

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ADLİ BİLİŞİM KAPSAMINDA WINDOWS TABANLI
SİSTEMLERDEN DİJİTAL DELİLLERİN OTOMATİK OLARAK
ELDE EDİLMESİ VE ANALİZİ

YÜKSEK LİSANS TEZİ

Şahin ÖZDEMİR

Bilgisayar Mühendisliği Anabilim Dalı

ARALIK 2025

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ADLİ BİLİŞİM KAPSAMINDA WINDOWS TABANLI
SİSTEMLERDEN DİJİTAL DELİLLERİN OTOMATİK OLARAK
ELDE EDİLMESİ VE ANALİZİ

YÜKSEK LİSANS TEZİ

Şahin ÖZDEMİR

Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı: Prof.Dr.İbrahim ÖZÇELİK

ARALIK 2025

Şahin ÖZDEMİR tarafından hazırlanan “Adli Bilişim Kapsamında Windows Tabanlı Sistemlerden Dijital Delillerin Otomatik Olarak Elde Edilmesi ve Analizi” adlı tez çalışması 30.12.2025 tarihinde aşağıdaki jüri tarafından oy birliği ile Sakarya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı’nda Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Jürisi

Jüri Başkanı : **Unvan Adı SOYADI**
Sakarya Uygulamalı Bilimler Üniversitesi

Jüri Üyesi : **Unvan Adı SOYADI (Danışman)**
Sakarya Üniversitesi

Jüri Üyesi : **Unvan Adı SOYADI**
Sakarya Üniversitesi



ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Sakarya Üniversitesi Fen Bilimleri Enstitüsü Lisansüstü Eğitim-Öğretim Yönetmeliğine ve Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesine uygun olarak hazırlamış olduğum “ADLİ BİLİŞİM KAPSAMINDA WINDOWS TABANLI SİSTEMLERDEN DİJİTAL DELİLLERİN OTOMATİK OLARAK ELDE EDİLMESİ VE ANALİZİ” başlıklı tezin bana ait, özgün bir çalışma olduğunu; çalışmamın tüm aşamalarında yukarıda belirtilen yönetmelik ve yönergeye uygun davrandığımı, tezin içerdiği yenilik ve sonuçları başka bir yerden almadığımı, tezde kullandığım eserleri usulüne göre kaynak olarak gösterdiğimi, bu tezi başka bir bilim kuruluna akademik amaç ve unvan almak amacıyla vermediğimi ve 20.04.2016 tarihli Resmi Gazete’de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince Sakarya Üniversitesi’nin abonesi olduğu intihal yazılım programı kullanılarak Enstitü tarafından belirlenmiş ölçütlere uygun rapor alındığını, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun ortaya çıkması halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi beyan ederim.

(30/12/2025)

Şahin ÖZDEMİR



TEŞEKKÜR

Bu çalışmanın yürütülmesi sırasında kıymetli bilgilerini ve desteğini esirgemeyen değerli danışman hocam Prof. Dr. İbrahim ÖZÇELİK’e teşekkür ederim.

Eğitim hayatım boyunca destekleriyle yanımda olan değerli aileme teşekkür ederim.

Şahin ÖZDEMİR





İÇİNDEKİLER

Sayfa

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ	v
TEŞEKKÜR	vii
İÇİNDEKİLER	ix
KISALTMALAR	xi
TABLO LİSTESİ	xiii
ŞEKİL LİSTESİ	xv
ÖZET	xvii
SUMMARY	xix
1. GİRİŞ	1
1.1. Literatür Araştırması	4
1.2. Çalışmanın Amacı ve Geliştirilen Çözüm Yöntemi	5
1.3. Tez Organizasyonu	7
2. ADLİ BİLİŞİM	9
2.1. Dijital Delil	10
2.2. Adli Kopya	10
2.3. Adli Bilişim Süreçleri	11
2.1.1. Tanımlama	12
2.1.2. Koruma/Zincirleme delil yönetimi	12
2.1.3. Toplama/Elde etme	12
2.1.4. İnceleme/Ön işleme	12
2.1.5. Analiz	12
2.1.6. Raporlama/Sunum	12
3. WINDOWS TABANLI SİSTEMLERDEKİ DİJİTAL DELİLLER	13
3.1. Windows Kayıt Defteri	13
3.2. Dosya Sistemi	18
3.3. Kullanıcı ve Sistem	21
3.4. Bellek (RAM)	31
4. MATERYAL VE METOT	35
4.1. Kopya Alma	35
4.2. Dijital Delillerin Elde Edilmesi	35
4.3. Zaman Çizelgesinin Oluşturulması	41
4.4. Silinmiş Dosyaların Kurtarılması	42
4.5. Analiz	42
4.5.1. Kural tabanlı analiz	43
4.5.2. Yapay zekâ destekli analiz	45
5. CAMGÖZ YAZILIMI	49
5.1. Disk Çalışması	51
5.2. RAM Çalışması	57
5.3. Analiz Çalışması	61
6. SONUÇ VE ÖNERİLER	69
KAYNAKLAR	73



KISALTMALAR

DLL	: Dynamic Link Library
EXE	: Executable
IE	: Internet Explorer
IOC	: Indicator of Compromise
KAPE	: Kroll Artifact Parser and Extractor
KDBG	: Kernel Debugger Block
LDR	: Loader Data
MAC	: Media Access Control
MD5	: Message Digest Algorithm 5
MFT	: Master File Table
NTFS	: New Technology File System
NTP	: Network Time Protocol
PEB	: Process Environment Block
PID	: Process Identifier
PPID	: Parent Process Identifier
RAM	: Random Access Memory
RDP	: Remote Desktop Protocol
RWX	: Read Write Executable
SAM	: Security Accounts Manager
SANS	: SysAdmin, Audit, Network and Security
SHA	: Secure Hash Algorithm
SSD	: Solid State Drive
UML	: Unified Modeling Language
USB	: Universal Serial Bus
UTC	: Universal Time Coordinated
VAD	: Virtual Address Descriptor
VPN	: Virtual Private Network



TABLO LİSTESİ

Sayfa

Tablo 1.1. Literatür Araştırması	4
Tablo 3.1. Windows Kayıt Defteri Önemli Kayıtları	14
Tablo 3.2. Takılan Depolama Birimlerine İlişkin Verilerin Konum Bilgileri.....	18
Tablo 3.3. Shimcache Verilerinin Konum Bilgileri	22
Tablo 3.4. SAM Verilerinin Konum Bilgileri	23
Tablo 3.5. SRUM Verilerinin Konum Bilgileri.....	23
Tablo 3.6. Jumplist Verilerinin Konum Bilgileri	23
Tablo 3.7. Shellbag Verilerinin Konum Bilgileri.....	24
Tablo 3.8. Lnk Dosyalarına İlişkin Verilerin Konum Bilgileri	25
Tablo 3.9. Olay Günlüğü Verilerinin Konum Bilgileri	26
Tablo 3.10. Silinmiş Dosya İzleri Konum Bilgileri	27
Tablo 3.11. Group Policy Verilerinin Konum Bilgileri	28
Tablo 3.12. Scheduled Tasks Verilerinin Konum Bilgileri	28
Tablo 3.13. WER Verilerinin Konum Bilgileri	29
Tablo 3.14. WBEM Verilerinin Konum Bilgileri	30
Tablo 3.15. BITS Verilerinin Konum Bilgileri	30
Tablo 3.16. WindowsIndexSearch Verilerinin Konum Bilgileri.....	31
Tablo 3.17. WindowsTimeline Verilerinin Konum Bilgileri	31
Tablo 4.1. Disk İmajından Elde Edilen Dijital Deliller	36
Tablo 4.2. RAM İmajından Elde Edilen Dijital Deliller	40
Tablo 4.3. Kural Tabanlı Analiz.....	43
Tablo 4.4. Yapay Zekâ Destekli Analiz	47
Tablo 5.1. Disk Çalışması Neticesinde Oluşturulan Dosyalar	57
Tablo 5.2. RAM Çalışması Neticesinde Oluşturulan Dosyalar.....	61
Tablo 5.3. Analiz Çalışması Neticesinde Oluşturulan Dosyalar	67
Tablo 6.1. CAMGÖZ Yazılımının Karşılaştırılması.....	69



