

MİLLÎ SAVUNMA ÜNİVERSİTESİ
HEZÂRFEN HAVACILIK VE UZAY TEKNOLOJİLERİ ENSTİTÜSÜ

**ADLİ BİLİŞİM ATLATMA TEKNİKLERİ VE
KARŞI TEDBİRLER**

YÜKSEK LİSANS TEZİ

Murat GÜL

Bilgisayar Mühendisliği Ana Bilim Dalı Başkanlığı

Siber Güvenlik Programı

HAZİRAN 2018



**MİLLÎ SAVUNMA ÜNİVERSİTESİ
HEZÂRFEN HAVACILIK VE UZAY
TEKNOLOJİLERİ ENSTİTÜSÜ**



**ADLİ BİLİŞİM ATLATMA TEKNİKLERİ VE
KARŞI TEDBİRLER**

YÜKSEK LİSANS TEZİ

**Murat GÜL
(3172106)**

Bilgisayar Mühendisliği Ana Bilim Dalı Başkanlığı

Siber Güvenlik Programı

Tez Danışmanı: Dr.Öğr.Ü. M.Ali AYDIN

HAZİRAN 2018

Millî Savunma Üniversitesi Hezârfen Havacılık ve Uzay Teknolojileri Enstitüsü'nün 3172106 numaralı Yüksek Lisans Öğrencisi **Murat GÜL**, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı “**ADLİ BİLİŞİM AT-LATMA TEKNİKLERİ VE KARŞI TEDBİRLER**” başlıklı tezini aşağıdaki imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı : **Dr.Öğr.Ü. M.Ali AYDIN**
İstanbul Üniversitesi

Eş Danışman : **Dr.Ömer ÇETİN**
Hezârfen HUTEN

Jüri Üyeleri : **Prof.Dr. Hasan Hüseyin BALIK**
Hava Harp Okulu Dekanlığı

Doç.Dr.Serhan YARKAN
İstanbul Ticaret Üniversitesi

Teslim Tarihi : **14 Mayıs 2018**
Savunma Tarihi : **05 Haziran 2018**



Bu tez alıřmasında belirtilen grř ve yorumlar yazara aittir. Trk Silahlı Kuvvetleri'nin ya da diğerk kamu kuruluşlarının grřlerini yansıtmaz. Ayrıca bu tez alıřması bilimsel ahlak ve etik değerklere uygun olarak yazılmış olup, yararlanılan tm eserler kaynaklarda gsterilmiştir.

Haziran 2018

Murat GL





*Aziz şehitlerimize ve kahraman gazilerimize,
Aileme*



ÖNSÖZ

Tez çalışmamı hazırladığım zorlu sürecin her aşamasında öncelikle, bana yol gösteren, her konuda yardımcı ve destek olan, her soruma sabırla yanıt veren ve tez çalışmasının son halini almasında eksik yönlerinin ortaya çıkarılması ve giderilmesi kapsamında gayretlerini eksik etmeyen ve değerli zamanını harcayan tez danışmanım Dr.Öğr.Ü.M.Ali AYDIN'a ve eş danışmanım Dr.Hv.Mu.Bnb.Ömer ÇETİN'e, başta Bilgisayar Mühendisliği Ana Bilim Dalı Başkanı Prof.Dr.Hasan Hüseyin BALIK olmak üzere, Bilgisayar Mühendisliği Ana Bilim Dalı Başkanlığı öğretim üyelerine, bize lisansüstü eğitimimiz boyunca her türlü imkânı sağlayan Hezârfen HUTEN Müdürü Dr.Öğr.Ü.Hv.Müh.Alb. Serdar MENEKAY ile tüm enstitü personeline, zorlu çalışma sürecimde sabırla destek olan, destekleri olmasaydı başaramayacağım, Sevgili Eşim'e ve çocuklarıma, bana bu imkânı sağlayan ülkem ve Türk Silahlı Kuvvetleri'ne teşekkürlerimi sunmayı bir borç bilir, sonsuz minnettarlığımı sunarım.

Haziran 2018

Murat GÜL

İÇİNDEKİLER

Sayfa

ÖNSÖZ	ix
İÇİNDEKİLER	xi
KISALTMALAR.....	xiii
ÇİZELGE LİSTESİ.....	xv
ŞEKİL LİSTESİ.....	xvii
ÖZET	xix
SUMMARY	xxi
1. GİRİŞ.....	1
1.1 Arka Plan ve Motivasyon	2
1.2 Tezin Amacı.....	3
1.3 Tez Organizasyonu	4
2. LİTERATÜR ARAŞTIRMASI	7
2.1 AF Tanımlanmasına Yönelik Çalışmalar	7
2.2 Bir Problem Olarak AF	7
2.3 AF'nin Sınıflandırılması ve Özelliklerinin Belirlenmesine Yönelik Çalışmalar	12
2.4 AF Araçlarının Kullanımına Ait Belirtilere ve Tespitine Yönelik Çalışmalar	15
3. ADLİ BİLİŞİM	19
3.1 Adli Bilişime Genel Bakış.....	19
3.2 Adli Bilişimde Delil Türleri, Özellikleri ve Süreç Modelleri.....	20
3.2.1 Dijital delillerin özellikleri	20
3.2.2 Adli bilişim süreçleri	22
3.3 Adli Bilişim Araçları ve Özellikleri	25
3.4 Adli Bilişim Türleri	26
3.4.1 Bilgisayar adli bilişimi (Computer forensics)	27
3.4.2 Dosya sistemi adli bilişimi (File system forensics).....	28
3.4.3 İşletim sistemi adli bilişimi (OS forensics)	33
3.4.4 Ağ adli bilişimi (Network forensics).....	35
3.4.5 Mobil cihaz adli bilişimi (Mobile forensics).....	38
3.4.6 Kötücül yazılım adli bilişimi (Malware forensics).....	41
3.4.7 Geçici bellek adli bilişimi (Memory forensics).....	43
3.4.8 Medya aygıtları adli bilişimi (Media device forensics).....	47
3.4.9 Sosyal ağ adli bilişimi (Social media forensics).....	48
4. ADLİ BİLİŞİM ATLATMA, KLASİK ADLİ BİLİŞİM ATLATMA TEKNİKLERİ ve KARŞI TEDBİRLER.....	55
4.1 Adli Bilişimi Atlatma	55
4.2 Klasik Adli Bilişim Atlatma Teknikleri ve Karşı Tedbirler.....	57

4.2.1 Sabit disk ve dosya temizleme	57
4.2.2 Şifreleme.....	63
4.2.3 Fiziksel yok etme.....	67
4.2.4 Steganografi	68
5. MODERN ADLİ BİLİŞİMİ ATLATMA TEKNİKLERİ ve KARŞI	
TEDBİRLER.....	75
5.1 Verilerin Toplanmasına Yönelik Kullanılan Adli Bilişim Atlatma Teknikleri ve Karşı Tedbirler.....	75
5.1.1 Veri doygunluğu	75
5.1.2 Standart olmayan disk RAID yapısı kullanma	76
5.2 Verilerin Analizine Yönelik Kullanılan Adli Bilişim Atlatma Teknikleri ve Karşı Tedbirler	78
5.2.1 Dosya imza bilgisini değiştirme	78
5.2.2 Dosya zaman damgalarında sahtecilik	81
5.2.3 Kısıtlanmış klasör veya dosya adlarının kullanılması	83
5.2.4 Döngüsel referanslama ve ASCII karakterli metin kullanımı	86
5.2.5 ABA'lara yönelik saldırı	87
5.3 Bulguların Sunulmasına Yönelik Kullanılan Adli Bilişim Atlatma Teknikleri ve Karşı Tedbirler.....	89
5.3.1 Hash çakışması	89
5.3.2 İşlevsiz sabit disk kullanımı	90
5.4 MS Windows İşletim Sistemlerinde İzlerin Yok Edilmesine Yönelik Uygulanan Adli Bilişim Atlatma Teknikleri	90
5.4.1 Kayıtları devre dışı bırakma	91
5.4.2 Son erişim kayıtlarını devre dışı bırakma.....	92
5.4.3 USB faaliyetleri için kayıtları devre dışı bırakma	93
5.4.4 Sistem geri yükleme noktalarını devre dışı bırakma	93
5.4.5 Microsoft hata bildirimlerinin devre dışı bırakılması.....	94
5.4.6 Üçüncü parti yazılımlar ile önemli kayıtları temizleme	95
5.4.7 Windows hata ayıklama bilgisi yazımını devre dışı bırakma	95
5.4.8 Windows olay kayıtlarını temizleme	97
6. SONUÇ VE ÖNERİLER	99
KAYNAKLAR.....	103
ÖZGEÇMİŞ	111

KISALTMALAR

AB	: Adli Bilişim
ABA	: Adli Bilişim Aracı
ABAT	: Adli Bilişim Atlatma Teknikleri
ABU	: Adli Bilişim Uzmanı
AF	: Anti-Forensics
AFT	: Anti-Forensics Techniques
BGU	: Bilgi Güvenliği Uzmanı
CF	: Computer Forensics
CFT	: Computer Forensics Tool
CMK	: Ceza Muhakemeleri Kanunu
DBAN	: Darik's Boot and Nuke
DCO	: Device Configuration Overlay
DF	: Digital Forensics
DoS	: Denial of Service
EoS	: Elimination of Source
FAT	: File Allocation Table
FTK	: Forensic Tool Kit
HFS	: Hierarchical File System
HPA	: Host Protected Area
IDE	: Integrated Disk Electronics
IEF	: Internet Evidence Finder
IoAF	: Indicators of Anti-Forensics
LBA	: Logical Block Addressing
LSASS	: Local Security Authority Subsystem Service
LSB	: Least Significant Bit
MACE	: Modification, Accessed, Created, Entry Created
MFT	: Master File Table
NOP	: No Operation
NTFS	: New Technology File System
PDA	: Personal Digital Assistant
RAID	: Redundant Array of Inexpensive Discs
SMTP	: Simple Mail Transfer Protocol
SSD	: Solid State Disk
SSH	: Secure Shell
TOR	: The Onion Routing
VPN	: Virtual Private Network



ÇİZELGE LİSTESİ

	<u>Sayfa</u>
Çizelge 1.1 : Adli bilişim atlatma konulu akademik çalışmalar istatistik bilgileri.	4
Çizelge 2.1 : AF tanımları.....	8
Çizelge 2.2 : Harris [14] AF sınıflandırması.....	13
Çizelge 3.1 : Adli bilişimde delil türleri.	21
Çizelge 3.2 : Adli bilişim araçları.....	26
Çizelge 3.3 : Dosya kurtarma olasılıkları.	32
Çizelge 3.4 : Windows OS geçici ve geçici olmayan bilgiler.	33
Çizelge 3.5 : Dünya geneli mobil cihaz istatistikleri (milyar kişi) [56].....	38
Çizelge 3.6 : Dünya geneli mobil cihaz işletim sistemi oranları.	39
Çizelge 3.7 : Sanallaştırma teknolojileri sanal bellek dosyaları.	46
Çizelge 3.8 : Android cihazda sosyal ağ adli bilişimi ile elde edilen bilgiler.....	52
Çizelge 4.1 : Disk temizleme (wipe) araçlarının karşılaştırılması.....	60
Çizelge 4.2 : Şifre çözme teknikleri.....	65
Çizelge 4.3 : Stegonagrafi analizi yöntemleri.....	72
Çizelge 5.1 : Bilinen dosya türlerine ait dosya imza listesi.	79
Çizelge 6.1 : Adli bilişimi atlatma teknikleri ve karşı tedbirler özet.	100



ŞEKİL LİSTESİ

	<u>Sayfa</u>
Şekil 1.1 : Türkiye’de 2003-2012 yılları arasında bilişim suçu istatistikleri.....	2
Şekil 2.1 : Wundram, Freiling ve Moch, [21] partition table loop örneği.	11
Şekil 2.2 : Rekhis ve Boudriga [29]’de AF farkındalıklı AB süreçleri.	17
Şekil 3.1 : Adli Bilişim Süreçleri.	23
Şekil 3.2 : Kuramsal Adli Bilişim Modeli.	24
Şekil 3.3 : Bilgisayar adli bilişimi [46].	27
Şekil 3.4 : Sabit disk yapısı (iz-sektör).....	28
Şekil 3.5 : Disk üzerinde HPA tahsisi.....	29
Şekil 3.6 : Disk üzerinde HPA ve DCO tahsisi.	29
Şekil 3.7 : NTFS MFT kayıt bölümleri.	31
Şekil 3.8 : Boşluk alan (slack space) oluşumu.	32
Şekil 3.9 : Windows OS kayıt defteri ayarları.	34
Şekil 3.10 : Windows OS olay günlükleri kayıtları.	35
Şekil 3.11 : Wireshark TCP 80 portu trafiği inceleme.....	37
Şekil 3.12 : Whois sorgusu ile IP/domain bilgi detayı.	37
Şekil 3.13 : Mobil telefon ABA yöntem sınıflandırma piramidi.	40
Şekil 3.14 : Mobil telefon örnek ABA sınıflandırma piramidi.	41
Şekil 3.15 : Virustotal zararlı yazılım tarama sitesi.....	42
Şekil 3.16 : Dumpit bellek birebir kopya alma.....	44
Şekil 3.17 : Volatility .dmp dosyası içeriğinin analizi.	45
Şekil 3.18 : ProcDump ile lsass.exe mini kopya alınması.	46
Şekil 3.19 : Mimikatz yazılımı ile mini kopyadan şifre elde etme.	47
Şekil 3.20 : Medya aygıtları adli bilişimi temel bileşenleri [70].	48
Şekil 3.21 : Facebook kullanıcı bağlantı çizgesi [75].....	51
Şekil 3.22 : Facebook kullanıcı faaliyeti zaman çizgesi [75].	52
Şekil 3.23 : Sosyal ağ adli bilişimi için IEF ABA kullanımı.....	53
Şekil 4.1 : DF soruşturması genel süreçleri.	56
Şekil 4.2 : E: sürücüsü metin dosyaları.	60
Şekil 4.3 : Autopsy ABA üzerinde dosya silinen dosyaya ait bilgi.....	61
Şekil 4.4 : DBAN boot işlemi.....	62
Şekil 4.5 : DBAN disk seçme işlemi.	63
Şekil 4.6 : DBAN disk üzerine yazma doğrulaması.	63
Şekil 4.7 : Disk temizleme sonrası autopsy uyarısı.	64
Şekil 4.8 : R-Studio ile disk analizi.	65
Şekil 4.9 : Eraser programı ile dosya temizleme.	66
Şekil 4.10 : Autopsy ile dosya temizleme inceleme sonuçları.	67
Şekil 4.11 : Passwire recovery forensics kit aracı kullanımı.	68

Şekil 4.12 :	Elcomsoft forensics disk decryptor ile trueCrypt anahtar elde etme. .	69
Şekil 4.13 :	Degausser cihazı.....	70
Şekil 4.14 :	OpenStego programı ile resim içine mesaj ekleme.	71
Şekil 4.15 :	Asıl resim ve stego resim dosyalarının karşılaştırılması.	71
Şekil 4.16 :	OpenStego programı ile resim içinden mesajı çıkarma.	72
Şekil 4.17 :	xStego programı ile steganografi dosyası tespiti.	73
Şekil 5.1 :	Adli bilişim veri kaynakları [96].	76
Şekil 5.2 :	Paralel veri kopyalama [46].	77
Şekil 5.3 :	Windows çalıştırılabilir dosyası (.exe) dosya imza örneği.	78
Şekil 5.4 :	Autopsy ile dosya imzası değiştirilmiş dosyanın filtrelenmesi.	79
Şekil 5.5 :	Magnet axiom ile dosya imzası değiştirilmiş dosyanın filtrelenmesi.	80
Şekil 5.6 :	Zaman damgalarında modifikasyon yapılmış dosya.	82
Şekil 5.7 :	Bir dosya için \$standart_info ve \$file_name öznitelikleri altındaki zaman damgalarının karşılaştırılması.	83
Şekil 5.8 :	NTFS dosya sistemi günlüğü (USN journal) içerisinde timestomp kayıtları.	84
Şekil 5.9 :	Rasgele BIOS saati ayarlanması durumunda log dosyalarının incelenmesi.	85
Şekil 5.10 :	Kısıtlanmış klasör adı kullanılmasına ait hata bildirimi.....	86
Şekil 5.11 :	Kısıtlanmış dosya adlı dosyanın açılması.	87
Şekil 5.12 :	ASCII simgelerle yazılan metinde arama işlemi.....	88
Şekil 5.13 :	MS Windows işletim sisteminde faaliyet zaman damgasını devre dışı bırakma ayarı.....	91
Şekil 5.14 :	MS Windows işletim sisteminde en son açılan programları göstermeme.	92
Şekil 5.15 :	MS Windows işletim sisteminde son erişim bilgilerini devre dışı bırakma.	92
Şekil 5.16 :	MS Windows işletim sisteminde USB cihaz kayıtlarını devre dışı bırakma.	93
Şekil 5.17 :	MS Windows işletim sisteminde sistem korumayı kapatma.	94
Şekil 5.18 :	MS Windows işletim sisteminde hata bildirimini devre dışı bırakma.	95
Şekil 5.19 :	CCleaner üçüncü parti yazılımı ile kayıt temizleme.	96
Şekil 5.20 :	Hata ayıklama bilgisi yazımının devre dışı bırakılması.	97
Şekil 5.21 :	Windows 10 olay günlüğünü temizleme işlemi.	98
Şekil 5.22 :	Windows 10 olay günlüğü hizmetini devre dışı bırakma.	98

ADLI BİLİŞİM ATLATMA TEKNİKLERİ VE KARŞI TEDBİRLER

ÖZET

Bilgi teknolojileri (BT), insanoğlunun yaşam biçimini önemli derecede değiştirmiştir. Özellikle 21'inci yüzyıl BT'nin yükselme dönemi olarak tarihe geçmiştir. BT ve dijital haberleşme yaşam standartlarını yükseltmiş, bilgiye ulaşmayı kolaylaştırmıştır. Bunun yanında BT ve dijital haberleşmedeki gelişmeler saldırganlara da suç işlemede yeni yöntemler sunmuştur. Kimlik hırsızlığı, çevrimiçi bilgisayar korsanlığı (hacking), siber terörizm siber suç olarak adlandırılan bu yöntemlerden bazılarıdır. Ayrıca siber suçlar milli güvenliği ve ekonomiyi tehdit etmektedir.

Suçların siber alana taşınmasıyla birlikte, suçun ispatı için delillerin bilimsel ve teknik yöntemlerle toplanması, incelemenin yapılması ve bulguların adli birimlere sunulmasına yönelik yeni bir disiplin oluşturulmasına gerek duyulmuştur. "Adli Bilişim" olarak adlandırılan bu disiplin, elektro-optik ve manyetik ortamlarda tutulmakta olan veya bu ortamlar arasında iletilen veri, bilgi, görüntü, ses ya da bunların bütününden oluşan her türlü bilişim nesnesinin, mahkemede sayısal delil özelliği taşıyacak şekilde tanımlanması, elde edilmesi, muhafazası, incelenmesi ve mahkemelere sunulması çalışmalarının bütünü olarak tanımlanmakta ve ele alınmaktadır.

Adli bilişim uzmanları, bir bilgisayardan kullanıcısına ait istihbarat elde edilmesi, silinen dijital verilerin kurtarılması, saldırganların faaliyetlerinin incelenmesi için "Adli Bilişim Araçları (ABA)"ndan faydalanmaktadır. Suçluların olay yerindeki delilleri yok etmeye çalıştıkları gibi, siber suçlular da dijital verilerin toplanmasında ve analizinde bilişim uzmanının veya ABA'ların çalışmalarına engel olan, aranan bilgiyi gizleyen, sahte delil ile masum üçüncü kişileri suçlu çıkartan bazı teknikler ve yöntemler kullanılmaktadırlar.

Adli Bilişim Atlatma Teknikleri (ABAT) ve araçları son dönemde ilgi çekici bir alan olmuştur. Adli bilişim süreçleri ve ABA'ların çalışma yöntemleri suçlular tarafından da bilinmekte ve karşı yöntemler geliştirilmektedir. Bu yöntemlerin bir kısmı, suç unsuru olan verinin tamamen yok edilmesine yönelik işlemleri içerirken, bir kısmı verinin şifrelenmesi veya gizlenmesine, bir kısmı da bilişim uzmanlarının ve ABA'ların aldatılmasına yönelik teknikleri içermektedir. Klasik ABAT'lar sabit disk üzerine yazma (disk overwrite), sürücülere fiziksel zarar verme veya şifreleme gibi verinin geri döndürülemeyeceği ya da geri döndürülmesinin çok uzun zaman alacağı yöntemlerden oluşmaktadır. Yeni gelişen ABAT'lar ise klasik yöntemlerin dışında, verilerin gizlenmesi, belgelere ait üst (metadata) verilerinde değişiklik yapma, belgelerin oluşturulma, değiştirilme ve erişim zamanlarında değişiklik yapma, belgelerin başlık bilgisini değiştirerek farklı tipte belge gibi davranmasını sağlama, belgelerin özet bilgisini (hash) çakıştırarak zararlı belgenin gizlenmesi, standart olmayan RAID yapısının kullanılması gibi, daha sık kullanılan, inceleme süresini uzatan, bilginin toplanmasını zorlaştıran yöntemleri içermektedir.

Bu tez çalışmasında, öncelikle adli bilişim uzmanları (ABU), bilirkişiler ve bilgi güvenliği uzmanları için, adli bilişim süreçlerini atlatma, ABA'ları aldatma, ABA'lara yönelik saldırılar, klasik ABAT'lar ve günümüzde kullanılan modern ABAT'lar ele alınmıştır. ABAT'ların nasıl yapıldıkları, hangi adli bilişim süreçlerini hedef aldıkları, ABAT'ların tespiti ve bu tekniklere karşı alınabilecek önlemler hakkında bilgi verilmiştir. ABAT'lar, kullanım amaçlarına göre belirli bir sınıflandırma altında incelenmiştir. Genel olarak, yaygın kullanımı nedeniyle Microsoft Windows işletim sistemi esas hedef olarak ele alınmıştır. Çok basit teknikler kullanılarak dahi, bir adli bilişim incelemesinin ne kadar karmaşık bir hal alabileceği bu çalışma içerisinde ortaya konulmaya çalışılmış ve bu tekniklere karşı dikkat edilecek hususlar ile alınabilecek tedbirlere ait bilgilere yer verilmiştir.



ANTI FORENSICS TECHNIQUES AND COUNTERMEASURES

SUMMARY

Information technology (IT), has significantly changed human lifestyle. Especially 21st century has been a rising period in the history of IT. IT and digital communications have raised living standards and have facilitated access to information. However, digital communications have provided criminals a newer way to commit crime. Amongst digital crime (cyber-crime) is the combination of wide range of crimes, such as identity theft, online piracy, hacking, and terrorism. Furthermore, cyber crime poses a threat to national security and the economy.

With the shifting of crimes to the cyber space, it has been necessary to establish a new discipline which covers gathering evidences scientifically and technically as a proof of a crime, analysing evidences and presenting findings to the judicial units or law enforcement agencies. This discipline, which is called as "Digital Forensics", is defined as combination of efforts of identifying, obtaining, capturing, analysing data, information, image, sound or an informatics object that is combination of all these as digital evidences which are kept in or transferred through electro-optical and magnetic medium and presenting them to the courts.

Forensics experts benefit from "Computer Forensic Tools" (CFT) to obtain intelligence from a computer, to recover deleted digital data, and to investigate the activities of attackers. Just as criminals are trying to remove evidences at the physical crime-scene, cyber-criminals also use some techniques and methods which cause disrupting CFTs and forensics experts at the phase of collecting and analysing of digital evidences, hiding suspicious data, incriminating innocent third parties by planting fake evidences into digital media.

The Anti-Forensics Techniques (AFT) and its tools have recently become an area of interest. Computer Forensics processes and CFT's working methods are also known to criminals and counter-methods are being developed by them. Some of these methods include procedures for the complete destruction of the data which is suspected as crime element, some of which are ciphering or concealing the data, and some of which are techniques for deceiving computer experts and CFTs. Classic AFTs consist of methods such as overwriting the hard disk, physically damaging the disk drives or encrypting which causes data not to be recovered or require a long time to be recovered. Newly developed AFTs, contrary to classical methods, include frequently used methods, which prolong analysis time, complicate gathering of digital evidences such as using data hiding techniques, changing metadata of documents, manipulating timestamps of a document's modified, access, change and entry times, making a file type seem like another file type by changing document header information, hiding malicious data by colliding its hash info with a good known file's hash and applying non-standard RAID types.

In this thesis study, it is dealt with describing countering digital forensics processes, deceiving CFTs, attacks targeting bugs of CFTs, classical AFTs and modern AFTs used frequently today for primarily digital forensics investigators, valuers and information security specialists. It is aimed to provide information about how AFTs are being implemented and which digital forensics process is targeted by AFTs and how to detect AFTs used and countermeasures against AFTs. AFTs have been studied under a specific classification for their intended use. In general, as it is widely used, the Microsoft Windows operating system is considered as the main target. It is shown in this study how complex a forensic examination can be, even using very simple techniques and the information on considerations against these techniques with the precautions are included.



1. GİRİŞ

Dijital ortamlar, mobilitedeki gelişmeler, bilgiye hızlı ve devamlı ulaşım ihtiyacı ve nesnelerin interneti teknolojilerindeki gelişmeler nedeniyle insan hayatının her aşamasında kendilerine yer bulmuşlardır. Bu durum kullanıcılara büyük kolaylıklar ve hizmetler sağlamaktadır. Veritabanı sistemlerinin, sanallaştırma teknolojilerinin ve dağıtılmış sistemlerin iş ve günlük hayata uygulanması birçok hizmete erişimi kolaylaştırmıştır. Türkiye İstatistik Kurumu 2017 (18 Ağustos 2017) Hanehalkı Bilişim Teknolojileri Kullanım Araştırması'na göre internet kullanan bireylerin oranı %66,8, her on haneden sekizinde internet erişimi mevcut ve hanelerin %97,8'inde cep telefonu kullanılmaktadır. Kullanım amaçlarının başında da sosyal medyanın ilk sırada olduğu, her dört kişiden birinin de internetten alışveriş yaptığı belirtilmektedir.

Günümüzde bu kadar yaygınlaşmış olan dijital ortamlar, suçlular tarafından da aktif olarak kullanılmaktadır. Dijital ortamların gerek vasıta olduğu gerekse hedef olarak saldırıya maruz kaldığı suçlarda da her geçen gün artış kaydedilmektedir. Ülkemizde bilişim suç dosyalarındaki artış Şekil 1.1'de görüldüğü üzere, bilişim teknolojilerine erişimin kolaylaşması ile doğru orantılı olarak artış göstermiştir [1]. Bunun dışında, bilişim suçu içermeyen fakat adli bilişim desteğiyle suçlunun tespitinin sağlandığı diğer suçlar da göz önüne alındığında, adli bilişimin ne derece önemli bir bilim dalı olduğu ortaya konmaktadır. Adli bilişim bilimsel bir faaliyet olduğundan, tüm dünyada geçerliliği kabul gören belirli süreçlerden oluşmaktadır. Bu süreçler uygulanırken adli bilişim uzmanları çeşitli adli bilişim araçları kullanmaktadırlar. Bu süreçleri ve kullanılan adli bilişim araçlarının çalışma prensiplerini bilen suçlular da, tespit edilmelerini imkansız hale getirmek maksadıyla, bazı teknikler geliştirerek adli bilişimi yanıltmaya, izlerin yok edilmesine ve bu suretle suçun ispatının engellenmesine yönelik çabalar göstermektedirler. Bu yöntemlerin adli bilişim uzmanlarınca bilinmesi ve tespiti, delillerin geçerliliği açısından önem arz etmektedir.

<i>Suçun Nevi Ve Yıllara Göre Olay Sayıları</i>	<i>Kredi Kartı Sahteciliği ve Dolandırıcılığı</i>	<i>Banka Dolandırıcılığı</i>	<i>Bilişim Suçları ve Dolandırıcılığı</i>	<i>İnternet Aracılığıyla Dolandırıcılık</i>	<i>Diğer</i>	<i>Toplam</i>
<i>Olay Sayısı 2003</i>	80	15	X	X	X	95
<i>Olay Sayısı 2004</i>	146	22	16	X	X	184
<i>Olay Sayısı 2005</i>	195	9	91	X	X	295
<i>Olay Sayısı 2006</i>	122	98	4	X	X	224
<i>Olay Sayısı 2007</i>	594	642	416	X	91	1.743
<i>Olay Sayısı 2008</i>	830	1.177	560	X	157	2.742
<i>Olay Sayısı 2009</i>	1.511	550	353	412	45	2.871
<i>Olay Sayısı 2010</i>	1.131	151	972	71	28	2.353
<i>Olay Sayısı 2011</i>	1.772	141	1.738	111	31	3.793
<i>Olay Sayısı 2012</i>	1.724	264	3.669	278	783	6.718

Şekil 1.1: Türkiye’de 2003-2012 yılları arasında bilişim suçu istatistikleri.

Bu bölümde tez çalışmasının kapsamına ilişkin temel bilgilere yer verilmekte, çalışmanın amacı ve tezin organizasyonu genel hatlarıyla sunulmaktadır.

1.1 Arka Plan ve Motivasyon

İnsanoğlunun yaşam biçimi, BT’nin gelişimi ile birlikte hızlı bir değişim geçirmiştir. BT ve dijital haberleşme yaşam standartlarını üst seviyelere taşımış [2], bilgiye ulaşmayı kolaylaştırmıştır. Dijital haberleşmenin sağladığı bu kolaylık, suçlulara da suçlarını dijital ortama kaydırma fırsatı tanımıştır. Dijital ortamda işlenen suçlar, siber suçlar olarak adlandırılmış ve suçun ispatı için gerekli delillerin toplanmasına ve işlenmesi sürecine yönelik yeni bir disipline ihtiyaç duyulmuştur. Elektro-optik ve manyetik ortamlarda tutulmakta olan veya bu ortamlar arasında iletilen veri, bilgi, görüntü, ses ya da bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemelerde sayısal delil özelliği taşıyacak biçimde tanımlanması, elde edilmesi, muhafazası, incelenmesi ve mahkemelere sunulması çalışmalarının bütünü olarak tanımlanan "Adli Bilişim (AB)" [3], bu nedenle ortaya çıkmıştır. Adında adli olduğu belirtilse de, bu uzmanlık alanı sadece adli veya idari bir vaka için değil, bir çalışanın şirket bilgisayarında neler yaptığını incelemek isteyen bir firmanın da başvurabileceği bir bilim dalı olarak karşımıza çıkmaktadır.

Bir siber güvenlik alanı olan AB, gerek ülkemizde gerekse yurt dışında henüz gelişimini tamamlamış bir disiplin değildir [4]. AB kapsamında el konulmuş olan

elektronik cihazların ve ortamların, hukuka uygun şekilde incelenmesi, delillerin değiştirilmeden toplandığının ve mahkemelere sunulduğunun ispatının sağlanması, dijital delilin geçerli sayılması açısından önem arz etmektedir. Bilimsel bir çalışma alanı olan AB, tüm dünyada geçerliliğe sahip olabilmek için belirli süreç ve yöntemlerden oluşmaktadır. Bu süreç ve yöntemler bilişim suçluları tarafından da bilinmekte, AB süreç ve yöntemlerini aldatmaya ve atlatmaya yönelik teknikler geliştirilmektedir.

Suçluların yakalanmamak için olay yerindeki delilleri yok ettiği gibi, bilişim suçluları da sayısal delilin ortadan kaldırılması veya masum başka bir şahısa zarar verecek şekilde değiştirilmesi gibi amaçlar güderek adli bilişimi atlatma tekniklerini ve araçlarını etkin bir şekilde kullanmaktadır. Adli bilişimi aldatma tekniklerinin neler olduğu, sınıflandırılması, hangi adli bilişim süreçlerini hedef aldıkları, kullanımının tespiti ve karşı önlemlerin bilinmesi, adli bilişim uzmanları (ABU) ve bilgi güvenliği uzmanları (BGU) tarafından soruşturmaların sağlıklı bir şekilde yürütülmesi bakımından önemli bir gerekliliktir.

Bilimsel bir yöntem olarak ortaya çıkmasına rağmen, adli bilişim konusunda yeterli seviyede akademik çalışma mevcut olmadığı, Çizelge 1.1'de verilen istatistiksel veriler ışığında, görülmektedir. Çizelge 1.1 ile ilgili detaylı açıklama tezin amacı alt başlığında yer almaktadır. Özellikle ülkemizde adli bilişim konusunda akademik çalışma (tez, makale, bildiri vb.) sayısı oldukça düşüktür. Adli bilişime yönelik tehditler ve saldırılar konusunda bilgi veren genel bir çalışma bulunmamaktadır. ABU ve BGU'na kaynak olabilecek, günümüz tehditlerinin ve güvenli delilin elde edilmesinde yaşanabilecek problemlerin incelenerek ABU ve BGU'nın gelişimlerine katkı sağlayacak çalışmalara ihtiyaç olduğu değerlendirilmektedir.

1.2 Tezin Amacı

Adli bilişimi atlatma, yakın geçmişte meşru bir çalışma alanı olarak tanınmıştır. Bu nedenle ilgi çekici bir alan olarak düşünülmektedir. Yeni bir çalışma alanı olması sebebiyle, adli bilişimi atlatma teknikleri hakkında yeterli seviyede çalışma mevcut değildir. Çizelge 1.1 birinci satırda "Google Akademik" web sitesinde "Computer Forensics" ve "Digital Forensics" aramaları yapılarak bulunan sonuç sayılarının toplamı ile "anti-forensic" araması ile bulunan sonuç sayısının oranı verilmiştir. İkinci

Çizelge 1.1: Adli bilişim atlatma konulu akademik çalışmalar istatistik bilgileri.

	Forensic (F) (Computer+Digital)	Anti-Forensic (AF)	Oran (AF/F)
Google Akademik [5]	38000	1970	%5,1
Ulusal Tez Merkezi [6]	32	2	%6

satırda ise "Ulusal Tez Merkezi" web sitesinde aynı aramalara ait sonuç sayısı ile "anti-forensic" araması sonuç sayısı oranı verilmiştir.

Bu verilerden de anlaşılacağı üzere ülkemizde adli bilişimi atlatmaya yönelik tekniklerin ve tehlikelerin ele alındığı çalışmaların sayısı yetersiz kalmaktadır. Ülkemizde 2006 yılından sonra, adli bilişime olan ilgi artmaya başlamış ve bunun sonucu olarak akademik çalışmalara da önem vermeye başlanmıştır. Bu kapsamda Polis Akademisi, Gazi Üniversitesi ve Fırat Üniversitesi'nde adli bilişime özel eğitimler vermeye başlanmış, yüksek lisans ve doktora programları uygulamaya konmuştur [7]. Buna rağmen akademik çalışmalar ve bu çalışmalara gösterilen ilgi yeterli bir seviyeye ulaşamamıştır.

Bu verilerden hareketle, bu tez çalışmasında adli bilişim atlatma olarak adlandırılan AF'nin tanımı, amacı, sınıflandırılması ve bu sınıflandırma çerçevesinde AFT'lerin nasıl yapıldıkları, yapıldığının nasıl tespit edileceği ve alınabilecek önlemler hakkında bilgilere yer verilmiştir. Bu çalışma ile ABU ve BGU'nın gelişimine katkıda bulunmak, üzerinde çalıştıkları olaylarda mahkemelere adli bilişime konu olan delili sunmadan önce nelere dikkat etmeleri gerektiğini vurgulamak, ABA'ların zayıflıkları ve güçlü tarafları hakkında bilgi vererek kullanıcıda farkındalık yaratmak amaçlanmıştır.

1.3 Tez Organizasyonu

Bölüm 2'de, adli bilişim atlatma üzerine yapılmış olan ilgili çalışmalara ait bir literatür araştırması sunulmuştur. İlgili çalışmalardan bazıları, adli bilişimi atlatma (AF) için resmi bir tanım sağlamak amacı güderken, bir kısmı tanımlamanın yanı sıra ABAT (AFT)'lerin kategorizasyonu üzerine çalışmış, bir kısmı da ABAT kullanımının tespitine yönelik çalışmalar olarak literatüre geçmiştir.

Bölüm 3’te, adli bilişimin tanımlanması, adli bilişim süreçleri ve bilişim suçlarına ait delillerin özelliklerine yer verilmiştir. Adli bilişim, incelediği alanlara göre türlere ayrılmıştır. Bu bölümde bu türlerin neler olduğu ve hangi konuları inceledikleri ele alınmıştır.

Bölüm 4’te, AF tanımı yapılarak, klasik ABAT’lar hakkında bilgi verilmiştir. Klasik ABAT’lar suç unsuru olan verinin ortadan kaldırılmasını veya ulaşılsa bile okunamayacak hale dönüştürülmesini hedefleyen teknikleri içermektedir. Bu nedenle günümüzde kullanımı çok fazla tercih edilen bir yöntem değildir.

Bölüm 5’te, günümüz modern ABAT’ları incelenmiştir. Modern ABAT’ların nasıl yapıldıkları, ne amaçla yapıldıkları, hangi adli bilişim süreçlerini hedef aldıkları, kullanımının nasıl tespit edilebileceği ve bu tekniklere karşı alınabilecek önlemler hakkında bilgi verilmiştir.

Bölüm 6 sonuç bölümü olarak ele alınmış, çalışmada anlatılan teknikler ile karşı tedbirlere ait özet bilgi içeren çizelge eklenerek (Çizelge 6.1), ABAT’ların kullanımının adli bilişim açısından nasıl sonuçlar doğurabileceği üzerine değerlendirmelere yer verilmiştir.



2. LİTERATÜR ARAŞTIRMASI

Adli bilişimi atlatma (AF) ve ABAT üzerine günümüze kadar yapılmış olan çalışmaların bir bölümü AF'nin tanımlanmasına yönelik iken, başka bir bölümü AF'yi bir problem sahası olarak ele almıştır. Bir başka bölümde ise AF'nin sınıflandırılması ve özelliklerinin belirlenmesine yönelik çalışmalar yapılmıştır. Bunun yanı sıra AF araçlarının kullanımına ait belirtilere ve tespitine yönelik çalışmalar da mevcuttur. Bu bölümde ele alınacak literatür araştırmaları kapsamlarına ve hedeflerine göre sınıflandırılarak açıklanmıştır.

2.1 AF Tanımlanmasına Yönelik Çalışmalar

AF, siber suçları inceleme ekipleri ve akademisyenler arasında ilgi çeken bir alan olarak ortaya çıkmıştır. Fakat hala genel bir geçerliliği bulunan resmi bir tanımlama mevcut değildir [8]. Ortak bir tanımlama bilimsel alanda incelenen konular için genel bir gerekliliktir. AF açısından genel, ortak bir tanımlama yapmanın zorluğu, sürekli değişen teknoloji nedeniyle ABAT'ların ve bu amaçla kullanılan araçların yenilenmesi, imkan ve kabiliyetlerinin artması, hedefledikleri etkinin büyümesinden kaynaklanmaktadır. Bu nedenle geçmişten günümüze yapılan tanımlamalar da tarih sıralamasına göre daha da karmaşık bir hal almıştır. Çizelge 2.1'de zamana göre sıralanmış, farklı yazarlara ait çalışmalardan elde edilmiş tanımlamalara yer verilmiştir.

2.2 Bir Problem Olarak AF

AF'yi bir problem olarak ele alan çalışmalar, AF tekniklerinin nasıl yapıldığından veya tespit edilebildiğinden daha çok, kullanımının bir adli bilişim soruşturmasında yol açabileceği sıkıntılardan söz etmektedir. Bu alanda yapılan çalışmaların bir kısmı AF'yi bir bütün şeklinde tek bir çalışma alanı olarak ele almaktadır. Diğer bir kısmı ise AF'nin alt alanlarını ele alan çalışmalar olarak göze çarpmaktadır.

Çizelge 2.1: AF tanımları.

Yazarlar	Adli Bilişim Atlatma Tanımları
Shirani [9]	Bir sistem sızmasını saklama girişimi.
Peron, Legary [10]	Elektronik verilerin tanımlanması, toplanması, geçerliliğinin sınırlandırılması girişimi.
Grugq [11]	Adli kanıt miktarını ve kalitesini sınırlamaya çalışmak.
Foster, Liu [12]	ABA'ları kırma veya tespit edilmekten sakınma çabaları.
Liu, Brown [13]	Adli inceleme için olgusal bilgileri geçersiz kılmak için bilimsel yöntemin sayısal medyaya uygulanması.
Harris [14]	Adli bilişim sürecine delillerin kullanılabilirliğini veya yararlılığını tehlikeye atmaya yönelik herhangi bir girişim.
Kessler [15]	Adli analizi engelleyen araçlar, yöntemler ve süreçler seti.
Garfinkel [16]	ABA'ları, soruşturmaları ve soruşturmacıları engelleyen giderek artan araçlar ve teknikler topluluğu.
Sremack, Antonov [17]	Uygun adli bilişim soruşturmasını engelleme uygulaması.
Stamm [18]	Bir dijital dosya oluşumunda dosyaya ait verilerde manipulasyon yapıldığı izlerini gizleme çabaları.

Thuen [19]'da, bilgisayar güvenliğinin adli bilişim açısından incelendiği ve adli bilişimi atlatmaya yönelik yöntemler ve alt dalların ele alındığı bir araştırma ortaya koymuştur. Yazara göre, ABAT'lara aşına olmayan bir adli bilişim uzmanı, soruşturmanın güvenliğini ve güvenilirliğini tehlikeye atmaktadır. En kötü senaryo olarak da soruşturmacının, bilmeden bir programı veya cihazı tetikleme ile suçun ispatında kullanılacak olan delilin ortadan kaldırılmasına sebep olabileceği vurgulanmıştır. Teknoloji ve bilgisayar kullanımını içeren suçlar ve siber suçların sayısı arttıkça, adli bilişime ve AF'yi anlamaya daha büyük bir ihtiyaç duyulacağı öngörülmüştür. Sırasıyla olay yerindeki bilişim cihazlarına güvenli bir şekilde el konulması ve güvenli bir şekilde olay yerinin emniyet altına alınması sağlanmaz ise AF'nin bu aşamada soruşturma için yıkıcı bir etki yaratacağı belirtilmiştir. Sabit disklerin yanı sıra hafızadaki elektrik gücüne bağlı verilere ve bilgilere de ihtiyaç olabileceği, bu nedenle geçici hafızanın da cihazlar kapatılmadan bir kopyasının alınmasının önemine dikkat çekilmiştir. Disklerin ve hafızaların kopyalanmasının bit bazlı yapılmasını, bu sayede diskteki boş veya kullanım dışı alanlarda suça ilişkin veri olup olmadığının incelenebileceği önerilmiştir. Yapılacak çalışmaların el konulan orijinal cihazda değil, bir kopyası üzerinde yapılmasının delilin geçerliliği açısından çok önemli bir yere sahip olduğu belirtilmiştir. Bunun yanında veri gizleme tekniklerinin, steganografi ve kriptolama yöntemlerinin kullanılmasının

elde edilen verilerin bulunmasını veya okunmasını zorlaştırdığı vurgulanmıştır. ABA'ların açıklıklarından ve zayıflıklarından faydalanarak, delilin geçerliliğini bozucu, ABA'ların hizmet dışı (DoS) kalmasını sağlayıcı ve belge işlemlerinde yanıltıcı yöntemlerin de, AF içerisinde değerlendirilmesi gerektiği söylenmiştir. Artık en basit ev kullanıcısının bile, bilgisayarındaki bir belgenin sil komutuyla kolayca silinmediğini bildiğini, bu nedenle başarılı bir adli bilişim soruşturması için ABU ve BGU'lar için ABAT'ların bilinmesinin artık bir zorunluluk olduğu sonuç bölümünde vurgulanmıştır.

