirilmesinde hukuki düzenlemelerin gerekleri yerine getirilirken, delillerin incelenmesi esnasında bilgisayar mühendisliği bilimi ve dijital adli analiz prensiplerinden faydalanılır. Kriminoloji ise suçluluk psikolojisinin bilgisayar kullanım alışkanlıklarına etkisini değerlendirir ve gigabytelarca veri arasından anlamlı ve ilgili olanların tespitine yardımcı olur.

Adli bilişim disiplininin bu tümleşik yapısı bazı problemleri de beraberinde getirebilmektedir. Görevi "suç unsuru içeren delillerin tespiti" olan bir dijital adli analiz uzmanı, hangi tür verilerin hangi kapsamda suç olabileceğini bilmeyebilir. Hukukçuların teknik uzmanları ve bilirkişileri doğru yönlendirmesine duyulan ihtiyaç burada kendini göstermektedir.

Dijital adli delillerin güvenilirliğinden kaynaklanan problemleri çözmek için "disiplinler arası yaklaşımın" önemi oldukça belirgindir. Bilgisayar sabit diskinde tespit edilen ancak güven problemi olan bir delil, harici başka bir delille desteklenebilir veya iddia çürütülebilir. Bir dosyanın erişim tarihi ile ilgili bir araştırma yapılıyorsa, hâkimler bilirkişilerden bu delile yönelik detaylı çalışma isteyebilirler. Söz gelimi, dosyanın belirli bir tarihteki durumu sorgulanır. Paralelde ISP verileri toplanarak kişinin o tarihte internette ne tür işlemler yaptığı sorgulanabilir. Hâkimlerin teknik bilirkişileri yönlendirmesi neticesinde, sabit diskten elde edilen verilerin güvenilirliği netleştirilebilir.

Dijital adli delillerin sunulduğu davalarda uzman tecrübe, tahkikat ve incelemeye ait bilgi, bağlamsal bilgi, hukuk bilgisi ve iletişim yeteneğinin gerek avukatlar gerekse uzman bilirkişilerde bulunması ve bu yetkinliklerin yeterli oranda paylaşılması gerektiği öngörülebilir[221].

Bir önceki bölümde bahsedilen ihtisaslaşmanın sağlanması halinde adli bilişimin farklı alanlarında çalışan kişiler daha verimli iletişim kurabilir, soruşturmaları aydınlatmak için gerekli veriler daha kolay elde edilebilir ve hâkimin yorumuna sunulabilir.

E- Kaynak ayrımı

Günümüzde dijital adli analiz çalışmalarını olumsuz etkileyen bir diğer unsur kısıtlı kaynaklardır. Dijital adli analiz çalışmalarının temelini oluşturan "boş sabit disk" temininde bile bütçelerden dolayı çeşitli sıkıntılar yaşandığı bilinmektedir. Yetişmiş personel ihtiyacı ise kaynak probleminin yaşandığı bir diğer başlıktır.

Her geçen gün daha çok kullanılagelen dijital adli delillerin toplanmasından incelenmesine ve rapor hazırlanıp mahkemeye sunulmasına kadar geçen süreçte çalışabilecek yetişmiş personel sayısı son derece kısıtlıdır. Dijital adli analizle ilgilenen teknik personelin sınırlı sayıda olmasının bir olumsuz etkisi de çalışmalara ayrılan zamanın giderek düşmesidir. Özellikle zararlı yazılım ve delil karartma gibi etkenlerle ileri düzey şüphe barındıran delillerin incelenmesi uzun zaman almaktadır. Kolluk kuvvetlerinin her gün onlarca imaj alıp inceleme yapmak durumunda kalması, delil güvenilirliğinin tartışıldığı soruşturmalarda ciddi problem oluşturmaktadır. İnceleme için gerekli iş gücünün ayrılamadığı durumlarda, gözden kaçabilecek ufak bir veri suçsuz insanların ceza almasına veya suçlu insanların serbest kalmasına neden olabilmektedir.