ŞEKİL LİSTESİ

Sayfa

Şekil 3.1. Regedit Ekran Görüntüsü	13
Şekil 3.2. MFT Mimarisi	19
Şekil 3.3. USNJournal Dosya Yapısı	20
Şekil 3.4. NTFS Meta Veri Yapıları Arasındaki İlişki	21
Şekil 3.5. Olay Günlüğü Ekran Görüntüsü	26
Şekil 5.1. Camgöz Balığı Görseli	49
Şekil 5.2. CAMGÖZ Yazılımı Ekran Görüntüsü.....	50
Şekil 5.3. Hakkında Menüsü Ekran Görüntüsü	50
Şekil 5.4. Aktivite UML Diyagramı	51
Şekil 5.5. Disk İmaj Dosyası Seçimi Uyarı Mesajı	52
Şekil 5.6. Disk İmaj Dosyası İşlemleri	52
Şekil 5.7. Tarih Aralığı Seçimi Uyarı Mesajı	53
Şekil 5.8. Disk Çalışması Ekran Görüntüsü	53
Şekil 5.9. Disk Çalışmasının Tamamlanması	54
Şekil 5.10. Disk Çalışması Sonuç Dosyası Renk Kategorileri	54
Şekil 5.11. Disk Çalışması Sonuç Dosyası Ekran Görüntüsü 1	55
Şekil 5.12. Disk Çalışması Sonuç Dosyası Ekran Görüntüsü 2.....	55
Şekil 5.13. Hash Bilgileri.....	55
Şekil 5.14. Silinmiş Dosyaları Kurtar İşlem Mesajı	56
Şekil 5.15. KurtarılanSilinmişDosyalarınHashDeğerleri.txt Dosyası.....	56
Şekil 5.16. RAM İmaj Dosyası Seçimi Uyarı Mesajı.....	57
Şekil 5.17. RAM İmaj Dosyası İşlemleri.....	58
Şekil 5.18. İşletim Sistemi Seçimi Uyarı Mesajı	58
Şekil 5.19. RAM Çalışması Ekran Görüntüsü	59
Şekil 5.20. RAM Çalışmasının Tamamlanması.....	59
Şekil 5.21. RAM Çalışması Sonuç Dosyası Ekran Görüntüsü 1	60
Şekil 5.22. RAM Çalışması Sonuç Dosyası Ekran Görüntüsü 2	60
Şekil 5.23. Zararlı Proses Tespit Sonucu	61
Şekil 5.24. Disk Çalışması Sonuç Dosyası Seçimi Uyarı Mesajı.....	62
Şekil 5.25. Disk Çalışması Sonuç Dosyası İşlemleri	62
Şekil 5.26. RAM Çalışması Sonuç Dosyası Seçimi Uyarı Mesajı	63
Şekil 5.27. RAM Çalışması Sonuç Dosyası İşlemleri	64
Şekil 5.28. Analiz Çalışması Ekran Görüntüsü	64
Şekil 5.29. Analiz Çalışmasının Tamamlanması	65
Şekil 5.30. Kural Tabanlı Analiz Sonucu Ekran Görüntüsü 1	66
Şekil 5.31. Kural Tabanlı Analiz Sonucu Ekran Görüntüsü 2.....	66
Şekil 5.32. Yapay Zekâ Destekli Analiz Sonucu Ekran Görüntüsü	67



ADLI BİLİŞİM KAPSAMINDA WINDOWS TABANLI SİSTEMLERDEN DİJİTAL DELİLLERİN OTOMATİK OLARAK ELDE EDİLMESİ VE ANALİZİ

ÖZET

İnternet ve bilişim sistemleri üzerinde işlenen suçların veya yapılan siber saldırıların tespit edilmesi amacıyla gerçekleştirilen adli bilişim incelemelerinin önemi her geçen gün artmaktadır. Adli bilişim incelemelerinde delillerin orijinalliğinin ve bütünlüğünün bozulmaması için incelemelerin adli kopya (imaj) üzerinde yapılması gerekmektedir. Dijital delil, dijital cihaz ve ortamlarda bulunan dosyaları, uçucu verileri, kullanıcı ve sistem etkinliklerinden geriye kalan dijital kalıntıları kapsayan adli nitelikli bilgilerin tümünü ifade eder. Adli bilişim incelemelerinde dijital deliller çeşitli yöntemler ile toplanmakta ve analiz edilmektedir. İşletim sistemleri bu yöntemlerin etkin biçimde uygulanabildiği başlıca dijital delil kaynaklarındandır. Küresel ölçekte olduğu gibi ülkemizde de kişisel ve kurumsal olarak Windows işletim sistemi yaygın olarak kullanılmaktadır.

Dijital delillerin toplanması, düzenlenmesi, ilişkilendirilmesi, anlamlandırılması ve analizi adli bilişim uzmanları tarafından gerçekleştirilmekte olup, uzun süreli ve maliyetli olabilmektedir. Bu çerçevede kullanılan adli bilişim araçlarından bazıları sistem/disk odaklı çalışırken bazıları da RAM odaklı çalışmaktadır. Özellikle açık kaynak kodlu veya ücretsiz olanlarda genellikle dijital delillerin toplanmasına ağırlık verilirken otomatik analiz hususunun arka planda kaldığı görülmektedir. Bu kapsamda adli bilişim incelemesinin ve analizinin etkin, verimli, hızlı ve kolay bir şekilde yapılabilmesi için dijital delillerin hem disk imajı hem de RAM imajı üzerinden toplanması ve ilişkilendirilmesi, zaman çizelgesinin oluşturulması, silinmiş dosyaların kurtarılması, zararlı/şüpheli/anomali tespiti işlemlerinin otomatik olarak gerçekleştirilmesine yönelik çalışma yapılmasına ihtiyaç duyulmuştur.

Bu çalışmada, günümüzde yaygın olarak kullanılan işletim sistemi olan Windows tabanlı sistemlerdeki dijital deliller/kalıntılar ve adli bilişim süreci teknik açıdan ele alınmıştır. Konuya yönelik literatür araştırması yapılmış, adli bilişim araçları incelenmiştir. Windows tabanlı sistemlerin disk ve RAM imajlarından dijital delillerin toplanmasını, zaman çizelgesinin çıkarılmasını, silinmiş dosyaların kurtarılmasını, toplanan dijital delillerin ilişkilendirilmesini, kural tabanlı analiz ile zararlı/şüpheli işlemlerin ve yapay zekâ destekli analiz ile anomalilerin tespit edilmesini otomatik olarak gerçekleştiren “CAMGÖZ” isimli bir yazılım geliştirilmiştir. Böylece adli bilişim incelemesinin ve analizinin etkin, verimli, hızlı ve kolay bir şekilde yapılması sağlanmıştır. Bahse konu yazılımın adli bilişim ve siber güvenlik alanında faydalı olacağı değerlendirilmektedir.



AUTOMATIC COLLECTION AND ANALYSIS OF DIGITAL EVIDENCE FROM WINDOWS-BASED SYSTEMS WITHIN THE SCOPE OF DIGITAL FORENSICS

SUMMARY

With advancing technology, information technologies and digital devices play a significant role in our daily lives. Cybercriminals and attackers also exploit information technologies and digital devices for malicious activities. Due to the increasing use of computers for criminal purposes, digital forensics has become a crucial part of criminal investigations.

The work involved in digital forensics can be summarized as the initial response at the crime scene, the collection of electronic evidence, the examination and analysis of evidence collected at the crime scene or in the laboratory, and reporting to the relevant authorities.