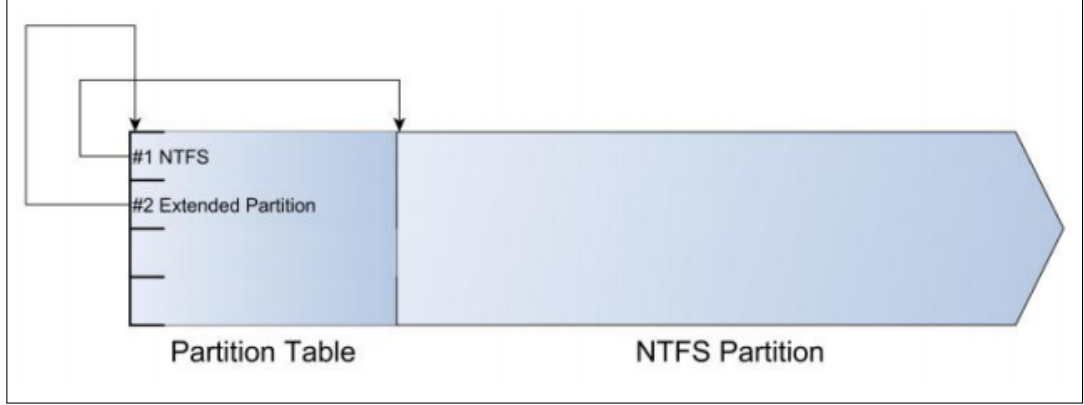
Pajek ve Pimenidis [20]'de, adli bilişim soruşturmasının her bir adımında AF tekniklerinin kullanımının, soruşturmanın çok pahalıya mal olmasına ve istenilen makul bir süre içerisinde tamamlanamamasına sebep olduğu belirtilmiştir. Çalışma, AF problemine teorik ve uygulamalı bir şekilde yaklaşmıştır. Çalışmanın asıl amacının ABAT'ların sadece tanımlanması değil, aynı zamanda ABA'lara karşı etkinliklerinin ve performansının test edilmesi olduğu vurgulanmıştır. Adli bilişim soruşturması süreçlerinin, her bir adımına özel ABAT'ların kullanıldığı bildirilerek tanımlamalarına yer verilmiştir. AB soruşturması birinci basamağında kullanılan ABAT, kaynağın yok edilmesi (EoS) yöntemidir. Bu tekniğin en kolay yöntemi, bilgisayar ayarlarının ve kayıt defteri verilerinin değiştirilmesi ve bu sayede işletim sisteminin (OS) kullanıcının aktivitelerini kayıt altına almasının engellenmesidir. Buna örnek olarak grup politikalarında (GP) yapılacak bir değişiklik ile tarayıcının kullanıcının gezindiği web sitelerine ait geçmiş bilgilerini tutmaması verilebilir. Diğer bir yöntem, kayıt ve disk temizlemedir. Güvenilir silme yapan bir araç ile HDD üzerinde hiç bir bilgi kırıntısı (MFT kayıtları, log belgeleri vb.) kalmayacak şekilde silme yapılabilir. İkinci basamakta, daha çok veri gizleme yöntemlerinin kullanıldığı belirtilmiştir. Bu bölüm, inceleme yapan kişinin elindeki kopyaları incelemeye başladığı, belgelerden çıkarım yaptığı bölümdür. İlk bölümdeki gibi verinin yok edilmesi değil, değişik yöntemlerle saklanması hedeflenmektedir. Kullanılan yöntemlerin başlıcaları, belge başlık bilgisi ile oynamak, veriyi HDD içinde OS tarafından kullanılmayan alanlarda (Slack Space) saklamak, stegonografi ve kriptoloji yöntemleridir. Üçüncü basamakta, ABA'ları hedef alan ataklar, en çok kullanılan ABAT'lar arasındadır. Bu bölümdeki ABAT'lar arasında belgelerin zaman damgasını değiştirme ve bu sayede suçun

işlendiği düşünülen zamana ait belgelerin tespitini zorlaştırma ile belge özet bilgisi çakıştırma (Hash Collision) yöntemleri yer almaktadır.

Kessler [15]'de, AF'nin tanımlamasını geniş bir perspektiften ele almıştır. ABAT'lar kategorilere ayrılarak incelenmiştir. Buna göre ana kategoriler, veri gizleme (data hiding), derin silme (artefact wiping), iz karartma (trail obfuscation) ve ABA'lara yapılan saldırılardır. ABAT'ları ayrı ayrı ilgili kategoriler altında sınıflandırmıştır. Veri gizleme kategorisinde, steganografi, ağ iletişimde gizli kanalların kullanılması, HDD üzerindeki tahsis edilmemiş (unallocated) bölgelere ve boş yerlere (slack spaces) veri yazılması ve belgelere ait metadata alanlarına veri yazılması yöntemleri bulunmaktadır. Derin silme kategorisi, BC Wipe, Eraser ve PGP Wipe gibi araçlar ile HDD üzerine yazarak verilerin kurtarılamayacak hale getirilmesi, tarayıcı ve işletim sistemlerine ait geçici dosyaların silinmesi yöntemlerini içermektedir. İz karartma kategorisinde ise, ağ incelemesine dayalı adli bilişim soruşturmasını engellemek amacıyla yapılan IP aldatması (IP Spoofing), onion routing, elektronik posta başlık bilgisi değiştirilerek SMTP aldatma, SSH kullanma, log belgelerinde değişiklik yapma veya silme, sistem olay belgelerinde değişiklik yapma veya silme, belgelere ait zaman damgalarını değiştirme yöntemlerinin bulunduğu belirtilmiştir. ABA'lara yönelik saldırılar kategorisinde, belgelere ait başlık bilgilerinde değişiklik yaparak ABA'nın filtrelemesinde belgeyi farklı bir belge türü olarak gösterme, ABA'ların bellek taşması vb. saldırılara açık olması ve diğer zayıflıkları ile açıklıklarından faydalanılması yöntemleri yer almaktadır.

Wundram, Freiling ve Moch [21]'de, ABA'ların test edilmesinde, ABAT'ların göz önüne alınmasını vurgulamıştır. ABA'ların test edilmesinin, ABA'ların adli bilişim soruşturmasında geçerli sonuçlar üretip üretmediğinin tespiti için gerekli olduğu belirtilmiştir. Adli bilişimin bir disiplin olarak ortaya çıkmasından sonra, AF'nin de ABA'ları aldatmaya yönelik araçları ortaya çıkmıştır. Steganografi ve kriptoloji bilinen ilk geleneksel ABAT'lardandır. Disk üzerine yazma (overwrite) diğer bir geleneksel yöntem olarak kullanılmaktadır. Modern tekniklerin ise, canlı CD kullanmak, sanal makine kullanımı, ABA açıklıklarından faydalanmak gibi yöntemleri içerdiği belirtilmiştir. Çalışmada basit bir kod enjeksiyonu saldırısı ile ABA'nın ürettiği HTML türü raporlar hedef alınmıştır. Şekil 2.1'de görüldüğü gibi, USB bellek bir NTFS bölümü (partition) ve başlangıç olarak NTFS bölümünü referans eden genişletilmiş

bölümleme (extended partition) hazırlanmak suretiyle bir döngü oluşturularak işletim sistemleri ve bazı ABA'lar DoS saldırısına yönelik test edilmiştir.



Şekil 2.1: Wundram, Freiling ve Moch, [21] partition table loop örneği.

Sonuç olarak, yazarlar hem kullanıcı hem de ABA geliştiricileri perspektifinden, ABA'lara yapılan saldırılara karşı alınabilecek önlemler hakkında önerilerde bulunmuşlardır. Akademik kurullarca, ABA'ların test senaryolarının belirlenmesi ve AF hakkında bilimsel çalışmalara yer verilmesi tavsiye edilmiştir.

Anobah, Saleem ve Popov [22]'de, Wundram ve arkadaşlarının çalışmalarının benzerini mobil cihazların adli bilişim incelemeleri için yapmışlar ve mobil cihazların adli bilişim araçları ile incelenmesine yönelik bir test platformu önermişlerdir.

Böhme ve Kirchner [23]'de, AF'nin tanımlanmasına yönelik bir çerçeve çalışmasını ele almışlardır. Resim dosyalarına ait adli bilişim analizlerini ve bu alanda yapılan ABAT'ları teknik seviyede, formüllerle anlatarak teorik bir çalışma ortaya koymuşlardır. Multimedya güvenliğini değişik perspektiflerden ele almışlardır.

Sremack ve Antonov [17]'de, eğer AF başarılı bir şekilde uygulanırsa, dijital delilin Daubert standartlarını karşılamayacağı belirtilmiştir. Kısacası delilin mahkemedeki geçerliliği şüpheli konuma geçecektir. AF sınıflandırılmasına yönelik bu çalışmada, ABAT'lar iki ana sınıfa ayrılmıştır. Bunlardan birincisi direkt olarak dijital delili hedef alan ABAT'lar, diğeri ise adli bilişim süreçlerinin kabul edilebilirliğine yönelik uygulanan ABAT'lardır. İlk sınıfa giren yöntemler, veri muhafazası, veri sahteciliği, veri gizleme ve veri yok etme teknikleridir. İkinci sınıftaki yöntemler ise, delil hakkında yeterli şüphe oluşturma, yargı yetkisi dışına çıkıldığını ispatlama, özel hayatın gizliliğinin ihlal edildiğini vurgulama, AB süreçlerine yönelik şüphe

oluşturmaktır. Ayrıca davalara yönelik iç davalar, sivil davalar ve suç davaları olarak bir sınıflama da çalışma içerisinde mevcuttur.

Brand [24]'de, zararlı yazılım kullanarak yapılan ABAT'ların gün geçtikçe daha karmaşık bir yapıya büründüğüne dikkat çekmiştir. Adli bilişim analizinden kaçınmak için zararlı yazılımın kullanabileceği vurgulanmıştır. Bu anlamda kullanılabilecek teknikler arasında, ABA'ların açıklarından faydalanma, ABA'ların kullanıldığı sistemi çalışamaz hale getirme gibi yöntemlerin varlığından söz edilmiştir. Kullanılan ABAT'lar arasında karartma (obfuscation), anti-disassembly, kriptolama ve veri sıkıştırma (encryption and compressed data), veri yok etme (data destruction) ve karşı derleme (anti-debugging) yöntemleri çalışmada ele alınmıştır. Bu tarz zararlı yazılımların otomatik tespitine yönelik çalışmaların sürdüğü belirtilmiştir.

2.3 AF'nin Sınıflandırılması ve Özelliklerinin Belirlenmesine Yönelik Çalışmalar

Bu bölümde AF'nin tanımlanması, sınıflandırılması ve kullanılan AF araçlarının özelliklerini inceleyen ve konu alan çalışmalar araştırılmıştır.

Harris [14]'te AF'yi, adli bilişim süreçlerinde kullanılacak olan delilin erişilebilirliğini ve kullanılabilirliğini engellemek amacıyla yapılan her türlü girişim olarak tanımlamaktadır. AF'leri kullanım amaçlarına göre sınıflarken, kullanılan araçlar ve yazılımlardan da faydalanılmıştır. Buna göre çalışmada yapılan sınıflandırma, Çizelge 2.2'deki gibi AF araçları üzerinden yapılmıştır. AF'nin bir adli bilişim soruşturmasına etkisini azaltmak için, sırasıyla "insan faktörü" nün önemine değinilmiştir. Buradaki insan faktöründen kasıt, ABU ve BGU'ların ABAT'lar hakkındaki farkındalık durumları ve eğitim seviyeleridir. Bu farkındalığın ve eğitim seviyesinin geliştirilmesi için ABU ve BGU'lardan yıl içerisinde belirli kurslara katılmaları ve AF üzerine pratik uygulamalar içeren eğitimleri tamamlamaları tavsiye edilmiştir. AF'nin etkisini azaltabilecek bir diğer yöntem olarak, ABA'ların çeşitlendirilmesi önerisi verilmiştir. Bu yöntemin bütçe kısıtları nedeniyle uygulanmasının mümkün olmadığı durumlarda da, istenen konuya özel (multimedya özel, dosya özel vb.) etkinliği ispatlanmış olan yazılımın tercih edilmesinin faydalı olacağı belirtilmiştir.

Çizelge 2.2: Harris [14] AF sınıflandırması.

ABAT Adı	Yok Etme	Gizleme	Kaynağı Yok Etme	Aldatma
MACE Değiştirme	MACE bilgisi silinir			Yanlış yönlendirme amaçlı farklı bir tarih girilir
Dosya Silme	Dosyaların üzerine gereksiz veri yazılır	Dosya işaretçisi silinir, içerik tutulur		
Veri Kapsülleme		Dosya içinde dosya saklanır		
Oturum Hackleme				İşlem başkası tarafından yapılmış gibi gösterilir
Arşiv/İmaj Bombası				Analiz sürecini aldatma
Log Engelleme			Aktiviteler kayıt altına alınamaz	

Peron ve Legary [9]'da, AF'ye yönelik bir sınıflandırma yapmışlardır. Yaptıkları sınıflandırma AF'yi dört kategoriye ayırır. Bunlar, veriyi yok etme, veriyi gizleme, veriyi değiştirme ve delil olabilecek verinin üretilmesini engelleme yöntemleridir.

Rogers tarafından [25]'te AF, bir olay yerinde delillerin varlığını, miktarını ve kalitesini negatif olarak etkilemeye yönelik girişimler ile delilin incelenmesini zorlaştıran veya imkansız kılan çabalar olarak tanımlanmıştır. ABAT'lar, veri gizleme, izleri ve veriyi derin silme, iz karartma, ABA'lara yapılan saldırılar olmak üzere dört kategoride ele alınmıştır. Genel olarak AF için, bu sınıflandırma geçerlilik kazanmıştır. AF araştırmalarının desteklenmesi gerektiği vurgulanmıştır.

Garfinkel [16]'da AF'yi, adli bilişim araçlarını, soruşturmalarını ve soruşturmacıyı engellemek amacıyla kullanılan ve sayısı gün geçtikçe artan araçlar ve teknikler bütünü olarak tanımlamıştır. Liu ve Brown'ın [13]'de açıkladığı AF'nin kullanım amaçlarını Garfinkel da aynı şekilde almıştır. AF araştırmacılarının, geliştirmiş oldukları AF araçlarını internet ortamında ücretsiz bir şekilde sunduklarını, sunmalarının sebebi olarak da ABA'ların geliştirilmesini zorlamak olduğunu belirtmiştir. ABAT'ları geleneksel yöntemler, izleri minimize eden ABAT'lar, ABA'ların açıklıklarını kullanan

ABAT'lar, ABA'ların çalıştığını tespit edip kendini gizleyen ABAT'lar olarak dört kategoride ele almıştır. AF araçlarının klasik ABA'lar karşısındaki performansı hakkında bilgiler verilmiştir. Son kısımda ABAT'ların tespit edilmesi ve alınabilecek önlemler hakkında tavsiyelerde bulunulmuştur.

Smith [26]'da AF'yi, disklere yönelik incelemelerden kaçınmayı sağlayan yöntemler açısından incelemiştir. Yazar, Grugq'ın [11]'de AF'nin üç temel prensip olan veriyi yok etme, veriyi gizleme ve kontrollü verileme olarak çevirdiği (data contraception) yöntemler üzerine inşa edildiğini vurgulamaktadır. Disk incelemekten kaçınma araçlarının kullanılmasının, kontrollü verileme başlığı altında değerlendirilmesi gerektiği belirtilmiştir. Kontrollü verileme, adli bilişim açısından önem ve değer arz eden bir delilin disk dışında tutularak niteliğinin ve niceliğinin sınırlandırılmasına yönelik girişimler olarak tanımlanmıştır. Diskten kaçınma yöntemi, delil kaynağının yok edilmesi kapsamına girmektedir. Diskten kaçınma araçları sadece geçici bellek üzerinde çalışarak disk üzerinde bir iz bırakmamayı hedefler. Geçici bellek incelemesinin disk inceleme teknikleri kadar olgunlaşmış olmadığı ve kolayca güç kesintisi ile bellekteki verinin yok edilebileceği belirtilmiştir. Diskten kaçınma araçları syscall proxying, memory resident compiler/assemblers, remote library injection, direct kernel object manipulation (DKOM), LiveDistros sınıflandırması altında incelenmiştir.

Blunden [28]'de rootkit'lerin AF aracı olarak kullanılmasına yönelik bir çalışma ele almıştır. Kalıcı rootkit uygulamaları ile, bir disk imajı üzerinde çalışan bir ABU'nun engellenmesine yönelik uygulanabilecek AF yöntemleri üzerinde çalışılmıştır. AF ile mücadelenin bilinen tek bir yöntemi olmayacağını, bu nedenle savunma stratejisi olarak "derinliğine savunma" konseptinin benimsenmesinin gerektiği belirtilmiştir. Disk incelemesinde, HPA (Host Protected Area) ve DCO (Device Configuration Overlay) gibi sistem tarafından rezerve edilmiş bölümlerin de dikkatle incelenmesi gerektiği vurgulanmıştır. Dosya sistemi incelemesinde rootkitin, disk kriptolama, dosya sistem saldırıları ve dosya gizleme yöntemleri ile korunabileceği belirtilmiştir. Dosya gizlemenin HPA ve DCO gibi alanlar ile diskteki boş alanların (slack space) kullanımı ile başarılabileceğine dikkat çekilmiştir. Alanında yapılmış detaylı bir çalışma olarak karşımıza çıkmaktadır.

Bu bölümde son olarak ele alınan çalışma olarak Dahbur ve Mohammad [27]'de, AF'nin getirmiş olduğu mücadele alanlarının altını çizmiştir. AF mekanizmaları, araçları ve tekniklerinin neler olduğu, ABAT'ların sınıflandırılması ve ABAT'ların amaçlarını yerine getirip getirmediğinin kontrolü ile performansları hakkında genel bilgilere yer verilmiştir. AF uygulanmasına karşın alınabilecek tedbirlerin kısıtlı olduğu ve zor bir alan olduğu yazarlar tarafından belirtilmiştir. Bunun yanı sıra uygulanabilecek bir kısım önlemler ve gelecek çalışmaları hakkında da bilgilere yer verilmiştir.

2.4 AF Araçlarının Kullanımına Ait Belirtilere ve Tespitine Yönelik Çalışmalar

Bu bölümde yer alan çalışmalar ABAT'ların bir kısmına ait, kullanıldığına dair belirtileri ve bu belirtileri takiben tespitine yönelik çabaları ele almaktadır.

Geiger [29]'da, AF amaçlı kullanılan bazı ticari araçların performanslarını analiz etmiştir. Çalışmasında disk temizleme araçları ile temizlenmiş olan disklere ait imajlar, Forensic Tool Kit (FTK) adli bilişim aracı ile kontrol edilmiştir. Bir takım araçların disk üzerinde tahsis yapılmamış (unallocated) alanlarda, delil olabilecek verilerin kurtarılmasını sağlayabilecek veri artıkları bıraktığı görülmüştür. Tüm bu incelemelerin ardından önemli bir not olarak, tüm AF araçlarının çalıştıklarına dair bir iz bıraktıklarını çalışmasında belirtmiştir.

Fairbanks ve arkadaşları [30]'da, honeypot kullanarak, honeypot sisteme ait dosya sistemi günlüğü (file system journal) aracılığı ile delil olabilecek bilgilerin, AF araçları kullanılmış olsa bile analiz edilebileceği bir yöntem önermişlerdir. TimeKeeper adını verdikleri dosya sistemi günlüğü izleme prototipi ile dosya sisteminde ulaşılamaz olan dosyaların incelenebileceğine dair sonuçlar sunmuşlardır. Bu bulgular sayesinde sistem kurtarma ve yapılan saldırı hakkında araştırma yapılabileceği vurgulanmıştır. Çalışma Linux tipi işletim sistemlerinin temel dosya yapısı olan Ext3 dosya sistemi üzerinde yapılmıştır. Yani Windows OS dosya sistemi olan NTFS için geçerli değildir. Ext3 dosya sisteminde dosyalar inode isimli, dosyalara ait metadataların tutulmasını ve her dosyaya eşsiz bir kimlik numarası verilmesini sağlayan bir nesne bulunmaktadır. Dolayısıyla bir Ext3 dosyası ile ilgili işlem yapılabilmesi için inode tablosu içinde o dosyaya ait bir inode kimliği bulunmalıdır. TimeKeeper örnek sonuçları ext3 türü

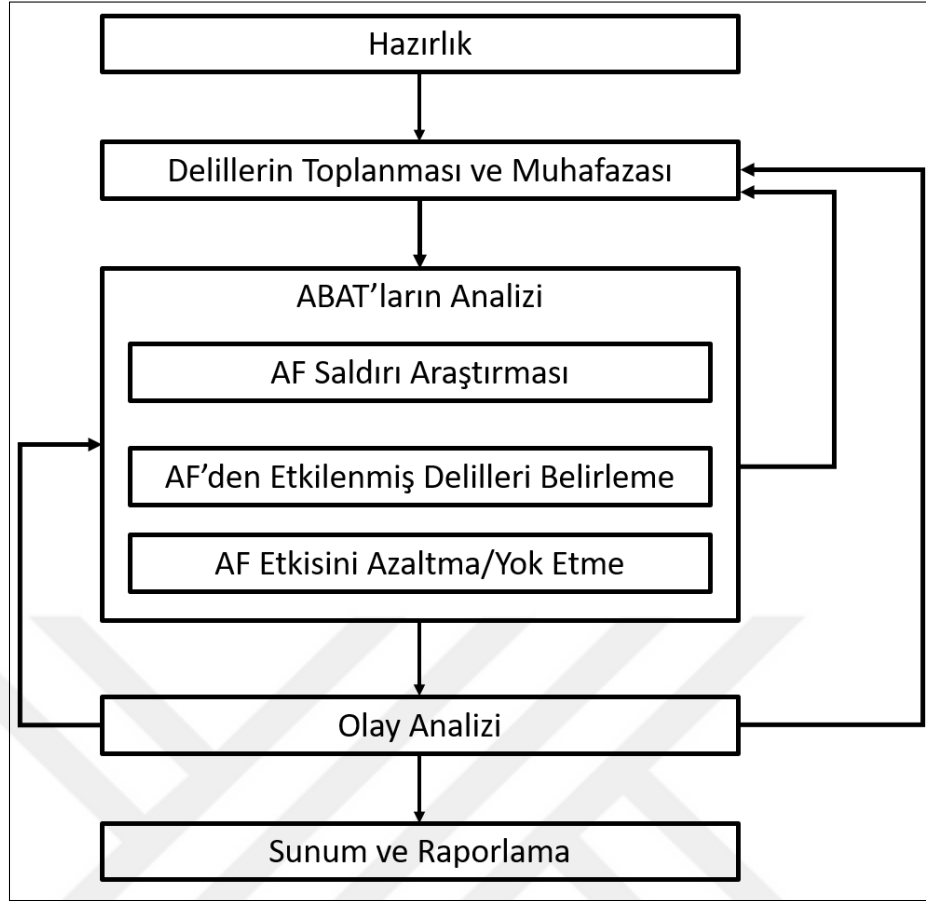
dosyaya ait her türlü işlemin (değişiklik, erişim, oluşturma) tespit edildiğini tablolarda sunmuşlardır.

Rekhis ve Boudriga [31]'de, AF farkındalıklı kuramsal bir adli bilişim soruşturması yaklaşımı geliştirmişlerdir. Çalışmayı, AF saldırıları içeren örnek bir soruşturma senaryosu üzerinden gerçekleştirmişlerdir. Adli bilişim soruşturmasının, dijital delinin kesin doğruluğuna yönelik yapıldığını, AF'nin ise tersi amaçla delilin kesinliğini zorlaştırmak, mümkünse imkansız kılmak amacını güttüğü belirtilmiştir. AF'nin temel olarak üç hedefi olduğunu belirtmişlerdir. Bu hedefler:

- İşletim sistemi veya uygulamaların oluşturduğu izleri silerek, değiştirerek veya gizleyerek delilin tespitinden kaçınmak,
- Suç unsuru sistemden delillerin toplanmasını engellemek,
- Dijital delilin toplanması, analiz edilmesi ve mahkemeye sunulması süreçlerini güçleştirmek ve gerekli çabayı arttırmaktır.

Çalışmada, adli bilişim süreçlerini modelleyen ilgili çalışmalara ve ilgili çalışmaların daha iyi bir adli bilişim soruşturma modeli oluşturma hedeflerine ait bilgilere yer verilirken, bu çalışmaların hiçbirinin AF tehdidini göz önüne almadığı, yazarlarca vurgulanmıştır. Bu nedenle, önerilen modellerdeki süreçlerin izlenilmesine rağmen başarılı bir adli bilişim soruşturmasına yöneltemeyeceği belirtilmiştir. Çalışmada AF saldırıları, kanıtlanabilir ve kanıtlanamaz olarak iki ayrı kategoride incelenirken, delil olarak incelenen log ve ikaz bilgilerindeki sahte bilgileri tespit edip, düzeltmeye yönelik çabalar da anlatılmaktadır. Tespit için, güvenilir bir delil ile saldırıya uğramış deliller karşılaştırılarak aralarındaki tutarsızlıklar incelenmiştir. Yazarlara göre, ABAT'lar arasında delil incelemesi açısından en tehlikeli olan yöntemin, hassas belgelere ait log ve metadata verilerinin değiştirilmesi ile yapılan iz karartma (Trail Obfuscation) olduğu belirtilmiştir.

Şekil 2.2'de yazarların önermiş olduğu AF farkındalıklı adli bilişim süreçleri iş akış şeması verilmiştir. Özellikle üçüncü aşama olan ABAT incelemesinde, delillerin zaman damgalarının incelenmesi, dosya sistemlerinin incelenerek veri gizleme yapılıp yapılmadığının analizi ve loglardaki tutarsızlıkların incelenmesi



Şekil 2.2: Rekhis ve Boudriga [29]'de AF farkındalıklı AB süreçleri.

gerektiği belirtilmiştir. Bütün aşamalar, çalışma içerisinde kuramsal bir formülasyona dönüştürülerek anlatım gerçekleştirilmiştir.

James [32]'de, aktif ve geliştirilmesine devam edilen bir proje olan "AF'nin Belirtileri (IoAF)", imza tabanlı yöntemlerle ABAT kullanımına ait izlerin otomatik tespitinin hedeflendiği bir projedir. Program, soruşturulan sistemdeki dosya sistemi metadatalarını ve kayıt defteri bilgilerini incelemektedir. İncelenen her bir nesneye ait imza bilgisi, daha önceden tanımlanmış bir imza veritabanındaki verilerle karşılaştırılmakta ve eşleşme durumunda AF aracının kullanıldığı belirlenmektedir.

Literatür araştırması dört alt başlıkta ele alınarak sunulmuştur. Her bir alt başlıkta, alanında genel geçerliliği kabul görmüş yazarların çalışmalarına ait bilgilere yer verilmiştir.



3. ADLİ BİLİŞİM

3.1 Adli Bilişime Genel Bakış

Dijital haberleşmedeki kolaylıklar, kullanıcıların hizmetlere erişimini kolaylaştırdığı gibi, saldırganların ve suçluların da suç işlemede, kolaylıklar sağlamıştır. Terörist organizasyonların birbirleri arasında haberleşmesi, illegal örgütlerin sanal ortamdaki illegal faaliyetleri ve buna benzer işlemler suç teşkil ettiğinden, fiziksel işlenen suçlarda olduğu gibi suçun ispatına yönelik delillerin toplanması, incelenmesi ve mahkeme veya otoritelere sunulması için, bilimsel bir disiplin olarak "Adli Bilişim (AB)" dalı oluşturulmuştur. Siber güvenliğin bir alt dalı olarak kabul gören AB, [3]' de elektromanyetik ve optik ortamlarda tutulmakta olan veya bu ortamlar arasında iletilen veri, bilgi, görüntü, ses veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal delil özelliği taşıyacak şekilde tanımlanması, elde edilmesi, muhafazası, incelenmesi ve mahkemeye sunulması çalışmalarının tamamı olarak tanımlanmıştır.

Bir diğer tanımda AB, bilgisayar depolama birimleri üzerinde bulunan dijital verilerin elde edilmesi ve toplanması, delilleştirilmesi ve raporlanması işlemlerinden oluşan bir bilim dalıdır [4]. Kaur adli bilişimi, soruşturmalarda ve yasal işlemlerde kanıt kaynağı olarak bilgisayarlar tarafından üretilen, depolanan ve iletilen dijital bilgilerin kullanılmasıyla ilgili adli bilim dallarından biri olarak tanımlamıştır [33]. Planlı operasyonları tahrip ettiği gösterilen yetkisiz işlemleri ya da suçu oluşturan olayların yeniden yapılandırılmasını kolaylaştırmak veya ilerletmek amacıyla, dijital kaynaklardan türetilen delillerin korunması, geçerliliği, tanımlanması, analizi, yorumlanması, dokümantasyonu ve sunumu için bilimsel olarak türetilmiş ve kanıtlanmış yöntemlerin kullanılması [34], adli bilişime yönelik yapılan geniş kapsamlı tanımlamalardan biridir. [35]'de adli olayların aydınlatılması amacıyla, olay yerinden, dijital veri saklama ve iletme özelliğine sahip cihazların toplanması, cihazların içerisindeki dijital delillerin tespit edilmesi ve adli otoritelere

raporlanması süreci içerisinde yapılan çalışmaların bütünü olarak tanımlanan AB, ülkemizde 5271 sayılı Ceza Muhakemeleri Kanununun (CMK) 134. Maddesine [36] göre uygulanmaktadır. İlgili madde, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoymaya yönelik işlemlerin yasal dayanağını oluşturmaktadır.

Başlangıçta devlet güvenlik kurumlarınca kullanılmaya başlanan AB, günümüzde ticari kurum ve kuruluşlarca da danışılan bir bilim dalıdır. Adli bilişimde en önemli unsur, dijital delilin güvenilirliğinin (credibility) korunmasıdır. Adli bilişimde dijital delilin, bütünlük, gerçeklik, üretilebilirlik ve müdahale edilemezlik ilkelerine uygun olması beklenmektedir [33].

AB kullanım alanlarına göre incelendiğinde genel olarak, veri saklama, silme ve kurtarma; şifreleme ve şifre çözme; gizlenmiş ya da stenagrofi kullanılarak gizlenen dosyayı bulma; finansal denetim ve ticari anlaşmazlıkların incelenmesi; fikri haklar üzerine uyuşmazlıkların incelenmesi gibi alanlarda kullanılmaktadır. Bu alanların bir kısmı suç içermeyen, kişisel verilerin korunması gibi maksatlarla kullanılan şifreleme vb. yöntemleri de içerdiği gibi, aynı yöntemler suç teşkil eden verinin adli makamlarca bulunmasını engellemek, bulunsu dahi içeriğinin okunmasına mani olmak amacıyla da kullanılabilen yöntemleri içermektedir.

AB'nin görevi delilleri yorumlamak değil, teknik bir incelemeyle verileri yorumlama makamlarına (yargı) ulaştırmaktır.

3.2 Adli Bilişimde Delil Türleri, Özellikleri ve Süreç Modelleri

Bir bilişim suçu soruşturmasında deliller iki türlü olarak ele alınmaktadır. Bunlardan birincisi mantıksal deliller olarak da adlandırılan dijital deliller; ikincisi her türlü bilişim malzemesi ve donanımını içeren fiziksel delillerdir. Dijital deliller, fiziksel delillerin üzerinde tutulan verilerden oluşmaktadır. Çizelge 3.1'de dijital ve fiziksel delil türlerine ait örnekler sunulmaktadır.

3.2.1 Dijital delillerin özellikleri

Mantıksal delil olarak da adlandırılan dijital deliller, donanım üzerindeki elektronik etkiden oluşmuş manyetik alanları ifade etmektedir. Dijital delillerin özellikleri:

Çizelge 3.1: Adli bilişimde delil türleri.

Adli Bilişim Delilleri	
Dijital Deliller	Fiziksel Deliller
Veri dosyaları	Bilgisayar,Sunucu
Kurtarılmış silinmiş dosyalar	Sabit Disk
Kayıp alanlardan kurtarılmış veriler	USB Bellek
Dijital fotoğraf ve videolar	CD, DVD
Sunucu kayıt dosyaları	Fax,Fotokopi Cihazı
İnternet Geçmişi	Ağ Cihazları
E-posta ve Chat Kayıtları	Mobil Cihazlar
Uygulama Logları	Diğer Donanım Türleri

- Eksiksiz kopyalanabilir ve bu sayede orijinal delil yerine aynı delilin birebir kopyası üzerinde çalışmalar, orijinal delilin güvenilirliğini tehlikeye sokmadan, yapılabilir,
- Fiziksel sınırları yoktur, kolaylıkla sınırları hızlı bir şekilde aşabilir,
- Dijital delilin kurtarılması, derin silme yapılmadıysa verilerin geri getirilebilmesi mümkündür,
- Diğer yandan bu özelliği ile kolayca değiştirilebilir, zarar verilebilir veya silinebilir,
- Kasıtlı olarak derin silme yapılsa bile dosya sistemi günlüğünde dosyaya ait metadata verileri bulunabilir.

Dijital deliller kalıcı veya uçucu olabilir. Geçici bellekteki veriler, uçucu delillere örnektir ve çok önemli bilgileri içerebilmektedir. Örneğin, şifreli bir dosyanın, açık hali o anda geçici bellekte bulunabilmektedir. Bu nedenle geçici belleğin bir kopyasının alınması soruşturma ve suçun ispatı açısından büyük önem taşıyabilmektedir. Kalıcı deliller sabit disk veya harici bellekler üzerinde tutulan verilerden oluşmaktadır.

Son yıllardaki adli bilişime ait uygulamalar incelendiğinde, ceza muhakemesinde delile esas niteliğe sahip olabilecek verilerin, yalnızca kişisel masaüstü veya dizüstü bilgisayarlardan değil, bunun yanı sıra cep telefonlarından, PS, Xbox vb. oyun konsollarındaki kayıtlardan, USB harici belleklerden, dijital video ve ses kayıt donanımları gibi birçok elektronik birimden de elde edildiği görülmektedir [37].

3.2.2 Adli bilişim süreçleri

AB süreçlerinin, bilimsel bir yol izleme ve delilin geçerliliğinin sağlanması açısından uygulanması ve her sürecin detaylı bir şekilde dokümente edilmesi gerekmektedir. Delillerin toplanması sürecinde, el konulacak bilgisayarlardan veri alınmasından, bilgisayarın dondurulması, verilerin kopyalanması, klonlanması, bilgisayarın kapatılması ve laboratuvara götürülmesine kadar bütün süreçler çok titiz bir biçimde yerine getirilmeli ve eldeki delillerden hiçbirinin kaybolmaması veya zarar görmemesi sağlanmalıdır [38].

AB süreçleri, temel olarak üç basamaktan oluşmaktadır: Elde Etme (Acquire), Belgeleme (Authenticate) ve Çözümleme (Analyse). İlk harflerinden dolayı 3A olarak adlandırılan [39] bu süreçler, AB süreçleri için basit bir tanımlama yapmaktadır. Öte yandan [40]'da, 3A ile özetlenen süreçlerin tamamını kapsayacak şekilde bir A daha eklenerek AF'nin bütün AB süreçlerinde ele alınması gerektiği vurgulanmaktadır. Biraz daha detaylı bir AB süreçleri tanımlaması, Şekil 3.1'de verilmiştir.

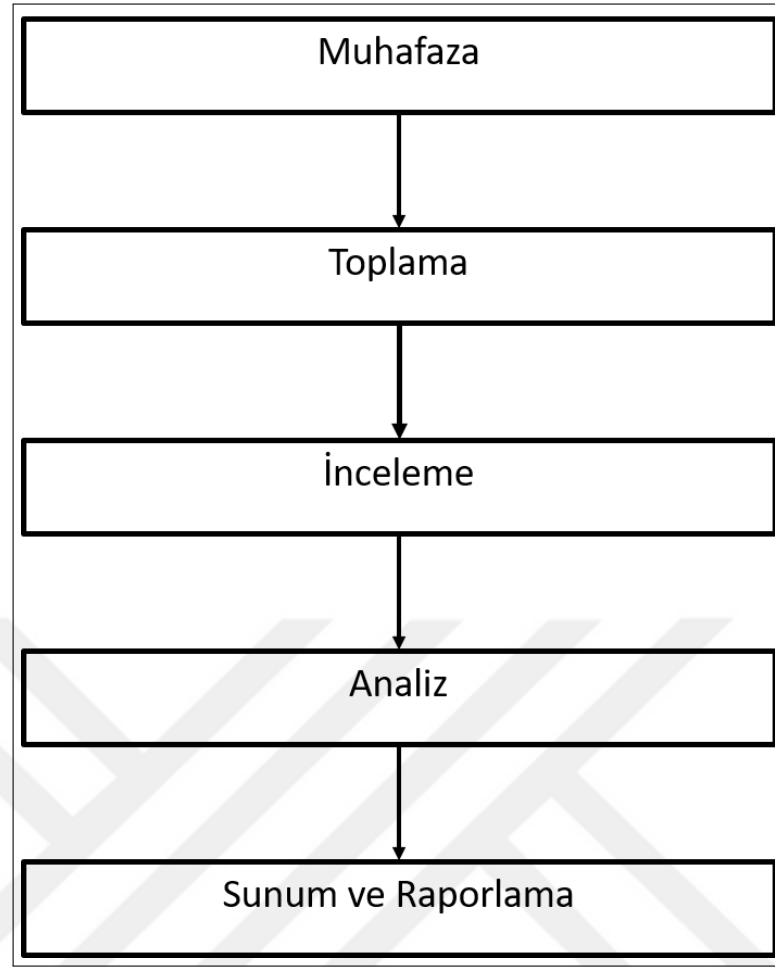
Muhafaza süreci, olay yerinin dondurulması anlamına gelmektedir. Bu aşama, toplanacak olan dijital delile zarar verebilecek her türlü işlemin önlenmesini içermektedir.

Toplama süreci, suç teşkil eden olaya ilişkin delil olabileceği düşünülen, ilgili her türlü dijital verinin toplanmasını içermektedir. Bu kısımdaki faaliyetler, bilgisayarlardaki verilerin toplanması, donanımların toplanması veya donanımlardaki verilerin başka bir ortama aktarılması şeklinde gerçekleştirilebilir.

İnceleme süreci, derinliğine araştırma prensibine dayalı, olayla ilgili anlamlı verilerin çıktı olarak kullanıldığı basamaktır. Bu aşamada veri dosyaları, zaman damgaları ve log dosyaları toplanan verilerden elde edilmektedir.

Analiz süreci, delillerin sonuç odaklı incelendiği ve delil olarak kullanılabileceğine karar verildiği aşamadır.

Sunum ve raporlama kısmı, bulguların mahkemeye veya yasal otoriteye sunulduğu ve sonuçlarla birlikte tüm soruşturma süreçlerinde yapılanların, bulguların ve yapılan işlemlerin kaydının tutulduğu bölümdür.



Şekil 3.1: Adli Bilişim Süreçleri.

Bir diğer AB süreçleri modeli de "Kuramsal AB Modeli" [41]'de önerilmiştir. Önerilen modele ait iş akış şeması Şekil 3.2'de verilmiştir.

Tanımlama kısmında, göstergelerden olay tanımlanmakta ve olayın türü tespit edilmektedir.

Hazırlık kısmında, ABA'ların ve AB tekniklerinin hazır edilmesi, yetkilendirmenin izlenmesi ve yönetsel desteğin sağlanması konuları işlenmektedir.

Yaklaşım stratejisi kısmında, delillerin bozulmadan toplanmasına yönelik prosedürler belirlenmektedir.

Muhafaza kısmında, fiziksel ve dijital delillerin izole edilmesi, güvenli bir ortama alınması sağlanmaktadır.

Toplama kısmında, fiziksel ortamın kayıt altına alınması, standart ve kabul görmüş yöntemler ile dijital delillerin kopyasının alınması işlemleri yapılmaktadır.



Şekil 3.2: Kuramsal Adli Bilişim Modeli.

İnceleme kısmında, suç unsuru olduğundan şüphelenilen deliller, derinliğine araştırma yöntemi ile incelenmektedir.

Çözümleme kısmında, verinin önemine göre gizlenmiş veya silinmiş verinin kurtarılmasına ve sonuçların bulunmasına çalışılmaktadır.

Sunum kısmında, teknik bir çalışma ile elde edilen geçerli bulgular özetlenmekte ve sonuç açıklaması yapılmaktadır.

Delilin iadesi kısmında, fiziksel ve dijital varlıklar sahibine iade edilmektedir.

Ülkemizde adli bilişim süreçleri:

- Ön İnceleme / Olay Yeri Tespiti,
- Delil Toplama,

- Analiz,
- Raporlama

şeklinde uygulanmaktadır [37]. Süreç modellerinde aşama sayısı ve isimlendirmeler değişse bile tüm modeller, kuramsal AB modelindeki aşamaların belirli kurallar çerçevesinde, bir veya birkaçının birlikte uygulanmasını içermektedir.

3.3 Adli Bilişim Araçları ve Özellikleri

ABA'lar, ABU ve BGU'ların adli bilişim süreçlerine uygun bir şekilde işlemlerini yerine getirmesinde, kolaylık ve zaman kazandıran yazılımlar ve donanımlardan oluşmaktadır. Bu araçlar, delillerin incelenmesinde kullanılırken bir takım özellikleri karşılamaları beklenmektedir. Bu özellikler [3] aşağıda sıralanmıştır.

1. Bit bit imaj alabilmeli,
2. Orijinal veride değişiklik yapmamalı,
3. Donanım çeşitliliğine uyumlu olmalı (IDE, SCSI, SATA, USB),
4. İmajı alınan diske ait dosyaların bütünlüğünü doğrulamalı,
5. Diğer inceleme programlarınca kullanılabilir olmalı,
6. Girdi/Çıktı hatalarını verebilmeli,
7. Hızlı imaj özelliğini desteklemeli,
8. Sıkıştırma yeteneği olmalı,
9. Anlaşılır raporlaması olmalı.