Çalışmamızda değerlendirilen "güven seviyesi" ve "karmaşıklık tabanlı niceliksel değerlendirme" modelleri de uzun zaman harcanarak detaylı araştırma

[221] Berber, sf. 75.

yapılmasını gerektirmektedir. Bu bağlamda dijital adli delillerin güvenilirliğinin sağlanması için yeterli kaynak ayrılması ihtiyacı kendini göstermektedir.

F- Teknik yetkinlikler

Dijital adli delillerin güvenilirliğini etkileyen unsurlara bakıldığında hemen hepsinin ileri düzey teknik incelemeyle tespit edilecek durumlar olduğu anlaşılmaktadır. Delil ağırlık dağılımları ve güven seviyeleri[222] yaklaşımlarıyla çözülmeye çalışılan belirsizlikler, temelde detaylı ve eksiksiz teknik araştırmalara ihtiyaç duymaktadır.

Dijital delillere duyulan güveni etkileyen belki de ilk unsur zararlı yazılımlardır. Truva atı savunmalarının da ilk noktası, incelenen bilgisayar imajında zararlı yazılım bulunuyor olmasıdır. Bu durumda adli analizi gerçekleştiren uzmanların bakması gereken nokta zararlı yazılımın etkisi olacaktır. Zararlı yazılımın türü, niteliği, kapasitesi ve en önemlisi delil bilgisayarındaki faaliyeti, ancak uzman zararlı yazılım analistleri tarafından ortaya çıkarılabilir. Dijital adli analiz uzmanlığına bir de zararlı yazılım analizi uzmanlığını ekleyince, bir önceki bölümde açıklanan kaynak ihtiyacı bir daha belirmektedir. Çünkü bu tür teknik bilgi birikimi olan uzman sayısı hem dünyada hem de ülkemizde oldukça kısıtlıdır.

Teknik zorluklardan bir diğeri, dijital adli delil üzerinde delil karartma yapılması durumunda ortaya çıkar. Delil karartmanın çok farklı türleri olması, şüpheli bilgisayar imajlarında bu tür bir işlemin yapılıp yapılmadığının tespiti edilmesini de zorlaştırır[223]. Kasıtlı bir delil karartmanın tespiti halinde sanıkların düşeceği durum ve soruşturmanın seyrinde yaşanacak diğer gelişmeler, konunun ne kadar hassas olduğunu gözler önüne sermektedir. Delil karartma işlemlerini algılayıp soruşturmada incelenen dijital adli delillerde bu etkiyi yorumlayacak uzmanların sayısı da ülkemizde oldukça sınırlıdır. Dijital adli delillerde yaşanabilen güven problemi, detaylı analiz yapacak zamanı ve motivasyonu olan

[222] Delillerin güven seviyesi hakkında detaylı bilgi için bkz. "Delil güven", sf. 117.

[223] Delil karartma hakkında detaylı bilgi için bkz. "

", sf. 82.

eğitimli dijital adli analiz uzmanlarınca hafifletilebilir. Olası belirsizliklerin gidermenin yolu hiç şüphesiz teknik olarak çok ileri düzeyde bilgi sahibi bilirkişilerle çalışmaktan geçer.

§9. Özgeçmiş

E-posta: emincaliskan@gmail.com
Telefon: 902626481067

İstanbul Kültür Üniversitesi Bilgisayar Mühendisliği bölümünden 2008 yılının temmuz ayında mezun olan yazar, aynı üniversitesitenin Endüstri Mühendisliği bölümünden 2009 yılının nisan ayında çift anadal programı kapsamında mezun olmuştur. Akademik kariyerine 2011 yılında Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı ile devam eden eser sahibi, 2013 yılında mezuniyet hakkı kazanmıştır. Yazarın profesyonel geçmişi ve teknik yetkinlikleri aşağıdaki gibidir.