In order to combat cybercrimes and crimes committed using information technologies more effectively, digital evidence (data and information transmitted or stored via electronic or magnetic media) is needed in addition to physical evidence in the process of identifying the facts of the crime and bringing criminals to justice. Data acquired from information technologies has become crucial in investigations and trial processes. Therefore, in order for legal processes to proceed without interruption, collected digital data must be analyzed accurately within the required timeframe and presented to the relevant authorities.

Digital evidence refers to data recorded on electronic or magnetic devices that contributes to the investigation of a crime. To examine seized digital material, it is generally necessary to create a forensic copy (an image) of the digital material and analyze this copy. This is done to prevent damage to the original digital material and to maintain the integrity of the evidence.

In the process of collecting digital evidence, examining the operating system in particular can provide access to evidentiary data. The operating system provides access to various structured data, including all searches, file operations, system logs, running applications, internet access history, email files, and more. Therefore, operating system-based digital forensics offers significant opportunities for the collection of digital evidence.

In Windows-based systems, digital evidence is generally divided into four main categories: Registry, File System, User and System, and Memory.

Registry evidence resides in a hierarchical database containing valuable information such as user activity, system configurations, and software traces. These records are loaded into memory during system startup, and changes are written to disk both at regular intervals during operation and when the system shuts down properly. These records allow digital forensics experts to retrospectively examine past user activity, program execution history, and changes made to the system.

File system evidence encompasses digital traces originating from the NTFS (New Technology File System) architecture used in the Windows operating system. NTFS records timestamps such as creation, modification, and access times for files and folders, as well as file permissions and alternate data streams. Furthermore, thanks to the Master File Table (MFT), even metadata from deleted files can remain in the system for some time. This structure is a significant source of evidence for identifying and creating a timeline of user actions on files.

User and system evidence is collected from audit logs generated by the operating system and applications. This evidence includes information such as when users logged into the system, which programs they ran, how often they used those programs, and which resources they accessed. Application, security, and system logs, especially Windows Event Logs, play a critical role in detecting unauthorized access, errors, and suspicious activity. These records allow for a chronological analysis of events.

Memory evidence consists of temporary data structures located in RAM while the system is running. Extremely sensitive information such as running processes, network connections, open files, passwords, and encryption keys can reside in memory. Acquisition of this type of evidence requires taking a memory image from the live system; otherwise, this data is lost when the system is shut down. However, files like `pagefile.sys` and `hiberfil.sys`, which consist of memory data written to disk, contain important memory remnants that can be examined even in static forensics. Memory records allow for the analysis of software and user activity.

Digital forensics tools can collect various types of digital evidence from live or offline systems. Tools operating on offline systems typically collect digital evidence via disk images or RAM images. The collection, organization, correlation, interpretation, and analysis of digital evidence are performed by digital forensics experts and can be time-consuming and costly. Some digital forensics tools focus on disks, while others focus on RAM. Open-source or free tools, in particular, often prioritize the collection of digital evidence while neglecting automated analysis. In addition to collecting digital evidence from both disk and RAM images, it is crucial to convert the collected digital evidence into an understandable format for digital forensics experts and to perform automated inferences based on that evidence.

In this study, in addition to collecting digital evidence from disk and RAM images of Windows-based systems and recovering deleted files, the following objectives have been achieved.

A timeline is created for digital evidence collected from disk and RAM images.

By correlating digital evidence collected from disk images with digital evidence collected from RAM images taken before the system was last shut down, detailed information such as the process ID, process name, start time, initiator username, parent process ID, parent process name, network connections, and file paths of malicious processes identified in the RAM image is obtained.

Digital evidence collected from disk and RAM images is analyzed in two stages. In the first stage, rule-based analysis identifies matters such as running malicious powershell commands, pass the hash attacks, installing malicious services, running psexec, deleting Windows event logs, connecting to the local area network via RDP from an external network, disabling Windows event log monitoring, suspicious scheduled tasks, suspicious failed logins, suspicious file writing, persistence indicators, system date and time setting information, changing the system date and

time, malicious process information, suspicious process, suspicious network connection, suspicious DLL. In the second stage, AI-assisted analysis identifies unusual activities from data such as the frequency, length, and structure of registry key changes, the timing of successful and unsuccessful login and logout operations, usernames, and the timing, frequency, and usernames of file deletions.

The analysis results are correlated with attacker behaviors within the MITRE ATT&CK framework.

A software called “CAMGÖZ” has been developed to perform all these operations.

In conclusion, in this study, digital evidence/artifacts in Windows-based systems, which are widely used in today’s computing environments, and the forensic process have been examined from a technical perspective. A literature research on the subject was conducted, and forensic tools were analyzed. Collection of digital evidence from disk and RAM images with Windows-based systems, extraction of a timeline, recovery of deleted files, correlation collected digital evidence, detection of malicious/suspicious activities with rule-based analysis and anomalies with artificial intelligence-assisted analysis have been automatically performed. In this context, a software called “CAMGÖZ” was developed. Thus, the digital forensic analysis has been made more effective, efficient, fast, and easy to perform. It is evaluated that the software in question will be useful in the field of forensic computer and cyber security.



1. GİRİŞ

Gelişen teknolojiyle birlikte bilgi teknolojileri ve dijital cihazlar günlük hayatımızda önemli role sahiptir. Siber suçlular ve saldırganlar da bilgi teknolojilerini ve dijital cihazları kötü amaçlı aktivitelerde kullanmaktadır. Bilgisayarların suç amaçlı kullanımının artmasıyla birlikte adli bilişim, soruşturmanın önemli bir parçası haline gelmiştir [1].

Adli bilişim kapsamındaki çalışmalar, olay yerinde ilk müdahale, elektronik delillerin toplanması ve zincirleme sorumluluk kapsamında saklanması, olay yerinde veya laboratuvarında delillerin incelenip analiz edilmesi, elde edilen bulguların raporlanması ve gerektiğinde ilgili mercilere sunulması olarak özetlenebilir.

Siber suçlarla ve bilgi teknolojileri kullanılarak işlenen suçlarla daha etkin bir şekilde mücadele kapsamında suçun gerçeklerinin tespit edilmesi ve suçluların adli makamlara intikal ettirilmesi sürecinde fiziksel deliller dışında elektronik veya manyetik ortamlar yoluyla iletilen veya bu ortamlarda kaydedilen delil niteliğindeki veriler ve bilgiler olarak tanımlanan dijital delillere ihtiyaç duyulmaktadır [2]. Soruşturma ve yargılama süreçlerinde bilgi teknolojilerinden elde edilen veriler çok önemli hale gelmiştir. Bu nedenle hukuki süreçlerin aksamadan devam edebilmesi için toplanan dijital veriler istenilen süre içerisinde doğru bir şekilde analiz edilerek ilgili mercilere sunulmalıdır.

Dijital delil, elektronik veya manyetik cihazlarda kaydedilen ve suçun aydınlatılmasına katkı sunan verilerdir [3]. Ele geçirilen dijital materyalin incelenebilmesi için her zaman dijital materyalin adli kopyasının (imajının) oluşturulması ve bu adli kopya üzerinde çalışılması gerekmektedir. Bunun nedeni orijinal dijital materyalin zarar görmemesi ve delil bütünlüğünün bozulmamasıdır.

Dijital delillerin elde edilmesi sürecinde özellikle işletim sisteminin incelenmesi, delil niteliğindeki verilere erişim olanağı sağlar. İşletim sistemi, tüm aramalar, dosya işlemleri, sistem kayıtları, çalışan uygulamalar, internet erişim geçmişi, e-posta dosyaları ve daha fazlasını içeren çeşitli yapısal verilere erişim sağlar. Bu nedenle,

iřletim sistemi bazlı dijital adli inceleme, dijital delil elde etmek iin nemli imkânlar sunar. Windows tabanlı sistemlerde dijital deliller genellikle drt ana kategoriye ayrılır:

- Kayıt Defteri,
- Dosya Sistemi,
- Kullanıcı ve Sistem,
- Bellek.