Bu araçların bir kısmı belirli bir konuda uzmanlık sağlarken (dosya kurtarma, chat kayıtlarını inceleme, OS bazında inceleme vb.), bir kısmı da AB süreçlerinin geneli için kullanım kolaylığı sağlamaktadır. Genel AB süreçlerine hizmet eden araçlar, ayrıca üçüncü parti yazılımlarla da (şifre çözme, script çalıştırma, hash kitaplığı vb.) uyumlu olarak çalışarak, daha verimli bir kullanım sağlamaktadırlar. Bu alanda kullanılan ABA örnekleri Çizelge 3.2'de verilmiştir. Büyük bir bölümü ücretli

Çizelge 3.2: Adli bilişim araçları.

Adli Bilişim Araçları	
Ücretsiz	Ücretli
PALADIN 4.0	Paraben's P2 Commander
AUTOPSY	Guidance Software EnCase Forensic
DEFT	AccessData FTK
KALI LINUX	X-Ways Forensic
	Belkasoft Evidence Center
	TechPathways ProDiscover
	MACQUISITION
	NEMX
	EMX
	CHAT EXAMINER

olan bu araçların, bir kısmı da ücretsiz açık kaynak olarak hizmet vermektedir. ABA'ların performansları üzerine çalışmalar mevcuttur. Bu çalışmalarda, yazarlar değişik kriterlere dayalı olarak ABA'ları değerlendirip, en fazla özelliğe sahip, imkan ve kabiliyetleri daha fazla olan araç ise performans bazında daha iyi olarak seçilmiştir. Bu alanda yapılan çalışmalardan biri olan [42], Paraben P2C'yi performans açısından diğerlerinden üstün bulmuştur.

Adli bilişimde delilin, geçerli olabilmesi için, olayla ilişkili ve güvenilir olması gerekmektedir. Adli bilişim araçları bir işçinin kovulmasını, bir kişinin suçlu ilan edilmesini veya aynı şekilde bir kişinin masumiyetininin ispatlanmasını sağlayacak olan yazılımlar olduğundan, diğer yazılımlardan farklılık göstermektedir. Bu kritik durum, adli bilişim yazılımlarının test edilmesini çok önemli kılmaktadır. Yani disk imajı alan bir yazılım, diskteki dosyaları eksiksiz bir şekilde kopyalayabilmeli, silinmiş dosyaları kurtarma yeteneği varsa silinmiş tüm dosyaları da eksiksiz ve hatasız şekilde kopyalayabilmelidir. [43]'e göre, açık kaynak ABA'lar da, bu kapsamda bir ABA'dan beklenen güvenilirliği karşılamaktadır.

3.4 Adli Bilişim Türleri

Adli Bilişim kavramı ilk ortaya çıktığı zamanlarda, kavram olarak tek başına yeterli iken, günümüzde yazılım, işletim sistemi, ağ cihazları, bilgi teknolojileri, mobil teknolojiler ve donanımlarda yaşanan gelişmeler ile AB'nin de farklı türlere bölünmesi

bir zorunluluk haline gelmiştir. Bu bölümde AB türleri, ilgi alanları ve özellikleri ele alınmaktadır.

3.4.1 Bilgisayar adli bilişimi (Computer forensics)

Adli bilişim alanında en sık kullanılan AB türüdür. Suçluya ait bilgisayara el konulması veya incelenmesi ile suçun ispatına yönelik delillerin elde edilmesi, en eski ve en çok bilinen alan olarak karşımıza çıkmaktadır. Bilgisayarlar büyük ölçekte veri muhafaza eden, kendine özel kayıtları oluşturan, elektronik posta gönderiminin yapıldığı, dahili sabit diske sahip, kullanıcılara ait hesapların yönetilebildiği ve en yaygın elektronik donanımlar olması nedeni ile, adli birimler için, önde gelen bir veri kaynağı durumundadır [44]. Bu nedenle en kapsamlı AB türü olarak karşımıza çıkmaktadır. Bu alanda incelenen suçlar, bilgisayarların araç olarak kullanılarak bir kişiliği (özel/tüzel) hedef alan suçlar olabileceği gibi, hedefin doğrudan bilgisayar sistemleri olduğu bir olay da olabilmektedir.

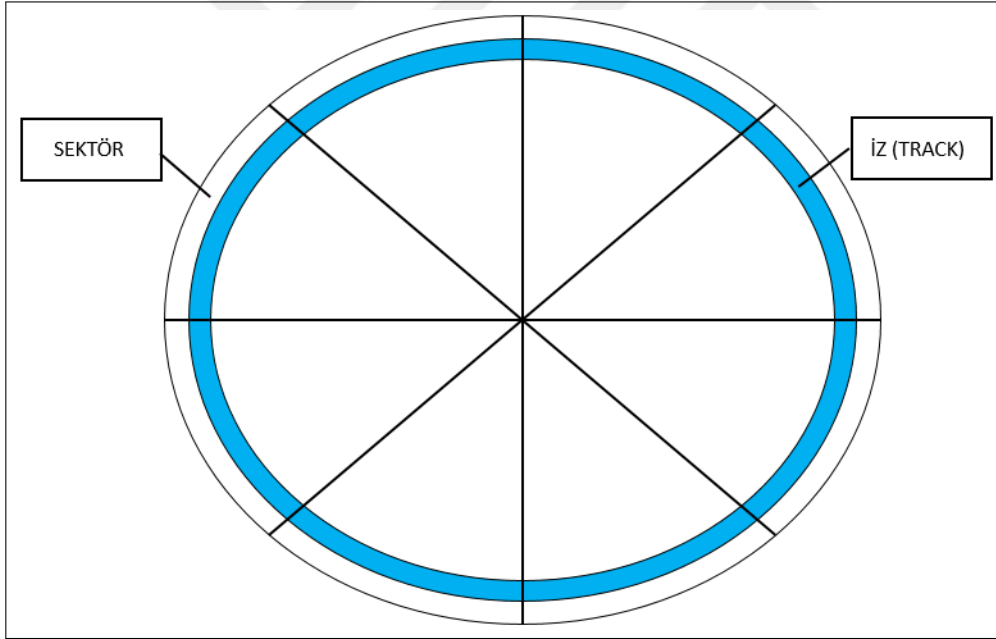
Bilgisayar AB, sadece olay kayıtlarını incelemeyi içeren bir AB türü değildir [45]. Olayların büyük bir bölümü, dosya sistemindeki belgelerin incelenmesi ve silinmiş verilerin kurtarılmasına yönelik işlemleri gerektirmektedir. Genel olarak bir bilgisayardan elde edilen veriler, sürekli veriler (sabit disk üzerine yazılı veriler) ve uçucu/geçici veriler (geçici bellekte (RAM) yer alan veriler) olarak karşımıza çıkmaktadır. Örnek bir bilgisayar imajı alma, veri kopyalama Şekil 3.3'te verilmiştir.



Şekil 3.3: Bilgisayar adli bilişimi [46].

3.4.2 Dosya sistemi adli bilişimi (File system forensics)

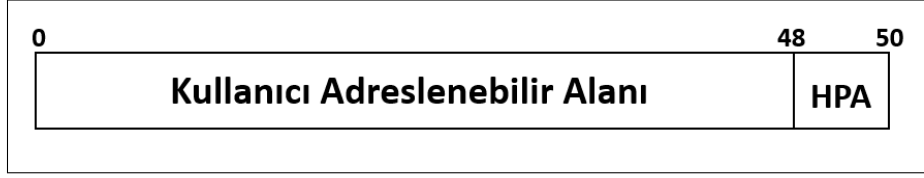
Dosya sistemi analizi, dosya sistemlerinin çeşitliliği (NTFS, FAT, EXT, HFS) nedeniyle farklı uzmanlıkları bir arada bulundurmayı gerektirmektedir. Dosya sistemi analizi için, öncelikle veri depolama cihazlarının (sabit disk, geçici bellek) yapısı, okuma-yazma işlemleri, disk üzerindeki sektörel yapının bilinmesi gibi ön gereksinimlere ihtiyaç duyulmaktadır. Disk üzerinde fiziksel ve mantıksal adreslemenin nasıl yapıldığı bilinmelidir. Disk üzerinde adreslenebilir en küçük yapı sektör olarak adlandırılır. Genellikle kapasiteleri 512 byte,yeni nesillerde 4096 byte (küme (cluster) yapısı:8 sektör), olarak belirlenmektedir. Bu sektörler disk üzerindeki silindir şeklindeki izler (track) üzerinde tutulmaktadır. Birden fazla disk yüzeyi (platter) kullanıldığından, herhangi bir sektöre disk yüzeyi-iz-sektör adreslerinin bileşimi ile ulaşılabilinmektedir. Örnek bir sabit disk yüzeyi Şekil 3.4’de verilmektedir.



Şekil 3.4: Sabit disk yapısı (iz-sektör).

Disk yüzeyi-iz-sektör adreslemesi fiziksel adresleme olup kapasite açısından yetersiz kalınca, Mantıksal Blok Adresleme (LBA) sistemine geçiş yapılmıştır. LBA’da sektörler eşsiz adreslere sahiptir. Örneğin 1.000.000 sektörün ilk sektörü 0 ile son sektörü 999.999 ile adreslenir.

Dosya sistemi analizinde disk ile ilgili bilinmesi gereken önemli konulardan biri de "Cihaz Korumalı Alan (HPA)" yapısıdır. HPA diskin son bölümünde varsayılan olarak



Şekil 3.5: Disk üzerinde HPA tahsisi.

kapasitesi sıfır olarak gelen alandır. ATA disklerde ATA komutları ile ayarlanabilen HPA, ABU'lar tarafından veri gizlemede kullanılan bir alan olarak kabul edilir ve tespit edilmesi zordur. Bu alan üretici firmaların, kullanıcıların ve işletim sistemlerinin erişimine kapalı olarak geliştirdikleri alandır. Temelde ticari amaçlarla ortaya çıkan bu alan, AF kullanıcılarına veri gizlemede kullandıkları bir alan olarak da hizmet verebilmektedir. Örneğin 50 GB'lık bir sabit disk üzerinde, 2 GB'lık bir HPA ayırıldığında işletim sistemi dosya sistemi olarak 48 GB'lık alanı adresleyebilir (Şekil 3.5).

HPA'ya benzer bir diğer alan da "Cihaz Konfigürasyonu Bölümü (DCO)" alanıdır. Bu alan da üreticilerin tarafından, kullanıcıya disk yeteneklerini kısıtlama imkanı sunmak üzere oluşturulan bir alandır (Şekil 3.6). HPA ile benzer bir yapıya sahip olduğundan AF kullanıcıları tarafından veri gizleme amaçlı kullanılabilir.



Şekil 3.6: Disk üzerinde HPA ve DCO tahsisi.

HPA üretici tarafından önyüklemeye kayıtlarını tutmak ve birtakım üretici araçlarını muhafaza etmek amacıyla kullanılmaktadır. HPA ve DCO varlığına, diskin sürümüne ve modeline göre AB soruşturması esnasında dikkat edilmelidir [47].

Sabit diskler, mantıksal kullanıma hizmet etmek üzere, yığın veya sürücülere (volume-drive) bölümlenebilir. Microsoft Windows'ta genel olarak gördüğümüz yığınlar, C: ve D: sürücüleridir. Bu sürücüler, kullanıcıları diskin karmaşık adreslemesinden soyutlamak ve mantıksal bölütler oluşturmak ve disk kullanımında performans artışı sağlamak için kullanılmaktadır. Çoklu disk yapısını tek bir disk gibi kullanmak ve performans artışı sağlamak amacıyla RAID yapısı kullanılmakta olduğundan, ABU'lar tarafından RAID yapısı da iyi derecede bilinmelidir.

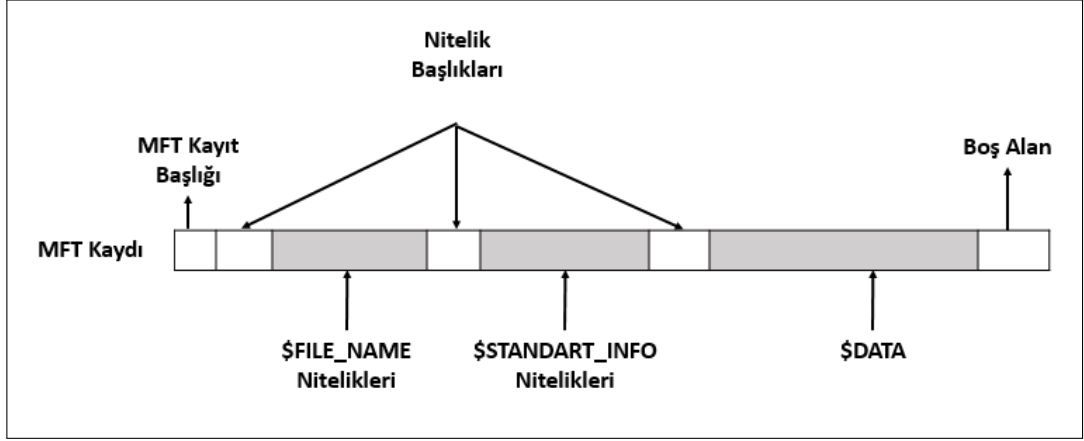
Buraya kadar anlatılanlar ışığında, dosya sistemi analizinin yapılmasına ait bilgiler daha anlaşılır olacaktır. Sabit diskler üzerinde bulunan sürücüler içerisindeki belgelerin (files) incelenmesi ve yorumlanması dosya sistemi adli bilişimini oluşturmaktadır.

Dosya sistemleri, kullanıcılara verilerini bir dosya ve izin hiyerarşisi içerisinde depolamalarını sağlayan yapılardır. Dosya sistemleri, bilgisayarın dosyaları nerede bulacağını belirleyen yapısal veriler ve kullanıcı verilerinden oluşmaktadır. İşletim sistemlerindeki dosya sistemleri ile kütüphanelerdeki kitap tahsis sistemi arasında bir analogi yapılabilir. Kütüphanede bir kitabın yerinin bulunması için bir etiketleme (Kitap adı, raf adresi, barkod vb.) gereklidir ki dosya sistemleri de dosyalar için aynı mantıkla faaliyet göstermektedir. En temel dosya sistemi modelinde, dosya sistemi (FAT, NTFS, Ext), içerik, üstveri (metadata), dosya adı ve uygulama kategorileri mevcuttur [47].

Bölümleme sayesinde, her bölüm aynı disk üzerinde farklı bir dosya sisteminden oluşabilmektedir. Aynı disk üzerinde bir sürücü NTFS iken, diğer bir sürücü FAT 32 olabilmektedir. Her dosya sistemi kendi yapısını ilk sektörden başlayarak oluşturmaktadır. Microsoft Windows'un varsayılan dosya sistemi olmakla beraber kullanım açısından en sık kullanılan dosya sistemi NTFS, bir örnek üzerinde açıklanacaktır. NTFS dosya sisteminde indeksleme görevi MFT (Master File Table) dosyasıdır. Boot kaydında adresi belirlenmiş olan MFT, 1024 byte'lık kayıtlar tutarak dosyalara ait üstverileri muhafaza etmektedir. MFT kayıtları arasında o kayda ait başlık bilgisi, \$FILE_NAME, \$STANDARD_INFO, \$DATA nitelikleri ve bu niteliklere ait başlık bilgileri ile diğer kullanılmayan alanlar mevcuttur. NTFS sistemlere ait MFT'de kayıtlı bir dosya örnek verileri Şekil 3.7'de verilmektedir.

MFT Kayıt Başlığı bilgilerinde, kaydın bir dosyaya mı yoksa klasöre mi ait olduğu, kullanımda olup olmadığı, dosyanın bozulup bozulmadığı gibi bilgilere yer verilmektedir.

\$FILE_NAME niteliğinde, dosyanın hangi klasör altında olduğu (Parent MFT Reference) ve dosyaya ait oluşturulma, erişim, değiştirme ve ilk kayıt oluşturma gibi zaman bilgileri mevcuttur.



Şekil 3.7: NTFS MFT kayıt bölümleri.

\$STANDART_INFO niteliğinde, bu bölümde \$FILE_NAME niteliği gibi dosyaya ait oluşturulma, erişim, değiştirme ve ilk kayıt oluşturma gibi zaman bilgileri ile maksimum versiyonlama, güncel versiyon bilgisi, sınıf kimliği, güvenlik kimliği, dosya sahibi kimliği, USN (Update Sequence Number) günlüğündeki sıra numarası gibi bilgiler tutulmaktadır. MS Windows OS'lerde kullanıcıya gösterilen dosyaya ait özellikler bilgileri, bu bölümdeki verilerden okunmaktadır.

\$DATA niteliği, adından da anlaşılacağı üzere, dosyalara ait içerikleri tutmakla görevli kısımdır. Dosya içeriği, MFT kayıt bilgilerinden (1024 byte içinde) kalan kısımdan küçükse, içeriğin tamamı aynı kayıt içerisinde tutulmaktadır. Büyük boyutlu dosyalar içinse, verilerin yazıldığı sektörler ait adres bilgileri, bu nitelikte tutulmaktadır [48].

Bunun dışında NTFS dosya sisteminde, üstverilerdeki değişiklikleri arşivleyen logfile, bölüm etiketini barındıran volume, MFT bilgilerini tutan AttrDef, içerisindeki sektörlerin bir dosya tarafından kullanılıp kullanılmadığını tutan bitmap isimli üstdosyalar da bulunmaktadır.

NTFS sisteminde bir dosya oluşturulduğunda, bitmap dosyasından ilk müsait sektör belirlenip 1 değeri atanır, MFT kaydı içerisindeki bilgiler oluşturulur, boyutuna göre bitmap dosyasındaki uygun sektörler dosyanın kullanımına tahsis edilir. Dosyanın MFT başlık bilgisinde kullanımda alanına 1 değeri atanır.

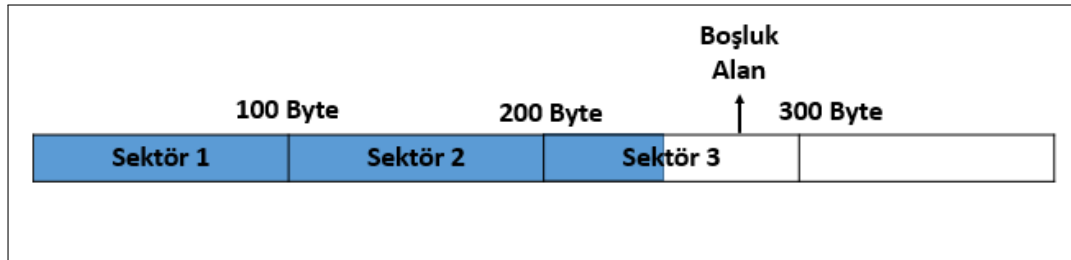
Dosyanın silinmesi işlemi dosya sistemi çeşidine göre değişmekle beraber, genel olarak yapılan işlem, dosyanın MFT başlık bilgisinde kullanımda alanına 0 değeri atamaktır. Aynı şekilde bitmap dosyasındaki dosyaya tahsis edilen sektörler ait kullanım değerlerine 0 atanmaktadır. Böylece ilgili alana yeni bilgiler yazılana

Çizelge 3.3: Dosya kurtarma olasılıkları.

MFT Kaydı	Dosya İçeriği	Sonuç
Var	Var	Dosyanın diskteki son hali aynı şekilde kurtarılabilir.
Var	Üzerine Yazılmış	Dosya içeriği kurtarılamasa da dosya ismi vb. bilgiler okunabilir.
Üzerine Yazılmış	Var	Dosya imzaları (başlık bilgileri) taratılarak içeriğe ulaşılabilir.
Üzerine Yazılmış	Üzerine Yazılmış	Dosyaya ait herhangi bir bilgi bulunamaz.

kadar eski veriler diskte muhafaza edilmektedir. Silinmiş verilerin kurtarılmasında bu işleyişin bilinmesi çok önem kazanmaktadır. Diğer dosya sistemleri hakkında detaylı bilgi [47]'de ele alınmaktadır.

Adli bilişim türleri üzerinde en çok durulan konu, dosya sistemi analizidir. Dosya sisteminde adli bilişim açısından en önemli konulardan biri de boşluk alanlar (slack space) konusudur. Boşluk alanlar dosya boyutunun birim sektör boyutunun katı olmadığı zamanlarda oluşmaktadır. Örnek olarak, sektör boyutu 100 byte olan bir sistemde dosyamız 250 byte ise, dosyamıza üç sektör atanmaktadır. Üçüncü sektörde 50 byte'lık bir alan burada boşluk alan olarak kalmaktadır. Bu alan AF kullanıcıları tarafından istismar edilen alanlardan biridir. Boşluk alan oluşumuna ait örnek Şekil 3.8'de verilmiştir.



Şekil 3.8: Boşluk alan (slack space) oluşumu.

Veri kurtarma, dosya sistemi analizi ile mümkündür. Bu kapsamda NTFS dosya sisteminde silinmiş bir dosyanın kurtarılması için MFT kaydı ve dosya içeriğinin durumlarına bakılır. Silinen dosyanın kurtarılmasına ilişkin olasılıklar Çizelge 3.3'de verilmiştir [48].

Çizelge 3.4: Windows OS geçici ve geçici olmayan bilgiler.

Geçici Bilgiler	Geçici Olmayan Bilgiler
Sistem Zamanı	Dosyalar
Aktif Kullanıcılar	Boşluk Alanlar
Açık dosyalar	Üstveriler
Ağ Bilgisi	Windows Arama İndekslemesi
Ağ Bağlantıları	Kayıt Defteri Ayarları
Görev Bilgisi	Bağlı Cihazlar
Görev Belleği	Olay Kayıtları
Ağ Durumu	Disk Belleği Dosyaları
Pano İçerikleri	
Komut Geçmişi	
Paylaşımlar	

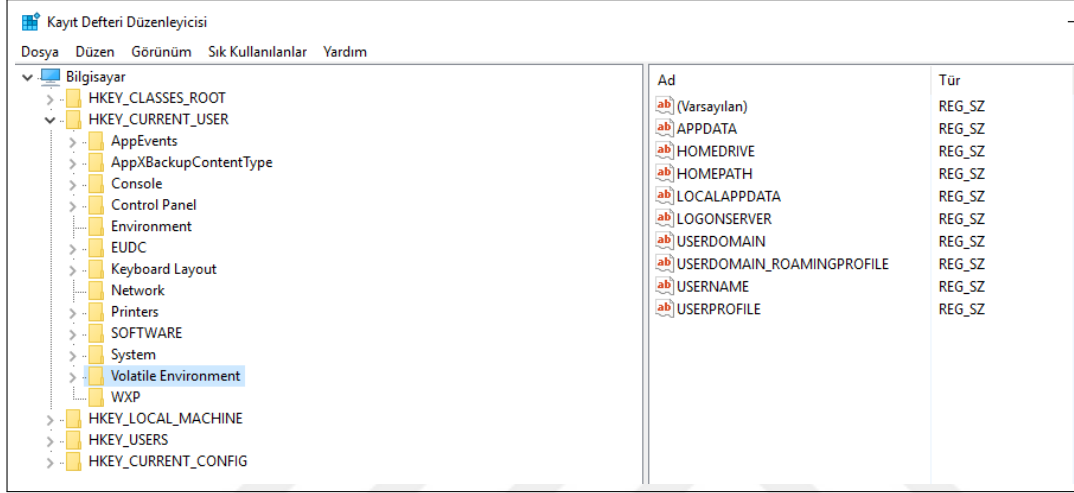
3.4.3 İşletim sistemi adli bilişimi (OS forensics)

İşletim sistemleri, kullanıcıların bilgisayar kaynaklarını kullanabilmeleri, dosya oluşturma için disk yönetimi yapabilmeleri, kısacası kullanıcıların bilgisayar üzerinde her türlü uygulamayı koşturmalarını sağlayan yazılımlardır. Her uygulama çalışmak ve hizmet sunmak için işletim sistemine gerek duymakta, işletim sistemi ile etkileşime geçmekte, her türlü etkileşim de işletim sistemi üzerinde değişikliklere sebep olmaktadır. Belgeler, videolar, resimler birer uygulama verileri iken, log dosyaları, sistem konfigürasyon dosyaları, dosya sistemi üstverileri işletim sistemi tarafından işlenen verilerdir.

İşletim sistemi adli bilişimi, kullanıcıların bilgisayardaki hareketleri ile işletim sistemindeki sistem kayıtlarındaki değişiklikler arasında bir korelasyon olup olmadığı konusunu incelemektedir.

İşletim sistemi adli bilişimi, MS Windows OS üzerinden örnekleme yapılarak anlatılacaktır. Windows işletim sisteminden bilgi toplamaya çalışan bir ABU, önce geçici ve geçici olmayan bilgilerin incelenmesi, sonrasında da işletim sistemine özel NTFS, Windows Kayıt Defteri (Registry) ve Windows Olay Kayıtları (Event Logs) verilerinden suç unsuru içeren olayı aydınlatıcı bilgiler elde etmeye çalışmaktadır [49]. Windows OS için geçici ve geçici olmayan bilgilere ait örnek veriler Çizelge 3.4’de sunulmuştur.

İşletim sistemi incelenirken en önemli unsurlar, NTFS, Windows Kayıt Defteri ve Windows Olay Kayıtları yapılarıdır. Windows işletim sistemlerinde Kayıt Defteri, işletim sistemi tarafından kullanıcılara, uygulamalara ve donanımlara ait bilgilerin tutulduğu hiyerarşik bir veritabanıdır. Kayıt Defteri amaçlarına göre gruplanmış anahtarlar ve bu anahtarlara atanmış değerlerden oluşmaktadır. Bu alandaki ayarlarda yapılan değişiklikler adli bilişim açısından önem arz etmektedir. Örnek bir kayıt defteri görüntüsü Şekil 3.9’da verilmiştir.

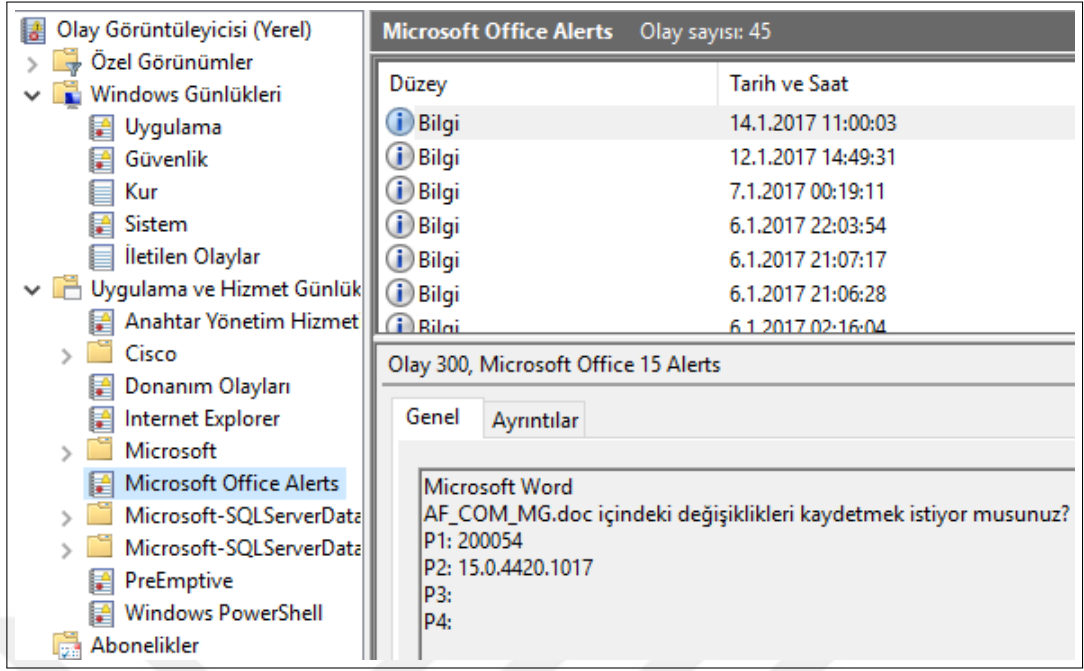


Şekil 3.9: Windows OS kayıt defteri ayarları.

Örneğin Çizelge 3.4’de geçici olmayan bilgiler arasında verilen disk belleği dosyaları (paging files), kayıt defterinde her kapanışta silinmesi şeklinde ayarlandı ise bu bilgi geçici olmayan bilgiler başlığının altına girmeyecektir. Ayrıca kayıt defterinde özellikle iz bırakmamak amaçlı yapılan ayarlar kullanıcının/şüphelinin profili hakkında bilgi sahibi olunmasını sağlamaktadır. Özellikle kötücül yazılımlara ait araştırmalarda, otomatik çalıştır (autorun) ile ilgili kayıtlar incelendiğinde, kendini bu kısma kaydettirmiş olan yazılımlar hakkında bilgi edinilebilir.

Diğer bir önemli işletim sistemi bilgi kaynağı da olay kayıtları verileridir. Sistemde oturum açma, güvenlik ile ilgili ikaz ve hatalar, uygulama verileri ve hatalar gibi bilgilere olay kayıtlarından ulaşılabilir. Windows işletim sisteminde olay kayıtları uygulama, sistem ve güvenlik ana başlıkları altında toplanmaktadır. Gerek sistem tarafından, gerekse kullanıcı tarafından yapılan her türlü işlem kayıt altına alınmaktadır. Örnek bir uygulama olay kaydı Şekil 3.10’da verilmiştir.

Olay kayıtlarında tutulan olay kimlikleri, özel bir anlam içermektedir. Örneğin bir dosyanın başarılı bir şekilde silinmesi, #4660 (eski sürümlerde #564) olay kimliği ile



Şekil 3.10: Windows OS olay günlükleri kayıtları.

kayıt altına alınmaktadır. Olay kimlikleri hakkında bilgi sahibi olmak, araştırma için kolaylık sağlayacaktır.

Bunların dışında işletim sistemi son açılan dosyalar ile web tarayıcılara ait önbellek (cache), çerezler (cookies) ve geçmiş (history) bilgilerinin tutulmasını sağlayarak araştırmalar için önemli bilgiler sağlamaktadır. İşletim sistemlerinin her biri için ayrı ayrı adli bilişim uzmanlığı gerekmektedir.

3.4.4 Ağ adli bilişimi (Network forensics)

Ağ adli bilişimi, bir ağa yapılan saldırılar, ağa bağlı bir sunucuya yapılan saldırılar gibi hedef sistemin bilgisayarlar olduğu olaylar olabileceği gibi, hedefin özel veya tüzel kişilik olduğu olaylarda da kullanılan bir uzmanlık alanıdır. Yerel alan, geniş alan ve internet ağlarında şüphelinin ağ aracılığı ile yapmış olduğu işlemlerin analizinde veya ağın sürekli izlenmesinde tespit edilen bir anomalinin tespitinden sonra başvurulmuş bir yöntemdir. Anomalinin tespiti, ağda normalin üzerinde bir trafiğin oluşması, ağ üzerinden hizmet veren bir sunucunun kaynak kullanımının artması veya olağan zamanların dışında ağ trafiği izlenmesi gibi durumların farkedilmesiyle mümkün olmaktadır.

Fırat Üniversitesi ağına ait bir web sunucusundan belirli zamanlarda, ağ çıkış trafiğinin anormal derecede arttığının tespiti üzerinde ağ trafiği incelenerek, kötücül yazılım

yardımıyla illegal bir internet sitesine ait farklı IP adreslerine yönelik istenmeyen trafik izlendiği [50]'de bulunmuştur. Kötücül yazılım temizlenerek illegal siteye trafik çıkışı güvenlik duvarı üzerinden kesilmiştir. Bu kısımda yapılan inceleme, ağ adli bilişim yöntemlerini içermektedir.

Günümüzde ağ türlerinin artmasıyla, her ağ türü hakkında yapılacak adli bilişim için ayrı ayrı uzmanlık gerekmektedir. Kablolu ağların yanısıra, kablosuz ağlar altında ele alınan Wi-Fi, mobil ağlar (3G, 4G, 5G), bluetooth, kablosuz sensör ağlar ve Ad Hoc ağların yapısı, işletilme mantığı detaylı bir şekilde incelenerek ağ hakkında detaylı bilgiler elde edilmektedir.

Ağ trafiğinin izlenmesi, kişilerin profili hakkında bilgi sağlayan bir yöntem olarak da karşımıza çıkmaktadır. Hangi e-posta adresini kullandığı, hangi banka müşterisi olduğu gibi bilgiler elde edilebilir.

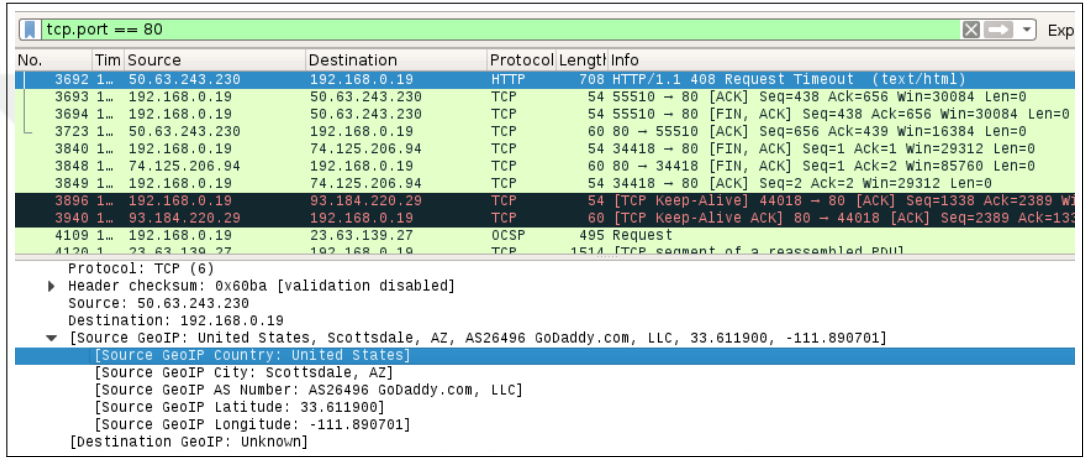
Çevrimiçi ağ analizi, belli bir zaman aralığına ilişkin trafiğin tutularak (snapshot), sonrasında detaylı incelenmesiyle gerçekleştirilmektedir [51]. Kullanılan paket analiz uygulamaları ne olursa olsun, ağ trafik bilgisinin bir adli bilişim uzmanı tarafından değerlendirilmesi [52],

- ağ üzerinde bulunan bütün sunuculardaki her türlü bilgi,
- sadece belirli bir incelemeye yönelik bilgiler (tek kullanıcının web istekleri, elektronik postaları gibi),
- girişim tespit cihazlarında olduğu gibi, sadece saldırı olarak tanımlanacak alarm bilgileri,
- tek başına anlam ifade etmeyen, ancak diğer bilgilerle beraber analiz edildiğinde önemli olan bilgiler, olmak üzere dört farklı grupta yapılabilir.

Ağ analizinde ağın topolojisi, ağ üzerindeki kullanılan kaynaklar ve yetkisiz erişimler incelenmektedir. Pasif ve aktif yöntemlerden oluşan ağ analizi ile adli kanıt elde edilmeye çalışılmaktadır. Pasif yöntemler "sniffer" adı verilen ağ koklayıcılar ile ağdaki her türlü trafiği izlemek için kullanılmaktadır. Aktif yöntemler ise port tarama, ağ topolojisi çıkarma (ping, traceroute, nmap) gibi [53] yöntemleri içermektedir. Aktif yöntemler içindeki port tarama ile bilinen protokollere ait portlar (SSH, DNS, POP3,

IMAP) taranarak kişilerin özel faaliyetleri incelenebilmektedir. Ağ üzerindeki anlık mesajlaşmalara ait protokoller ile filtreleme yapılarak anlık mesajlaşma paketleri üzerinde çalışma yapılabilir.

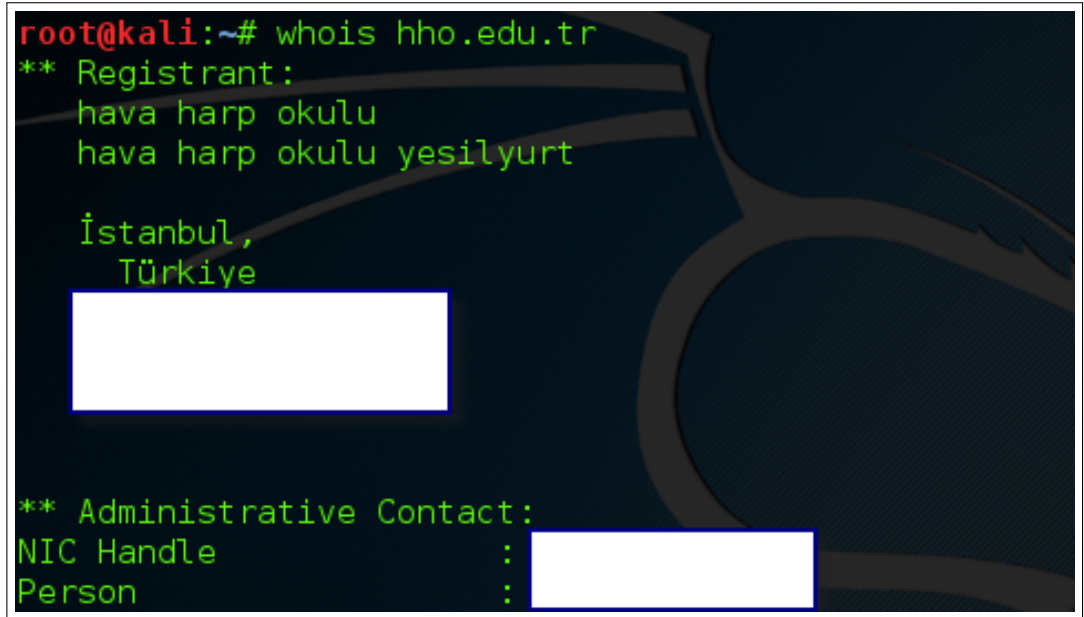
Ağ adli bilişimi internet kullanımının yaygınlaşmasıyla birlikte, bilgisayar adli bilişiminin ayrılmaz bir parçası haline gelmiştir [54]. Pasif yöntemlerden olan ağ izleme aracı "Wireshark" ile yapılan bir incelemeye ait örnek Şekil 3.11’de verilmiştir. Kaynak ve hedef IP adreslerine ait coğrafik lokasyonlara kadar bilgi sağladığı görülebilmektedir. Bir diğer bilgi edinme yöntemi "whois" sorgularını kullanmaktır (Şekil 3.12).



No.	Time	Source	Destination	Protocol	Length	Info
3692	1...	50.63.243.230	192.168.0.19	HTTP	708	HTTP/1.1 408 Request Timeout (text/html)
3693	1...	192.168.0.19	50.63.243.230	TCP	54	55510 → 80 [ACK] Seq=438 Ack=656 Win=30084 Len=0
3694	1...	192.168.0.19	50.63.243.230	TCP	54	55510 → 80 [FIN, ACK] Seq=438 Ack=656 Win=30084 Len=0
3723	1...	50.63.243.230	192.168.0.19	TCP	60	80 → 55510 [ACK] Seq=656 Ack=439 Win=16384 Len=0
3840	1...	192.168.0.19	74.125.206.94	TCP	54	34418 → 80 [FIN, ACK] Seq=1 Ack=1 Win=29312 Len=0
3848	1...	74.125.206.94	192.168.0.19	TCP	60	80 → 34418 [FIN, ACK] Seq=1 Ack=2 Win=85760 Len=0
3849	1...	192.168.0.19	74.125.206.94	TCP	54	34418 → 80 [ACK] Seq=2 Ack=2 Win=29312 Len=0
3896	1...	192.168.0.19	93.184.220.29	TCP	54	[TCP Keep-Alive] 44018 → 80 [ACK] Seq=1338 Ack=2389 Win=0 Len=0
3940	1...	93.184.220.29	192.168.0.19	TCP	60	[TCP Keep-Alive ACK] 80 → 44018 [ACK] Seq=2389 Ack=1338 Win=0 Len=0
4109	1...	192.168.0.19	23.63.139.27	OCSP	495	Request
4120	1...	23.63.139.27	192.168.0.19	TCP	1514	TCP segment of a reassembled chunk

Protocol: TCP (6)
▶ Header checksum: 0x60ba [validation disabled]
Source: 50.63.243.230
Destination: 192.168.0.19
▼ [Source GeoIP: United States, Scottsdale, AZ, AS26496 GoDaddy.com, LLC, 33.611900, -111.890701]
[Source GeoIP Country: United States]
[Source GeoIP City: Scottsdale, AZ]
[Source GeoIP AS Number: AS26496 GoDaddy.com, LLC]
[Source GeoIP Latitude: 33.611900]
[Source GeoIP Longitude: -111.890701]
[Destination GeoIP: Unknown]

Şekil 3.11: Wireshark TCP 80 portu trafiği inceleme.



```
root@kali:~# whois hho.edu.tr
** Registrant:
hava harp okulu
hava harp okulu yesilyurt

İstanbul,
Türkiye

** Administrative Contact:
NIC Handle : 
Person :
```

Şekil 3.12: Whois sorgusu ile IP/domain bilgi detayı.

Çizelge 3.5: Dünya geneli mobil cihaz istatistikleri (milyar kişi) [56].

	2014	2015	2016	2017	2018
Dünya Geneli Mobil Kullanıcı Sayısı	5,674	5,808	5,945	6,085	6,228
Toplam Mobil Cihaz	7,733	8,627	9,628	10,825	12,165

Ağ adli bilişimini kolaylaştırmak amacıyla, gerçek zamanlı ağ sızmalarını tespit eden sistemler üzerinde çalışmalar devam etmektedir. Bu alandaki zorluklar içerisinde, TOR olarak adlandırılan anonim ağların kullanılması sebebiyle saldırı kaynağının tespit edilememesi, anonim e-posta sağlayıcılarının kullanılması, IP aldatması yapılması, vekil sunucu (proxy) kullanılması, tünelleme ve VPN kullanımı gibi AF teknikleri yer almaktadır.

3.4.5 Mobil cihaz adli bilişimi (Mobile forensics)

Dijital haberleşmedeki gelişmeler ve insan hayatına getirdiği kolaylıklar, mobil cihazların (akıllı telefon, tablet vb.), hayatın her alanında yaygınlaşmasına sebep olmaktadır. 2017 yılı sonu itibariyle dünya genelinde mobil cihaz sayısının 4,77 milyar olduğu tahmin edilmektedir [55]. Mobil cihazlara ait işletim sistemleri, telefonlar için arama kayıtları, hafızalarındaki belgeler, konum bilgileri, medya verileri ve baz istasyonu sinyalleri gibi her türlü veri mobil cihaz adli bilişimi tarafından delil niteliği olan veriler olarak kullanılmaktadır. Mobil cihaz kullanımının yıllara göre artışını gösteren istatistik bilgileri Çizelge 3.5’te sunulmuştur.

Mobil iletişim cihazları, kablosuz çift yönlü (duplex) iletişimi sağlayan, içeriğinde gömülü sistem veya işletim sistemi bulunduran, en ilkelinin SMS alma gönderme yaptığı, en gelişmişinin internete ve görsel-işitsel ortamlara erişebildiği bütün donanımlar şeklinde tanımlanabilir [57]. Mobil cihaz adli bilişiminde en önemli konu, işletim sisteminin iyi bilinmesi ve işletim sisteminden elde edilecek verilerin tespit edilmesidir. Çizelge 3.6’da görüldüğü üzere, dünya genelinde baskın olan işletim sistemi Android OS olmuştur (IDC Mayıs 2017 [58]).