Profesyonel Geçmiş

2011-...	Araştırmacı, TÜBİTAK UEKAE, Gebze/KOCAELİ
2008-2011	Uzman, TURKCELL, Müşteri Veri Ambarı Yönetim Grubu, İstanbul/TÜRKİYE
2008	Stajyer, TURKCELL, Analiz ve Raporlama Grubu, İstanbul/TÜRKİYE
2007	Stajyer**,** NEW YORK EIC Design, Web Development Team, New York/USA

Deneyimler

E-Belgem elektronik belge yönetimi projesi kapsamında TCCB ve NVİ'ye kurulacak sistemler için Bilgi Güvenliği Yönetim Sistemi ve Ortak Kritikler (Common Criteria) sertifikası almasında konularında danışmanlık görevinde bulunmuştur.

BDDK'nın yönettği bir proje kapsamında Türkiye'deki bankaların büyük çoğunluğunda ve kamu ile özel sektöre ait birçok kuruluşta veritabanı testleri ana sorumlusu olarak görev almıştır. Banka testlerinde gerçekleştirdiği gibi halen Oracle, MSSQL, MySQL ve DB2 gibi sektörde sıkça kullanılan veritabanlarında

sızma, denetleme, ISO 27001 ve COBIT uyumluluk çalışmalarını gerçekleşmektedir.

Mahkemelere adli bilişim konusunda danışmanlık yapmaktadır.

TURKCELL DWH & DataQuality ekibinde veri madenciliği sistemlerinin yöneticiliğini yapmıştır.

TURKCELL Datawarehouse Reporting ekibince yönetilen 250+ TB hacimdeki veritabanı sistemlerinde, verinin oluşumundan analiz yapılabilir hale gelmesine kadar olan süreçlerde çeşitli görevler almıştır.

New York/Manhattan'da EIC Design firmasında CSS ve Macromedia Dreamweaver ürünleri kullanarak web uygulamaları geliştirmesinde görev almıştır.

Eğitimler

2012 SANS 401, İstanbul
2012 ISO 27001 Baş Denetçi Eğitimi, İstanbul
2012 Mobile Forensics, Forensic People, İstanbul
2012 Windows Forensics, Forensic People, İstanbul
2012 Bilirkişilik Eğitimi, Türkiye Bilişim Derneği, İstanbul
2012 Bilgi Güvenliği ve Teknik İnceleme, Y.Lisans/Bilgi Üniversitesi
2011 Encase Dijital Adli Analiz Eğitimi, İstanbul
2011 Telekomünikasyon Sistemleri Altyapısı, Y.Lisans/ Bilgi Üniversitesi
2011 NATO Cyber Security Workshop, Brüksel/BELÇİKA
2011 Linux Operating Systems Security, İstanbul
2011 Mobile Forensics Dijital Adli Analiz Eğitimi, ForensicsPeople, İstanbul
2011 Oracle & MSSQL Database Security, İstanbul
2011 Computer Network Infrastructure & Security, İstanbul
2011 E-Devlet, Konsept ve Uygulama, Y.Lisans/ Bilgi Üniversitesi
2010 Bilgi ve İletişim Teknolojileri Hukuku, Y.Lisans/ Bilgi Üniversitesi
2010 SAS M2010 Datamining Conference & Workshops, Las Vegas/ABD
2010 ETL tool Abinitio (GDE) Basics, İstanbul
2009 Oracle Data Integrator Administration, İstanbul
2009 Oracle10g:Introduction to SQL, İstanbul
2009 Unix Essentials, İstanbul
2008 SAS Programming 2: Manipulating DATA with DataStep, İstanbul
2008 DataFlux dfPower Studio v.8.1, İstanbul, İstanbul

Çalışma Alanları

Kurumsal güvenlik
Açık kaynak kodlu sistemler ve güvenliği
Veritabanı güvenliği
Uygulama güvenliği
Sızma testleri ve güvenlik denetlemeleri

Yabancı Dil Bilgisi

İngilizce, TOEFL IBT 91/120 (KPDS 90 denkliği), 2011 yılı.

Burslar

2009	Turkcell Profesyonelliğe Adım Formasyonu, Lisans
2004-2009	Kültür Üniversitesi, Lisans, Tam Burs