Kayıt defteri delilleri, kullanıcı etkinlikleri, sistem yapılandırmaları ve yazılım izleri gibi deęerli bilgileri ieren hiyerarřık bir veri tabanında bulunur. Bu kayıtlar sistem aılıřı sırasında belleęe yklenir ve yapılan deęiřiklikler hem alıřma esnasında belirli aralıklarla hem de sistemin dzgn řekilde kapatılması sırasında diske yazılır. Bu kayıtlar, adli biliřim uzmanlarının gemiř kullanıcı faaliyetlerini, program alıřtırma gemiřini ve sistem zerinde yapılan deęiřiklikleri geriye dnk olarak incelemesine olanak tanır.

Dosya sistemi delilleri, Windows iřletim sisteminde kullanılan NTFS (New Technology File System – Yeni Teknoloji Dosya Sistemi) yapısından kaynaklanan dijital izleri kapsar. NTFS, dosya ve klasrlere ait oluřturulma, deęiřtirilme ve eriřilme zamanları gibi zaman damgalarını, dosya izinlerini ve alternatif veri akıřlarını (alternate data streams) kayıt altına alır. Ayrıca Ana Dosya Tablosu (Master File Table - MFT) sayesinde silinmiř dosyalara ait meta veriler dahi belirli bir sre boyunca sistemde kalabilir. Bu yapı, kullanıcıların dosyalar zerinde gerekleřtirdięi iřlemlerin tespit edilmesinde ve zaman izelgesi oluřturulmasında nemli bir delil kaynaęıdır.

Kullanıcı ve sistem kaynaklı deliller, iřletim sistemi ve uygulamalar tarafından oluřturulan denetim gnlkleri (loglar) zerinden elde edilir. Bu deliller; kullanıcıların sisteme ne zaman giriř yaptıęı, hangi programları alıřtırdıęı, bu programları ne sıklıkta kullandıęı ve hangi kaynaklara eriřtięi gibi bilgileri ierir. Windows Olay Gnlkleri (Event Logs) bařta olmak zere uygulama, gvenlik ve sistem gnlkleri; yetkisiz eriřimlerin, hataların ve řpheli faaliyetlerin tespit edilmesinde kritik rol oynar. Bu kayıtlar, olayların kronolojik olarak analiz edilmesini saęlar.

Bellek delilleri ise sistem alıřır durumdayken RAM zerinde bulunan geici veri yapılarından oluřur. alıřan iřlemler, aę baęlantıları, aık dosyalar, řifreler ve řifreleme anahtarları gibi son derece hassas bilgiler bellek zerinde yer alabilir. Bu tr

delillerin elde edilebilmesi için canlı sistemden bellek imajı alınması gerekir; aksi halde sistem kapatıldığında bu veriler kaybolur. Bununla birlikte, diske yazılan bellek verilerinden oluşan pagefile.sys ve hiberfil.sys gibi dosyalar, statik adli bilişimde de incelenen önemli bellek kalıntılarını barındırır. Bellek verileri, yazılım ve kullanıcı aktivitelerinin incelenmesine olanak tanır.

Elde edilen verilerin değerini ortaya çıkaran önemli nokta, bu verilerin karar verme aşamasında geçerli olması ve karar vermeyi etkileyen bilgiler sunabilmesidir. Genel anlamda adli bilişim inceleme ve analiz süreci, analiz uzmanının, toplanan verilerin anlamlı sonuçlarını yorumlamak amacıyla çeşitli araçlar kullanarak raporlar hazırladığı geleneksel bir çalışmadır. Analiz uzmanları tarafından yapılan değerlendirmeler için veriler farklı cihazlar ve yazılımlar kullanılarak uygun ve anlaşılır bir formata dönüştürülebilmektedir [4].

Adli bilişim araçlarından bazıları sistem/disk odaklı çalışırken bazıları da RAM odaklı çalışmaktadır. Dijital delillerin hem disk imajı hem de RAM imajı üzerinden toplanması önemlidir. Özellikle açık kaynak kodlu veya ücretsiz araçlarda genellikle dijital delillerin toplanmasına ağırlık verilirken otomatik analiz hususunun arka planda kaldığı görülmektedir. Dijital delillerin toplanması, düzenlenmesi, ilişkilendirilmesi, anlamlandırılması ve analizi adli bilişim uzmanları tarafından gerçekleştirilmekte olup, uzun süreli ve maliyetli olabilmektedir. Bu kapsamda adli bilişim analizinin etkin, hızlı ve kolay bir şekilde yapılabilmesi için dijital delillerin hem disk imajı hem de RAM imajı üzerinden toplanması ve ilişkilendirilmesi, zaman çizelgesinin oluşturulması, silinmiş dosyaların kurtarılması, zararlı/şüpheli/anomali tespiti işlemlerinin otomatik olarak gerçekleştirilmesine yönelik çalışma yapılmasına ihtiyaç duyulmuştur.

Bu çalışmada, günümüzde yaygın olarak kullanılan işletim sistemi olan Windows tabanlı sistemlerdeki dijital deliller/kalıntılar ve adli bilişim süreci teknik açıdan ele alınmıştır. Konuya yönelik literatür araştırması yapılmış, adli bilişim araçları incelenmiştir. Windows tabanlı sistemlerin disk ve RAM imajlarından dijital delillerin toplanması, zaman çizelgesinin çıkarılması, silinmiş dosyaların kurtarılması, toplanan dijital delillerin ilişkilendirilmesi, kural tabanlı analiz ile zararlı/şüpheli işlemlerin ve yapay zekâ destekli analiz ile anomalilerin tespiti otomatik olarak gerçekleştirilmiştir. Bu kapsamda dijital delillerin otomatik olarak elde edilmesine ve analiz edilmesine yönelik “CAMGÖZ” isimli bir yazılım geliştirilmiştir. Böylece adli bilişim

incelemesinin ve analizinin etkin, verimli, hızlı ve kolay bir şekilde yapılması sağlanmıştır.

1.1. Literatür Araştırması

Dijital delillerin ortaya çıkarılmasında genel olarak, statik adli bilişim ve canlı adli bilişim teknikleri uygulanmaktadır. Statik adli bilişim, sistem kapalıyken delil elde etme sürecine odaklanırken, canlı adli bilişim, sistem çalışırken delil elde etme sürecine odaklanır. Windows adli bilişim teknikleri ise Windows tabanlı sistemlerden delil toplanmasına ve analiz edilmesine ilişkin yöntemleri kapsamaktadır. Literatür araştırmasına ilişkin bilgiler Tablo 1.1’de sunulmuştur.