Herhangi bir adli olayda, denilebilir ki, ilk inceleme alanı, kişilere ait mobil cihaz verileridir. Son aramalar, çekilen fotolar, anlık mesajlaşma bilgileri, videolar, belgeler ve ses kayıt dosyaları en önemli delil kaynakları arasında bulunmaktadır. Verilerin toplanması sırasında adli bilişim süreçlerinin izlenmesi delilin geçerliliği açısından

Çizelge 3.6: Dünya geneli mobil cihaz işletim sistemi oranları.

Periyot	Android	iOS	Windows Phone	Diğerleri
2016 1.Çeyrek	83.4%	15.4%	0.8%	0.4%
2016 2.Çeyrek	87.6%	11.7%	0.4%	0.3%
2016 3.Çeyrek	86.8%	12.5%	0.3%	0.4%
2016 4.Çeyrek	81.4%	18.2%	0.2%	0.2%
2017 1.Çeyrek	85.0%	14.7%	0.1%	0.1%

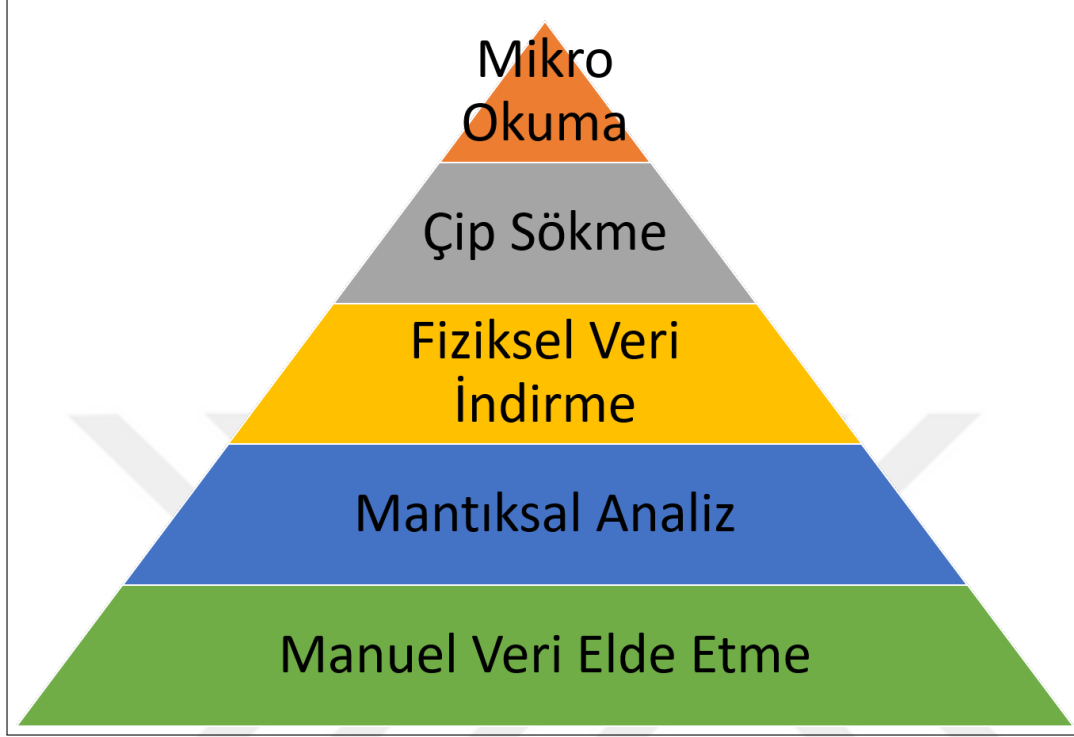
önemlidir. Mobil teknolojilerin çok hızlı gelişmesi, mobil adli bilişimin bilgisayar adli bilişiminden geri kalmasına sebep olmaktadır [59]. Mobil cihazların adli bilişim açısından incelenmesindeki en önemli zorluk, delilin toplanması aşamasında karşılaşılan donanım çeşitliliğidir. Her donanımla uyumlu çalışan imaj alma, verileri kopyalama gibi cihazların bulundurulmasını gerektirmektedir. Verilerin toplanması aşamasında, olay yerinin muhafazasında olduğu gibi mobil cihazında muhafaza edilmesi gerekmektedir. Kablosuz erişim imkanı sunan mobil cihazların ivedilikle ağ etkilerinden korunması için bir Faraday çantasına konularak muhafazası önem taşımaktadır. Aksi halde şüpheli tarafından uzaktan silme komutu çalıştırılabilmektedir [60].

Mobil cihazların adli olarak incelenmesini mümkün kılan tek bir ABA yoktur. Her aracın zayıf ve kuvvetli tarafları bilinerek incelemede yol alınmalıdır. Donanım çeşitliliğinin yanısıra Mobil OS farklılıkları, mobil cihaz güvenlik özellikleri, gerekli kaynak ihtiyacı eksikliği, cihazın anlık durumu, şifre koruması ve kötücül yazılımlar bu alanda mobil ABU'ların yaşadığı zorluklar arasındadır.

Mobil telefonlara yönelik ABA'lardaki çeşitlilik bu araçları bir sınıflandırma ihtiyacı doğurmuş ve bunun sonucunda Mobil Telefon ABA piramidi, cep telefonlarının adli olarak incelenmesi için kullanılan ABA'lara bir model önermiştir [61]. Mobil telefon ABA sınıflandırmasına ait piramit Şekil 3.13'te verilmektedir. Bu piramitte mobil ABA'lar, icra ettikleri inceleme yöntemine göre sınıflandırılmışlardır. Aşağıdan yukarıya ABA'ların teknik seviyesi karmaşılaşmakta ve uzmanlık gereksinimi artmaktadır. Mobil cihazın kendisinin dışında, yüklü uygulamalar ile yapılan bilgi alışverişine ait veriler, hafıza kartları, SIM kartı, operatörler de veri elde etmede başvurulan kaynaklardır. Tüm bu veri kaynakları için, uygun okuyucuları içeren ABA'lara (SIM için PC/SC okuyucu gibi) ihtiyaç duyulmaktadır. SIM den elde edilen

veriler yardımıyla operatörden detaylı arama kayıtları ile abone bilgilerine ait bilgiler istenebilmektedir.

Şekil 3.13’te verilen piramitteki sınıflar aşağıda kısaca açıklanmaktadır.



Şekil 3.13: Mobil telefon ABA yöntem sınıflandırma piramidi.

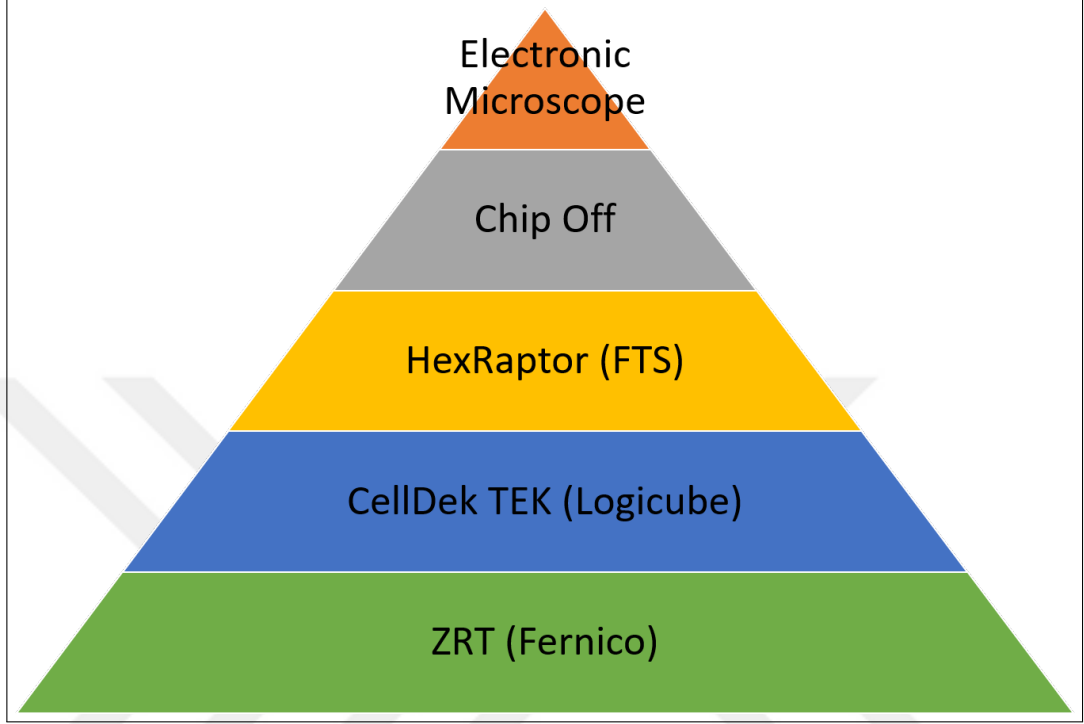
Manuel veri elde etme, direkt olarak cihazın kendisini kullanarak verilere göz atılması işlemidir. Halihazır verilere ulaşılabilir fakat silinmiş dosyalar gibi her türlü veriye ulaşmak mümkün değildir.

Mantıksal analizde, mobil cihaza veri kablosu yardımıyla bağlanmayı sağlayan ABA’lar kullanılmaktadır. Birçok verinin elde edildiği bu yöntemde dosya işlemlerinde bazı komutlar kullanılabilmekte, yalnız veri kurtarma yapılamamaktadır. Ayrıca verinin değişmesine de sebep olabilmektedir.

Fiziksel Veri İndirmede, teknik bilgi ihtiyacı fazladır. Bu kısımdaki yazılımlar, verinin ham halinin kopyalanmasını sağlar. Bu sayede veri kurtarımına imkan vermektedir. Birçok bağlantı kablosu ve çiplerin çıkartılarak kopyasının alınmasını gerektirebilir.

Çip sökmede, dahili bellek olarak kullanılan çip sökülerek farklı bir telefon ya da çip okuyucu ile içindeki verilerin alındığı araçlar kullanılmaktadır. Pahalı ve teknik bilgi gereksinimi oldukça fazladır.

Mikro okuma ise telefonun mikroskoplar ile elektronik devrelerinin en ince ayrıntısına kadar incelendiği, genellikle fiziksel olarak zarar görmüş telefonlarda kullanılan araçları içeren sınıftır. Bu sınıflara ait örnek ABA'ların sunulduğu piramit Şekil 3.14'de verilmektedir [62].



Şekil 3.14: Mobil telefon örnek ABA sınıflandırma piramidi.

Mobil Adli Bilişim için diğer bir zorlukta, cihazın fiziksel zarar görmesi durumunda kullanıcıya ait verilerin buluttaki yedeğine ulaşma sorunudur. Bulut yapının doğası gereği dağıtık olan verilerin konumunu belirlemek ve ilgili makamlardan bu bilgileri istemek bile zor bir süreçtir.

3.4.6 Kötücül yazılım adli bilişimi (Malware forensics)

Kötücül yazılım adli bilişimi, kendini gizleyerek kullanıcıdan habersiz şekilde çalışan zararlı yazılımların tespiti için başvurulan bir yöntemdir. Kendini ağ bağlantılarından, çalışan işlemlerden (process) ve kayıt defterinden bile gizleyebilen yazılımlar, çalışma zamanlarında RAM bellek üzerinde açık bir şekilde çalışmak zorundadırlar [4]. RAM kopyası indirilerek (Live Memory Dump) üzerinde yapılacak analiz, zararlı yazılımların tespitinde önemli rol oynamaktadır.

Günümüzde zararlı yazılım bulaşmamış bilgisayarın neredeyse olmadığı düşünüldüğünde, zararlı yazılımın sadece tespiti yeterli olmamakta aynı zamanda

zararlı yazılımın işlevinin suç unsuru taşıyıp taşımadığı da tespit edilmelidir. RAM belleğin kopyasının, imajların güvenilir bir antivirüs (AV) programı ile taranması da zararlı yazılımların tespit edilmesini sağlayabilmektedir.

Zararlı yazılımlar doğası gereği, analiz araçlarından kaçınma tekniklerini kullanırlar. Öyle ki zararlı yazılımlar için analizden kaçınma araç ve tekniklerinin sayısı, tespiti için hazırlanan araç ve yöntemlerin sayısından oldukça fazladır [63]. Zararlı yazılımlar, karartma (obfuscation), parçalara ayrılmama (anti-disassembly), şifreli ve sıkıştırılmış veri, veriyi yok etme ve derletmeme gibi adli bilişim analizinden kaçınma yöntemlerini kullanmaktadırlar [24]. Zararlı yazılımlar arasında mantıksal bombalar (logic bombs), virüs, solucan, truva yazılımları ve arka kapı (backdoor) yazılımları yer almaktadır. Zararlı yazılımlar, ABA'ların açıklıklarını istismar edebilir, analiz edildiğini tespit edip sistemi çökertebilir. Özellikle rootkit yazılımlar, diske taşınmadan sadece geçici bellek üzerinde ve çalışan legal işlemlere (process) gömülü olarak çalışarak, tespit edilmekten sakınılmaktadırlar.

Bilinen zararlı yazılımların tespiti için her türlü dosya ve URL adresi [64]'de taratılarak bilgi alınabilir (Şekil 3.15). Fakat unutulmamalıdır ki, zararlı olarak tespit edilmeyen her yazılım zararsız olarak kabul edilmemeli, sadece bilinen kötücül yazılımları içermediği göz önünde bulundurulmalıdır.



The image shows the VirusTotal website interface. At the top is the VirusTotal logo. Below it, a text line states: "VirusTotal **Şüpheli URL ve dosyaları inceleyen** ücretsiz bir servistir ve virüslerin , solucanların ve tüm zararlı yazılımların tespitini kolaylaştırır." Below this text are three tabs: "Dosya" (selected), "URL", and "Arama". Under the "Dosya" tab, there is a text input field containing "Dosya seçilmedi." and a button labeled "Dosyayı seç.". Below the input field, it says "Maksimum dosya boyutu: 128MB". Further down, there is a disclaimer: "Tara'ya tıklayarak, Kullanım Koşullarını kabul etmiş ve VirusTotal in bu dosyayı toplulukla paylaşmasına izin vermiş olursunuz. Ayrıntılar için Gizlilik Politikamızı görün." At the bottom, there is a large blue button labeled "Tara!".

Şekil 3.15: Virustotal zararlı yazılım tarama sitesi.

3.4.7 Geçici bellek adli bilişimi (Memory forensics)

Adli bilişim genellikle sabit disk üzerinde yürütülen çabalardan meydana gelmektedir. Fakat birebir kopyalanıp, sabit disk üzerindeki incelemelerden daha fazla yarar sağlayacak olan diğer bir yöntem ise "Geçici Bellek Adli Bilişimi"dir. Geçici bellek adli bilişimi ile açık durumda olan bilgisayar belleği verilerinden, işletim sistemi, e-posta ve sosyal medya şifreleri, açık olan web siteleri, çalışan uygulamalar, şifreli bir dokümanın açık haline ait bilgiler gibi çok önemli ve delil niteliği oluşturabilecek verilere ulaşmak mümkün olmaktadır. Bu önemi nedeniyle adli bilişim süreçleri içerisinde, zorunlu bir standart haline getirilmesi gerekmektedir.

Geçici belleklerde veriler, kısa süreli depolarda (bellek, CPU'daki önbellek (Cache), grafik kartı arabirimi bellekleri) muhafaza edilmektedir. Enerji kesintisi durumunda üzerinde veri tutamazlar. Bu nedenle çalışan sisteme ait belleğin zaman kaybedilemeden ve sistem kapatılmadan kopyasının alınması çok önemlidir.

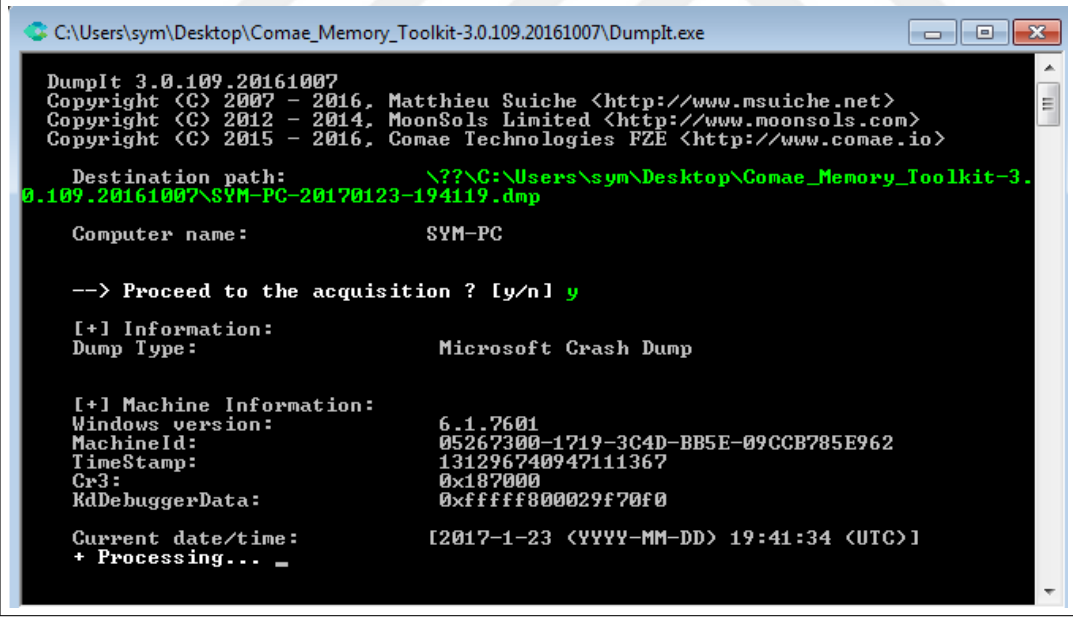
Bellek üzerinde tutulan bilgiler [65]:

- Çalışmakta olan işlemler ile hizmet bilgileri,
- Sisteme ait bilgiler,
- Kullanıcı hesabı bilgileri,
- Ağ bağlantı durum bilgileri,
- Kopyalama panosunda bulunan bilgiler,
- Çalışmakta olan yazılımların bilgileri,
- Komut işleticisinden girilen komutlar,
- İşletim sistemi kayıt defterine ait bilgiler,
- Sosyal uygulamalar ve e-posta parolaları,
- Tarayıcı geçmiş site bilgileri,
- Elektronik posta bilgileri,
- Disk şifrelemesine ait parolalar,

- İşletim sistemi parolaları verileri bulunmaktadır.

Kötücül yazılımların diskte iz bırakmamak için, kendisini bellekte çalıştırması bilinen bir yöntemdir. Bu yazılımlar özellikle bir ABA ile analiz edildiğini tespit edip NOP durumuna geçerek, analiz araçlarının kendisini tespit edememelerini sağlamaktadır. Bellekteki veriler, kötücül yazılımların tespiti açısından da çok kıymetlidir. Bellek imajı almak için de disk imajı almadaki gibi işletim sistemlerine özel yazılım ve donanımlar bulunmaktadır.

MS Windows OS için, Dumpit, Belkasoft Live RAM Capturer, Mandiant Memoryze, F-Response, Mantech Memory DD, KnTDD, Fastdump, Win32dd yazılımları ön plana çıkmaktadır [66]. Dumpit yazılımı günümüzde Comae firması tarafından sunulmaktadır [67]. Dumpit yazılımının yanında Hibr2Bin programı da sunulmaktadır. Hibr2Bin MS Windows'ta Hibernate dosyasının incelenmesini sağlayan popüler bir yazılımdır. Yazılım çalıştırılmasına ait ekran görüntüsü Şekil 3.16'da verilmektedir. Oluşturulan dump dosyası, program ile aynı dosya yoluna oluşturulmaktadır.



```
C:\Users\sym\Desktop\Comae_Memory_Toolkit-3.0.109.20161007\DumpIt.exe

DumpIt 3.0.109.20161007
Copyright (C) 2007 - 2016, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2016, Comae Technologies FZE <http://www.comae.io>

Destination path:      \??C:\Users\sym\Desktop\Comae_Memory_Toolkit-3.0.109.20161007\SYM-PC-20170123-194119.dmp
Computer name:         SYM-PC

--> Proceed to the acquisition ? [y/n] y

[+] Information:
Dump Type:             Microsoft Crash Dump

[+] Machine Information:
Windows version:       6.1.7601
MachineId:             05267300-1719-3C4D-BB5E-09CCB785E962
TimeStamp:             131296740947111367
Cr3:                   0x187000
KdDebuggerData:        0xfffff800029f70f0

Current date/time:     [2017-1-23 <YYYY-MM-DD> 19:41:34 <UTC>]
+ Processing... _
```

Şekil 3.16: Dumpit bellek birebir kopya alma.

Oluşturulan .dmp uzantılı dosya içeriğini okumak için "Volatility" adlı açık kaynak ABA kullanılabilmektedir. Bu yazılım aracılığı ile komut satırı yardımıyla .dmp dosyasının içeriğindeki işlemler ve servisler, dll listeleri, zararlı yazılım bulma, dosyaları inceleme ve yardım (-h) menüsünden ulaşabileceğiniz daha birçok özelliği ile ABU'lar için çok kıymetli veriler sağlamaktadır. Örnek olarak belleğin birebir

kopyasında volatility aracılığı ile çalışan işlemleri (process list) gösteren ekran görüntüsü Şekil 3.17’de verilmektedir.

Offset(U)	Name	Exit	PID	PPID	Thds	Hnds	Sess	Wo
0xfffffa80018ad040	System		4	0	121	590	-----	
0 2017-01-23 20:28:30 UTC+0000								
0xfffffa8002b51040	smss.exe		376	4	2	30	-----	
0 2017-01-23 20:28:30 UTC+0000								
0xfffffa8003359b10	csrss.exe		452	440	9	570	0	
0 2017-01-23 20:28:38 UTC+0000								
0xfffffa80034448f0	wininit.exe		488	440	3	77	0	
0 2017-01-23 20:28:39 UTC+0000								
0xfffffa8003352b10	csrss.exe		500	480	8	242	1	
0 2017-01-23 20:28:39 UTC+0000								
0xfffffa80034738f0	winlogon.exe		536	480	4	119	1	
0 2017-01-23 20:28:39 UTC+0000								
0xfffffa80034bcb10	services.exe		580	488	10	218	0	
0 2017-01-23 20:28:40 UTC+0000								
0xfffffa80034d3b10	lsass.exe		596	488	7	614	0	
0 2017-01-23 20:28:41 UTC+0000								
0xfffffa80034e4b10	lsm.exe		608	488	10	143	0	
0 2017-01-23 20:28:41 UTC+0000								
0xfffffa80032c2b10	svchost.exe		712	580	10	360	0	
0 2017-01-23 20:28:52 UTC+0000								
0xfffffa80036c3060	VBoxService.exe		776	580	12	120	0	
0 2017-01-23 20:28:53 UTC+0000								
0xfffffa80036d4b10	svchost.exe		832	580	8	300	0	
0 2017-01-23 19:28:56 UTC+0000								
0xfffffa8003707b10	MsMpEng.exe		884	580	12	433	0	
0 2017-01-23 19:28:56 UTC+0000								
0xfffffa800337b060	svchost.exe		988	580	21	476	0	
0 2017-01-23 19:28:58 UTC+0000								
0xfffffa8003387b10	svchost.exe		108	580	22	458	0	
0 2017-01-23 19:28:58 UTC+0000								
0xfffffa80033a6b10	svchost.exe		408	580	16	391	0	
0 2017-01-23 19:28:58 UTC+0000								
0xfffffa80033d5b10	svchost.exe		484	580	42	1665	0	

Şekil 3.17: Volatility .dmp dosyası içeriğinin analizi.

Belleğin birebir kopyasında belleğin tamamı kopyalanabileceği gibi, çalışan sistemdeki belirli işlemlerin kopyası da alınabilmektedir. Bu kapsamda kullanılan yazılımlardan olan "ProcDump" [68] ile herhangi bir işleme ait mini kopya (minidump) alınabilmektedir. MS Windows sistemlerde kullanıcı hesaplarına ait şifre bilgilerini içeren lsass.exe (Local Security Authority Service) işleminin mini kopyası alınabilir (Şekil 3.18). Oluşturulan .dmp dosyası ProcDump ile aynı dosya yolunda bulunacaktır.

Sonuç olarak oluşturulan lsass.dmp dosyası da "Mimikatz" [69] yazılımı yardımı ile incelenebilmekte ve aktif kullanıcılara ait sistem şifreleri elde edilebilmektedir. Mimikatz ile elde edilmiş şifreleri gösteren görüntü Şekil 3.19’da verilmektedir.

TrueCrypt, BitLocker gibi disk şifreleme yazılımlarına ait parolalar da Forensic Disk Decryptor gibi programlar vasıtasıyla elde edilmekte ve şifrelenmiş sürücülere ait veriler deşifre edilebilmektedir. MS Windows sistemler için anlatımı yapılan tüm bu işlemler Linux ve Mac OS’ler için de yapılabilmektedir.

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd\

C:\>cd Procdump

C:\Procdump>procdump.exe -ma lsass.exe lsass.dmp

Procdump v8.2 - Sysinternals process dump utility
Copyright (C) 2009-2016 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[23:37:43] Dump 1 initiated: C:\Procdump\lsass.dmp
[23:37:46] Dump 1 writing: Estimated dump file size is 30 MB.
[23:37:48] Dump 1 complete: 30 MB written in 4.2 seconds
[23:37:48] Dump count reached.

C:\Procdump>_
```

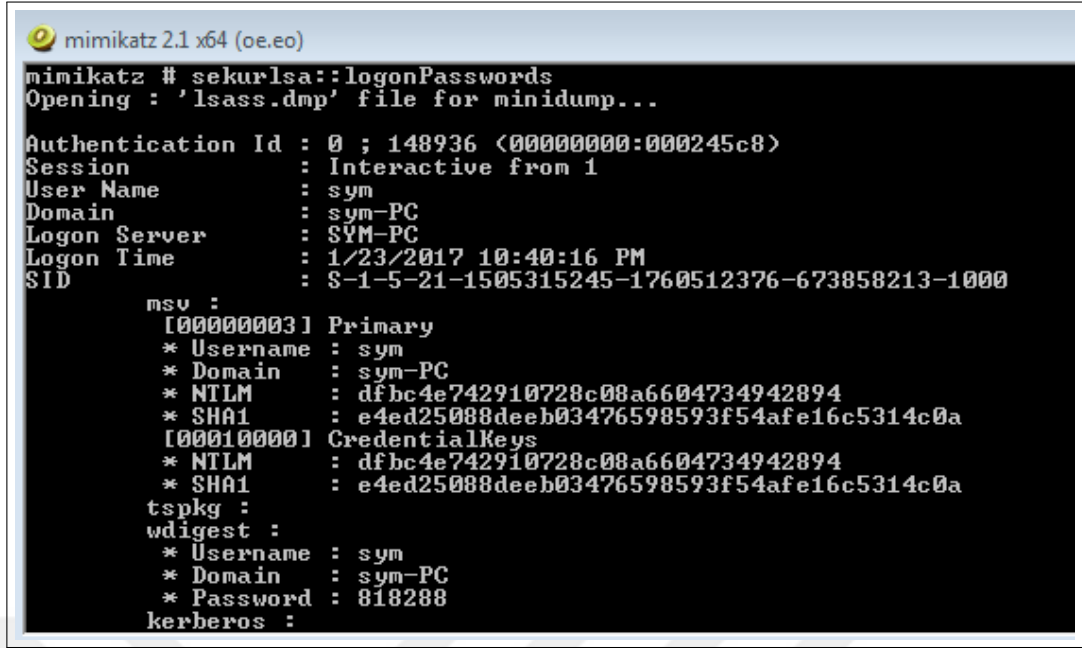
Şekil 3.18: ProcDump ile lsass.exe mini kopya alınması.

Çizelge 3.7: Sanallaştırma teknolojileri sanal bellek dosyaları.

Sanallaştırma Teknolojisi	Bellek Dosya Uzantısı
VirtualBox	.sav
VMware	.vmem
Hyper-V	.bin

Sanallaştırma teknolojisi kullanılan bilgisayarlar da bellek yönetimi, sanal makineye ait bir dosya aracılığı ile gerçekleştirildiğinden, sanal makinelerin bellek analizi bu dosyaların incelenmesi ile mümkün olmaktadır. Bilinen sanallaştırma teknolojilerine ait bellek dosyalarını gösteren tablo Çizelge 3.7’de verilmektedir. Sanal makinelerin adli bilişim açısından sağladığı birtakım kolaylıklar bulunmaktadır. "Snapshot" adı verilen makinenin çalıştığı bir ana ait tüm çalışan işlemleri de içeren anlık kopya, makine klonlama, disk dosyasının direkt olarak incelenebilmesi gibi kolaylıklar sağlamaktadırlar.

Tüm bu bilgiler ışığında, elde edilen veriler incelendiğinde adli bilişim soruşturması açısından çok önemli bilgilere ulaşılabildiği, bu nedenle de geçici bellek adli bilişiminin her dönemde önemli bir alan olarak kalacağı öngörülmektedir. Bu alanda çalışmaların artarak devam edeceği, yetişmiş personel ihtiyacının da artacağı değerlendirilmektedir.



```
mimikatz 2.1 x64 (oe.eo)
mimikatz # sekurlsa::logonPasswords
Opening : 'lsass.dmp' file for minidump...

Authentication Id : 0 ; 148936 (00000000:000245c8)
Session : Interactive from 1
User Name : sym
Domain : sym-PC
Logon Server : SYM-PC
Logon Time : 1/23/2017 10:40:16 PM
SID : S-1-5-21-1505315245-1760512376-673858213-1000

msv :
[00000003] Primary
* Username : sym
* Domain : sym-PC
* NTLM : dfbc4e742910728c08a6604734942894
* SHA1 : e4ed25088deeb03476598593f54afe16c5314c0a
[00010000] CredentialKeys
* NTLM : dfbc4e742910728c08a6604734942894
* SHA1 : e4ed25088deeb03476598593f54afe16c5314c0a
tspkg :
wdigest :
* Username : sym
* Domain : sym-PC
* Password : 818288
kerberos :
```

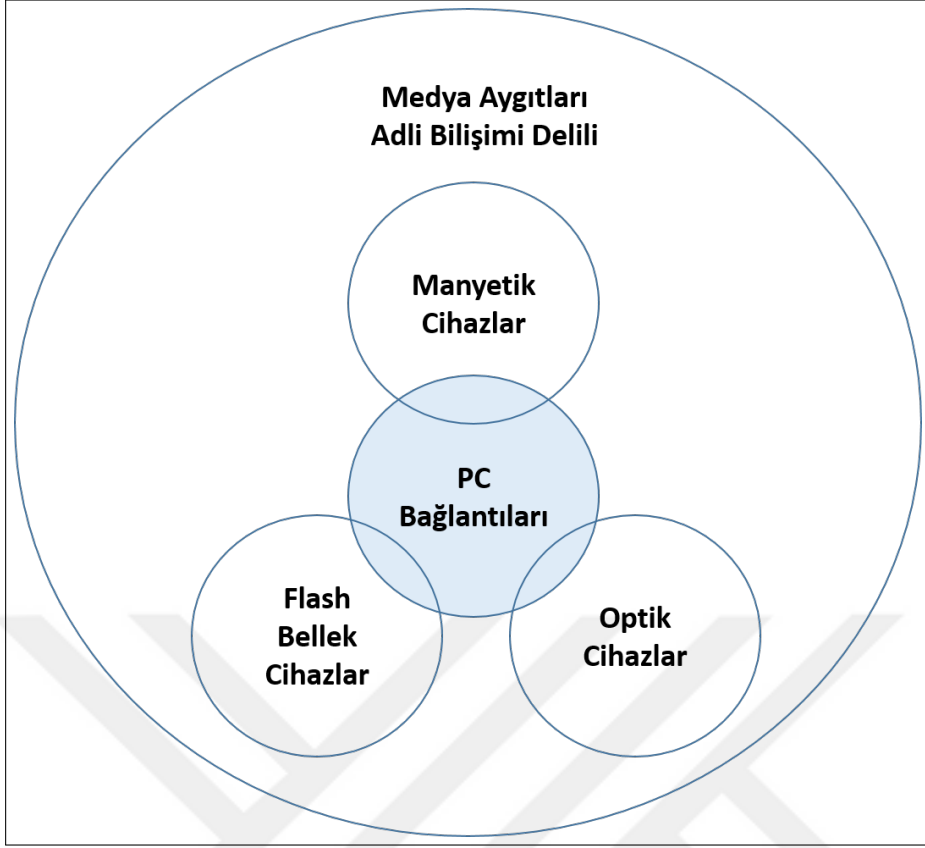
Şekil 3.19: Mimikatz yazılımı ile mini kopyadan şifre elde etme.

3.4.8 Medya aygıtları adli bilişimi (Media device forensics)

Medya cihazları olarak adlandırılan USB bellekler, taşınabilir diskler, dijital müzik çalarlar, dijital fotoğraf makineleri, ses kayıt cihazları, navigasyon cihazları, PDA ve oyun konsolları günümüz dünyasının vazgeçilmez aksesuarları haline gelmiştir. Adli bilişim açısından delil niteliği taşıyabilecek verileri de muhafaza etmek amacıyla kullanılabilen araçlardır. Bu alanda adli bilişim açısından yaşanan zorluklardan en önemlisi, teknolojilerinin çok hızlı ilerlemesidir. Bu kategorideki cihazlar "küçük ölçekli dijital cihazlar" olarak da adlandırılmaktadır.

Suç unsuru olan dijital verilerin taşınması, illegal olarak ses kaydı yapılması veya görüntü elde edilmesi medya aygıtları adli bilişimi tarafından incelenmektedir. Sabit disklerle aynı mantıkta çalışan sistemler, silme imkanı da sağladığından, suçlulara verilerini yok etme fırsatı da tanımaktadır. Bu kapsamda bu alanda da verilerin kurtarılması, suç unsuru verinin analiz edilmesi gerekmektedir.

Medya aygıtları adli bilişimi ile dijital delilin elde edilmesi için, medya aygıtı temel iç bileşenleri açısından ayrı ayrı incelenerek analiz yapılması gerekmektedir. Bu temel bileşenler [70]'de Şekil 3.20'de verilmektedir. Her bir bileşen, veriyi manyetik ortamda, optik ortamda, SSD olarak tabir edilen flash bellekte veya bilgisayar bağlantısı yoluyla muhafaza edebilecek alt yapılardır.



Şekil 3.20: Medya aygıtları adli bilişimi temel bileşenleri [70].

Örnek olarak PDA'lerin adli analizi için Paraben'e ait E3:DS [71] adlı ürün, bu alanda de facto bir standart haline gelmiştir [72]. Gelişmiş özellikleriyle, dosya sistemlerinin ve içeriklerinin analizi, anahtar kelime arama, kötücül yazılım tespiti gibi imkanlar sunmaktadır. Fakat bu alanda tüm medya aygıtları için uyumlu tek bir ABA bulunmamaktadır.

3.4.9 Sosyal ağ adli bilişimi (Social media forensics)

Sosyal ağlar, günümüzde dünya genelinde yaygın olarak kullanılmaktadır. Sadece Facebook uygulamasının 2017 dördüncü çeyreğinde aktif kullanıcı sayısı 2,2 milyar kişiye ulaşmıştır ve bu kullanıcıların 1,74 milyarı mobil uygulama üzerinden sosyal ağa katılmaktadır [73]. Bu rakamlar bile göstermektedir ki, sosyal ağ üzerinde işlenen herhangi bir suça yönelik araştırma için özel bir adli bilişim alt alanına ihtiyaç bulunmaktadır.

Sosyal ağ hizmetleri ile kullanıcılar etkileşim ve sosyalleşme sağlamakta, bilgi ve fikirlerini paylaşabilmekte, yorum ve güncel olayları paylaşabilmekte, dosya ve resim yükleyebilmekte, anlık mesajlaşma ve görüşme imkanı bulmaktadırlar. Fakat bunun

yanında sosyal ağlarda masum görünümlü hesaplar açan suçlular, phishing, sahtekarlık ve çocuk istismarcılığı gibi suçlar için profil oluşturup faaliyetlerde bulunabilmektedir. Ayrıca suçlular, bu ağlardaki kullanıcılara ait profil bilgilerinden faydalanarak suçlar işleyebilmektedir. Bu ağlarda işlenmesi mümkün olan suçlar arasında, illegal paylaşımlarda bulunmak, hakaret ve küfür gibi kişilere yönelik aktivitelerde yer almaktadır. Bu alanda bilgi kaynağı olabilecek, ABU'lara delil niteliği sağlayacak veriler iki kaynaktan elde edilmektedir. Bunların birincisi kullanıcı cihazından elde edilen bilgiler, diğeri ise sosyal ağ uygulamasının hizmet sağlayıcısından elde edilen bilgilerdir. Genel olarak suçu ispatlamayı sağlayacak olan veriler de hizmet sağlayıcısında tutulmaktadır. Delilin geçerliliği ve güvenilirliği açısından normal adli bilişim süreçlerinin izlenmesi yeterli kalmamaktadır. Sosyal ağ uygulamaları kullanıcı sayılarının çokluğu nedeniyle, bulut bilişim ve dağıtık yapının sağlamış olduğu hizmetlerden faydalanmaktadırlar. Hizmet sağlayıcının dağıtık yapısı gereği uluslararası ortak bir yapı bulunmadığından istenilen bilgiye ulaşılamamakta ya da kabul edilebilir zaman dilimi içerisinde işlemler gerçekleştirilememektedir. Hizmet sağlayıcıya başvurmadan Facebook üzerinden API geliştirmek suretiyle kullanıcılara ait kimlik bilgisi ile kullanıcıların bağlı oldukları sosyal ağ hakkında bilgi edinebilecek bir algoritma [74]'te açıklanmıştır. Ancak bu çalışmada yapılan işlemler sosyal ağların analizi yöntemlerinden faydalanmaktadır. Elde edilen veriler sadece arkadaşlık ilişkilerini ve aktif kullanım zamanı bilgilerini içermektedir.

Sosyal ağlara ait sunucuların sabit disklerinin bir kopyasını almak büyük ölçekli sosyal ağlarda uygulanabilir olamamaktadır. Şüpheliye ait hesabın tutulduğu sunucu tespit edilse bile hizmet sağlayıcının işbirliği gerekmektedir. Bir yöntem olarak sistemin çalışması şartıyla geçici bellek adli bilişimi yöntemleriyle kullanıcının sosyal ağdaki hareketleri, lokal web tarayıcısının önbelleğindeki bilgilerden faydalanılarak tespit edilebilir. Mahkeme kararıyla şüphelinin genel ağ hareketleri pasif olarak dinlenebilir ve sosyal ağ uygulamasına bağlantıları ve paketleri incelemeye alınabilir. Fakat bu yöntemde veri elde etmek oldukça zaman alıcı ve tüm uygulamaların https protokolü kullanması nedeniyle elde edilen bilgiler şifreli olduğundan geçerli bir veri sağlayamamaktadır. Bu yöntem içerik olarak bilgi sağlamasa da, bir iletişim olduğunu ispatlamakta geçerlidir.

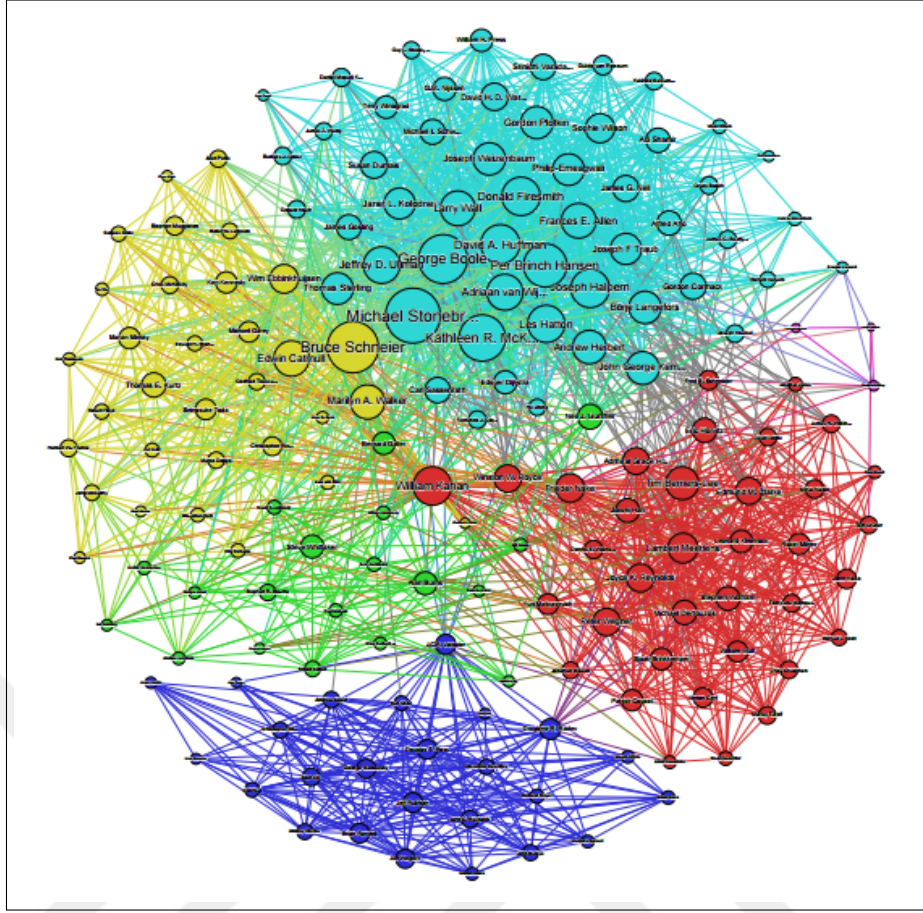
Bir sosyal ağ analizinde öncelikle aşağıdaki izler belirlenmektedir [75]:

- Sosyal Ayak İzi: Kullanıcı kimlerle arkadaşlık/bağlantı içerisindedir?
- İletişim yöntemi: Kullanıcı hangi yöntemler ile iletişim kurmakta ve kimlerle bu iletişimi sağlamaktadır?
- Video ve Resimler: Kullanıcı hangi video ve resimleri sosyal ağı yükledi, resimlerde başka kimleri etiketledi?
- Aktivite zamanları: Şüpheli kullanıcı sosyal ağı ne zaman bağlandı, şüpheli aktiviteyi ne zaman yaptı?
- Uygulamalar: Kullanıcı sosyal ağı üzerinde hangi uygulamaları kullanmaktadır, bu uygulamaların kullanım amacı nedir, herhangi bir sosyal içeriğe sahip midir?

Bu bilgilerin dışında konum bilgisi de kullanıcı faaliyetleri arasında önemli yer tutmaktadır. Tüm bu bilgiler adli bilişim açısından çok önemli iken, şüphelinin bilgisayarından elde edilemezler. Bu bilgilerin çoğu hizmet sağlayıcıda muhafaza edilmektedir. Öyle ki günümüzde Facebook kullanıcılara, anılarını paylaşma imkanı sunmaktadır. Bazı bilgiler kişilere ait bilgisayarlarda tarayıcı önbelleklerinde bulunabilir, fakat bu bilgiler devamlı ve bütün bir bilgi olmadığından bütünüyle güvenilir bir bilgi kaynağı olamamaktadır. Bilgiyi elde etmenin en kolay yolu kullanıcıdan kullanıcı adı ve şifrenin elde edilerek, uygulamanın incelenmesi ile mümkündür.

Sosyal ağı ABA'ndan beklenen olay izleme (kötücül bir yazılımın yayılmasının ilk kaynağını belirleme gibi), zaman çizelgesi karşılaştırma gibi özelliklere sahip olmasıdır. [75]'te bir geliştirme arayüzü ile API yardımıyla Facebook kullanıcısının bağlantılı oldukları kişilere ait Şekil 3.21'deki bağlantı çizgesi oluşturulmuştur. Bunun dışında API sorgusu ile kullanıcının paylaştığı resimlerde etiketli olan kişiler ile arkadaşlık bağı sorgulanmış, kullanıcının 24 saatlik zaman çizelgesi de farklı bir sorgu yardımıyla elde edilmiştir (Şekil 3.22). Böylece kişinin iş, aile, okul arkadaşlık gruplamaları, en çok iletişimde olduğu kişileri ve günlük aktiviteleri elde edilmiştir.

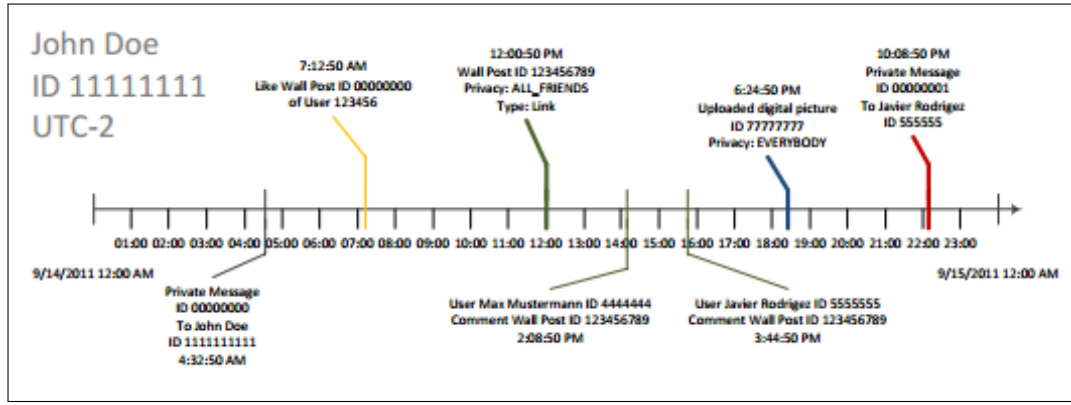
Aynı çalışmanın sonuç kısmında, bulguların faydalı olabileceği fakat tamamıyla geçerlilik özelliği taşıma yönünde eksikliklerinin olduğu vurgulanmıştır. Yapılan işlemler sonucunda bulunan bağlantı ve iletişim bilgileri sürekli değişiklik göster-



Şekil 3.21: Facebook kullanıcı bağlantı çizgesi [75].

mekte, inceleme yapıldıktan sonra kullanıcının herhangi biri ile bağlantısını kesmesi de mümkün olmaktadır.

Bir başka çalışmada Facebook uygulaması üzerinde yapılan sohbetlerin, kullanıcı bilgisayarındaki disk üzerinden kurtarılmasına yönelik çalışmalar anlatılmaktadır [76]. Ayrıca aynı yazarlar akıllı telefonlar üzerinde sosyal ağ izlerine ulaşmak amacıyla farklı bir çalışma daha yürütmüşlerdir [77]. Çalışmada akıllı telefonlar üzerinde root yetkisi alınması durumunda, uygulamaların normalde kullanıcıya göstermediği veritabanı dosyalarının içeriğine ulaşılabildiği, telefondaki uygulamalara ait dosyaların birebir kopyasının alınmasının ise root yetkisi gerektirmediği vurgulanmıştır. Yapılan çalışmada Blackberry, Iphone ve Android telefonlarda, Facebook, Twitter ve MySpace uygulamalarına ilişkin adli bilişim ile elde edilebilen verileri bir çizelgede sunmuşlardır. Çizelgedeki sonuçlardan kullanım yaygınlığı sebebiyle sadece Android işletim sistemi üzerindeki bulgular Çizelge 3.8’de sunulmuştur.



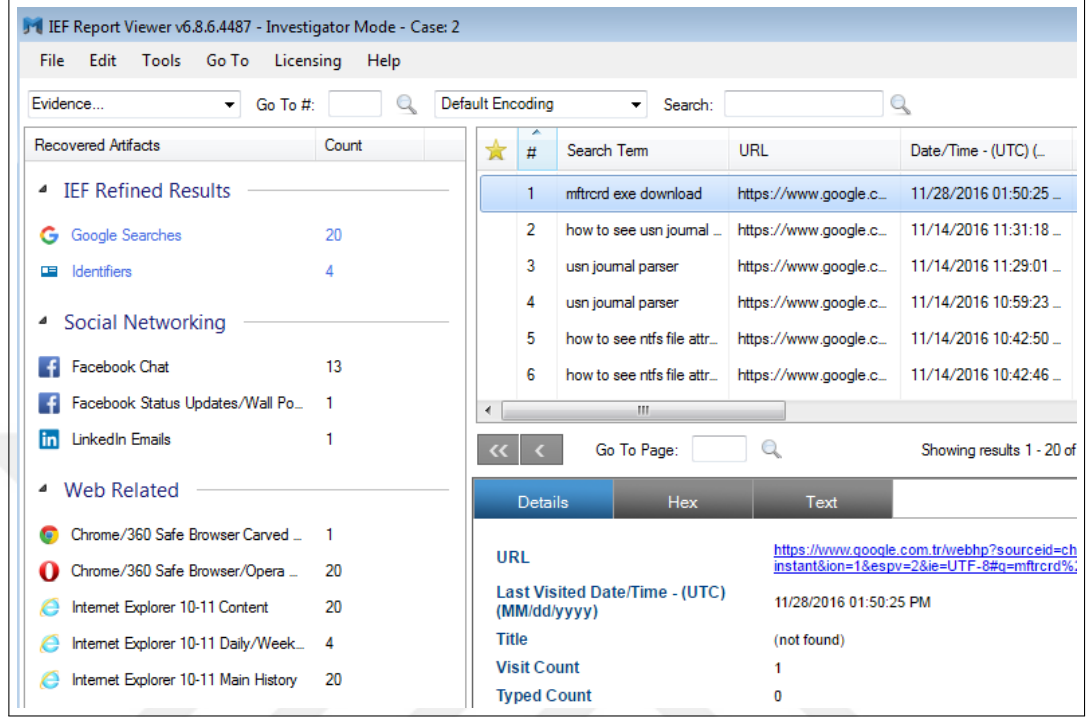
Şekil 3.22: Facebook kullanıcı faaliyeti zaman çizgesi [75].

Çizelge 3.8: Android cihazda sosyal ağ adli bilişimi ile elde edilen bilgiler.

Mobil Uygulama	Adli Bilişim İle Elde Edilen Bilgiler
Facebook	Kullanıcı ve arkadaş Bilgileri Bağlantı Detayları ve Profil Foto Yüklemeleri Oluşturulan Albümler Görüntülenen Resimler E-posta/Sohbet mesajları
Twitter	Kullanıcı ve Takip Ettikleri İçin: Kullanıcı Adları Paylaşılan Tweetler ve Fotolar Cihaz Bilgileri vb.
MySpace	Kullanıcı Adı/Şifre Çerezler ve Önbellek Dosyaları

Sosyal ağ ve bulut bilişimin adli bilişim açısından incelenmesindeki zorluklar, sosyal ağ hizmet sağlayıcılarının işbirliği göstermesi durumunda aşılacak durumlardır. Süreklilik sağlaması açısından, sosyal ağların mobil cihazlarda kullanımının artacağı değerlendirilmektedir. Mobil cihazlarda yapılan inceleme ile sosyal ağlara ait değerli bilgilere ulaşmanın, masaüstü bilgisayarlardan elde etmeye oranla daha kolay olduğu söylenebilmektedir. Sadece sosyal ağ aktiviteleri için değil, aynı zamanda internet üzerinde yapılan faaliyetlerin önbellek üzerinde tutulan bilgiler aracılığı ile görüntülenmesi, paylaşılan fotoğrafların tespiti ve anlık mesajlaşma verileri gibi sosyal ağlara ait bilgilerin CacheBack ABA'sı ile elde edilebildiği üreticisi tarafından iddia edilmektedir. Öte yandan aynı amaçlara hizmet etmek amacıyla Internet Evidence Finder (IEF) ABA'sının da etkin olduğu üreticisi tarafından iddia edilmektedir. Söz konusu ABA'lar bilgisayar adli bilişiminde kullanılan disklerin birebir kopyası formatları ile sanal makine disk formatlarını girdi olarak kabul etmektedir. Bütün tarayıcıları destekleyen ABA'lar, tarayıcılara ait önbellek verilerini kullanarak görsel

şekilde geçmiş verilerin görüntülenmesini sağlamaktadır. Sosyal ağ adli bilişimi ve internet kullanımına ait delil tespitine yönelik Internet Evidence Finder kullanımına ait örnek görüntü Şekil 3.23'te verilmektedir.



Şekil 3.23: Sosyal ağ adli bilişimi için IEF ABA kullanımı.

Adli bilişime ait alt adli bilişim alanları, inceleme yapılan alanlara göre bu bölümde anlatılanların dışında da çoğaltılabilir. Bu bölümde, alt alan olarak, kullanım sıklığı açısından en çok başvuru alan yöntemlere göre adli bilişim türleri ele alınmıştır. Bunun dışında (navigasyon) GPS, Bulut Bilişim adli bilişimi gibi alt dallar da gittikçe öne çıkan adli bilişim dalları arasında göze çarpmaktadır.



4. ADLİ BİLİŞİM ATLATMA, KLASİK ADLİ BİLİŞİM ATLATMA TEKNİKLERİ ve KARŞI TEDBİRLER

Siber/dijital suçların işlenme sıklığı günümüzde artış göstermiş ve karmaşıklık seviyeleri de aynı şekilde gelişmiş durumdadır [78]. Bu nedenle günümüzde, sayısal delilleri elde etmek için dijital adli bilişim (DF) önemli rol oynamaktadır. Dijital adli bilişim soruşturmaları, konumu belirsiz (sınırı belli olmayan) yerlerin bulunduğu bir suç mahali, dijital adli bilişim araçlarını veya süreçlerini yenmeye çalışan saldırganlar ve analiz edilmesi için elde edilmesi gereken veri miktarının büyüklüğü gibi zorluklarla karşılaşmaktadır. Bilgisayar adli bilişimi alanında asıl hedef, adli bilişim araştırmaları sırasında elde edilen verilerden doğru ve güvenilir dijital deliller sunmaktır.

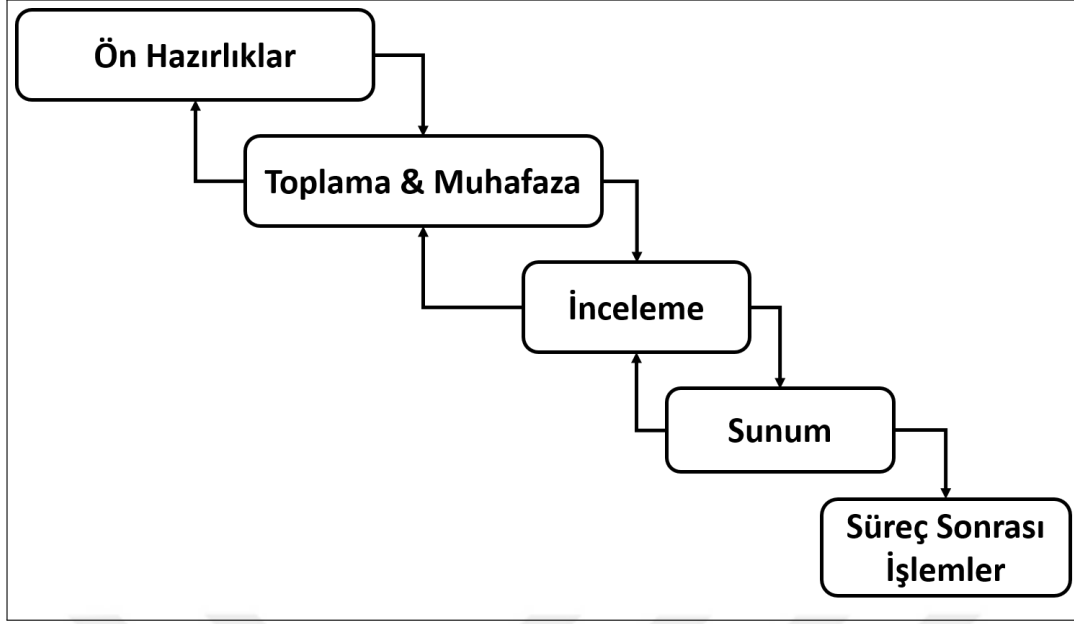
DF [79]'da, "Bir mahkemede tutarlı ve anlamlı bir biçimde sunulabilen, bilgi işlem ekipmanından ve çeşitli depolama aygıtlarından, dijital ortamlardan, delil elde etmek için kullanılan yöntemsel teknikler ve prosedürler serisi" olarak tanımlanmaktadır.

Genel bir DF soruşturmasının aşamaları Şekil 4.1'de gösterilmektedir [80]. Kısaca bu aşamalar veri toplama, veri analizi ve bulgular sunumu olarak da adlandırılabilir. Adli bilişimi atlatma teknikleri, DF soruşturmacılarının saldırganı bulmalarını zorlaştırmak için her aşamayı veya aşamaların bir kısmını hedefleyerek kullanılabilir.

4.1 Adli Bilişimi Atlatma

Elektronik aygıtlar ve BT muazzam ve yaygın bir şekilde, kullanıcılar tarafından hizmet almak amacıyla kullanılmaktadır, ancak suçlular ve saldırganlar tarafından da kötü niyetli amaçlar için kullanılmaktadırlar [81]. ABAT'lar hakkında bilgi eksikliği, adli bilişim analizinin odağını sınırlar; bu nedenle dijital deliller, şüphelinin suçluluk veya masumiyetini ispatlayamazlar. Benzer şekilde, adli bilişimi atlatma araçlarının ayrıntılarını bilmeden, adli bilişim soruşturmacıları, ceza soruşturmacılarına geçerli dijital delilleri sunamazlar.

Adli Bilişimi Atlatma (AF), "Bir olay mahallinden kanıtların varlığını, miktarını ve / veya kalitesini olumsuz yönde etkileme girişimleri veya kanıtların incelenmesini ve



Şekil 4.1: DF soruşturması genel süreçleri.

analizini zorlaştıran ya da imkansız kılan negatif girişimler" olarak tanımlanmıştır [82]. Tanımdan anlaşılacağı üzere, AF'nin amacı, adli bilişim araçlarını ve soruşturmacılarını şaşırtmak ve yanıltmak, yakalanmaktan kaçınan saldırganı bulmayı zorlaştırmak veya adam - saat (TL) ücretinin artmasını sağlamak ve davanın maliyetini çok daha yüksek hale getirmektir. Garfinkel'e göre [16], AF, adli bilişim araçlarını, soruşturmalarını ve soruşturmacılarını yanıltan, giderek artan araçlar ve teknikler topluluğudur. Adli bilişimi atlatma araçlarının ve yöntemlerinin yaratıcıları tarafından AF, adli incelemeye ilişkin olgusal bilgileri geçersiz kılmak için bilimsel yöntemlerin dijital ortama uygulanması olarak belirtilmektedir [13].

AF araçlarını ve tekniklerini kullanan saldırganların hedefleri:

- Dijital delil toplama işlemini aksatmak,
- Tespit edilmeyi önlemek,
- Adam - saat (TL) eklemek ve böylece bir AB uzmanının DF soruşturması için ihtiyaç duyduğu süreyi uzatmak,
- Delile ait adli raporu şüpheli konuma düşürmek,
- Adli bilişim aracını çalışmaz hale getirmek,
- AF araçlarının kullanıldığına dair iz bırakmamak,

- Son ve en masum amaç olarak AB analizcisini, süreçlerini ve araçlarını iyileştirmeye zorlamaktır.

ABAT'ların genel sınıflandırması aşağıda sunulmuştur [83]:

- Veri Gizleme, Karartma ve Veri Şifreleme,
- Silme veya Veri Yok Etme,
- Veri Sahteciliği,
- Analiz Önleme,
- İzlerin Toplanmasını Engelleme,
- ABA'ları Çalışmaz Hale Getirme.

Bu bölümde klasik adli bilişimi atlatma teknikleri ele alınacaktır.

4.2 Klasik Adli Bilişim Atlatma Teknikleri ve Karşı Tedbirler

Klasik adli bilişim atlatma teknikleri, verinin veya verinin muhafaza edildiği ortamların temizlenmesi, verilerin varlığı bilinmesine rağmen ikinci kişilerin okumasını engellemek amacıyla şifrenmesi, fiziksel olarak veri ortamının yok edilmesi ve verinin farklı bir veri türü (resim) içerisine gizlenmesi gibi yöntemlerin kullanımını içermektedir. Bu bölümde sabit disk temizleme/dosya temizleme (Hard Disk/ File Wiping), şifreleme (encryption), fiziksel yok etme (physical destruction) ve bir dosya içerisine veri gizleme (steganografi) konuları ve varsa bu konularda alınabilecek karşı tedbirler ele alınacaktır.

4.2.1 Sabit disk ve dosya temizleme

Klasik ABAT'lardan birisi olan sabit disk temizleme, sabit diskteki tüm verileri silmeyi amaçlamaktadır. Bunun yerine daha karmaşık olan dosya silme, belirli belgeyi (örneğin, dijital suç kanıtı, vb.) temizlemek / silmek amacını taşımaktadır. Bu teknikte sabit sürücünün tüm veya belirli bölümlerinin üzerine sıfır verisi veya rasgele bir veri tekrar tekrar yazılmaktadır. Böylece delillerin adli bilişim soruşturmacısı tarafından kurtarılması imkansız hale gelmektedir. [84]'e göre, 2001'den sonra üretilen ATA

disklerinden verileri temizlemek için tek bir üzerine yazma yeterliyken, Gutmann tarafından [85]'te 35-kez üzerine yazma yaklaşımı uygulanması önerilmiştir.

Verilerin yok edilmesi için, genel bir yöntem olarak disk temizleme yazılımları kullanılmaktadır. Bu yazılımlar sadece illegal bir amaca hizmet etmek için değil, aynı zamanda legal bir bilginin korunması, telif hakkı gerektiren verilerin veya şirket/kurum verilerinin güvenli silinmesi gibi yasal amaçlarla da kullanılabilir. Hızlı sabit sürücüyü biçimlendirme, verilerin kendisini silmek değildir, yalnızca verileri işletim sistemlerine (OS) görünmez hale getirmektedir. Sabit disk temizleme işlemi daha az kullanılırken, dosya temizleme günlük olarak kullanılabilir.

Üzerine yazma programları genellikle üç moddan birinde çalışmaktadır [16]:

- Program, tüm disk ortamının üzerine yazabilir.
- Program, tek tek dosyaların üzerine yazmaya çalışabilir. Bu görev dosya sistemlerinin, dosya günlüğüne (file journaling) kaydedilmesi nedeniyle karmaşıktır, öyle ki dosyanın kendisi üzerine yazma yapılabilir ancak dosyaya ait bazı bölümler hala dosya günlüğünde kalmış olabilir.
- Program, önceden "silinmiş" ancak sürücüde temizleme yapılmamış dosyaları bulup üzerine yazmaya çalışabilir. Programlar bunu genellikle, sürücüde bu türden alanlarda bir veya daha fazla dosya oluşturup daha sonra bu dosya içerisinde boş alan kalmayana kadar üzerine yazma yapmaktadır; küçük boyutlu dosyaları temizlemek için özel tedbirler alınmaktadır - örneğin, bir NTFS bölümlemesinin, Windows MFT'de içeriği bütünüyle bulunan dosyalar.

Disk üzerine yazma programları, genel olarak aşağıdaki disk temizleme yöntemlerini kullanıcılara seçenek olarak sunmaktadır:

- DoD 5220.22-M
- RCMP TSSIT OPS-II
- Gutmann
- Random Data

- Write Zero

Bu seçenekler, disk üzerine kaç kez yazma yapılacağını ve nasıl yapılacağını yöntemi belirlemektedir.

DoD 5220.22-M Amerika Birleşik Devletleri Savunma Bakanlığı'nın belirlemiş olduğu güvenli veri temizleme yöntemidir. Bu yöntemde üzerine yazma işlemi üç turda tamamlanmaktadır. Birinci turda seçilen diske 0 bitleri yazılmaktadır, ikinci turda 1 bitleri yazılmaktadır ve üçüncü turda rasgele karakterler yazılmakta ve tüm turlarda yazım işleminin başarı ile tamamlandığı doğrulanmaktadır.

RCMP TSSIT OPS-II yönteminde tur sayısı yedi olarak belirlenmiştir. İlk altı turda sırasıyla temizlenmek istenen diske, önce sıfırlar sonra birler yazdırılır. Son turda rasgele karakterler yazdırılarak yazım işleminin başarı ile tamamlandığı doğrulanmaktadır.

Gutmann yönteminde tur sayısı otuz beş olarak belirlenmiştir. Tüm turlarda rasgele karakter yazma işlemi yapılan bu yöntem, 1990'lı yıllarda temizleme ihtiyacını karşılamak için kullanılmakta iken, günümüz disk teknolojisinde kullanım açısından uzun zaman almakta ve gereksiz üzerine yazmalar yapmaktadır.

Random Data, tur sayısının kullanıcıya bırakıldığı ve her turda disk üzerine rasgele karakter yazma yapan yöntemdir.

Write Zero yöntemi, tek geçişte tüm disk üzerine 0 bitleri yazılmaktadır. Bu yöntem disk temizleme yapmakta, fakat disk üzerine farklı bir karakter bulunmadığından, bilinçli bir şekilde disk temizleme yapıldığına ve bir disk temizleme aracının kullanıldığına dair izler taşımaktadır.

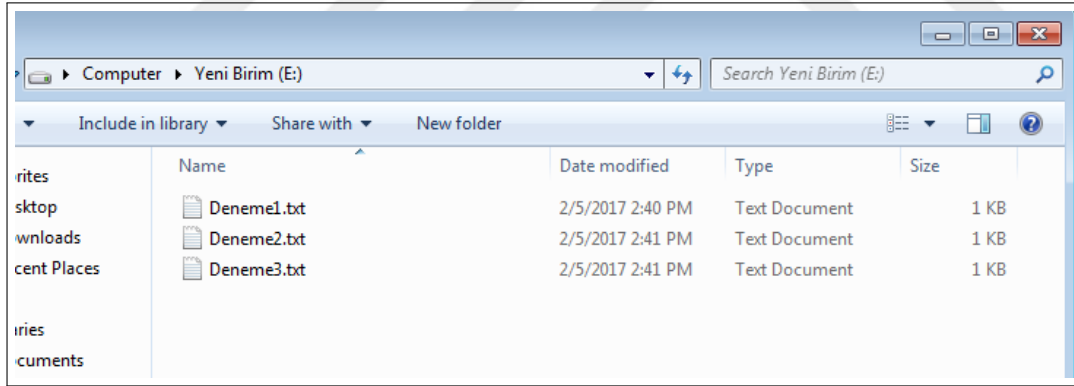
Bu yöntemleri kullanan disk temizleme araçları, ücretli veya ücretsiz olarak hizmet sunabilirler. Çizelge 4.1'de, bilinen ve çok kullanılan bir kısım disk temizleme araçlarına ait bilgiler verilmektedir.

Windows 7 OS, iki ayrı sanal sabit diske sahip olan sanal bir makine üzerinde, örnek bir uygulama çalışması yapılmıştır. Bu çalışmada, disk temizleme aracı olarak DBAN kullanılmıştır. Uygulama öncesi, ikinci disk NTFS olarak tahsis edilerek E: sürücüsü oluşturulmuştur. Oluşturulan NTFS disk bölümünde, üç adet deneme isimli metin dosyası (.txt) oluşturulmuştur (Şekil 4.2). İlk aşamada Deneme3.txt isimli dosya

Çizelge 4.1: Disk temizleme (wipe) araçlarının karşılaştırılması.

Araç	Avantajları	Dezavantajları
DBAN	Ücretsiz OS'lerden bağımsız ATA, SATA ve SCSI disklerde kolay kullanım	Bootable CD/USB gerekliliği SSD desteği yok Güncelleme yapılmamaktadır.
Disk Wipe	Ücretsiz Taşınabilir, kolay kurulum Harici diskler için kullanım	Windows OS'te kurulum OS kurulu disk bölümüne uygulanamaz.
Secure Erase-SSD	Ücretsiz OS'lerden bağımsız SSD Diskleri için temizleme sağlamaktadır. Kolay kullanım	Bootable CD/USB gerekliliği
Blancco 4	Kolay kullanım OS'lerden bağımsız Tüm disk tipleri için kullanım	Ücretli

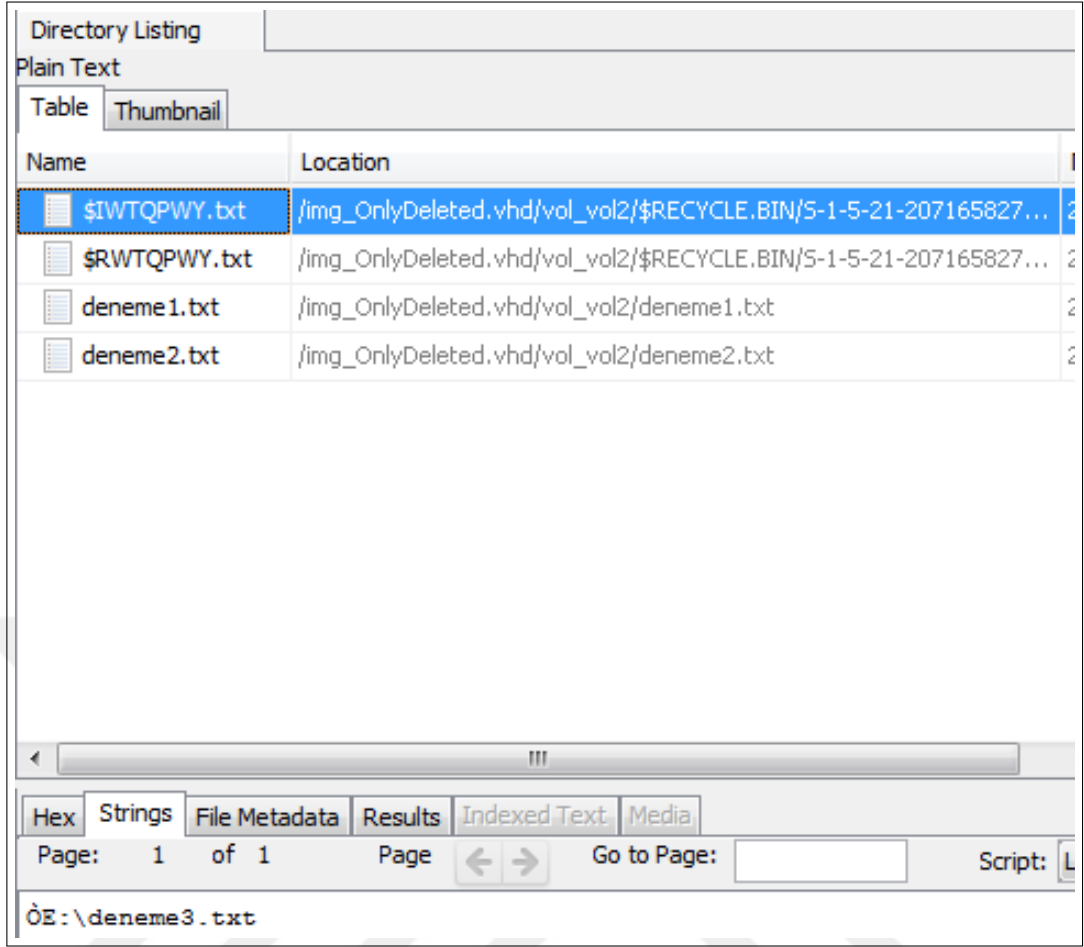
sadece silme (delete) işlemi ile silinmiştir. İkinci disk "Autopsy" adlı bilişim aracı ile açılmış ve dosyalar incelendiğinde silinen deneme3.txt dosyası ve içeriği kolayca görülebilmıştır (Şekil 4.3).



Şekil 4.2: E: sürücüsü metin dosyaları.

İkinci aşamada, DBAN programına ait .iso dosyası indirilmiş ve sanal makinenin bu dosya ile boot işlemine girmesi sağlanmıştır (Şekil 4.4). "ENTER" ile devam edilerek temizleme (wipe) yapılacak disk seçimine geçilmiştir. Farklı bir parametre verilmemesi durumunda DoD yöntemi kullanılmaktadır (Şekil 4.5).

Disk temizleme işlemi başlatılarak DoD yönteminin sırasıyla üç tur üzerine yazma işlemi takip edilebilir. İşlemin başarılı bir şekilde sonlandığı Şekil 4.6'da görüldüğü gibi bildirildiğinde, sorunsuz bir şekilde üzerine yazmanın tamamlandığı doğrulanmaktadır.



Şekil 4.3: Autopsy ABA üzerinde dosya silinen dosyaya ait bilgi.

İşlem sonunda temizlenmiş olan disk, Windows OS tarafından "tahsis yapılmamış (unallocated)" olarak görünmektedir. Temizlenmiş olan disk ilk aşamadaki gibi Autopsy ABA'sı ile incelenmek istenmektedir. Fakat program Şekil 4.7'deki gibi disk incelemenin başarısız olduğu uyarısını vermiştir. Bu uygulamada görülmektedir ki klasik bir yöntem olan disk temizleme sonrası veri artık ulaşılamaz hale gelmiştir.

Bu durumda, ilgili birebir kopya R-Studio [86] programı üzerinde açıldığında disk verileri görüntülenebilmektedir. Ve Şekil 4.8'de görülmektedir ki, disk üzerinde bazı sektörler sadece 1 bitlerinden (Hex-FF) oluşurken bazı sektörler de rasgele verilerden oluşmaktadır. Buradan da kullanıcının bir disk temizleme aracı kullandığı anlaşılmaktadır.

Geiger, çalışmasında 2005 yılındaki bir kısım ticari AF disk temizleme araçlarını değerlendirmiş ve bunların çoğunun hassas bilgileri bıraktığını tespit etmiştir [29]. Bir AB analizcisi, bir sabit sürücünün kullanılmayan kısmının tamamen temizlenerek silinmiş dosyalara ait artık verilerin kalmamış olmasından şüphelenmelidir.

```
Darik's Boot and Nuke

Warning: This software irrecoverably destroys data.

This software is provided without any warranty; without even the implied
warranty of merchantability or fitness for a particular purpose. In no event
shall the software authors or contributors be liable for any damages arising
from the use of this software. This software is provided "as is".

http://www.dban.org/

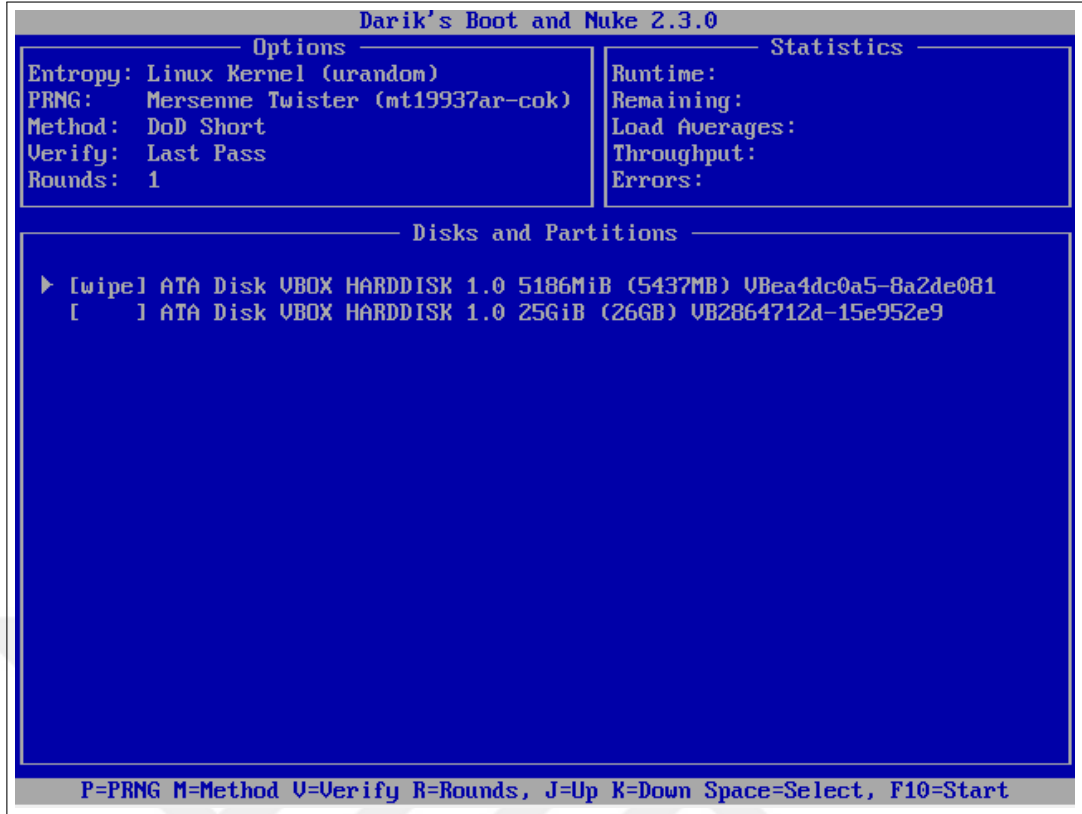
* Press the F2 key to learn about DBAN.
* Press the F3 key for a list of quick commands.
* Press the F4 key to read the RAID disclaimer.
* Press the ENTER key to start DBAN in interactive mode.
* Enter autonuke at this prompt to start DBAN in automatic mode.