Tablo 1.1. Literatür Araştırması

Kaynak	Kategori	Açıklama
[5]	Statik Adli Bilişim	Statik adli bilişim yöntemleri çerçevesinde dijital delillerin toplanması, korunması, doğrulanması ve analiz edilmesine yönelik süreçlere ilişkin bilgiler sunulmaktadır.
[6]		Sabit disklerde statik adli bilişim yöntemlerinin nasıl uygulandığına ve silinmiş ya da veri kaybı yaşanmış disklerde dijital delil elde etme süreçlerine yönelik bilgiler sunulmaktadır.
[7]	Statik Adli Bilişim	Statik ve canlı adli bilişimde imaj alma yöntemleri karşılaştırılarak, hangi senaryoda hangi yöntemin tercih edilmesi gerektiği, yöntemlerin delil bütünlüğü, doğruluk, uygulanabilirlik açısından avantaj ve dezavantajları hakkında bilgiler sunulmaktadır.
[8]	Canlı Adli Bilişim	Canlı adli bilişim tekniklerinin fidye yazılımı saldırıları sırasında nasıl kullanılabileceğine ve bu tekniklerin saldırının etkisini azaltmada ne kadar etkili olduğuna dair bilgiler sunulmaktadır.
[9]	Windows Adli Bilişimi	Sistem çalışırken dijital delil toplama teknikleri, RAM analizinin önemi ve canlı adli bilişim yöntemlerinin avantajları ile dezavantajları hakkında bilgiler sunulmaktadır.
[10]		
[11]		
[12]		Windows tabanlı sistemlerde farklı kanıt türlerinin bir araya getirilmesi, analiz sürecinin çeşitli aşamaları, adli bilişim prensipleri ve bazı adli bilişim araçları, değişken ve değişken olmayan verilerin analiz edilmesi için farklı teknikler hakkında bilgiler sunulmaktadır.
[13]		
[14]		
[15]		
[16]		

Tablo 1.1. (Devamı) Literatür Araştırması

Kaynak	Kategori	Açıklama
[17]		Windows işletim sistemini çalıştıran bilgisayarlardan kanıtların çıkarılmasına ve analiz edilmesine yönelik yöntemler sunulmaktadır.
[18]		Windows 10 tabanlı sistemin RAM dökümü ve hazırda bekletme dosyasından çıkarılan uçucu eserleri toplayan tekniğin uygulanması sunulmaktadır.
[19]	Windows Adli Bilişimi	Windows tabanlı sistemin uçucu belleğinden aktif süreçler, şifreleme anahtarları ve kayıt defteri bilgileri gibi dijital delilleri çıkaran bir çerçeveye ilişkin bilgiler sunulmaktadır.
[20]		RAM analizinde gelişmiş tehditlerin ve kötü amaçlı yazılımların tespit edilmesi için bellek analizinin temelleri ve araçları hakkında bilgiler sunulmaktadır.
[21]		RAM içindeki kalıntıların elde edilmesi, karşılaştırılması ve yorumlanması süreçlerinin Windows sürümüne göre nasıl değiştiğine yönelik yöntemler sunulmaktadır.

Statik adli bilişimin ve canlı adli bilişimin süreçleri ile tekniklerine yönelik yapılan çalışmalar neticesinde aralarındaki farkın özellikle delil bütünlüğünün korunması olduğu tespit edilmiştir. Windows adli bilişimi çerçevesinde ise disk üzerinden veya RAM üzerinden elde edilebilen çeşitli dijital deliller ve bu delillerin anlamlandırılmasına yönelik çalışmalar yapıldığı görülmüştür. Bu çalışmada disk ve RAM imajları üzerinden dijital delillerin toplanması, zaman çizelgesinin çıkarılması, silinmiş dosyaların kurtarılması, dijital delillerin ilişkilendirilmesi, kural tabanlı analiz ile zararlı/şüpheli işlemlerin ve yapay zekâ destekli analiz ile anomalilerin tespiti otomatik olarak gerçekleştirilerek adli bilişime katkı sağlanmıştır.

1.2. Çalışmanın Amacı ve Geliştirilen Çözüm Yöntemi

Adli bilişim araçları tarafından canlı sistemlerden veya kapalı sistemlerden çeşitli dijital deliller toplanabilmektedir. Kapalı sistemler üzerinde çalışan araçlar tarafından ise genellikle disk imajı ya da RAM imajı üzerinden dijital deliller toplanabilmektedir. Dijital delillerin toplanması, düzenlenmesi, ilişkilendirilmesi, anlamlandırılması ve analizi adli bilişim uzmanları tarafından gerçekleştirilmekte olup, uzun süreli ve maliyetli olabilmektedir. Adli bilişim araçlarından bazıları disk odaklı çalışırken bazıları da RAM odaklı çalışmaktadır. Özellikle açık kaynak kodlu veya ücretsiz olanlarda genellikle dijital delillerin toplanmasına ağırlık verilirken otomatik analiz

hususunun arka planda kaldığı görülmektedir. Dijital delillerin hem disk imajı hem de RAM imajı üzerinden toplanmasının ve silinmiş dosyaların kurtarılmasının yanı sıra toplanan dijital delillerin adli bilişim uzmanı için anlaşılabilir formata dönüştürülmesi ve bahse konu dijital delillerden otomatik çıkarımlar yapılması önem arz etmektedir. Bu kapsamda adli bilişim analizinin etkin, verimli, hızlı ve kolay bir şekilde yapılabilmesi amacıyla:

- Toplanan dijital delillere yönelik zaman çizelgesinin oluşturulması,
- Disk imajı üzerinden toplanan dijital deliller ile sistemin son kapatılmasından önce alınmış RAM imajı üzerinden toplanan dijital delillerin ilişkilendirilmesi,
- Disk imajı ve RAM imajı üzerinden toplanan dijital delillerin analiz edilerek zararlı/şüpheli/anomali tespitinin otomatik olarak yapılması,
- Analiz sonuçlarının, MITRE ATT&CK çerçevesindeki (siber saldırgan davranışlarının sınıflandırıldığı ve açıklandığı, sürekli güncellenen bilgi tabanı) saldırgan davranışları ile ilişkilendirilmesi,

adli bilişim uzmanlarına büyük kolaylık sağlamakla birlikte kurum/kuruluşların siber güvenlik birimlerine de önemli veriler sunarak fayda sağlayacaktır.

Bu çalışmada, Windows tabanlı sistemlerin disk ve RAM imajları üzerinden dijital delillerin toplanması ve silinmiş dosyaların kurtarılması ile birlikte yukarıda belirtilen hususların gerçekleştirilmesi kapsamında:

- Disk ve RAM imajları üzerinden toplanan dijital delillere yönelik zaman çizelgesi oluşturulmaktadır.
- Disk imajı üzerinden toplanan dijital deliller ile sistemin son kapatılmasından önce alınmış RAM imajı üzerinden toplanan dijital deliller ilişkilendirilerek RAM imajı üzerinden tespit edilen zararlı proseslere yönelik proses ID, proses adı, başlama zamanı, başlatan kullanıcı adı, parent proses ID, parent proses adı, ağ bağlantıları, dosya yolları gibi detaylı bilgilere ulaşılmaktadır.
- Disk ve RAM imajlarından toplanan dijital deliller 2 aşamalı analiz edilerek, ilk aşamada kural tabanlı analiz ile zararlı powershell komutu çalıştırma, pass the hash saldırısı, zararlı servis kurulumu, psexec çalıştırılması, Windows eventlog silinmesi, yerel alan ağına dış ağdan rdp bağlantısı, Windows olay günlüğü denetiminin devre dışı bırakılması, şüpheli zamanlanmış görev,

şüpheli başarısız oturum açma, şüpheli dosya yazma, kalıcılık göstergesi, sistem tarih ve saat ayarı bilgisi, sistem tarih ve saatinin değiştirilmesi, zararlı proses bilgileri, şüpheli proses, şüpheli ağ bağlantısı, şüpheli DLL gibi hususlar; ikinci aşamada yapay zekâ destekli analiz ile registry anahtarlarının değişim sıklığı, uzunluğu ve yapısı, başarılı ve başarısız oturum açma ve kapatma işlemlerinin zamanları ile kullanıcı adları, dosya silme işlemlerinin zamanları, sıklığı ve kullanıcı adları gibi verilerden olağan dışı işlemler tespit edilmektedir.

- Analiz sonuçları MITRE ATT&CK çerçevesindeki saldırgan davranışları ile ilişkilendirilmektedir.
- Tüm bu işlemleri yapan CAMGÖZ isimli bir yazılım geliştirilmiştir.

Sonuç bölümünde bu çalışma kapsamında geliştirilen CAMGÖZ yazılımı ile açık kaynak kodlu ve ücretsiz araçlar karşılaştırılmıştır.

1.3. Tez Organizasyonu

Bölüm 1’de giriş, literatür araştırması, çalışmanın amacı ve geliştirilen çözüm yöntemi ile tez organizasyonu sunulmuştur. Bölüm 2’de adli bilişimle ilgili bilgiler sunulmuştur. Bölüm 3’te Windows tabanlı sistemlerden temin edilebilecek dijital deliller hakkında bilgiler sunulmuştur. Bölüm 4’te kullanılan materyaller ve metotlar sunulmuştur. Bölüm 5’te geliştirilen yazılıma ilişkin bilgiler ve performans sonuçları sunulmuştur. Bölüm 6’da ise sonuçlar değerlendirilerek yapılan çalışmanın katkıları sunulmuştur.



2. ADLİ BİLİŞİM

Dijital çağın hızla gelişmesiyle birlikte suçlar da giderek dijitalleşmiş ve karmaşık hale gelmiştir. Günümüzde, suç işleme yöntemleri ve kanıtların doğası, dijital teknolojilerin etkisiyle köklü bir değişim geçirmiştir. Bu değişime ayak uydurmak ve adaleti sağlamak için hukuk ve suç bilimi alanında adli bilişim disiplini önemli bir role sahiptir.

Adli bilişim, suçla ilişkilendirilmiş dijital aygıtlarda bulunan verilerin toplanması, analiz edilmesi, korunması ve sunulmasıyla ilgilenen bir alandır. Bu veriler bilgisayarlar, mobil cihazlar, dijital depolama medyaları ve bulut tabanlı platformlar gibi çeşitli kaynaklardan elde edilebilir. Adli bilişim uzmanları bu dijital kanıtları toplar, analiz eder, yorumlar ve sunar, böylece suçların çözülmesine ve adaletin sağlanmasına katkıda bulunurlar.

Adli bilişim bir dizi adımdan oluşur. İlk adım genellikle olay yeri incelemesi ve dijital kanıtların elde edilmesiyle başlar. Bu adımlar yasal prosedürlere sıkı sıkıya bağlı olarak gerçekleştirilir ve potansiyel kanıtların doğru şekilde toplanmasını sağlar. Ardından elde edilen verilerin güvenliği ve bütünlüğünün korunması için önlemler alınır ve dijital kanıtların analizi başlar. Analiz süreci verilerin detaylı incelenmesini, silinmiş verilerin kurtarılmasını, meta verilerin incelenmesini ve diğer analitik yöntemleri içerir. Analiz sonuçları adli raporlar şeklinde belgelendirilir ve mahkemede delil olarak sunulabilir.

Adli bilişim sadece suçları çözmekle kalmaz, aynı zamanda suçların önlenmesine ve gelecekteki suçların azaltılmasına da yardımcı olur. Bu disiplin bilgisayar korsanlığı, siber suçlar, veri ihlalleri, sanal dolandırıcılık ve diğer dijital suçlarla mücadelede hayati bir role sahiptir. Ayrıca adli bilişim yasal davaların ve kurumsal iç soruşturmaların yönetilmesinde de önemlidir.

Genel olarak adli bilişim disiplini, dijital kanıtların doğru şekilde toplanması, incelenmesi, analiz edilmesi ve raporlanması açısından önemlidir. Adli bilişim uzmanlarının teknik bilgi ve yasal prosedürler konusunda yetkin olması, doğruluk ve bütünlük ilkelerine sıkı sıkıya bağlı kalması gerekmektedir.

2.1. Dijital Delil

Dijital delil, dijital cihaz ve ortamlarda bulunan dosyaları, uçucu verileri, kullanıcı ve sistem etkinliklerinden geriye kalan dijital kalıntıları (artifacts) kapsayan adli nitelikli bilgilerin tümünü ifade eder. Bu kapsamda yalnızca dijital cihaz ve ortamlarda bulunan dosyalar ve uçucu veriler değil; silinmiş dosya izleri, sistem ve uygulama günlükleri, meta veriler, zaman damgaları, tarayıcı geçmişleri ve önbellek verileri gibi bilgiler de dijital delil olarak değerlendirilir [5]. Söz konusu veriler, dijital olayların kronolojik olarak analiz edilmesini mümkün kılar. Ancak dijital delillerin kolaylıkla değiştirilebilir ve yok edilebilir olmasından dolayı bu verilerin uygun yöntemlerle toplanması, bütünlüğünün korunması ve bağlam içinde yorumlanması büyük önem taşımaktadır.

2.2. Adli Kopya

Adli kopya alma, adli bilişim uzmanlarının dijital delil toplamak için kullandıkları bilgisayar araştırma ve analiz tekniklerinin uygulanması olan bilgisayar adli biliminin bir ögesidir.

Adli kopya, tüm dosyalar, klasörler ve tahsis edilmemiş, boş alan dahil olmak üzere fiziksel bir depolama aygıtının bit bit, sektör sektör doğrudan kopyasıdır. Adli kopyalar, işletim sistemi tarafından görülebilen tüm dosyaların yanı sıra silinen dosyaları ve boş alanda bırakılan dosya parçalarını da içerir [26].

Tüm kopya alma ve yedekleme yazılımları adli kopyalar oluşturmaz. Örneğin, Windows yedekleme, fiziksel aygıtın tam kopyaları olmayan yedeklerini oluşturur. Adli kopyalar, uygun adli bilişim araçları ile oluşturulabilir. Adli kullanım için pazarlanmayan bazı disk kopyalama yardımcı programları da tam disk kopyaları oluşturabilir.

Bir incelemede, işletim sistemi aracılığıyla erişilebilenlerden farklı ek deliller keşfedilebilir. Bu tür orijinal deliller, elektronik/dijital keşfi önlemek için silinen suçlayıcı verileri içerir. Veriler güvenli bir şekilde silinmediği ve üzerine yazılmadığı sürece, genellikle adli bilişim veya veri kurtarma yazılımlarıyla kurtarılabilir. Adli kopyalar oluşturmak ve bunları yedeklemek, sürücü arızalarından kaynaklanan veri kaybını önler. Adli kopyalar, genel olarak kritik dosyaların kaybını da önleyebilir.

Bir depolama cihazının içeriğini yakalarken üç tür adli kopya oluşturulabilir. Hangi yaklaşımın kullanılacağı mevcut teknolojiye ve iş gereksinimlerine bağlıdır. Bahse konu kopya türleri aşağıda belirtilmiştir.

- Fiziksel kopya: Etkin veriler, kullanılmayan veya ayrılmamış alan ve depolama biriminde hâlâ bulunan silinmiş veriler dahil olmak üzere depolama cihazının tüm içeriği veya aktif süreçler, geçici veriler ve bellek alanında hâlâ bulunan silinmiş/yer değiştirilmiş veriler dahil olmak üzere belleğin tüm içeriği elde edilir.
- Mantıksal kopya: Depolama cihazının içeriğinden etkin veriler elde edilir.
- Hedeflenen kopya: Yasal bir inceleme için gerekli olanlar gibi belirli veriler tanımlanır ve elde edilir.

Başarılı bir adli kopya aşağıdaki özelliklere sahiptir:

- Taranan cihaz ve tarama teknolojisi başarıyla bağlanmıştır.
- Kaynak cihaz ve verileri değiştirilmemiştir.
- Tarama teknolojisi, taranacak verilerin gerçek bir kopyasını oluşturmuştur.

Bir depolama cihazının ve belleğin adli kopyasını oluşturmak için çeşitli araçlar/yazılımlar kullanılmaktadır. Yazma engelleyici ise, tarama işleminden önce ve tarama işlemi sırasında kaynak cihazda herhangi bir değişiklik yapılmasını önleyen bir teknolojidir. Yazma engelleyiciler genellikle kaynak ve tarama sistemi arasında yer alır [27].

Adli kopya orijinal verilerin kaybolmasını önler. Adli kopya alma araçları ve teknikleri, dijital verilerin bir mahkemede veya yasal işlemde başarılı bir şekilde delil olarak kabul edilebilmesini sağlar. Bir bellek sisteminin veya depolama cihazının adli kopyası, içerik hakkında doğru bilgi sağlayarak adli bilişim uzmanlarının mevcut ve olası olayları teşhis etmesine olanak tanır.