boot: _
```

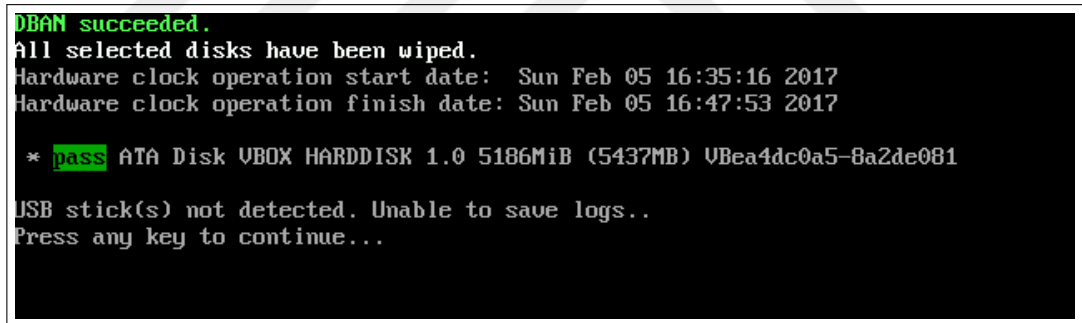
Şekil 4.4: DBAN boot işlemi.

Dosya temizleme araçları ile temizlenmek istenen belirli bir dosyaya ait diskteki verilerin, üzerine yazma yapılarak dosyaya ait verilerin güvenli ve geri döndürülemeyecek şekilde silinmesi sağlanmaktadır. Bu kısımda yöntem olarak, Schneier yöntemi de kullanılmaktadır. Bu yöntemde yedi türlü bir üzerine yazma yapılırken, bunun ilk iki turunda önce 0 bitleri sonra 1 bitleri yazılmaktadır. Geri kalan turlarda ise rasgele karakter dizileri yazılmaktadır. Bu alanda hizmet sunan yazılımlar arasında Eraser, Securely File Shredder ve Freeraser programları sık kullanılan programlar olarak görülmektedir. Dosya temizleme araçları kullanıcılara planlanmış görevler atayarak, yeniden başlatmalarda, belirli zaman aralıklarında vb. periyotlarda belirtilen bir dosyayı temizleme imkanı sunmaktadır. Dosya temizleme araçları SSD tabanlı depolama aygıtları dosyaları üzerinde sağlıklı çalışmamaktadır. SSD tabanlı disklerde yapılan dosya temizlemelerin, dosyaları yok etmediği ve verilerin kurtarılabildiği, tüm SSD ortamının, üreticinin sunmuş olduğu komutlarla başarılı bir şekilde silinebildiği [87]'de belirtilmiştir. Bu nedenle, SSD tabanlı disklerde fiziksel olarak yok etme uygulanmasının, daha faydalı olacağı değerlendirilmektedir.

Dosya temizleme örnek uygulamamızda, disk temizlemede sadece silme (delete) yapılan diskteki deneme2.txt dosyası "Eraser [88]" programı kullanılarak Şekil 4.9'daki görüldüğü gibi temizlenmiştir. Eraser programı, varsayılan olarak Guttman yöntemini kullanmaktadır. Bunun dışında diğer yöntemlerin de seçilebilmesine, klasör, disk bölümlenmesi veya diskteki kullanım dışı alanların temizlenmesine imkan tanınmaktadır.



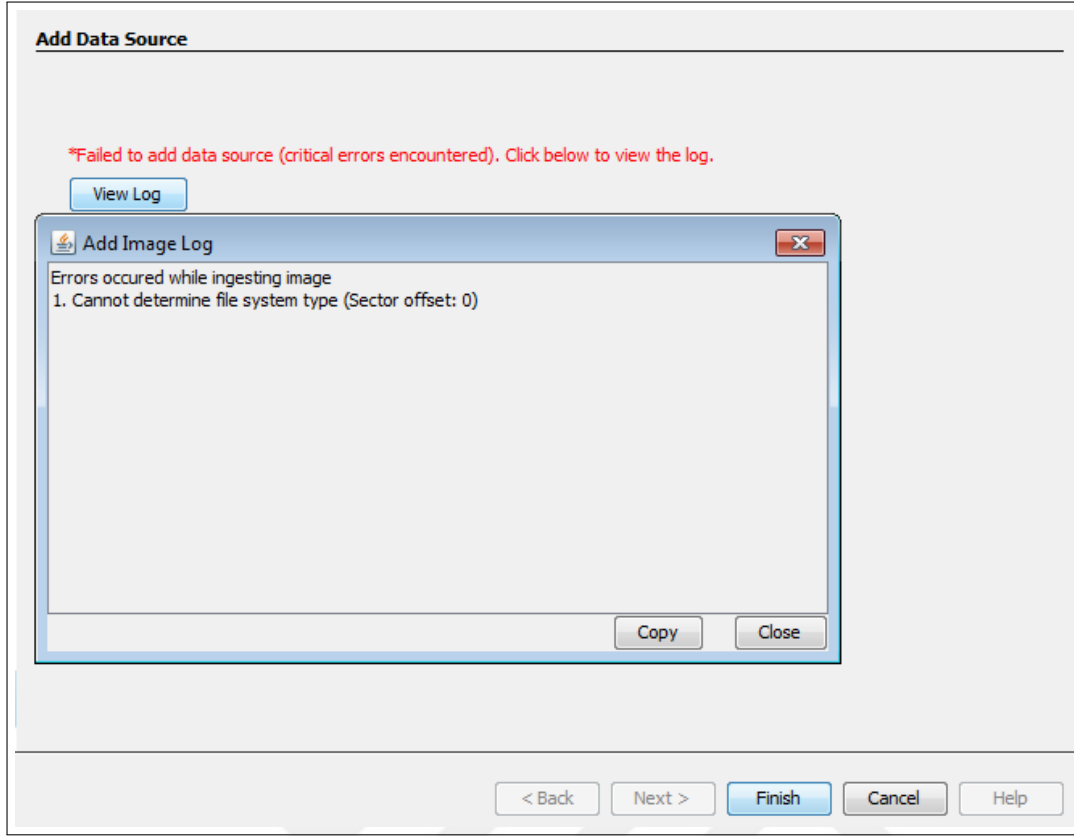
Şekil 4.5: DBAN disk seçme işlemi.



Şekil 4.6: DBAN disk üzerine yazma doğrulaması.

Temizlenen disk Autopsy ABA'sı yardımıyla incelendiğinde Şekil 4.10'da görüldüğü üzere sadece silme (delete) işlemi yapılan dosya (deneme3.txt) görülmesine rağmen, deneme2.txt dosyasına ait herhangi bir bilgi görülmemektedir. Dosya temizleme işlemi sonucunda veri kurtarılamamakta, fakat dosya sistemi günlüğünde dosya temizleme aracı kullanıldığına dair izler bırakılmaktadır. Bu durum kullanıcı/zanlı hakkında şüphe uyandırmaktadır. Bunun dışında disk/dosya temizleme uygulanmış bir verinin okunması veya kurtarılması mümkün değildir.

4.2.2 Şifreleme

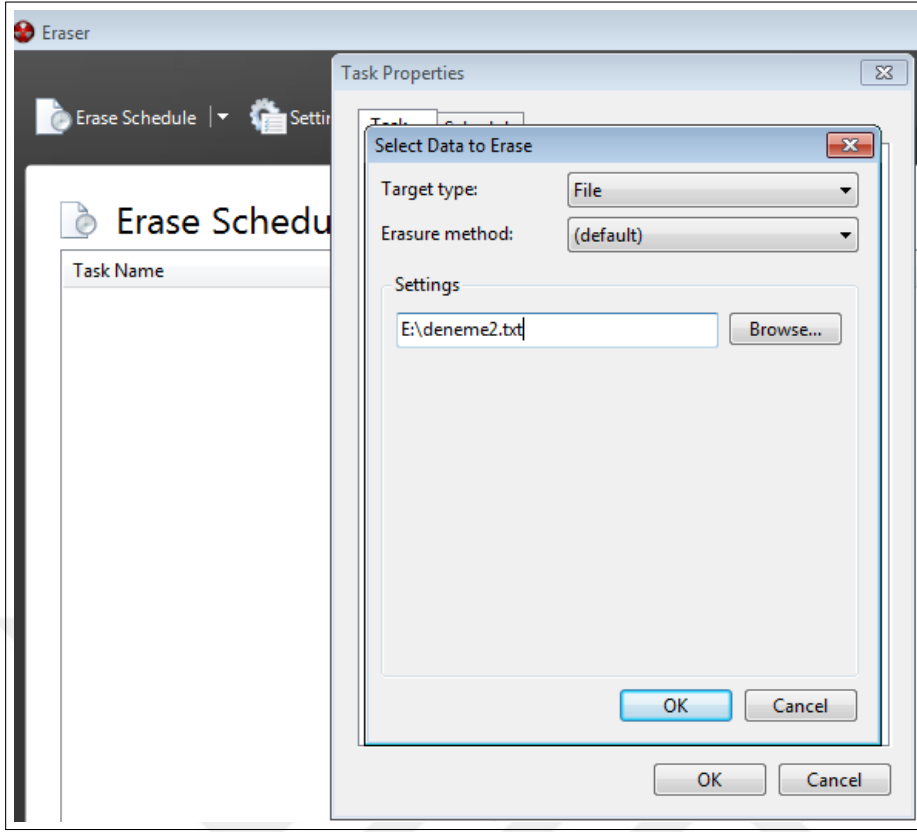


Şekil 4.7: Disk temizleme sonrası autopsy uyarısı.

Şifreleme, dijital adli bilişim analizine karşı çok etkili bir şekilde kullanılabilir. Şifreleme, karanlık veriler üretir; bu verilerin varlığı gizli değilken, sadece şifre çözme anahtarına sahip kişiler tarafından okunabilen ve kullanılabilen bir içeriğe sahiptir [89]. Şifreleme, veri gizleme tekniklerinin bir türü olarak kabul edilmesine rağmen, şifreli verilerin kendisi kolayca algılanabilmektedir. Şifreleme (PGP, TrueCrypt gibi) ile verileri gizlemedeki temel hedef, şifre çözme anahtarına sahip olunmadıkça verilerin okunamaz hale getirilmiş olmasıdır. Bir ABA aracılığı ile şifrelenmiş verilerin incelenmesi için, şifre çözme anahtarına ihtiyaç duyulmaktadır. Şifreleme işlemleri için uygulanan yöntemler arasında tamamen diskin şifrelenmesi, bir veya birkaç disk bölümünün (partition) şifrelenmesi, istenilen bir boyutta oluşturulacak sanal disk dosyasının (container) şifrelenmesi gibi değişik yöntemler kullanılmaktadır [65].

Şifreleme dosya sistemleri, dosyaları / verileri diske yazıldığında şifrelemekte ve diskten okunduğunda da şifreleri çözmektedir. ABU'ların elinde şifre çözme anahtarı yoksa, şifreleme adli bilişim analizine engel teşkil etmiş olmaktadır.

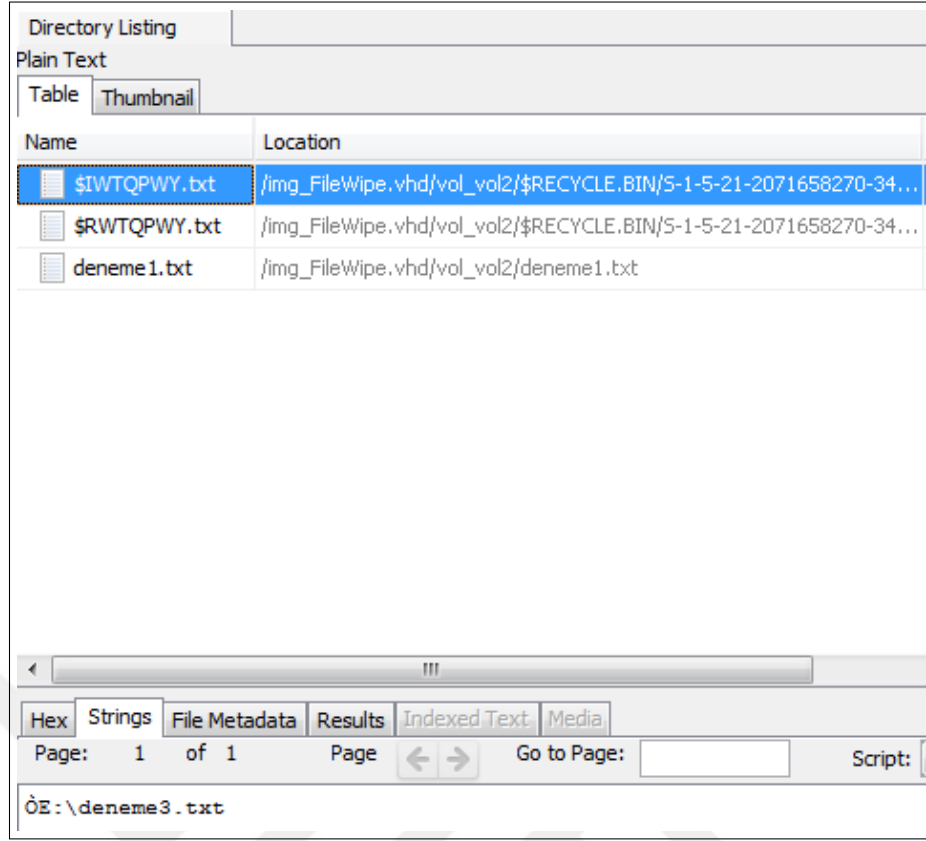
MS Office belgelerindeki şifreleme gibi, uygulama katmanı düzeyinde de şifreleme kullanmak mümkündür. Daha eski şifreleme protokollerini kullanan eski uygulamalar,



Şekil 4.9: Eraser programı ile dosya temizleme.

Passwire Recovery Forensics Kit aracı ile tarama yapılarak şifrelenmiş dosya veya disk bölümleri tespit edilebilmektedir. Şekil 4.11’de sunulan seçenekler ile diskin tamamı veya bir bölümü taratılabilmektedir. Şifreli dosyalara karşı sözlük oluşturularak, kaba kuvvet saldırısı imkanı sunmaktadır. Bir diğer disk şifre çözme aracı olarak, Elcomsoft Forensics Disk Decryptor sık kullanılan bir yazılım olarak öne çıkmaktadır. Bu yazılım aracı ile birebir kopyası alınan geçici bellek imaj dosyası üzerinden PGP, Truecrypt, BitLocker gibi şifreleme programlarına ait anahtarların HEX hali bulunabilmekte (Şekil 4.12) ve bu HEX anahtar ile aynı program aracılığı ile şifreli disk bölümleri çözülerek bağlanılabilmektedir.

Şifrelemenin bir diğer kullanımı, içeriği adli bilişim analizinden gizlemek amaçlı ağ trafiğini şifrelemek (SSL veya SSH kullanarak) olarak karşımıza çıkmaktadır. Fakat bu teknikler sadece içeriği gizler, kurulan bağlantı hakkında bilgilerin varlığını gizlemez. Suçun tarafları arasındaki veri iletişimi belgelenebilir. Hem içeriğin hem de ağ trafiğinin analizine karşı koruma, her iki yaklaşımı birden fazla şifreleme katmanı ile birleştiren soğan yönlendirmeyi (onion routing) [90] kullanarak sağlanabilir; böylece



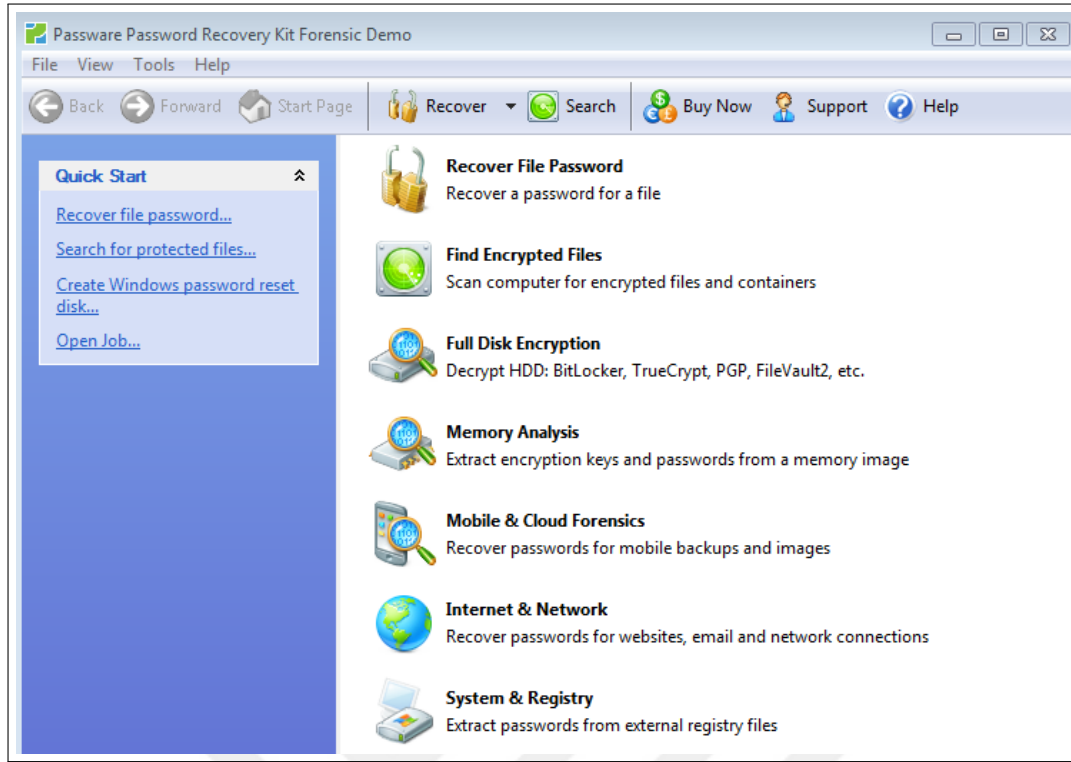
Şekil 4.10: Autopsy ile dosya temizleme inceleme sonuçları.

herhangi bir aracın iletişimin her iki ucunu ve düz metin içeriğini bilmesi mümkün değildir. Adli bilişim incelemesi açısından en zor olay türlerinden biridir.

4.2.3 Fiziksel yok etme

Fiziksel yok etme, veri temizleme tekniğinin diğer yaygın bir yoludur. Ulusal Standartlar ve Teknoloji Enstitüsüne (NIST) Özel Yayını'na [91] göre , "Medyanın yok edilmesi veri temizlemenin nihai şeklidir" olarak tanımlanmaktadır. NIST, fiziksel yok etmenin parçalanma, yakma, pudra haline getirme, kırpma ve eritme gibi çeşitli yöntemleri kullanarak yapılması gerektiğini önermektedir.

Bir sabit disk sürücüsündeki ve manyetik teyp kasetlerindeki manyetik alanları kullanılamaz hale getiren bir makine olan, Şekil 4.13'de görülen bir degausser de kullanılabilir. Önemli olan unsur, degausser kullanıldığında sabit diskin sabit yazılımının (firmware) da silineceğini bilmektir. Çok etkili olmakla birlikte, degaussing nadiren kullanılan bir tekniktir. Modern manyetik ortamlar göz önüne alındığında, bu tekniği kullanmak, gelecekteki yazmalar için ortamı tamamen kullanışsız hale getirmek demektir [92]. Manyetik teyp kasetlerinin büyük bir



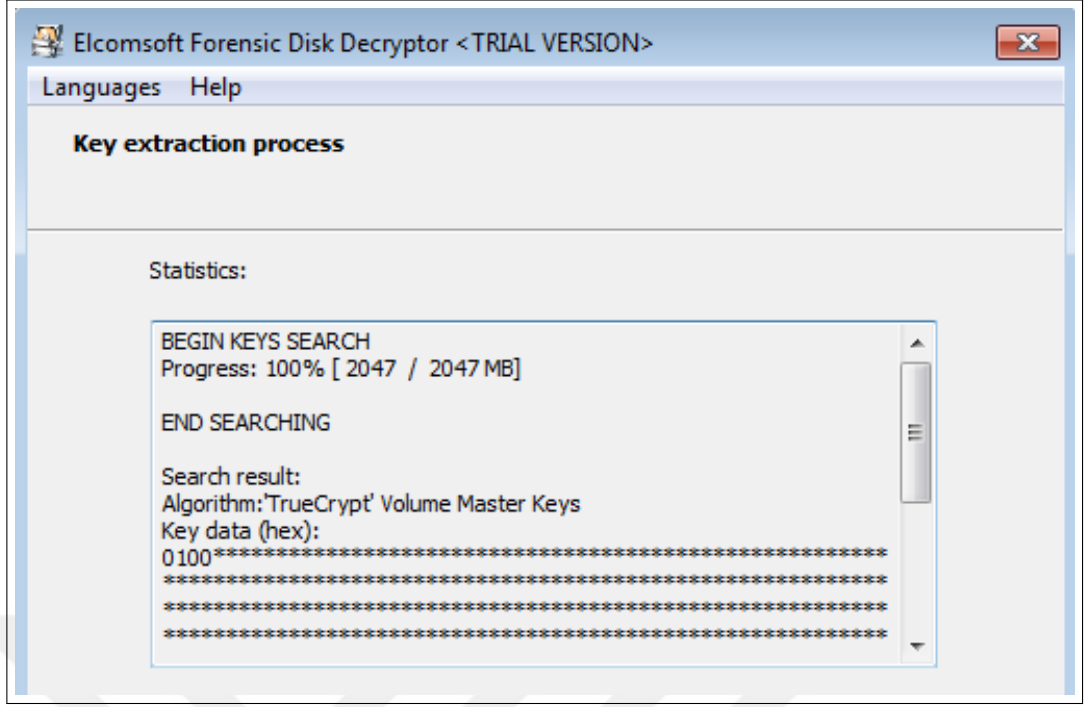
Şekil 4.11: Passwire recovery forensics kit aracı kullanımı.

çoğunluğu, sabit disklerin aksine tekrar kullanılabilir. Degausser ile veri yok etme çok kısa süren bir işlemdir. Fakat maliyetli bir yöntem olduğundan çok fazla tercih edilmemektedir.

Bu bölümde anlatılan fiziksel yok etme tekniklerinden biri ile yok edilmiş olan bir sabit diskten veri kurtarılamamaktadır.

4.2.4 Steganografi

Steganografi kelime anlamı itibarı ile gizlenmiş yazı anlamına gelmektedir. Bilgisayar bilimlerinde ise "bir dosya, mesaj, resim veya videonun başka bir dosya, mesaj, resim veya video içerisine gizleme uygulaması" olarak tanımlanmaktadır [93]. Steganografi veri gizleme mantığı açısından şifreleme ile benzerlik göstermektedir. Şifrelemede verinin varlığı herkes tarafından bilinir, sadece anahtar sahipleri tarafından veri okunabilir. Steganografide ise verinin varlığı gizlidir. Bu durumda şifreleme bir şeylerin gizlendiğini açıkça ortaya koyarken, steganografi verinin gizlendiğini de gizleme amacı gütmektedir. Fakat steganografi de iki taraf arasında bir iletişim olduğunu gizleyememektedir.



Şekil 4.12: Elcomsoft forensics disk decryptor ile trueCrypt anahtar elde etme.

Steganografinin günümüzde en yaygın kullanımı resim (image) steganografisi olarak karşımıza çıkmaktadır. Resim steganografisi uygulanması kolay ve içine veri gizlendiğinin anlaşılması en zor veri gizleme yöntemidir. Resim steganografisi [94]'te "internet ağlarında bilginin çok kolay ve güvenli taşınması" olarak tanımlanmıştır.

Resim steganografide temel bileşenler, gönderilmek istenen mesaj (şifreli veya şifresiz), taşıyıcı/gizleyici resim dosyası ve stego anahtarıdır. Bu üçünün bileşiminden ortaya çıkmaktadır. Stego anahtarı gizlenen verinin şifreleme ve şifre çözmesinde veya stego şemasına göre rasgelelik sağlamada kullanılmaktadır. Bu bileşimi sağlayan araçlara "Stego Kodlayıcılar (Stego Encoders)" denilmektedir. Resim steganografisinde en çok kullanılan yöntem, en küçük değerli bitlerin (LSB) kullanılması yöntemidir. Resim dosyalarına ait piksel bilgilerinin en küçük değerli bitleri kullanılarak, taşınmak istenen mesaj gizlenmektedir. En küçük değerli bitler kullanıldığından resmin kendisinde gözle görülür bir bozulma görmek imkansızdır.

Steganografi sadece illegal amaçlar için kullanılmamaktadır. Örnek olarak dijital bir ürüne ait sahiplik hakkının ürün bozulmadan damgalanması (watermark) ve herhangi bir anlaşmazlık durumunda sahiplik verisini ortaya çıkarması şeklinde de kullanılabilir. Basit uygulamalarla veri gizlemede çok etkili sonuçlar alınabilmektedir. Örneğin bir MS Powerpoint belgesinde bir resim altına metin mesajı



Şekil 4.13: Degausser cihazı.

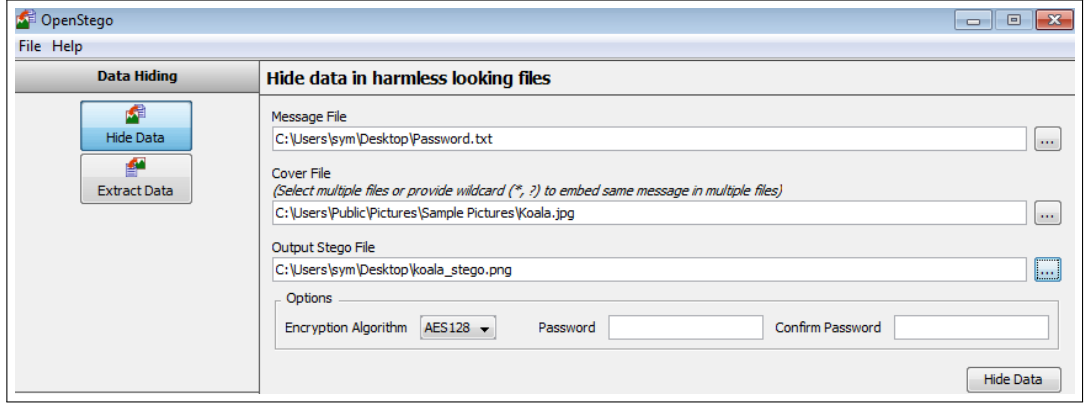
saklanabilir, MS Office dokümanlarının özellikler bölümünde yer alan bilgiler içerisine veri gizlenebilir, belge arka planı rengi ile aynı renkte yazılmak suretiyle, gözle görülemeyecek bilgiler paylaşılabılır ve web sitelerinin tarayıcıda dikkate alınmayan bölümleri (açıklama, yorum satırı vb.) içerisine veri gizlenebilir.

Resim belgeleri RGB ikili dosyaları (RGB binary files) şeklinde kullanılarak, LSB üzerine veri eklemek suretiyle resim steganografisi uygulanmaktadır. Her piksel verisi üç adet 0-255 arası bir değerle belirtilmektedir (0,0,0 : Siyah; 255,255,255 : Beyaz). RGB dışındaki renk kodlayıcıları kullanıcılara daha az renk seçeneği sunarken, verinin boyutunun az olmasını sağlamaktadır.

Örnek uygulamamızda "OpenStego" isimli araç kullanılarak gizli bir mesaj dosyası (password.txt) "koala.jpg" isimli MS Windows OS örnek resim dosyasına gömülmüştür. OpenStego programı açık kaynak, ücretsiz bir programdır. Şekil 4.14'de görüldüğü üzere taşıyıcı resim, gizlenecek olan veri bilgileri girilerek, çıktı olarak üretilen dosya ismini de belirterek steganografi işlemi başlatılabilir. Ayrıca program gizlenen veriyi şifreleme imkanı da sunmaktadır.

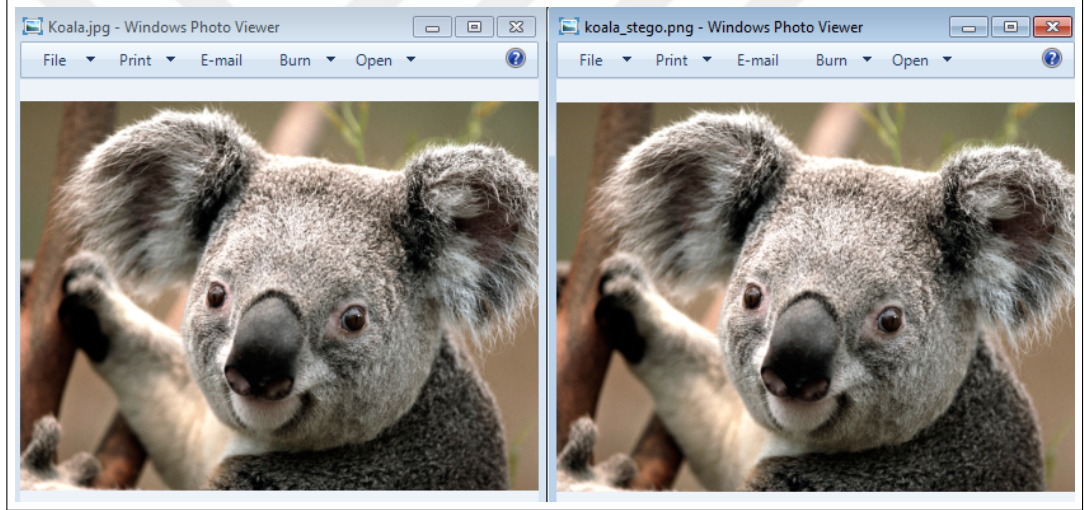
Şekil 4.15'te (sağdaki stego resim dosyası) görüleceği üzere işlem tamamlandığında oluşan resim dosyası ile asıl resim dosyası arasındaki farkı, gözle tespit etmek imkansızdır.

Steganografi aracı kullanarak gizlenen verinin gönderilen kişi tarafından okunabilmesi için aynı programın kullanılması gerekmektedir. Hangi program kullanılırsa aynı program ile içindeki veri elde edilebilmektedir. Şekil 4.16'da stego resim içerisinden



Şekil 4.14: OpenStego programı ile resim içine mesaj ekleme.

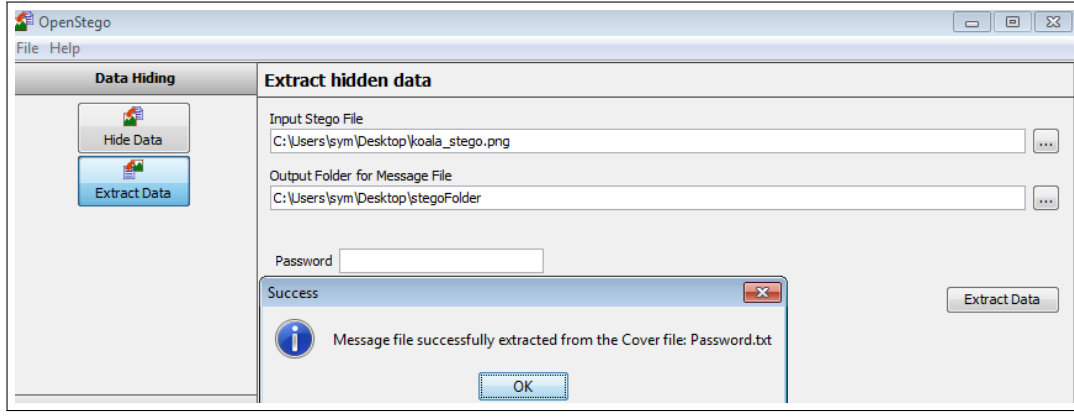
aynı program aracılığı ile resim içine gizlenen veri okunabilmektedir. Farklı dosya türlerine göre ve farklı tekniklere göre çalışan ve ücretsiz olarak kullanılabilen steganografi araçlarına ait bilgilere [95]'ten ulaşılabilir.



Şekil 4.15: Asıl resim ve stego resim dosyalarının karşılaştırılması.

Steganografi analizi kriptanalizine çok benzemektedir. Bazı durumlarda stego uygulanmış verinin varlığının bulunması yeterli olmamaktadır. Stego analiz olarak adlandırılan sürece ait Çizelge 4.3'te belirtilen yöntemler kullanılmaktadır.

Stego dosyaların tespiti amacıyla, öncelikle birebir kopyası alınan sistemde herhangi bir steganografi aracının bulunup bulunmadığı araştırılmalıdır. WetStone Technologies firmasına ait Stego Suite yazılımı, Stego Expose ve Xstego gibi araçlar ile stego dosya tespitinin yanı sıra FTK, EnCase gibi ABA'lar da stego araçlarının tespitine yardımcı olmaktadır. Bu ABA'lar belirli stego yazılımlarını bulabilmektedir. Bilinen yöntemler (jphide, jsteg vb.) ile steganografi dosyası haline getirilmiş bir jpeg dosyasının xSteg programı ile tespit edilmesi Şekil 4.17'de gösterilmiştir.



Şekil 4.16: OpenStego programı ile resim içinden mesajı çıkarma.

Çizelge 4.3: Stegonagrafi analizi yöntemleri.

Yöntem	Açıklama
Tek Steganografi Saldırısı	Analiz için sadece stego dosyası mevcuttur.
Bilinen Taşıyıcı Saldırısı	Taşıyıcı dosya ve stego dosyası mevcuttur.
Bilinen Mesaj Saldırısı	Gizlenen veri bilinmektedir.
Seçilmiş Stego Saldırısı	Stego dosyası ve algoritması bilinmektedir.
Seçilmiş Mesaj Saldırısı	Bilinen mesaj ve stego algoritması yardımıyla inceleme için stego dosyası oluşturulmaktadır.
Bilinen Stego Saldırısı	Taşıyıcı ve stego dosyası ile stego algoritması bilinmektedir.

Kullanıcıların kendi geliştirdikleri farklı algoritmaları bulmak oldukça zordur. Bu yazılımlar, tespit için geniş ölçekli dosya özet (hash) veritabanından faydalanmaktadır. Stego araçlarının tespitini zorlaştıran bir diğer etken de, yazılımların işletim sistemine, sabit diske yüklenmeden bir flash bellek vasıtasıyla çalıştırılabilmesidir.



Şekil 4.17: xStego programı ile steganografi dosyası tespiti.



5. MODERN ADLİ BİLİŞİMİ ATLATMA TEKNİKLERİ ve KARŞI TEDBİRLER

Modern adli bilişimi atlatma teknikleri, genelde suçlunun ayak izlerini en aza indirmeyi, adli bilişim araçlarının açıklık ve hatalarını kullanmayı hedeflemekte ve klasik adli bilişimi atlatma tekniklerinden daha sık kullanılmaktadır.

Bu bölümdeki teknikler, delil amaçlı veri toplama sürecine yönelik (Acquire), toplanan verilerin analizi sürecine yönelik (Analysis) ve bulguların sunulması sürecine yönelik teknikler başlıkları altında gruplandırılarak incelenecektir. Ayrıca son kısımda MS Windows İşletim sistemlerinde, adli bilişim takibini zorlaştırmaya yönelik uygulanan izlerin yok edilmesi teknikleri hakkında bilgi verilecek ve ekran görüntüleri ile ayarların nasıl yapıldıkları anlatılarak, bu sayede kontrol edilmesi gereken bölümler gösterilecektir.

Bu bölümde detayları verilen teknikler, adli bilişim uzmanlarınca dikkate alınması gereken konulardandır.

5.1 Verilerin Toplanmasına Yönelik Kullanılan Adli Bilişim Atlatma Teknikleri ve Karşı Tedbirler

Bu kısımda anlatılan teknikler, adli bilişim uzmanlarının olay yerinden verilerin toplamasını güçleştiren ya da verilerin toplanması için gerekli olan zamanı arttırmayı hedefleyen yöntemleri içermektedir.

5.1.1 Veri doygunluğu

Bu basit teknik, saldırganların çok fazla veri depolama medyasına sahip olmaları anlamına gelmektedir. Saldırganlar Şekil 5.1'deki gibi tüm USB bellekleri, tüm yazılmış CD / DVD, tüm cep telefonları, tüm dizüstü bilgisayarları ve tüm sabit diskler gibi sahip oldukları tüm dijital medyayı tutmak niyetindedir. Eğer tüm bu medyalar sıklıkla kullanılırsa adli bilişim soruşturmacılarının, medyaların tamamını araştırması ve işlenen suç öncesi son birkaç ay içinde kullanılmaları nedeniyle de tüm cihazlara

bakması gerekecektir. Bu durum, soruşturmanın tamamlanmasına çok fazla zaman ve maliyet katacaktır. Sonuç olarak soruşturmanın ne kadar süreceği sorusu, toplanan cihazların sayısına bağlıdır. Bu teknik, doğrudan bir adli bilişim olayında veri toplama aşamasını hedeflemektedir.



Şekil 5.1: Adli bilişim veri kaynakları [96].

Bu tekniğe karşı önlem olarak iki tedbir uygulanabilir [97]. Birinci teknik, soruşturmacıların veri toplama sürecinin Şekil 5.2'deki gibi paralel hale getirilebilmesidir. Veri toplama sürecini paralel hale getirme, bütçeyle sınırlı bir şekilde daha fazla sürücü çoğaltıcı veya çoklu disk kopyalama cihazları kullanılarak yapılabilir. Sürücü çoğaltıcıları, şüphelinin kaynak sürücüsünün birebir kopyasını, boş bir sürücüye kopyalar.

İkinci teknik, şüphelilerin cihazlarını/donanımlarını kendilerine karşı kullanmaktır. Şüphelilere ait dizüstü bilgisayarları veya masaüstü bilgisayarları kullanmak mümkünse, önyüklenebilir bir yazma engellemeli Linux Live CD'si kullanılabilir. İşletim sistemi önyüklendiğinde, tüm disk verileri harici bir sabit sürücüye kopyalanabilmektedir. Son olarak, adli bilişim triyaj süreçlerinin uygulanması, delil niteliği taşıyabilecek verilerin bu süreçlere uygun bir şekilde toplanması [98], büyük önem arz etmektedir.

Veri doygunluğundaki asıl sorun, bir adli bilişim olayında büyük veri merkezlerinin (amazon.com, ebay vb.) birebir kopyasının nasıl alınacağıdır [33].

5.1.2 Standart olmayan disk RAID yapısı kullanma

Bağımsız Disklerden Yedek Dizge (RAID), veri depolama sanallaştırması amacıyla birden fazla fiziksel sürücüyü, tek bir mantıksal birimle birleştiren bir disk



Şekil 5.2: Paralel veri kopyalama [46].

teknolojisi [99]. RAID 0, RAID 1 ve RAID 5 gibi yaygın RAID'ler, şerit örüntüleri, blok boyutu ve benzeri gibi parametreleri paylaşmaktadır. Bu basit adli bilişimi atlatma tekniğinde, rastgele disk sıralama, şerit sırası, şerit boyutu, blok boyutu ve bit sıralaması (endianness) gibi nadir kullanılan ayarlar düzenlenmektedir. Ayrıca, farklı ayarlara ve parametrelere sahip olan nadir RAID kontrolörlerinin kullanılması, adli bilişim uzmanlarının RAID dizilerini düzgün şekilde birleştirememelerine yol açabilmektedir. Örneğin, hatalı biçimde yeniden bir araya getirilen jpeg dosyaları bir fotoğrafın yapbozu gibi görünebilmektedir. Bu teknik de veri doygunluğu tekniğinin yaptığı gibi, veri toplama sürecini engellemeyi amaçlamaktadır.

Bu tekniğe karşı önlem olarak, şüphelilerin kendi sistemlerindeki RAID kontrolcüsünü kullanabilen bir önyükleme diski kullanarak birimler de-RAID yapılabilir. Şüphelilerin bilgisayarını soruşturmacı için verileri yeniden bir araya getirecektir.

İkinci önlem olarak, fiziksel sürücüler yerine diskteki bölümlerlerin (volume) kopyasını almak uygulanabilmektedir [97]. Son önlem olarak, R-Studio RAID

Recovery gibi araçlardan faydalanılarak, RAID yapısının parametreleri tespit edilmeye ve içeriğindeki verilerin kurtarılması hedeflenmektedir.

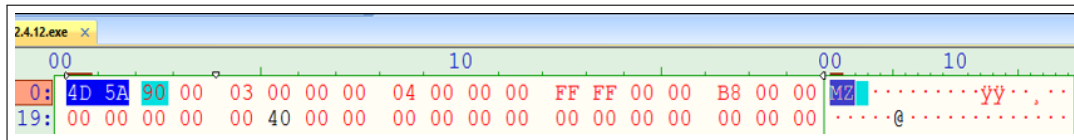
5.2 Verilerin Analizine Yönelik Kullanılan Adli Bilişim Atlatma Teknikleri ve Karşı Tedbirler

Bu kısımda, adli bilişim uzmanının toplanan veri üzerinde inceleme yapmasını zorlaştırmak, verinin analizi sürecini hedef alarak soruşturma için gereken zamanı arttırmak, delilleri karartmak ve böylece soruşturmayı engellemek amacıyla kullanılan adli bilişimi atlatma teknikleri ele alınmaktadır.

5.2.1 Dosya imza bilgisini değiştirme

Adli bilişim uzmanı tarafından yapılan dosya imza (file signature) analizi, bir dosyanın değiştirilip değiştirilmediğine karar vermenin etkili bir yoludur. Dosyalar, Windows tabanlı sistemlerde uzantıları (.exe, .pdf, .jpg ve benzeri) ile belirtilir. Windows işletim sistemi, kullanıcı belirli bir dosyayı açmak için tıkladığında, gerekli yazılımı yüklemek için bu uzantıları kullanmaktadır. Herhangi bir dosya uzantısı değiştirildiğinde, o dosyayı açacak olan uygulama ikonunun da değişmesinin sebebi budur. UNIX tabanlı sistemler, bir dosyanın uzantısını göstermesine rağmen, işletim sistemi dosyayı açacak doğru yazılımı yüklemek için dosya uzantısına ihtiyaç duymamaktadır. UNIX tabanlı sistemler, dosyayı açmak amacıyla hangi yazılımın gerekli olduğunu belirlemek için, dosya imzasına bakabilmektedir. Bu nedenle UNIX tabanlı sistemler dosya uzantılarına ihtiyaç duymamaktadır [100].

Dosya imzası, dosya türünü belirlemek için kullanılan küçük bir onaltılık kod bloğudur. Bir dosyanın dosya imzaları, bir onaltılık kod düzenleme aracı vasıtasıyla görülebilmektedir. HexEdit programı ile açılan bir .exe Windows çalıştırılabilir dosyasının, dosya imza örneği (Hex: 4D 5A; ASCII: MZ) , Şekil 5.3'te gösterilmiştir.



Şekil 5.3: Windows çalıştırılabilir dosyası (.exe) dosya imza örneği.

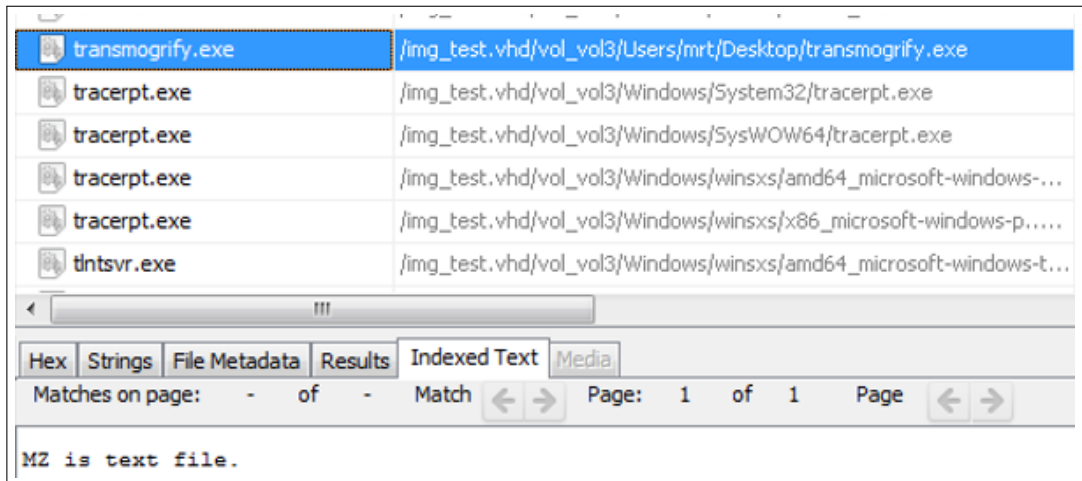
Bazı tanınmış dosya uzantılarına ait dosya imzalarının listesi [101] Çizelge 5.1'de sunulmaktadır.

Çizelge 5.1: Bilinen dosya türlerine ait dosya imza listesi.

Dosya Uzantısı	Dosya İmzası (Onaltılık)	Dosya İmzası (ASCII)
Adobe PDF	25 50 44 46	%PDF
MS Office 2007 ve Sonrası (.docx)	50 4B 03 04 14 00 06 00	PK.....
MS Office 97-2003 (.doc)	D0 CF 11 E0 A1 B1 1A E1	Đİ.à.á
JPEG Resimler	FF D8 FF E0	ÿØÿà
GIF Resimler	47 49 46 38 37 61	GIF87a

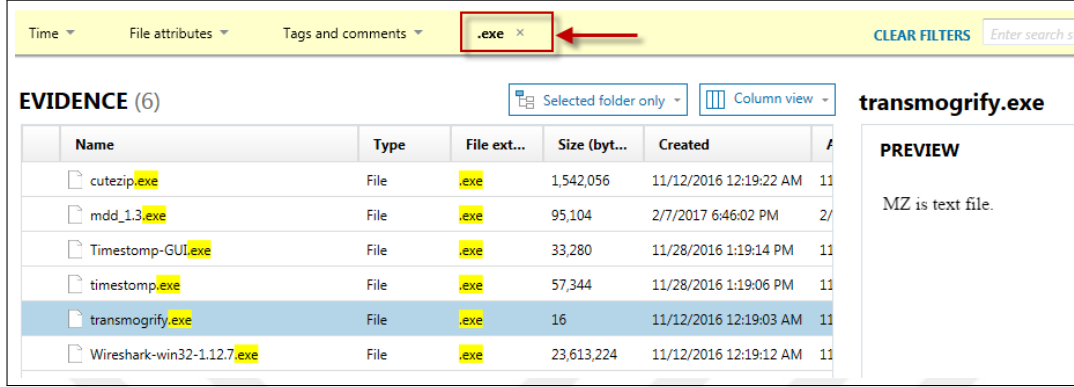
Metasploit 2009 Projesi MAFIA aracı olan Transmogrify, bir saldırgan için dosya üstbilgisini ve uzantısını değiştirebilme özelliğine sahip bir program olarak bilinmekteydi. Ve bu işlem, bir sabit sürücünün imaj dosyasını analiz etmek için kullanılan bir adli bilişim aracı olan EnCase'in, örneğin bir jpeg dosyasını bir Windows çalıştırılabilir dosyası (.exe) olarak tanımasına yol açmıştır. Bu araç, şimdilik beş yıldan fazla güncellenmediğinden, Metasploit Veritabanı'nda erişilebilir değildir. Fakat dosya başlığını ve uzantısını elle bir Hex düzenleme programı aracılığı ile değiştirmek hala mümkündür.

Şekil 5.4'te gösterilen örnekte, bir metin dosyasının (transmogrify.exe) başlık bilgisi HexEdit aracında MZ (Windows .exe başlığı) olarak değiştirilmiştir ve dosya uzantısı el ile .exe olarak değiştirilmiştir. Açık kaynak kodlu bir adli bilişim aracı olan Autopsy 4.1.1 ile filtrelendiğinde, orijinalinde bir metin dosyası olmasına rağmen, transmogrify.exe çalıştırılabilir bir dosya olarak gösterilmektedir. Daha da ötesi, transmogrify.exe dosyasına ait içerik bilgisi Şekil 5.4'te alt bölümde "Indexed Text" sekmesi altında görülebilmektedir.



Şekil 5.4: Autopsy ile dosya imzası değiştirilmiş dosyanın filtrelenmesi.

Aynı sabit disk imajı üzerinde, Magnet Axiom adlı bilişim aracının deneme sürümü ile de, .exe dosyaları filtrelenebilir istenmiştir. Transmogrify.exe isimli dosyanın, bu ABA'da da Şekil 5.5'te görüldüğü üzere, içeriği metin dosyası olarak görüntülense bile, bir çalıştırılabilir dosya (.exe) gibi listelenmesi sağlanabilmektedir.



Şekil 5.5: Magnet axiom ile dosya imzası değiştirilmiş dosyanın filtrelenmesi.

Bu başlık altında kullanılan bir yöntem de, dosyada oyuk oluşturarak gizli verileri saklamaktır. İkili dosyaların (binary files) birbirine eklenmesi (örneğin, Windows komut satırında copy / b kullanılarak) ile de bir dosya imza bilgisinin maskelenmesi için kullanılabilir. Bu komutla birleştirilen dosyalar, uzantıları değiştirilerek uygun uygulamalar aracılığı ile görülebilmektedir. Örneğin bir resim dosyasına bir pdf dosyası birleştirildiğinde, yeni oluşan birleşik dosyanın uzantısı .pdf yapıp bir pdf okuyucuda açıldığında pdf dosyasının içeriği görülebilmekte, uzantısı resim dosyası (.jpg, .gif, .png) olarak değiştirilirse ve bir resim gösterici ile açılırsa resim içeriği görülebilmektedir. Bu teknikler, bir adli bilişim soruşturmasının veri analizi sürecini bozmayı amaçlamaktadır ve ayrıca, adli bilişim aracının hata/zayıflığından istifade ettiğinden adli bilişim araçlarına saldırı olarak da sayılabilmektedir.

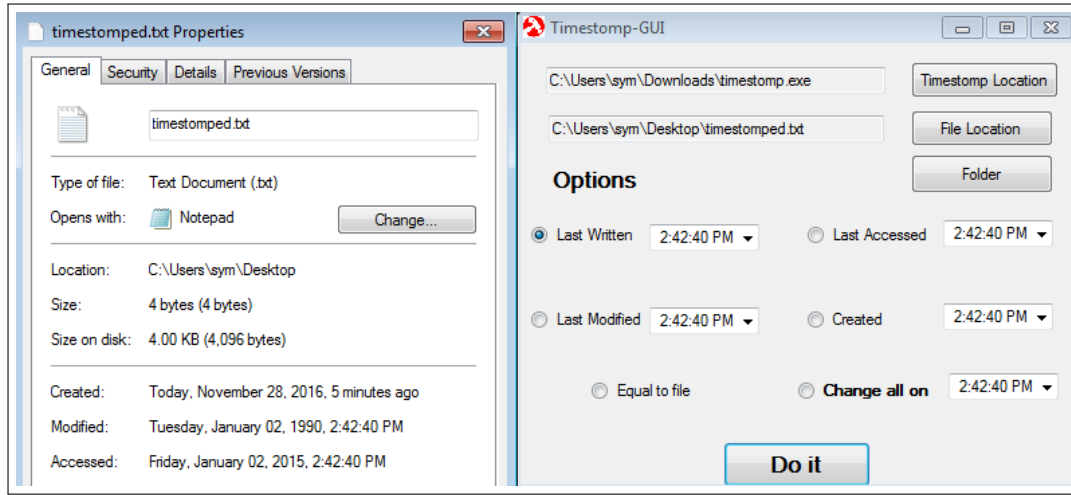
[102]'de tanımlanan "Bulanık Hash (Fuzzy Hashing)" i kullanarak, dosyalar arasındaki benzerliği belirleme, kullanılabilecek karşı önlemlerden birisidir. Eğer şüpheli, gizli veriyi birleştirmek için kendi sisteminden bir dosya seçerse, benzerlik bulunabilir. Bulanık Hash özelliği, Access Data FTK adli bilişim aracında bulunan bir özelliktir. İkinci karşı önlem, bir ".dll" dosyasını not defteri ile açma gibi şüpheli etkinlikleri araştırmak için uygulamaların "En Son (Recent)" listesini analiz etmektir [97].

5.2.2 Dosya zaman damgalarında sahtecilik

Adli bilişim uzmanını yanıltmak amacıyla, adli bilişime konu olan izleri maskeleye ve değiştirme (bozma), en sık kullanılan adli bilişimi atlatma yöntemlerinden biridir. Değiştirme (M-Modification), Erişim (A-Access), Oluşturulma (C-Created), MFT Girdi Kaydı (E-Entry) kısaca MACE olarak adlandırılan zaman damgalarının maskelenmesi veya değiştirilmesi bu başlık altında değerlendirilmektedir. MACE öznitelikleri, bir dosyanın oluşturulduğu, değiştirildiği, erişildiği veya girdi kaydı değiştirildiğinde tutulan zaman damgalarını gösteren, herhangi bir dosyaya ait zaman verilerdir. NTFS dosya sisteminde zaman damgası bilgileri, bir Ana Dosya Tablosu (MFT) girdisinin \$ STANDART_INFORMATION ve \$ FILE_NAME öznitelikleri altında saklanmaktadır. Bu zaman damgaları, adli bilişim soruşturmacısı için belli bir zamanda meydana gelen bir faaliyeti göstermek açısından kanıt sağlamak için çok önemli olabilmektedir. El konulan bir donanımdan elde edilebilecek veri miktarına bakıldığında, bir adli bilişim uzmanının her dosyayı gerekli ayrıntıda incelemesi mümkün görülmemektedir. Genel ve çok mantıklı bir analiz iş akışı, aramayı belirli bir zaman aralığında - veri ihlali veya diğer şüpheli olay meydana gelmeden hemen öncesi ve sonrasını önceliklendirmek gibi- daraltmaktır [103].

Timestomp, geliştiricileri James C. Foster ve Vincent Liu'nun birlikte yazdığı, bir adli bilişimi atlatma amaçlı yardımcı programdır. Yazılımın amacı, dosyalar üzerinde zaman damgasıyla ilgili bilgilerin silinmesine veya değiştirilmesine izin vermektir [104]. Bir dosyanın değiştirilme veya erişilme zaman damgaları genellikle oluşturulma zamanına eşit ya da daha ileri bir tarih olmalıdır ancak Şekil 5.6'da görüldüğü üzere bazen de olmayabilmektedir. Ayrıca bir GUI (Grafik Kullanıcı Arayüzü) aracılığı ile timestomp kullanmak, herhangi bir uzmanlık gerektirmemektedir.

Timestomp programı yalnızca \$ STANDART_INFORMATION özniteliğinde bulunan zaman damgalarını değiştirmektedir. \$ FILE_NAME özniteliğinin altındaki zaman damgalarını değiştirmemektedir. Eğer bu durum kullanıcı tarafından bilinmiyorsa, MFT girdi verilerini okumak için [105]'te bulunan mftcrd.exe gibi bir araç kullanarak şüphelenilen dosyalar için her iki özellik de karşılaştırılabilmektedir. Şekil 5.7'deki iki öznitelik altındaki zaman damgaları arasında farklar kolayca görülebilir. Ancak,



Şekil 5.6: Zaman damgalarında modifikasyon yapılmış dosya.

basitçe zaman damgaları değiştirilmiş olan dosyayı başka bir konuma taşımak ve timestomp.exe dosyasını tekrar çalıştırmak, \$ STANDART_INFORMATION zaman damgaları ile \$ FILE_NAME zaman damgalarını eşit hale getirmektedir. Defiler's Toolkit vasıtasıyla ayrıca birçok Unix sisteminde inode (Unix dosya sistemindeki veri yapısı) zaman damgalarının ve silinmiş izin girdilerinin üzerine yazma yapılabilen; dosyalar üzerindeki zaman damgaları Unix touch komutu [11] kullanılarak da değiştirilebilmektedir. Dahası, [106]'da geliştirilmiş ve tespit edilmesi zor olma özelliklerine sahip SetMACE yazılımı, \$ STANDARD_INFORMATION, \$ FILE_NAME, \$ INDEX_ROOT ve \$ INDEX_ALLOCATION özniteliklerinin altındaki zaman damgalarını aynı anda değiştirebilmektedir.

Farklı zaman aralıklarında BIOS saatini rasgele değiştirmek ve son erişim zamanı kaydını devre dışı bırakmak, zaman damgalarını değiştirmek için kullanılan diğer iki adli bilişim atlatma yöntemidir. Son erişim zamanı kaydı, Windows "HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Control \FileSystem" kayıt defteri anahtarında DWORD "NtfsDisableLastAccessUpdate" ayarından veya komut satırında "FSUTIL behavior set disablelastaccess 1" komutunu kullanarak da devre dışı bırakılabilmektedir.

Bu tekniklere karşı tedbir olarak, öncelikle adli bilişim aracı olarak kullandığımız program vasıtasıyla, anahtar kelime olarak "timestomp" kelimesi aratılabilir. Şüpheli bilgisayarından timestomp.exe ve kullanıcı arayüzünü silmiş dahi olsa, çalıştırılabilir dosyanın çalıştırılması ile dosya sistemi günlüğü (USN Journal) ile NTUSER.dat veritabanında en son kullanılanlar listesinde (MRU List), bu dosyaların daha