2.3. Adli Bilişim Süreçleri

Adli bilişim süreçleri, dijital delillerin tanımlanması, korunması, toplanması, incelenmesi, analizi ve raporlanması aşamalarından oluşan sistematik bir inceleme modeline dayanır [22]. Dijital delilin tanımlanmasından raporlanmasına kadar uzanan aşamalar adli bilimlerde tutarlılık ve mahkeme geçerliliği açısından kritik öneme

sahiptir [23]. Güncel araştırmalar ise bulut, nesnelerin interneti ve büyük veri ortamlarının yaygınlaşmasıyla birlikte bu süreçlerin daha karmaşık hale geldiğini ve ek aşamalar eklenmesi gerektiğini belirtmektedir [24].

2.1.1. Tanımlama

Bu aşama, olayla ilişkili dijital varlıkların, cihazların, hesapların veya veri kaynaklarının belirlenmesini kapsar. Tanımlama, inceleme sürecinin başlangıcı olup soruşturmanın kapsamını belirlemek ve hangi verilerin delil niteliği taşıyacağını tespit etmek için kritik bir aşamadır.

2.1.2. Koruma/Zincirleme delil yönetimi

Koruma aşaması, delillerin bütünlüğünün sağlanması ve değişmeden muhafaza edilmesini içerir. Bu aşamada adli imaj alma, hash değeri oluşturma ve zincirleme delil yönetimi kayıtları kritik rol oynar. Elektronik delillerin çabuk değişebilir yapısından dolayı koruma süreçlerinin titizlikle uygulanması gerekmektedir.

2.1.3. Toplama/Elde etme

Toplama aşaması, delil niteliği taşıyan verilerin uygun yöntemler ve araçlarla elde edilmesini kapsar. Bu aşama disk, RAM, mobil cihaz, ağ, bulut vb. sistemlerin/bileşenlerin verilerinin edinilmesini içerir.

2.1.4. İnceleme/Ön işleme

İnceleme aşaması, toplanan verilerin filtrelenmesi, işlenmesi ve olayla ilgili olabilecek unsurların ortaya çıkarılması sürecidir. Burada dosya kurtarma, zaman damgası inceleme ve veri sınıflandırma gibi işlemler yürütülür.

2.1.5. Analiz

Analiz aşaması, incelenmiş verilerden olaya ilişkin anlamlı sonuçların çıkarılmasını içerir. Analiz aşaması, delilin gerçekte neyi ifade ettiğini ortaya koyduğu için en kritik adımlardan birisidir. Bu analiz sonuçları potansiyel kanıtların belirlenmesine ve olayla ilişkilendirilmiş verilerin ortaya çıkarılmasına yardımcı olur [25].

2.1.6. Raporlama/Sunum

Raporlama aşaması, elde edilen bulguların teknik doğruluk, bütünlük ve anlaşılabilirlik ilkelerine uygun olarak sunulmasını gerektirir. Raporun, bulgular ile birlikte kullanılan yöntemleri, araçları, hash değerlerini ve zincirleme delil kayıtlarını da içermesi gerekmektedir.

3. WINDOWS TABANLI SİSTEMLERDEKİ DİJİTAL DELİLLER

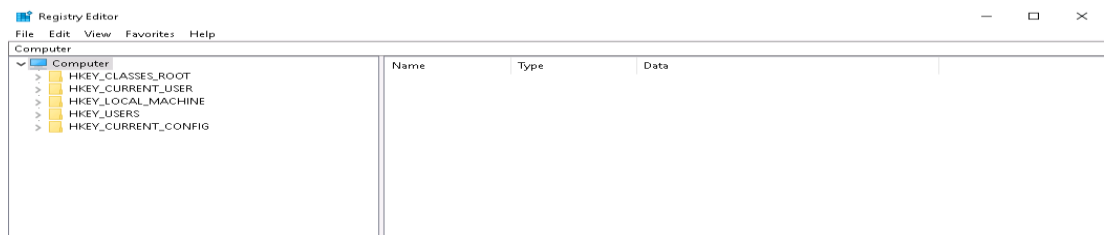
Bilişimin geniş dijital ortamında her eylem iz bırakır. Windows tabanlı sistemlerde bu izler, kullanıcı etkileşimlerinin ve sistem işlemlerinin delilleri/kalıntıları olarak ortaya çıkar. Bir kullanıcının oturum açtığı andan kapatma işlemine kadar Windows, kullanıcı davranışı, sistem performansı ve olası güvenlik ihlalleri hakkında öngörüler sunan verileri kaydeder.

Windows üzerindeki deliller, kayıt defteri girdileri ve dosya sistemi meta verilerinden olay günlükleri ve internet geçmişine kadar çok çeşitli dijital izleri kapsar. Her iz, gerçekleşen etkinliklere ışık tutar. Yeni bir kullanıcı profilinin oluşturulması, bir uygulamanın yüklenmesi veya bir web tarayıcısının tarama geçmişi vb. bilgiler dijital ortamda önemlidir.

Adli bilişim uzmanları ve siber olay müdahale ekipleri Windows izlerini titizlikle inceleyerek siber olayları analiz edebilir ve siber olay müdahalesine, adli soruşturmalara, proaktif güvenlik önlemlerine katkıda bulunabilir.

3.1. Windows Kayıt Defteri

Windows Kayıt Defteri (Windows Registry), sistemin yapılandırma verilerini içeren bir veri tabanları koleksiyonudur [28]. Bu yapılandırma verileri donanımla, yazılımla veya kullanıcı bilgileriyle ilgilidir. Ayrıca kullanılan programlar, son kullanılan dosyalar veya sisteme bağlı cihazlar hakkındaki verileri de içerir [16]. Kayıt defterinin görüntülenmesi ve düzenlenmesi için yerleşik bir Windows yardımcı programı olan regedit.exe (regedit) kullanılabilir. Regedit çalıştırılmasına ilişkin ekran görüntüsü Şekil 3.1’de sunulmuştur.



Şekil 3.1. Regedit Ekran Görüntüsü

Windows kayıt defteri anahtarlar ve değerlerden oluşur. Kayıt defterini görüntülemek için regedit.exe yardımcı programı açıldığında, görülen klasörler kayıt defteri anahtarlarıdır. Bu kayıt defteri anahtarlarında saklanan veriler kayıt defteri değerleridir. Windows kayıt defterindeki önemli kayıtlar ve konumları Tablo 3.1’de sunulmuştur.

Tablo 3.1. Windows Kayıt Defteri Önemli Kayıtları

Kayıt	Kayıt Defteri Yolu	Açıklama
Başlangıç (STARTUP)	- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	İşletim sistemi başlatıldığında otomatik olarak çalışan uygulamalar hakkında bilgiler tutulur.
Sistem Geri Yükleme Bilgisi	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SystemRestore	Sistem geri yükleme ayarları ve bilgileri tutulur.
USB Bilgileri	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR	Sisteme takılan USB aygıtlarının bilgileri tutulur.
Bağlı Aygıtlar (Mounted Devices)	HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices	Disk ve volume eşleştirme bilgileri tutulur.
MRU – Son Ziyaret Edilen	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU	En son açılan veya ziyaret edilen dizinlerin bilgileri tutulur.
MRU – Son Açılan/Kaydedilen	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU	Son kaydedilen dosya adları ve yolları tutulur.
MRU – Son Kullanılan Belgeler	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	Son erişilen dosyaların bilgileri tutulur.
MRU – RunMRU	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	“Çalıştır” (Run) kutusunda kullanılan en son komutlar tutulur.
Geri Dönüşüm Kutusu Bilgisi	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume	Her sürücü için geri dönüşüm kutusu ayarları tutulur; NukeOnDelete ile (0 = Geri Dönüşüm Kutusu kullanılıyor, 1 = Geri Dönüşüm Kutusu atlanıyor) silme davranışı kontrol edilir.
Hesap Süresi (Account Expiration)	HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\F Key	33-40 byte olarak hesap süresinin dolması bilgisi tutulur. Süre ayarlanmadıysa FF FF FF FF görülür.