```
Administrator: C:\Windows\System32\cmd.exe

$STANDARD_INFORMATION 1:
File Create Time <CTime>: 2016-11-28 12:42:40:000:0000
File Modified Time <ATime>: 1990-01-02 12:42:40:000:0000
MFT Entry modified Time <MTime>: 1981-01-01 12:42:40:000:0000
File Last Access Time <RTime>: 2015-01-02 12:42:40:000:0000
DOS File Permissions: archive
Max Versions: 0
Version Number: 0
Class ID: 0
Owner ID: 0
Security ID: 677
Quota Charged: 0
USN: 1099524744

$FILE_NAME 1:
Parent MFTReference: 531
ParentSequenceNo: 2
File Create Time <CTime>: 2014-09-15 20:53:56:000:0000
File Modified Time <ATime>: 2014-09-15 20:53:56:000:0000
MFT Entry modified Time <MTime>: 2014-09-15 20:53:56:000:0000
File Last Access Time <RTime>: 2014-09-15 20:53:56:000:0000
```

Şekil 5.7: Bir dosya için \$standart_info ve \$file_name öznitelikleri altındaki zaman damgalarının karşılaştırılması.

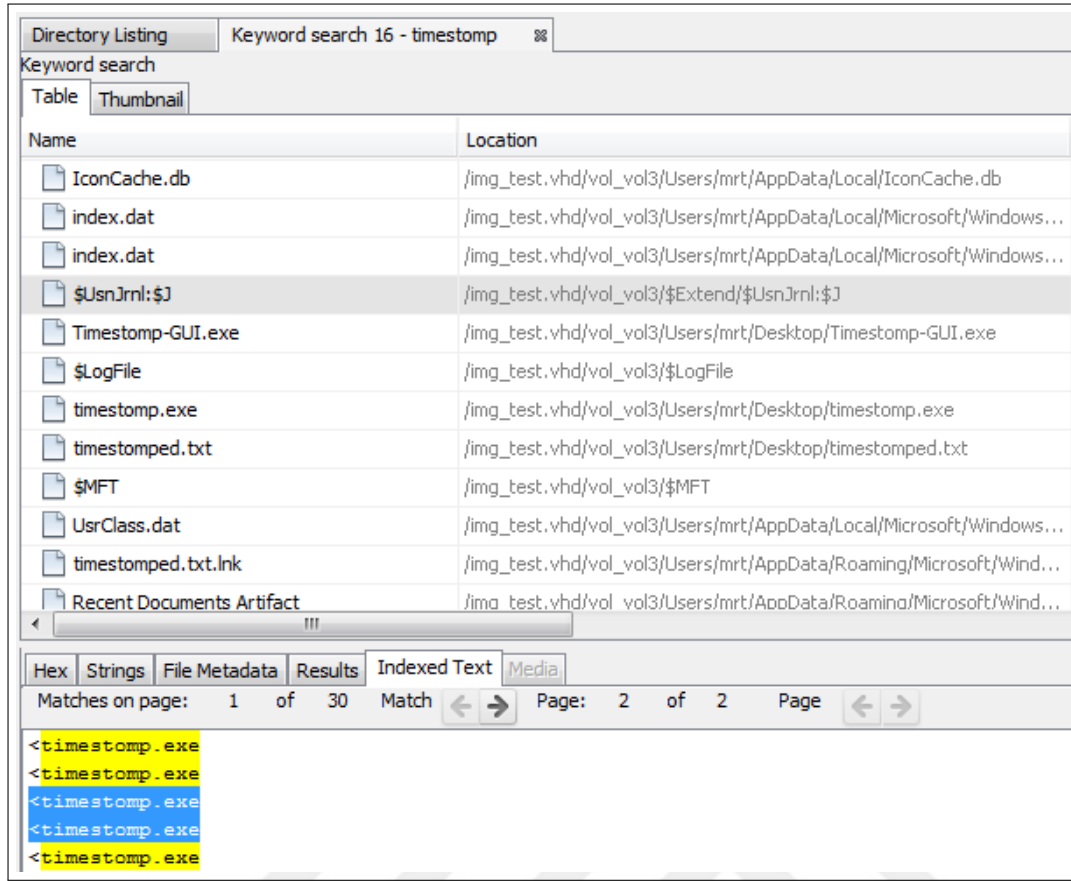
önce çalıştırıldığına dair iz aranabilmektedir. MRU Listesindeki kayıtların, kayıt defterinden HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Explorer\RunMRU kaydı altından temizlenebileceği her zaman göz önünde bulundurulmalıdır. Bu nedenle Şekil 5.8'deki gibi USN Journal atındaki verileri incelemek gerekmektedir.

Zaman damgalarının değiştirildiği kesin olarak biliniyorsa, öncelikle dosyalara ait meta verilerdeki zaman damgaları göz ardı edilerek, varsa dosyaların içeriğinde bulunan tarih bilgileri dikkate alınmalıdır. Eğer zaman damgaları, BIOS saatinin rasgele değiştirilmesi ile ayarlanıyor ise, bu durumda da herhangi bir uygulamaya ait kayıt (log) dosyası incelenerek olayların oluş sırasına karar verilebilmektedir. Çünkü log dosyaları kayıtları zamana göre değil Şekil 5.9'deki gibi oluş sırasına göre muhafaza etmektedir. Böylece log dosyalarındaki kayıtlar incelenerek bilgisayarda yapılan işlemlerin önceliklendirilmesi hakkında bilgi sahibi olunabilmektedir.

5.2.3 Kısıtlanmış klasör veya dosya adlarının kullanılması

Windows sistemleri, DOS günlerinden kalma kısıtlanmış klasör ve dosya adları gibi bazı özelliklere sahiptir.

- CON,



Şekil 5.8: NTFS dosya sistemi günlüğü (USN journal) içerisinde timestomp kayıtları.

- PRN,
- AUX,
- NUL,
- COM1,
- COM2,
- COM#,
- LPT1,
- LPT2,
- LPT# gibi klasör ve dosya adları kısıtlıdır ve normal olarak herhangi bir klasöre veya dosyaya verilememektedir.

Bunlar, sistem aygıt sürücülerini, yazıcılara ait port tanımlamaları ve seri iletişim için kullanılan, MS-DOS'ta adları ayrılmış bağlantı noktalarıdır. Örneğin, Windows

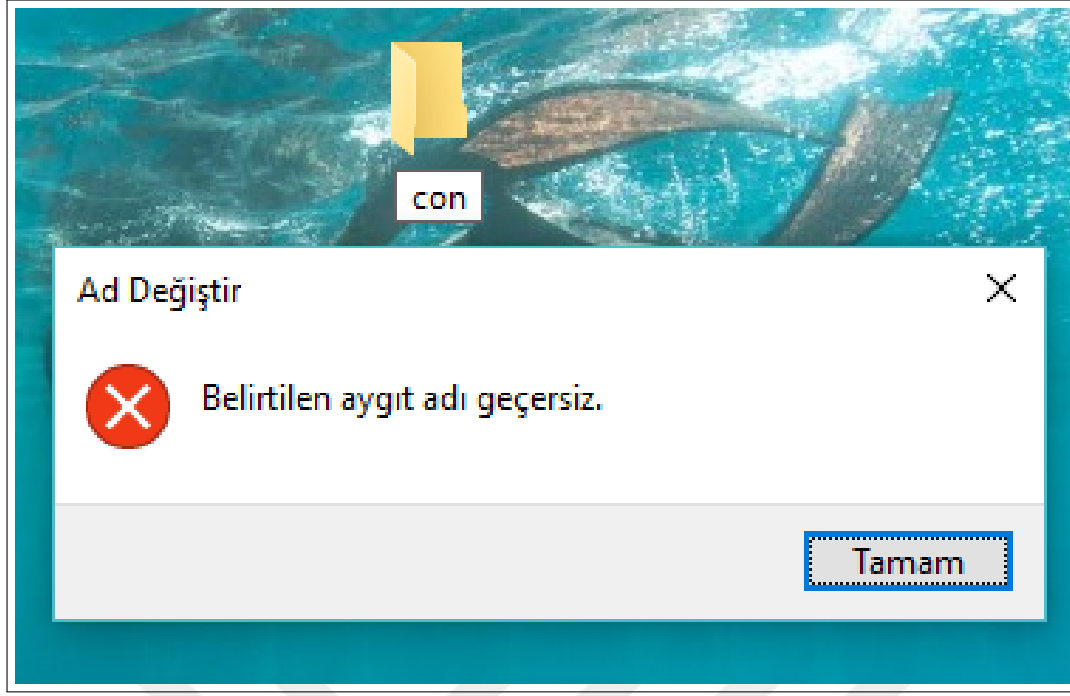
2023-12-01	Disk bağlandı
2023-12-01	Hata
2023-12-01	Giriş başarısız
2023-12-01	Uyarı
1907-05-12	İşlem kayıt altına alındı.
1907-05-12	Hata
1907-05-12	Giriş başarısız
1907-05-12	Uyarı
1999-12-22	İşlem kayıt altına alındı.
1999-12-22	Hata
1999-12-22	Giriş başarısız
1999-12-22	Uyarı

Şekil 5.9: Rasgele BIOS saati ayarlanması durumunda log dosyalarının incelenmesi.

sistemde CON adlı bir klasör veya dosya oluşturmaya çalıştığınızda Şekil 5.10'daki gibi "Belirtilen aygıt adı geçersiz" hata mesajını verip farklı bir ad kullanarak isimlendirme yapılmasını istemektedir.

Ancak, saldırgan için bu kısıtlanmış klasör ve dosya adlarını kullanmanın yolları mevcuttur. Herhangi bir kullanıcı, bir komut istemi penceresi açıp, Evrensel Adlandırma Konvansiyonu (Universal Naming Convention-UNC) yolunu (\\hostname \c \$ \folder) kullanan "md \\.\C:\aux" yazarak bu adlara sahip bir klasör veya dosya oluşturabilir veya yeniden adlandırabilir. İkinci yol olarak, NTFS destekli bir Linux sistemi önyükleme (boot) yapmak ve dosyayı veya klasörü taşımak veya yeniden adlandırmak ile kısıtlanmış adlar dosya veya klasöre verilebilmektedir. İçinde deliller bulunan "secret.txt" adlı bir metin dosyası, birinci yöntemdeki komut satırı kullanılarak "aux.txt" olarak yeniden adlandırılmıştır. Dosya, içeriğindeki bilgileri görmek için, açılmaya çalışınca, Şekil 5.11'deki gösterildiği gibi bir hata mesajı vermektedir.

Bu teknik, veri analizi süreci için gerekli olan süreyi uzatmaktadır. Adli bilişim uzmanları böyle bir klasör veya dosyayı tespit ettiğinde, sadece klasör veya dosyanın adını değiştirerek kolayca içeriğin, delil olabilecek bir bilgi olup olmadığını görebilmektedir. Görüldüğü üzere, bu teknik çok karmaşık değildir, ancak bunun



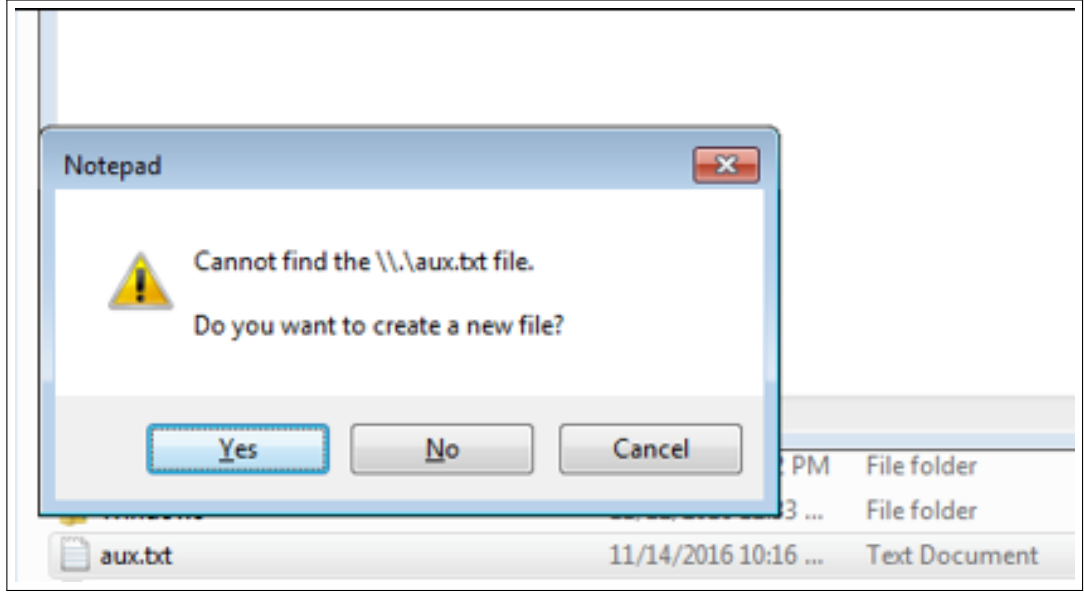
Şekil 5.10: Kısıtlanmış klasör adı kullanılmasına ait hata bildirimi.

gibi çok fazla dosya veya klasör analiz edilmesi çok fazla zaman alacaktır. Ayrıca bu dosyaların sistem dosyaları ile aynı konumda saklanması, ABA'ların bir şekilde bu dosyaları sistem dosyası gibi sınıflandırmalarına sebep olmaktadır. Bu sayede verilerin gizlenmesi mümkün olabilmektedir.

Bu tekniğe karşı tedbir olarak, imajı alınan bilgisayara ait imaj dosyalarındaki belge ve klasörler yerel dosya adlarıyla dışa aktarılmamalıdır. ABU'lar detaylı analiz için dosyaları dışarı aktarırken farklı bir isimlendirme kullanmalıdırlar. FTK 4 adli bilişim aracı, 1.jpg, 2.jpg ve benzeri isimleri vermek suretiyle bu gereksinimi destekleyen bir özelliğe sahiptir. Dosyaların Dosya Kimliği (File ID) ile dışa aktarılması da kullanılabilecek başka bir seçenektir.

5.2.4 Döngüsel referanslama ve ASCII karakterli metin kullanımı

NTFS dosya sisteminde, Windows API'si nedeniyle boyutu varsayılan olarak 260 karakter olan bir dosya yolu uzunluğu kısıtlaması vardır. Ancak, Long Path Tool [107] gibi üçüncü parti araçları kullanarak daha uzun yollar oluşturma yolları vardır. Bir üst klasöre referans veren birleşim noktalarının (junctions) veya sembolik bağların (symbolic links) oluşturulması, döngüsel referanslama için kullanılabilen bir yöntemdir. Bu yöntem, C: \ÜstDosya \AltDosya \ÜstDosya \AltDosya \ÜstDosya



Şekil 5.11: Kısıtlanmış dosya adlı dosyanın açılması.

\AltDosya.... gibi özyinelemeli bir yol yaratacaktır ve kötü niyetli kullanıcılar bu iç içe geçmiş klasörlerde kötü amaçlı verileri depolayabilmektedir. Bu yapıdaki bir dosya veya klasör açmaya çalışıldığında, dosya adını veya dosya yolunun bulunamadığı ya da dosya yolunun çok uzun olduğunu belirten bir hata iletisi vermektedir.

ABA'lar bu saldırıdan etkilenebilir. Adli bilişim uzmanları, küçük boyutlu dosyaları bile dışa aktarırken uzun süre beklemek zorunda kalabilirler. Bu saldırıya karşı tedbir olarak, adli bilişim uzmanı daima bir imaj dosyası üzerinden çalışmalı ve klasörleri değil dosyayı dışa aktarmalıdır.

ASCII karakterli metin kullanımı, iki taraf arasındaki mesajlaşmanın içindeki veya iletilen dosyalardaki mesajlarda geçen kelimelerde, kelimenin anlaşılmasını güçleştirmeyecek fakat farklı karakterler kullanarak, ABA'ların anahtar kelime arama özelliklerinden kaçınacak girişimdir. Örneğin içeriğinde şifre bilgisi bulundurulmuş herhangi bir dosyanın varlığı için "Password" kelimesi ile arama yapılabilir, eğer saldırgan bu dosyayı "P@ssw0rd" şeklinde isimlendirmiş ise ABA bu dosyayı bulamayacaktır. Şekil 5.12'de de görülebileceği gibi arama işlemi birebir karakter eşleşmesi veya düzenlenmiş ifade (Regular Expression) ile gerçekleştirildiğinden harf yerine farklı karakterlerin kullanılması soruşturmayı aldatıcı bir rol üstlenmekte ve analizi zorlaştırmaktadır.

5.2.5 ABA'lara yönelik saldırı



Şekil 5.12: ASCII simgelerle yazılan metinde arama işlemi.

Verinin analizine yönelik olarak kullanılan ABA'lar, ABU'ların işlerini kolaylaştırmak ve zaman kazanmak amacıyla kullanılmaktadır. Saldırganlar bilinçli olarak ABA'ların çalışmasını engellemek amacıyla, bazı teknikleri kullanmaktadır.

Bu tekniklerden en yaygın olarak kullanılanı zip bombası olarak adlandırılan, dosyaları imajı alınacak bilgisayarda muhafaza etmektir. Örneğin sadece 42 KB'lık boyutu nedeniyle 42.zip olarak adlandırılan dosyayı bulunduran bir imaj dosyası, bir ABA vasıtasıyla incelenmek istendiğinde, PB'lar boyutundaki içeriğinin açılması oldukça uzun zaman alacaktır. Bu aşamada ABA'nın yüklü olduğu bilgisayar hizmet dışı kalacaktır. Bunun yanı sıra dosya açma işlemi, ABA'nın çalışmasını da engelleyecek ve programın kilitlenmesine yol açacaktır.

Bu nedenle zip dosyalarının içerik kontrolünün ABA'lar içinde değil, daima dışarı aktarılarak yapılması önerilmektedir.

5.3 Bulguların Sunulmasına Yönelik Kullanılan Adli Bilişim Atlatma Teknikleri ve Karşı Tedbirler

Bu kısımda kullanılan adli bilişim atlatma teknikleri, bulguların raporlanması ve sunulmasında adli bilişim uzmanını yanıltmak, legal otoriteler üzerinde delilin geçerliliği konusunda şüphe uyandırmak amacını gütmektedirler.

5.3.1 Hash çakışması

Hash (özet) fonksiyonları, herhangi bir miktarda veriye sahip olan bir dosyayı tanımlamak amaçlı, benzersiz bir sabit dize değeri oluşturmak için kullanılan algoritmalar. Şifrelemenin aksine, hash algoritmalar geri döndürülemezler yani tek yönlüdürler. Elde bulunan bir özet bilgi ile kullanılan hash algoritması bilinse dahi dosya içeriği geri elde edilemez. Hash bilgisi, bilgisayar adli bilişiminde, soruşturma süreci boyunca dijital delillerin değişmediğini garanti etmektedir [108]. Hash fonksiyonlarından beklenen tüm girdiler için farklı özet bilgisi çıkarmasıdır. Fakat [109]'de iki farklı girdi verisi için aynı hash çıktılarının oluşturulabileceği gösterilmiştir. ABA'lar dosyaları analiz ederken, hash veritabanlarını kullanarak bilinen zararlı dosyalar ya da bilinen iyi dosyalar (sistem dosyaları vb.) hakkında adli bilişim uzmanlarına yardımcı olmaktadır. Dolayısıyla hash bilgisinin saldırganlar tarafından istenildiği şekilde sonuçlandırılması, oluşturmuş oldukları her türlü dosyanın ABA'larca bilinen iyi dosyalar arasında gösterilmesini sağlamaktadır. Bu olasılık, dijital delillerin geçerliliğini zayıflatabilmektedir. Bir çalıştırılabilir dosyanın zararlı olup olmadığının tespiti için, kötü amaçlı bir çalıştırılabilir dosyanın hash bilgisinin, yalnızca kötü amaçlı dosyaların hash değerleri veritabanına sahip bir kara liste içinde aratılması, yanlış bir yaklaşım olarak değerlendirilmektedir. HexEdit gibi bir program aracılığı ile dosyadaki bazı karakterleri değiştirmek suretiyle dosyanın hash bilgisi kolayca değiştirilebilmektedir. Bu sayede dosya, kötücül olmayan bir dosya olarak gösterilebilmektedir. Bunun yanı sıra, suç unsuru olan dosyalara veri ekleme, hash değerini değiştirerek bilinen iyi dosyalardan biriyle eşleşebilmelerine sebep olabilmektedir. Bazı hash algoritmalarının zayıflıklarını ve hash çakışmalarını oluşturma ihtimalini göstermek için HashClash [110] gibi kullanılabilen araçlar bulunmaktadır.

Hash çakışmalarından kaçınmak için, Whirlpool, SHA 3 ailesi, SHAKE ailesi gibi daha az çakışma olasılığına sahip hash algoritmalarının kullanılması ve dosyaları bulmak için hash bilgisi ile arama yapılmaması önerilmektedir. Elimizde aynı hash değere sahip iki dosya varsa, bu iki dosyayı sektör sektör hash (örneğin, her 512 bayt için hash) fonksiyonundan geçirerek , farkın nerede olduğu gösterilebilmektedir.

5.3.2 İşlevsiz sabit disk kullanımı

Bir kişisel bilgisayarın (PC) sabit diski, verileri tutmak için kullanılmadığı takdirde delil toplamak açısından bir değer barındırmamaktadır. Saldırganlar, kullanılmayan (işlevsiz) bir sabit disk bulundurdıkları bir bilgisayara sahip olabilirler. Bir PC, USB'den önyükleme yapılarak da kullanılabilmekte ve sabit disk günlük kullanımda yok sayılabilmektedir. Bu tür kullanım, verileri bulut veya uzaktaki bir makinede saklama niyetiyle kullanılmaktadır. Buna ek olarak saldırgan, sabit diskin düzenli olarak kullanıldığı algısını oluşturmak için sabit diske rasgele yazmaları otomatikleştiren bir hizmet kullanabilmektedir. Sabit diskin "En Son (Recent)" girdilerinde bilgi olduğu sürece, adli bilişim uzmanı sabit diskin son zamanlarda kullanıldığını düşünecektir [97].

Bu tekniğe karşı tedbir olarak, bir adli bilişim uzmanının el konulan donanımın USB yuvalarını kontrol etmesi ve herhangi bir USB sürücüsünün bağlı olup olmadığını incelemesi gerekmektedir. Günümüzde USB sürücülerin gittikçe küçülmesi, adli bilişim uzmanlarınca bu donanımların fark edilememesine sebep olabilmektedir. Ayrıca USB sürücüsünün Pagefile dosyasının dikkatli bir şekilde kontrol edilmesi gerekmektedir, çünkü bu USB sürücü dosyası, bir ağ konumuna işaret edebilmektedir. Son olarak, mümkünse, donanıma el koymadan önce, herhangi bir uzak sürücü konumunun bulunup bulunmadığını tespit etmek için ağ trafiğinin izlenmesi önerilmektedir [97].

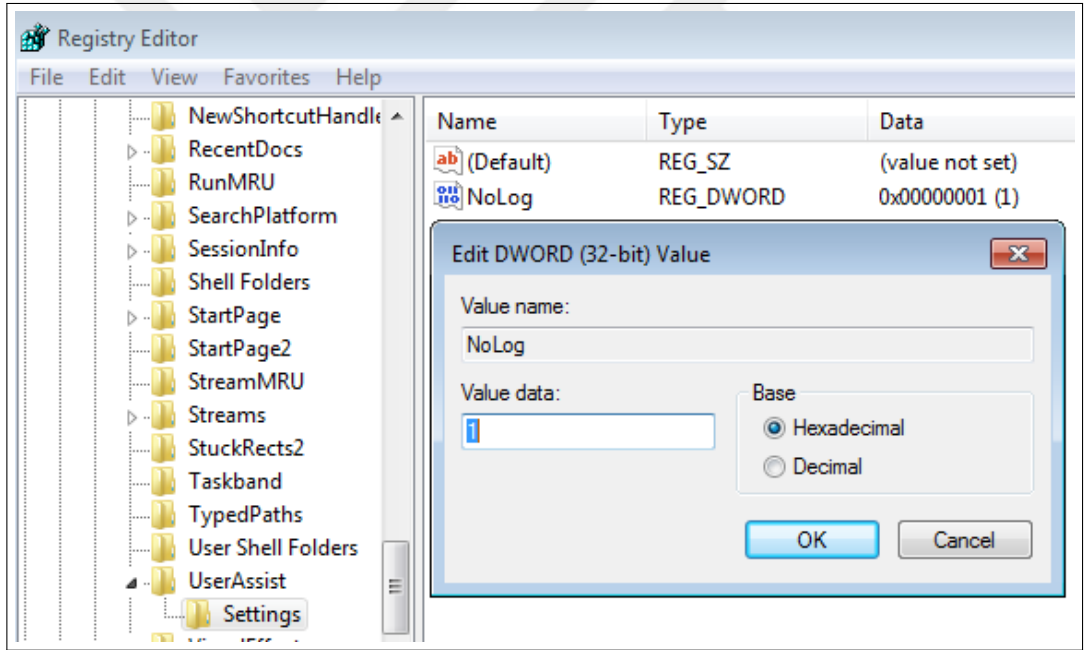
5.4 MS Windows İşletim Sistemlerinde İzlerin Yok Edilmesine Yönelik Uygulanan Adli Bilişim Atlatma Teknikleri

Bu kısımda, ABU'ların el konulan bir MS Windows işletim sistemli cihazda, kullanıcının profili (teknik ya da normal kullanıcı vb.) hakkında da bilgi

sahibi olmalarını sağlayabilecek, izlerin yok edilmesi ve bu sayede adli bilişim soruşturmasının engellenmesi amaçlı kullanılan yöntemler anlatılmaktadır.

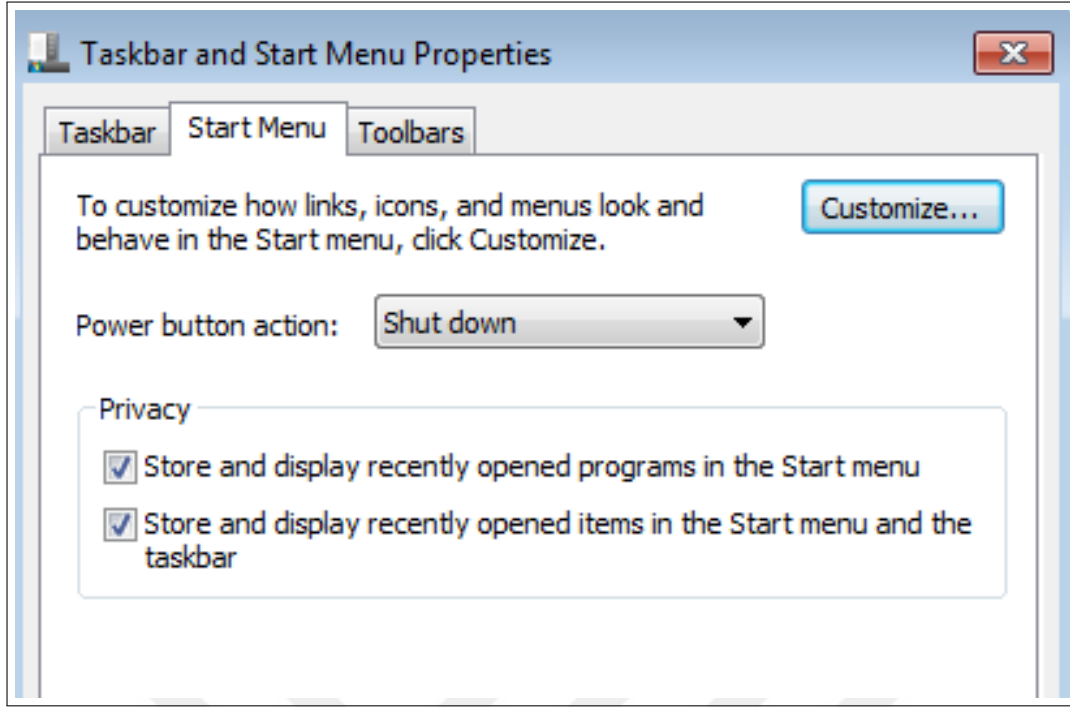
5.4.1 Kayıtları devre dışı bırakma

Teknik bir kullanıcının, sahip olduğu bilgisayarda adli bilişime esas bilgileri gizlemek için genel olarak ilk başvurduğu yöntem kayıtları devre dışı bırakmaktır. Bunu başarmak için öncelikle MS Kayıt Defterinde (Registry) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist anahtarı altındaki bütün anahtarlar silinmekte ve "Settings" adıyla yeni bir anahtar oluşturulmaktadır. Bu anahtar altında, Şekil 5.13'teki gibi "NoLog" isimli yeni DWORD 32 bit değeri oluşturularak "1" değeri atanmaktadır. Bu işlemden sonra işletim sistemi, Windows Explorer ile yapılan dosya işlemlerindeki faaliyetlerinize ait kayıtları (log) tutmayacaktır.



Şekil 5.13: MS Windows işletim sisteminde faaliyet zaman damgasını devre dışı bırakma ayarı.

Bunun yanı sıra başlat menüsü veya görev çubuğunda, son açılan programlara ait kayıtların gösterilmemesi için Şekil 5.14'teki görülen mahremiyet (Privacy) ayarlarındaki kutucuklardan işaretleri kaldırılabilir.



Şekil 5.14: MS Windows işletim sisteminde en son açılan programları göstermeme.

5.4.2 Son erişim kayıtlarını devre dışı bırakma

MS Windows işletim sisteminde son erişim kaydının devre dışı bırakılmasına Bölüm 5.2.2’de değinilmişti. Bu ayarı yapmak için "Komut İstemi (Yönetici)" çalıştırılarak, "FSUTIL behavior set disablelastaccess 1" komutu çalıştırılmaktadır. Şekil 5.15’te görüleceği gibi bu işlem yeniden başlatılmayı müteakip devreye girmektedir.

```
C:\> Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

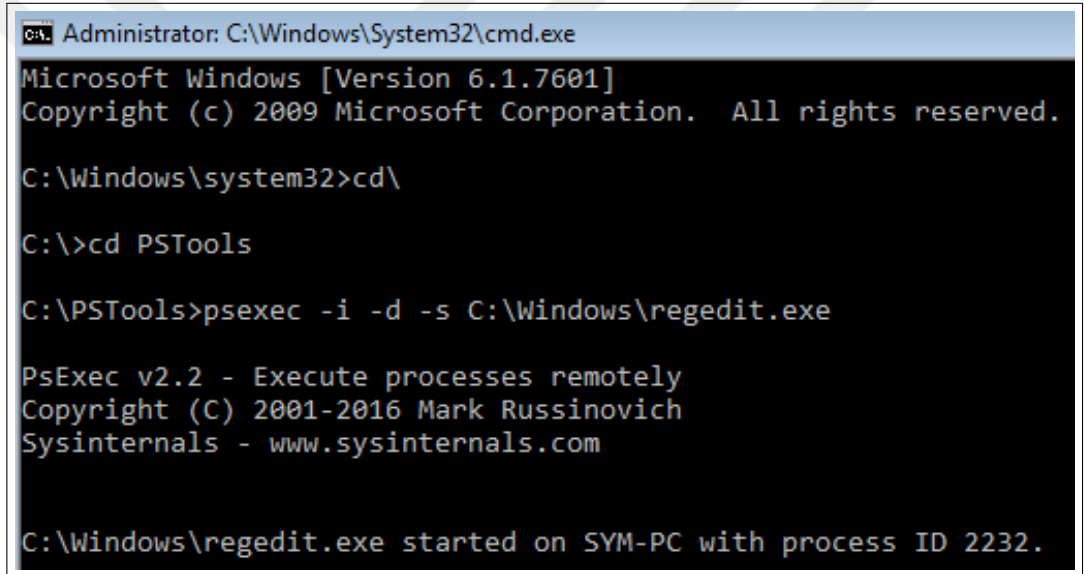
C:\Windows\system32>FSUTIL behavior set disablelastaccess 1
NOTE: Changes to this setting require a reboot to take effect.
DisableLastAccess = 1

C:\Windows\system32>_
```

Şekil 5.15: MS Windows işletim sisteminde son erişim bilgilerini devre dışı bırakma.

5.4.3 USB faaliyetleri için kayıtları devre dışı bırakma

Bu kısımda yapılacak ayar için öncelikle HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR isimli anahtarın silinmesi gerekmektedir. Yalnız silme işlemini gerçekleştirmek için özel izinler gereklidir ve bunu sağlamak için de [111]'daki PsExec programının indirilmesi gerekmektedir. Program indirildikten sonra Şekil 5.16'daki gibi program çalıştırılmaktadır. Bu işlem başarı ile başlatıldıktan sonra, Kayıt Defteri Düzenleyicisi (regedit.exe) bir Windows Explorer dosyası gibi masaüstünde açılmakta ve ilgili anahtarın silinmesine imkan vererek USB cihazlarına ait kayıtların artık tutulmaması sağlanmaktadır.



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd\

C:\>cd PSTools

C:\PSTools>psexec -i -d -s C:\Windows\regedit.exe

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Windows\regedit.exe started on SYM-PC with process ID 2232.
```

Şekil 5.16: MS Windows işletim sisteminde USB cihaz kayıtlarını devre dışı bırakma.

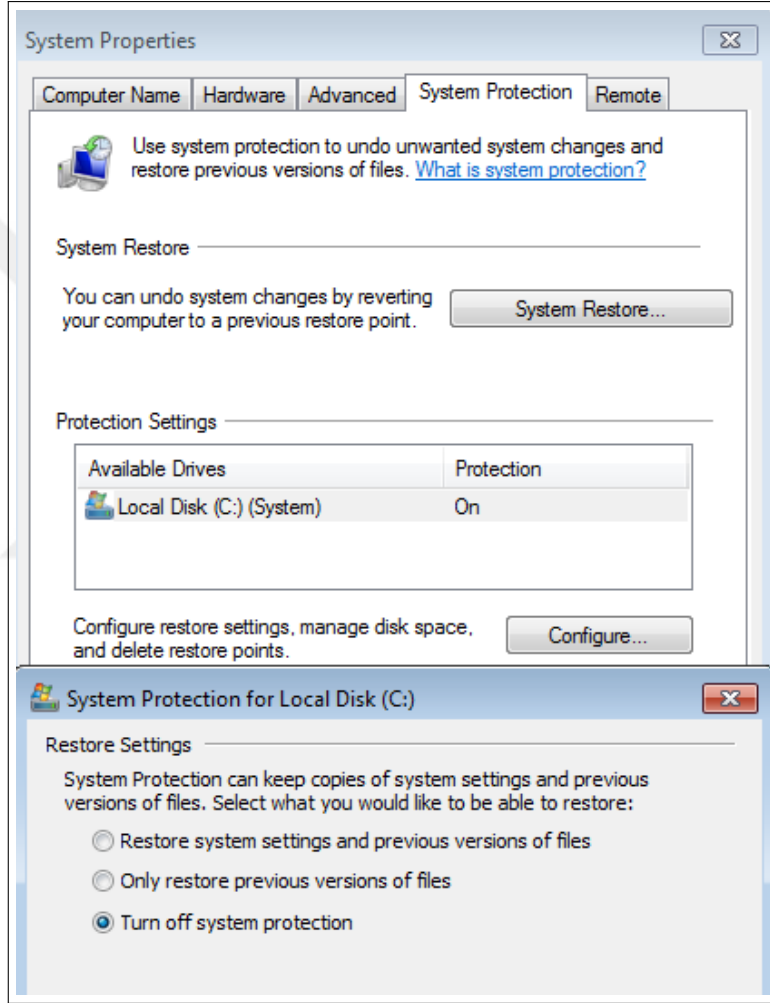
Özellikle bu yöntem ABU'ları, Bölüm 5.1.1'de ele alınan veri doygunluğu yönteminde anlatıldığı üzere, şüpheliler ilgili ilgisiz mümkün olduğunca fazla sayıda USB belleği muhafaza edeceklerinden, hangi USB belleğin kullanıldığı hangilerinin kullanılmadığı bilgisinden mahrum bırakmaktadır.

5.4.4 Sistem geri yükleme noktalarını devre dışı bırakma

Sistem geri yükleme noktaları bilgisayarların, önemli bir güncelleştirme sonrasında veya kullanıcı isteğinde belirli zamanlarda oluşturulabilen sistem zamanlarındaki durumlarına geri dönmelerini sağlamaktadırlar. Bir adli bilişim olayında sistem

geri yükleme noktalarının oluşturduğu tarihler kullanılarak, bilgisayarın suça ilişkin tarihlerdeki durumuna dönüşü sağlanarak incelemeler yapılabilir.

Bu nedenle suçlular, bu geri yükleme noktalarının oluşturulmasını devre dışı bırakmaktadırlar. Bunun için Bilgisayar Özelliklerinden "Gelişmiş Sistem Ayarları" na giriş yapılmakta ve Şekil 5.17'de görüldüğü gibi "Sistem Koruması" sekmesi altındaki yapılandırma (configure) tuşu yardımıyla sistem koruması kapalı konuma getirilebilmektedir.

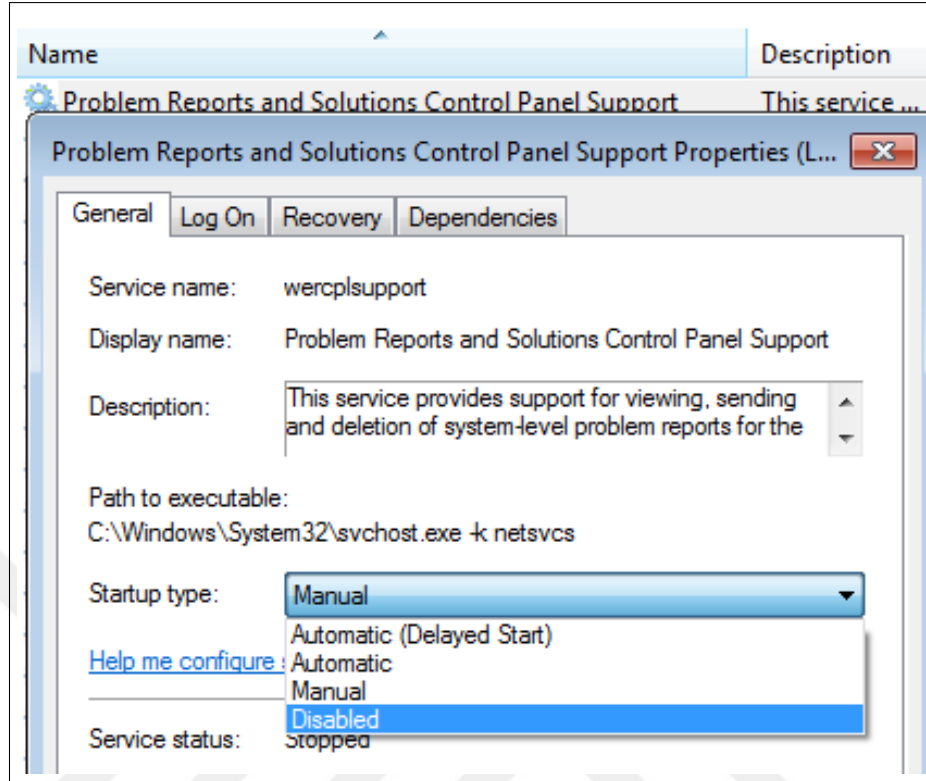


Şekil 5.17: MS Windows işletim sisteminde sistem korumayı kapatma.

5.4.5 Microsoft hata bildirimlerinin devre dışı bırakılması

Herhangi bir servis veya program, bilinmeyen bir nedenle durur veya kapanırsa, uygulamalar hata bildirimlerini Microsoft'a göndermektedirler. Bu işlemin devre dışı bırakılması için "services.msc" çalıştırılarak servisler penceresi açılmaktadır. Bu pencereden Şekil 5.18'de görüldüğü üzere "Sorun Raporları ve Çözüm Desteği

Denetim Masası Desteği (Problem Reports and Solutions Control Panel Support)" özelliklerinden servis devre dışı bırakılabilmektedir.



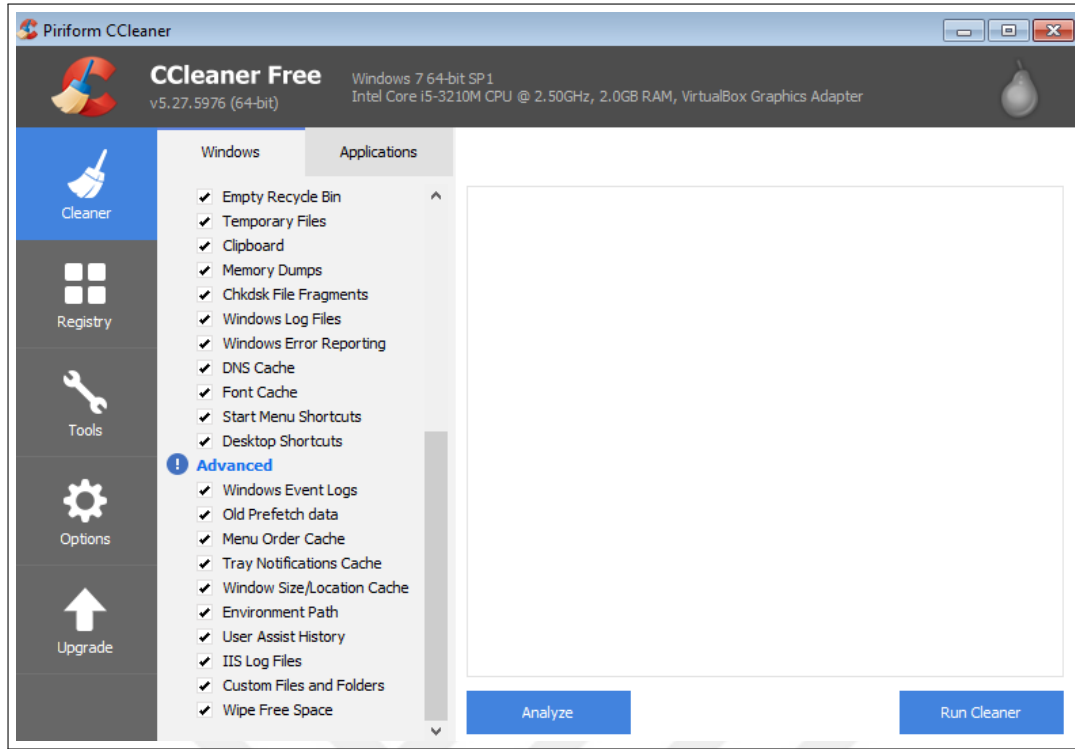
Şekil 5.18: MS Windows işletim sisteminde hata bildirimini devre dışı bırakma.

5.4.6 Üçüncü parti yazılımlar ile önemli kayıtları temizleme

Üçüncü parti programlar aracılığı ile Windows işletim sistemindeki kayıtlar ve uygulamalara ait kayıtlar, güvenli bir şekilde üzerine yazma işlemi ile temizlenebilmektedir. CCleaner ücretsiz bir güvenli silme aracıdır. Bu program çalıştırıldığında, güvenli silme seçeneğini kullanıcıya sunmaktadır. Kullanıcı seçeceği yöntem ile temizlik işlemini başlatabilmektedir. Üç kere üzerine yazma yöntemi ile Şekil 5.19'da görülen Windows'taki kayıt dosyaları temizlenebilmektedir.

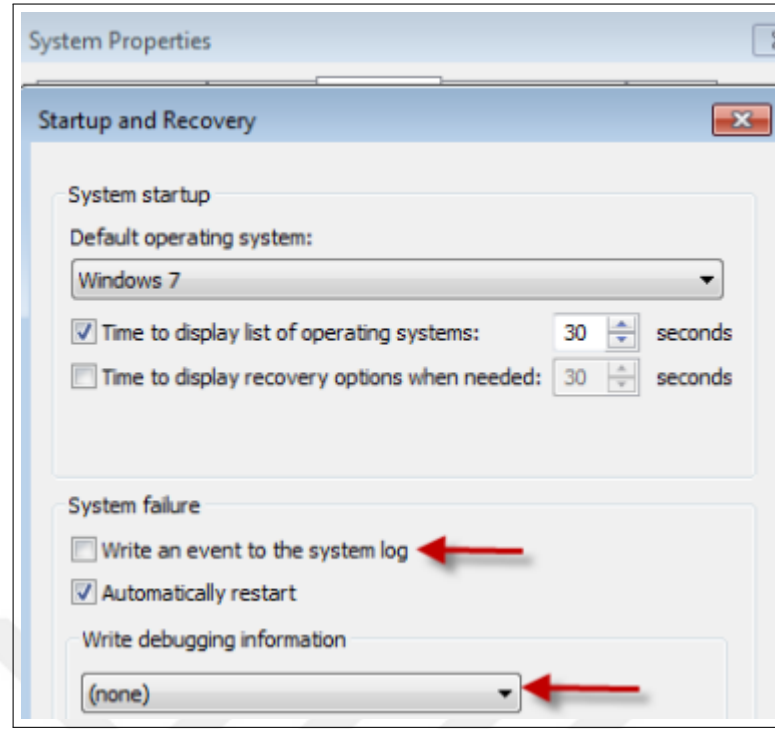
5.4.7 Windows hata ayıklama bilgisi yazımını devre dışı bırakma

Bilgisayarın açılmaması veya mavi ekran hatası durumlarında, hata kayıtları hata ayıklama bilgisi olarak yazılmaktadır. Bu hataların yazımının devre dışı bırakılması için bilgisayar özelliklerinden, gelişmiş sistem ayarları, gelişmiş sekmesi altında, başlangıç ve kurtarma (startup and recovery) ayarlarından, Şekil 5.20'de görüldüğü gibi "Sistem Günlüğüne Olay Olarak Yaz (Write an event to the system log)"



Şekil 5.19: CCleaner üçüncü parti yazılımı ile kayıt temizleme.

kontrol kutucuğundaki işaret kaldırılabilmekte ve "Hata Ayıklama Bilgisini Yaz (Write debugging information)" kısmında "Yok (None)" seçeneği seçilmesi gerekmektedir.



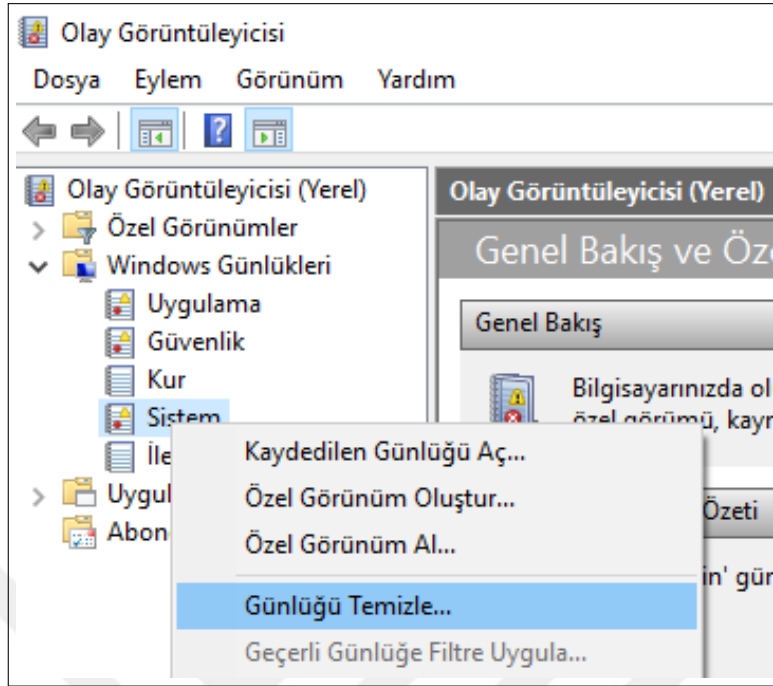
Şekil 5.20: Hata ayıklama bilgisi yazımının devre dışı bırakılması.

5.4.8 Windows olay kayıtlarını temizleme

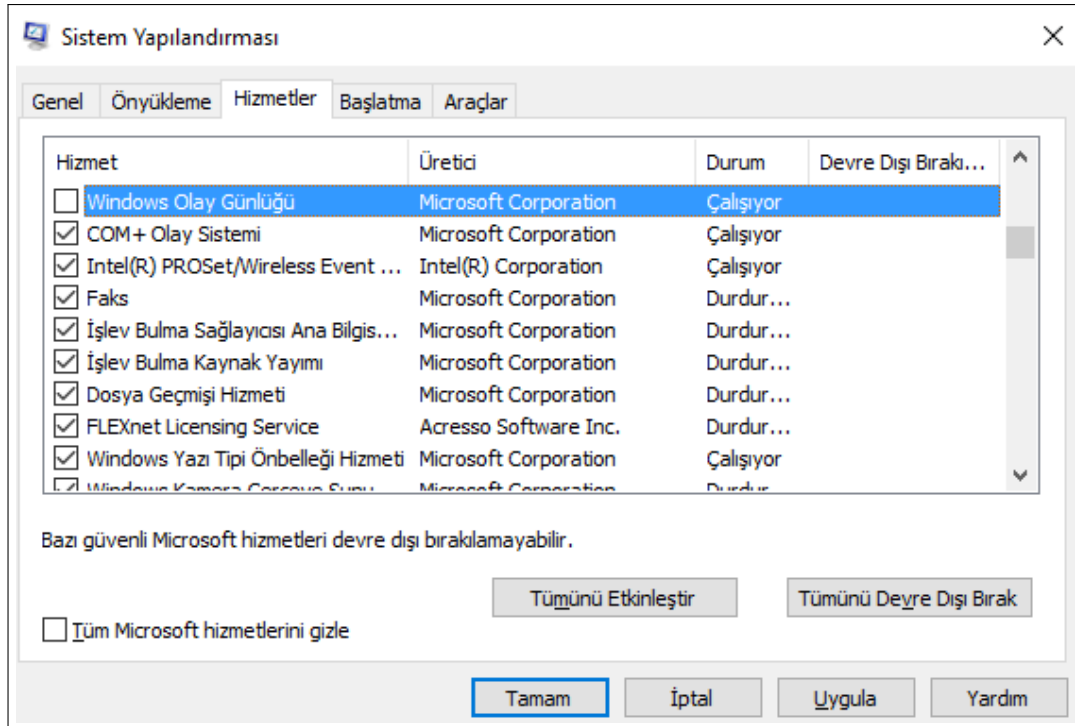
Windows Olay Günlükleri, işletim sistemi tarafından sistem ve uygulamalara ait olayları, uyarıları ve hataları kayıt altında tutmaktadırlar. Bu günlüklerde tutulan kayıtları silmek için "Denetim Masası" "Sistem ve Güvenlik" altındaki "Olay Günlüklerini Görüntüle" ile günlük açılarak Windows Günlükleri altından sistem üzerine sağ tıklayarak Şekil 5.21'de görüldüğü gibi "Günlüğü Temizle" komutu çalıştırılabilmektedir.

Bu temizleme işlemi şeklinde yapılabileceği gibi, msconfig komutu çalıştırılarak Şekil 5.22'de görülebileceği gibi gelen pencereden "Hizmetler" sekmesi altında "Windows Olay Günlüğü" hizmeti kutucuğundaki işaret kaldırılarak olay günlüğü hizmeti devre dışı bırakılabilmektedir.

Bölüm 5.4'te anlatılan iz yok etme ayarlarının tamamı, adli bilişim uzmanınca yapıp yapılmadığı, ayarların değiştirilip değiştirilmediği görülebilen olaylar olduğundan, işlemlerin kullanımı bile kullanıcı hakkında gerekli şüpheyi oluşturmakta yeterli olmaktadır. Fakat delilin yokluğu, sonuç olarak suçun ispatını mümkün kılmayacaktır.



Şekil 5.21: Windows 10 olay günlüğünü temizleme işlemi.



Şekil 5.22: Windows 10 olay günlüğü hizmetini devre dışı bırakma.

6. SONUÇ VE ÖNERİLER

Bu tez çalışmasında, bir adli bilişim vakasında soruşturma süresini uzatmak veya soruşturmayı engellemek amacıyla kullanılan adli bilişimi atlatmanın (anti-forensics) ne olduğu, bu amaçla hangi tekniklerin kullanıldığı ve bu tekniklerin nasıl kullanıldıkları, hangi adli bilişim süreçlerini hedef aldıkları detaylı bir şekilde uygulamalarla desteklenerek açıklanmaya çalışılmıştır. Klasik ABAT'lar, verileri yok etmek ya da verilerin okunmasını imkansız hale getirmek amacıyla kullanılırken, modern ABAT'ların, bir soruşturma için gerekli zamanı uzatmayı, dijital adli bilişim izlerini yok etmeyi ve adli bilişim süreçlerini karmaşıklaştırmayı hedeflemekte olduğu vurgulanmıştır. Bu tür saldırılar, adli bilişim soruşturmalarının maliyetinin artmasına veya delilin inandırıcılığının ve geçerliliğinin azalmasına neden olabilmektedir. Bölüm 5'teki modern adli bilişim atlatma tekniklerinde belirtildiği üzere, tekniklerin çoğunun kullanımında teknik uzmanlık gerekli değildir.

Bu çalışmanın öncelikli amacı, adli soruşturma süreçleri ve araçlarının geliştirilmesine katkıda bulunmaktır. İkinci amaç, adli bilişim soruşturmacılarına ve bilgi güvenliği uzmanlarına, bu ABAT'lardan herhangi birinin kullanılıp kullanılmadığını tespit etmek maksadıyla, kontrol etmeleri gerekli olan yerleri göstermektir. En basit ve en az karmaşık ABAT kullanımını bile, bir soruşturmayı büyük ölçüde karmaşık hale getirebilmektedir. Bu nedenle soruşturmacıların bu teknikler hakkında, durumsal farkındalığa sahip olmaları ve bir adli bilişim soruşturması esnasında ABAT'lar ile baş etmeye hazır olmaları gerekmektedir.

Tez çalışmasında incelenen adli bilişimi atlatma teknikleri ve karşı tedbirler Çizelge 6.1'de özetlenmiştir.

Teknolojideki gelişmelerin hızına bakıldığında, donanımlardaki ve uygulamalardaki çeşitliliğin artarak devam edeceği düşünülmektedir. Bu gelişmelerle birlikte doğru orantılı olarak, teknolojinin hedef veya vasıta olarak kullanıldığı suçlarda da artış olacağı değerlendirilmektedir. Özellikle mobil, gerçek zamanlı ve nesnelerin interneti (IoT) teknolojilerinin kullanımının artacağı, siber saldırılarla ev eşyalarının, ulaşım

Çizelge 6.1: Adli bilişimi atlatma teknikleri ve karşı tedbirler özet.

Teknikler	Karşı Tedbirler
Sabit Disk/Dosya Temizleme	Başarılı bir üzerine yazma sonrası veri kurtarılamamaktadır. R-Studio ile disk incelemesinde temizlemeye ait izler görülebilmektedir.
Şifreleme	Zorlama veya mahkeme kararı, Sosyal Mühendislik, Sözlük/Kaba Kuvvet/Gökküşağı Tabloları ile şifre elde edilebilmektedir.
Fiziksel Yok Etme	Veri kurtarılamamaktadır.
Steganografi	Stego Suite, Stego Expose, XStego ile dosya tespit edilebilmekte ve stegoanaliz teknikleri kullanılabilmektedir.
Veri Doygunluğu	Veri toplama sürecini paralelleştir. Şüphelilerin cihazlarını kullan. (Live CD) Triyaj süreçlerini uygula.
Standart Olmayan RAID	Şüphelinin cihazında Live CD ile de-RAID yap. Disk bölümlerlerinin (volume) kopyasını al. R-Studio RAID Recovery kullan.
Dosya İmza Bilgisini Değiştirme	Şüphelinin cihazında bir HexEditor var mı? En Son işlemleri kontrol et. (Bir .exe dosyasının notepad ile açılması).
Dosya Zaman Damgalarında (MACE) Sahtecilik	\$ STANDART_INFO ve \$ FILE_NAME altındaki zaman damgalarını karşılaştır. Varsa belge içindeki zaman bilgilerini kullan. BIOS saati rasgele değişiyorsa, işlem sırası bilgisi için log dosyalarını incele.
Kısıtlı Klasör veya Dosya Adı	İmajdaki belge ve klasörler yerel dosya adlarıyla dışa aktarılmamalıdır. Dosya Kimliği (File ID) ile dışa aktar.
Döngüsel Referanslama	Klasörleri değil, dosyayı dışa aktar.
ABA'lara Yönelik Saldırı	Zip dosyalarının içeriğini dışa aktar.
Hash Çakışması	Güçlü hash algoritmaları kullan. Zararlı dosya aramasını hash bilgisi ile yapma.
İşlevsiz Sabit Disk	El konulan cihazın USB yuvalarını kontrol et. USB sürücüsünün Pagefile dosyasını incele. Ağ sürücülerinin uzak bir konuma erişiyor mu?

araçlarının bile hedef alınacağı öngörülmektedir. Bu durumda, adli bilişimin de her türlü ortama uygun şekilde işlevini yerine getirebileceği, her alt branşta ayrı ayrı uzmanlık gerektireceği, sürekli yeni adli bilişim dallarının oluşacağı esnek bir yapıda değerlendirilmesi gerekmektedir. Artık günümüzde neredeyse suçların tamamında, adli bilişim imkanlarından yararlanılmaktadır. En basit suçlarda bile suçluların sosyal ağlardaki mesajlarına, mobil telefon konuşmalarına ve içeriklerine bakılarak suçlarının tespit edildiği günümüzde, adli bilişim uzmanlarının çok daha karmaşık siber suçların analizine hazırlıklı olması gerekmektedir. Adli bilişim uzmanları, görevlerini yaparken, işlerini kolaylaştırıcı donanımsal veya yazılımsal araçlardan faydalanmaktadır. Adli bilişim araçları olarak adlandırılan bu uygulamalar, özellikle silinmiş verinin kurtarılması, verilerin uygulamalara göre (e-posta, doküman, çalıştırılabilir dosya vb.) sınıflandırılması, zaman bilgileri ve USN dosya günlüğü işlemlerinin takip edilebilmesi, bazı anahtar kelimelere göre arama yapılabilmesi ve bulguların sunulabilmesi için raporlama yapılabilmesini mümkün kılmak ve orijinal delilin bozulmaya uğramadan delil niteliği sağlayacak bilgilerin elde edilmesine olanak sunmak için kullanılmaktadırlar. ABA'ların çalışma yöntemleri ABU'lar tarafından bilindiği gibi, suçlular tarafından da iyi bilinmektedir. Suçlular ya da beyaz şapkalı hackerlar araçların çalışma prensibinden hareketle, onları aldatıcı, çalışmasını engelleyici teknikler geliştirmişlerdir. Geliştirilen teknikler karşısında, ABA'ların gelişim veya reaksiyon hızı ise oldukça düşük seviyelerde kalmaktadır. Bu nedenle adli bilişimi atlatmaya yönelik tekniklerin bilinmesi, ABU veya BGU'ların adli bilişim soruşturmalarında yanıltma olasılığını düşürecek ve delillerin geçerliliği üzerindeki soru işaretlerinin kaldırılmasına hizmet edecektir.

Her soruşturmada, adli bilişimi atlatmanın kullanım olasılığını detaylı bir şekilde kontrol etmek kolay değildir. Bu nedenle soruşturmacı, bir adli bilişim vakasına konu olan şüphelinin profiline (teknik veya normal kullanıcı vb.) bakarak, adli bilişim atlatma tekniklerinin kullanıldığına dair incelemenin gerekli olup olmadığına karar vermektedir. Bu çalışma kapsamındaki, adli bilişimi atlatma teknikleri anlatım olarak tek tek ele alınmış olsa da, bu tekniklerin birkaçının birlikte kullanımı adli bilişim alanında daha büyük zorluklara yol açacaktır.



KAYNAKLAR

- [1] **Ufuk TAŞÇI ve Ali CAN**, “Türkiye’de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014.” *Fırat Üniversitesi Sosyal Bilimler Dergisi* 25.2 (2015).
- [2] **H. Jahankhani ve E. Beqiri**, *Handbook of Electronic Security and Digital Forensics* (Google eBook), vol. 2. 2010.
- [3] **A. Gürel**, “Adli Bilişim Nedir?” [Online]. Available: <http://www.gurelahmet.com/adli-bilism-nedir/> (Erişim tarihi: Ocak 2018).
- [4] **H. Çakır ve M. S. Kılıç**, “Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bakış,” *Turkish Police Studies Journal./ Polis Bilim Dergisi*, 2013.
- [5] **Google Akademik**, [Online]. Available: <https://scholar.google.com.tr/> (Erişim tarihi: Mart 2018).
- [6] **Ulusal Tez Merkezi**, [Online]. Available: <https://tez.yok.gov.tr/UlusalTezMerkezi/> (Erişim tarihi: Mart 2018).
- [7] **C. Varol, P. A. Cooper ve A. Varol**, “Türkiye’de Adli Bilişim Eğitimi,” *1st International Symposium on Digital Forensics and Security (ISDFS’13)*, 2013, no. May, pp. 20–21.
- [8] **R. Harris**, “Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem,” *Digit. Investig.*, vol. 3, no. SUPPL., pp. 44–49, 2006.
- [9] **B. Shirani**, “Anti-forensics,” *High Technology Crime Investigation Association*; 2002.
- [10] **C. S. J. Peron ve M. Legary**, “Digital anti-forensics: emerging trends in data transformation techniques,” *Proc. 2005 E-Crime Comput. Evid.*, 2005.
- [11] **Grugq**, “The art of defiling: defeating forensic analysis,” *Blackhat Brief.*, 2005.
- [12] **Foster J ve Liu V.**, “Catch me if you can. . . . *Blackhat Briefings.*”, 2005.
- [13] **V. Liu ve F. Brown**, “Bleeding-Edge Anti-Forensics,” *InfoSec World*, 2006.
- [14] **R. Harris**, “Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem,” *Digit. Investig.*, vol. 3, no. SUPPL., pp. 44–49, 2006.
- [15] **Gary C. Kessler**, “Anti-forensics and the digital investigator,” *Australian Digital Forensics Conference*; 2007. p. 1

- [16] **S. Garfinkel**, "Anti-Forensics: Techniques , Detection and Countermeasures," *2nd Int. Conf. Inf. Warf. Secur.*, pp. 77–84, 2007.
- [17] **JC Sremack, AV Antonov**, "Taxonomy of anti-computer forensics threats," *IMF* 2007:103-12.
- [18] **MC Stamm, WS Lin, K. Liu**, "Forensics vs. anti-forensics: a decision and game theoretic framework," *Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on. IEEE*; 2012. p. 1749-52.
- [19] **C. Thuen**, "Understanding counter-forensics to ensure a successful investigation," *Univeristy of Idaho*, 2007.
- [20] **P. Pajek ve E. Pimenidis**, "Computer anti-forensics methods and their impact on computer forensic investigation," *Commun. Comput. Inf. Sci.*, vol. 45, pp. 145–155, 2009.
- [21] **M. Wundram, F. C. Freiling ve C. Moch**, "Anti-forensics: The next step in digital forensics tool testing," *Proc. - 7th Int. Conf. IT Secur. Incid. Manag. IT Forensics, IMF* 2013, pp. 83–97, 2013.
- [22] **M. Anobah, S. Saleem ve O. Popov**, "Testing Framework for Mobile Device Forensics Tools," *J. Digit. Forensics, Secur. Law*, vol. 9, no. 2, pp. 221–234, 2014.
- [23] **R. Böhme ve M. Kirchner**, "Counter-forensics: Attacking image forensics," *Digit. Image Forensics There is More to a Pict. than Meets Eye*, pp. 327–366, 2013.
- [24] **M. Brand**, "Forensic Analysis Avoidance Techniques of Malware," *5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia*, 2007.
- [25] **M. Rogers**, "Anti-forensics: the coming wave in digital forensics.," 2006.
- [26] **A. Smith**, "Describing and Categorizing Disk-Avoiding Anti-Forensics Tools," *J. Digit. Forensic Pract.*, vol. 1, no. 4, pp. 309–313, 2007.
- [27] **K. Dahbur ve B. Mohammad**, "Toward understanding the challenges and countermeasures in computer anti-forensics.," *Int. J. Cloud Appl. Comput.*, p. 14, 2011.
- [28] **B. Blunden**, "Anti-Forensics: The Rootkit Connection," *Commentary*, pp. 1–44, 2009.
- [29] **M. Geiger**, "Evaluating commercial counter-forensic tools," *5th Annu. Digit. Forensic.*, pp. 1–12, 2005.
- [30] **K. D. Fairbanks, C. P. Lee, Y. H. Xia ve H. L. Owen**, "Timekeeper: A metadata archiving method for honeypot forensics," *2007 IEEE Work. Inf. Assur. IAW, no. June*, pp. 114–118, 2007.

- [31] **S. Rekhis ve N. Boudriga**, “A system for formal digital forensic investigation aware of anti-forensic attacks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 635–650, 2012.
- [32] **J. I. James**, “IoAF.” [Online]. Available: <https://github.com/hvva/IoAF> (Eriřim tarihi: Mart 2018).
- [33] **R. Kaur ve A. Kaur**, “Digital Forensics,” *Int. J. Comput. Appl.* (0975 – 8887), vol. 50, no. 5, pp. 5–9, 2012.
- [34] **Gary L Palmer**, “A Road Map for Digital Forensic Research. *Technical Report DTR-T0010-01, DFRWS*”. *Report for the First Digital Forensic Research Workshop (DFRWS)*, 2001.
- [35] **Adli Biliřim**, [Online]. Available: http://www.adlibilisim.org.tr/index.php?option=com_content&view=article&id=21&Itemid=170 (Eriřim tarihi: Ocak 2018).
- [36] **CMK**, [Online]. Available: <http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf> (Eriřim tarihi: Ocak 2018).
- [37] **M. Özen ve G. Özocak**, “Adli Biliřim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134),” *Ankara Barosu Derg.*, vol. 1, pp. 43–77, 2015.
- [38] **Garfinkel, S.L.**, “Digital forensics research: The next 10 years”, *Digital Investigation* 7, 2010.
- [39] **Thomas Alfred Johnson**, “Forensic Computer Crime Investigation.” *Connecticut: CRC Press* p. 57, 2006.
- [40] **K. Shanmugam**, “Validating Digital Forensic Evidence,” no. September, 2011.
- [41] **Mark Reith, Clint Carr ve Gregg Gunsch**, “An Examination of Digital Forensic Models” *International Journal of Digital Evidence*, Fall 2002, Volume 1, Issue 3.
- [42] **Rodrigo Fernando Morocho Román, Nancy Magaly Loja Mora, Johnny Paúl Novillo Vicuña, Josias Israel Piña Orozco**, “Digital Forensics Tools,” vol. 11, no. 19, pp. 76–91, 2016.
- [43] **B. Carrier**, “Open Source Digital Forensics Tools,” October, no. October, 2002.
- [44] **řeref SAđIROđLU ve M. KARAMAN**, “Adli Biliřim.” [Online]. Available: <http://www.telepati.com.tr/agustos12/konu8.htm> (Eriřim tarihi: Ocak 2018).
- [45] **S. Peisert, M. Bishop ve K. Marzullo**, “Computer forensics in forensics,” *SADFE 2008 3rd Int. Work. Syst. Approaches to Digit. Forensic Eng.*, pp. 102–122, 2008.
- [46] **Computer Forensics**, [Online]. Available: <http://victorypi.com/services/computer-forensics-deleted-data-recovery/> (Eriřim tarihi: řubat 2018).

- [47] **M. Gupta, M. Hoeschele ve M. Rogers**, “Hidden disk areas: HPA and DCO,” *Int. J. Digit. Evid.*, vol. 5, no. 1, pp. 1–8, 2006.
- [48] **H. Ç. Yusuf Güllüce, Recep Benzer**, “Adli Bilişimde Silinmiş Dosyaların Kurtarılması Üzerine Karşılaştırmalı Yöntemler,” *Yönetim Bilişim Sistemleri Dergisi*, 2016.
- [49] **EC-Council**, Computer Forensics Investigating Hard Disks, File Operating Systems. 2010.
- [50] **F. E. İ. Kılıç**, “Adli Bilişim Vakası Öncesinde Ağ Yapılan Saldırı ve Anormallik Tespiti Bir Olay İncelemesi,” *ISDFS*, 2013, no. May, pp. 20–21.
- [51] **T. ERCAN, D. NACAK**, “Kablosuz Ağlardaki Paket Trafikine Adli Bilişim Yaklaşımı,” *Yaşar Univ. J.*, vol. 4, no. 13, pp. 1909–1921, 2009.
- [52] **Keith J. Jones, Richard Bejtlich ve Curtis W. Rose**, “Real Digital Forensics: Computer Security and Incident Response.” *Addison-Wesley Professional*, 2005.
- [53] **M. Gül ve M. A. Aydın**, “Exploits in information security,” 2016 24th *Signal Processing and Communication Application Conference (SIU)*, Zonguldak, 2016, pp. 1729-1732. doi: 10.1109/SIU.2016.7496093.
- [54] **N. Meghanathan, S. R. Allam ve L. a. Moore**, “Tools and techniques for Network Forensics,” *Int. J. Netw. Secur. Its Appl.*, vol. 1, no. 1, pp. 14–25, 2010.
- [55] **Mobil Cihaz Kullanımı**, [Online]. Available: <https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/> (Erişim tarihi: Ocak 2018).
- [56] **S. Radicati**, “Mobile Statistics Report, 2014-2018,” *Mob. Stat. Report*, 2014-2018, vol. 44, no. 0, pp. 1–4, 2014.
- [57] **O. Köroğlu**, “En Yaygın İletişim Ortamı: Mobil İletişim Ortamında İçerik ve Yayıncılık,” *Civilacademy*, pp. 55–86, 2010.
- [58] **IDC**, “Mobil OS.” [Online]. Available: <https://www.idc.com/promo/smartphone-market-share/os> (Erişim tarihi: Mart 2018).
- [59] **R. Ahmed ve R. Dharaskar**, “Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective,” *6th Int. Conf. E- Gov.*, pp. 312–323, 2008.
- [60] **U. Akalin ve Ç. Uluyol**, “Mobil Cihazlar , Mobil Adli Bilişim ve Önerilen Süreç Modeli,” 2015.
- [61] **S. Brothers**, “How Cell Phone Forensic Tools Actually Work Cell Phone Tool Leveling System, Mobile Forensic.” World, Chicago, IL, USA, 2008.
- [62] **A. Zareen ve S. Baig**, “Mobile phone forensics challenges, analysis and tools classification,” *5th Int. Work. Syst. Approaches to Digit. Forensic Eng. SADFE* 2010, no. May, pp. 47–55, 2010.

- [63] **M. Brand, C. Valli ve A. Woodward**, “Malware Forensics: Discovery of the Intent of Deception,” *J. Digit. Forensics, Secur. Law*, vol. 5, no. 4, pp. 31–42, 2010.
- [64] **Virus Total**, “Virus Total.” [Online]. Available: <https://www.virustotal.com> (Eriřim tarihi: Ocak 2018).
- [65] **Y. Bolat**, “Memory Forensics,” İstanbul Bilgi Üniversitesi, 2015.
- [66] **C. H. Malin, E. Casey ve J. M. Aquilina**, *Malware Forensics Field Guide for Linux Systems*. 2014.
- [67] **Comae**, “Dumpit.” [Online]. Available: <http://www.comae.io/> (Eriřim tarihi: řubat 2018).
- [68] **M. Russinovich**, “ProcDump.” [Online]. Available: <https://technet.microsoft.com/en-us/sysinternals/dd996900.aspx> (Eriřim tarihi: řubat 2018).
- [69] **B. Delpy**, “Mimikatz.” [Online]. Available: <https://github.com/gentilkiwi/mimikatz> (Eriřim tarihi: řubat 2018).
- [70] **D. C. Harrill ve R. P. Mislán**, “A Small Scale Digital Device Forensics ontology,” *Small Scale Digit. Device Forensics J.*, vol. 1, no. 1, pp. 1–7, 2007.
- [71] **Paraben**, “Paraben.” [Online]. Available: <https://www.paraben.com/> (Eriřim tarihi: Ocak 2018).
- [72] **R. J. Shaw ve A. S. Atkins**, “Unified Forensic Methodology for the Analysis of Embedded Systems,” 2010.
- [73] **Facebook İstatistięi**, “Facebook İstatistięi.” [Online]. Available: <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> (Eriřim tarihi: Mart 2018).
- [74] **S. A. Sam, F. Year ve F. Year**, “Social Network Forensics,” *Int. J. Pharm. Technol.*, vol. 8, no. 4, pp. 22395–22404, 2016.
- [75] **M. Mulazzani, M. Huber ve E. Weippl**, “Social Network Forensics: Tapping the Data Pool of Social Networks,” *Eighth Annu. IFIP WG 11.9 Int. Conf. Digit. Forensics*, 2012.
- [76] **N. Al Mutawa, I. Al Awadhi, I. Baggili ve A. Marrington**, “Forensic artifacts of Facebook’s instant messaging service,” *6th Int. Conf. Internet Technol. Secur. Trans.*, no. December, pp. 771–776, 2011.
- [77] **N. Al Mutawa, I. Al Awadhi, I. Baggili ve A. Marrington**, “Forensic analysis of social networking applications on mobile devices,” *Digit. Investig.*, vol. 9, no. SUPPL., 2012.
- [78] **A. Joshi ve D. Bhilare**, “Emerging trends and research in digital forensics,” *Oijrj.Org*, no. I, pp. 293–304, 2014.

- [79] **H M Wolfe**, “Web Solutions and Technologies After the Hack,” *ICE Conference*, 2003.
- [80] **Y. Yusoff, R. Ismail ve Z. Hassan**, “Common Phases of Computer Forensics Investigation Models,” *Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 3, pp. 17–31, 2011.
- [81] **D. Lillis, B. Becker, T. O’Sullivan ve M. Scanlon**, “Current Challenges and Future Research Areas for Digital Forensic Investigation,” *11th Annu. ADFSL Conf. Digit. Forensics, Secur. Law (CDFSL 2016)*, pp. 9–20, 2016.
- [82] **M. K. Rogers**, “Anti-Forensics,” in Presentation given to Lockheed Martin, 2005.
- [83] **D. Franco, D. Fuschini ve T. Rodrigues**, “How To Detect Anti-Forensic Techniques,” *eForensics*, pp. 45–69, 2016.
- [84] **R. Kissel, A. Regenscheid, M. Scholl ve K. Stine**, “*NIST Special Publication 800-88 Guidelines for Media Sanitization*,” 2014.
- [85] **P. Gutmann**, “Secure Deletion of Data from Magnetic and Solid-State Memory,” *Sixth USENIX Secur. Symp. Proc.*, vol. Volumel, pp. 77–90, 1996.
- [86] **R-Studio Recovery Tool**, “R-Studio Recovery Tool.” [Online]. Available: <http://www.r-studio.com/downloads/RStudio8.exe> (Erişim tarihi: Şubat 2018).
- [87] **M. Wei, L. Grupp, F. Spada ve S. Swanson**, “Reliably Erasing Data from Flash-based Solid State Drives,” *9th USENIX Conf. File Storage Technol.*, pp. 8–8, 2011.
- [88] **Eraser Tool**, “Eraser Tool.” [Online]. Available: <https://eraser.heidi.ie/download/> (Erişim tarihi: Şubat 2018).
- [89] **H. Berghel**, “Hiding Data, Forensics, and Anti-Forensics,” vol. 50, no. 4, pp. 15–20, 2007.
- [90] **D. Goldschlag**, “Onion Routing for Anonymous and Private Internet Connections 1 Introduction,” 1999.
- [91] **R. Kissel, A. Regenscheid, M. Scholl ve K. Stine**, “Onion Routing for Anonymous and Private Internet Connections 1 Introduction,” 1999.
- [92] **E. De Lucia**, “Disk Degaussing.” [Online]. Available: <http://resources.infosecinstitute.com/anti-forensics-part-1/> (Erişim tarihi: Şubat 2018).
- [93] **N. M. Patterson ve S. F. Lee**, “Image Steganography: A Closer Look at the Least Significant Bits Method,” no. April, p. 26, 2015.
- [94] **S. Kumar, G. Singh, T. Kumar ve M. S. Nehra**, “Hiding the Text Messages of Variable Size using Encryption and Decryption Algorithms in Image Steganography,” *Int. J. Comput. Appl.*, vol. 61, no. 6, pp. 47–52, 2013.

- [95] **Steganografi Araçları**, “Steganography Tools.” [Online]. Available: <http://resources.infosecinstitute.com/steganography-and-tools-to-perform-steganography/gref> (Erişim tarihi: Şubat 2018).
- [96] **Veri Doygunluğu**, “Veri Doyumlama.” [Online]. Available: <http://www.tictotec.co.uk/data-recovery> (Erişim tarihi: Şubat 2018).
- [97] **M. Perklin**, “Anti-Forensics and Anti-Anti-Forensics,” *DefCon*, 2012.
- [98] **Moser, Andreas ve Michael I. Cohen**, “Hunting in the enterprise: Forensic triage and incident response.” *Digital Investigation* 10.2 (2013): 89-98.
- [99] **RAID**, “RAID.” [Online]. Available: <https://en.wikipedia.org/wiki/RAID> (Erişim tarihi: Şubat 2018).
- [100] **R. Spishock**, “Impact of Steganography on a Forensic Investigation,” *Stevenson Univ. Forensic J.*, pp. 30–35, 2013.
- [101] **G. Kessler**, “File Signatures.” [Online]. Available: http://www.garykessler.net/library/file_sigs.html (Erişim tarihi: Şubat 2018).
- [102] **D. Hurlbut**, “Fuzzy Hashing for Digital Forensic Investigators,” *AccessData*, no. January, pp. 1–9, 2009.
- [103] **Timestomping**, “Identifying Anti-Forensics:Timestomping.” [Online]. Available: <https://www.nuix.com/2014/11/19/identifying-anti-forensics-timestomping> (Erişim tarihi: Şubat 2018).
- [104] **Timestomp**, “Timestomp.” [Online]. Available: <http://www.forensicswiki.org/wiki/Timestomp> (Erişim tarihi: Şubat 2018).
- [105] **J. Schicht**, “MFT Records Data.” [Online]. Available: <https://github.com/jschicht/MftRcrd> (Erişim tarihi: Şubat 2018).
- [106] **J. Schicht**, “Set MACE.” [Online]. Available: <https://github.com/jschicht/SetMace> (Erişim tarihi: Şubat 2018).
- [107] **Long Path Tool**, “Long Path Tool.” [Online]. Available: <http://longpathtool.com/> (Erişim tarihi: Şubat 2018).
- [108] **P. Pajek ve E. Pimenidis**, “Computer anti-forensics methods and their impact on computer forensic investigation,” *Commun. Comput. Inf. Sci.*, vol. 45, pp. 145–155, 2009.
- [109] **I. Mironov**, “Hash functions: Theory, attacks, and applications Theory of hash functions,” *Microsoft Res. Silicon Val. Campus*, pp. 1–22, 2005.
- [110] **M. Steven**, “HashClash.” [Online]. Available: <https://marc-stevens.nl/p/hashclash/> (Erişim tarihi: Şubat 2018).
- [111] **PsExec**, “PsTools.” [Online]. Available: <https://technet.microsoft.com/en-us/sysinternals/pxexec.aspx> (Erişim tarihi: Şubat 2018).



ÖZGEÇMİŞ



Ad Soyad: Murat GÜL

Doğum Yeri ve Tarihi: İstanbul, 25/05/1981

Adres: Millî Savunma Üniversitesi Hava Harp Okulu, Yeşilköy, İstanbul

E-Posta: muratgul2003@gmail.com

Lisans: Kara Harp Okulu, Sistem Mühendisliği

Mesleki Deneyim: 3'üncü Kor.K.lığı Bilgi Sistemleri Yönetim Merkezi Kısım Amirliği

Millî Savunma Üniversitesi Bilgi İşlem Daire Başkanlığı Ağ ve Sistem Yöneticiliği

Yayın ve Patent Listesi:

- **Gül, M.,** Aydın, M. A., "Exploits in information security," *2016 24th Signal Processing and Communication Application Conference (SIU), Zonguldak, 2016, pp. 1729-1732.* doi: 10.1109/SIU.2016.7496093.
- **Gül, M.,** "Intrusion detection for Wireless Sensor Networks using ant colony," *2016 24th Signal Processing and Communication Application Conference (SIU), Zonguldak, 2016, pp. 1453-1456.* doi: 10.1109/SIU.2016.7496024.
- **Gül, M.,** Yılmaz, G., "Location Search in UAV Video Using Telemetry Data," *2016 International Conference on Computer Science and Engineering, 2016, pp. 758-762.*

TEZDEN TÜRETİLEN YAYINLAR/SUNUMLAR

- **Gül, M.,** Kugu, E., "A survey on anti-forensics techniques," *2017 International Artificial Intelligence and Data Processing Symposium (IDAP), Malatya, 2017, pp. 1-6.* doi: 10.1109/IDAP.2017.8090341.