Tablo 3.1. (Devamı) Windows Kayıt Defteri Önemli Kayıtları

Kayıt	Kayıt Defteri Yolu	Açıklama
Makine SID Bilgisi	HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\V	Bilgisayarı benzersiz şekilde tanımlayan makine SID bilgisi V değerinin son 12 byte'ında tutulur.
Parola İpucu	HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\<RID>\UserPasswordHint	Yerel kullanıcı hesaplarının parola ipuçları tutulur.
Kullanıcı Adı ve SID	HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\V Key	Kullanıcı adı ve SID hex formatında tutulur.
Yüklü Uygulama Listesi	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	Sistem üzerinde yüklü olan uygulamaların bilgileri tutulur.
Son Giriş Yapan Kullanıcı	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	Sisteme en son giriş yapan kullanıcı bilgileri tutulur.
İşletim Sistemi Kurulum Tarihi	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	İşletim sisteminin kurulum tarihi bilgisi tutulur.
İşletim Sistemi Sürümü	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	İşletim sisteminin mevcut sürüm bilgisi tutulur.
İşletim Sistemi Ürün Kimliği	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	İşletim sistemi ürün kimliği bilgisi tutulur.
İşletim Sistemi Ürün Adı	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	İşletim sisteminin adı bilgisi tutulur.
Profil Listesi	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList	Sistemde bulunan kullanıcı profillerinin SID bilgileri tutulur.
Güvenlik Duvarı	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\EnableProfile	Windows güvenlik duvarının açık kapalı durum bilgisi tutulur. 1 = etkin, 0 = devre dışıdır.
Antivirüs	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\DisableAntiVirus	Windows antivirüs sisteminin açık kapalı durum bilgisi tutulur. 1 = kapalı, 0 = açıktır.
Ağ Kartları	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\<guid>	Ağ kartlarının bilgileri tutulur.
Sayfa Dosyası	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\Memory Management	Sayfa dosyasıyla ilgili bilgiler (konum, boyut, temizleme ayarı vb.) tutulur.
Uzak Masaüstü	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Terminal Server\ fDenyTSConnections	Uzak masaüstü özelliğinin açık kapalı durum bilgisi tutulur. fDenyTSConnections = 1 ise Uzaktan Masaüstü kapalı, 0 ise açıktır.
Servisler	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services	Servislerin bilgileri tutulur.
Boot Komutları	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\<BootExecute>	Boot sürecinde (başlangıcında) çalıştırılacak komutlar tutulur.

Windows tabanlı sistemde kayıt defteri aşağıdaki kök anahtarları içerir:

- HKEY_CURRENT_USER,
- HKEY_USERS,
- HKEY_LOCAL_MACHINE,
- HKEY_CLASSES_ROOT,
- HKEY_CURRENT_CONFIG.

HKEY_CURRENT_USER: Bu anahtar, oturumu açık olan kullanıcıya ait yapılandırma verilerinin kökünü temsil eder. Masaüstü ve tema ayarları, kişisel klasör yolları, denetim masası tercihleri, başlat menüsü ve görev çubuğu düzeni, uygulama konfigürasyonları, ağ ve bağlantı ayarları ile klavye ve bölgesel tercihleri gibi kullanıcıya özel bilgileri içerir. Tüm bu bilgiler kullanıcı profiline bağlıdır. Genellikle HKCU kısaltmasıyla gösterilir.

HKEY_USERS: Sisteme yüklenmiş tüm kullanıcı profillerine ait bilgileri barındırır. HKU kısaltmasıyla ifade edilebilir. HKEY_CURRENT_USER anahtarı ise HKEY_USERS anahtarının alt dalıdır.

HKEY_LOCAL_MACHINE: Bilgisayarda genel olarak tüm kullanıcıları kapsayan sistem yapılandırma bilgilerini içerir. HKLM şeklinde kısaltılır.

HKEY_LOCAL_MACHINE\Software: Bu bölümde kayıtlı olan bilgiler, dosyaların uygun programlarla açılmasını sağlar. Örneğin bir belgeye çift tıklandığında, hangi yazılımın çalıştırılacağını buradaki ayarlar belirler. Bu anahtar, Windows 2000'den itibaren hem HKEY_LOCAL_MACHINE hem de HKEY_CURRENT_USER altında yer alan bilgilerle birlikte çalışır.

HKEY_LOCAL_MACHINE\Software\Classes: Tüm kullanıcılar için geçerli olan varsayılan ayarları içerir.

HKEY_CURRENT_USER\Software\Classes: Yalnızca oturumu açık kullanıcı için geçerli olan ve varsayılan ayarları geçersiz kılan bilgileri içerir.

HKEY_CLASSES_ROOT: Bu anahtar, yukarıda belirtilen iki anahtarın (HKLM\Software\Classes ve HKCU\Software\Classes) birleştirilmiş halidir ve kayıt defterinde programların dosya türleriyle nasıl ilişkilendirileceğini gösterir. HKCR şeklinde kısaltılır.

HKEY_CURRENT_CONFIG: Sistem başlatılması sırasında donanım profiline bağlı olarak oluşturulan geçerli donanım yapılandırmasına dair bilgileri içerir.

Kayıt defteri canlı bir sistemde regedit.exe aracılığıyla görüntülenebilir. Ancak bir disk imajında kayıt defteri kovan dosyaları genellikle \Windows\System32\Config klasörü içerisinde yer alır. Burada aşağıdaki dosyalar bulunur ve her biri kayıt defterinin farklı anahtarlarına karşılık gelir:

- DEFAULT: HKEY_USERS\DEFAULT anahtarındaki verileri barındırır.
- SAM: HKEY_LOCAL_MACHINE\SAM anahtarının içeriğini depolar.
- SECURITY: HKEY_LOCAL_MACHINE\Security kayıt defteri bilgilerinin saklandığı dosyadır.
- SOFTWARE: HKEY_LOCAL_MACHINE\Software bölümüne ait yapılandırma verilerini içerir.
- SYSTEM: HKEY_LOCAL_MACHINE\System altındaki sistem ayarlarını barındırır.

Kullanıcının profil klasöründe, kullanıcıya ait bilgileri barındıran iki ek kayıt defteri kovanı daha bulunabilir. Windows 7 ve sonrası işletim sistemlerinde, kullanıcı profili genellikle \Users\<kullanıcı_adı>\ yolunda yer alır ve bazı dosyalar gizli konumlandırılmıştır:

- NTUSER.DAT: Bu dosya, kullanıcı oturum açığında HKEY_CURRENT_USER anahtarına yüklenir ve doğrudan \Users\<kullanıcı_adı>\ dizininde bulunur.
- USRCLASS.DAT: Bu dosya HKEY_CURRENT_USER\Software\CLASSES anahtarına karşılık gelir ve \Users\<kullanıcı_adı>\AppData\Local\Microsoft\Windows\ dizininde yer alır.

Adli bilişim incelemelerinde, bilgisayarlara takılan depolama birimleri (disk, USB vb.) registry kayıtları ile tespit edilebilir. Bu kayıtlar takılan depolama biriminin seri numarası, takılma tarihi ve takılma sayısı gibi bilgileri içerir. Bir sunucuda bulunan depolama biriminin veya ortak bir alanın başka bilgisayarlara bağlanabileceği (mount edilebileceği) göz önünde bulundurulduğunda bu durumu sadece fiziksel olarak takılan depolama birimleriyle sınırlamamak gerekir. Bilgisayarlara takılan depolama birimlerine ilişkin kayıtların konumları Tablo 3.2’de sunulmuştur [29].

Tablo 3.2. Takılan Depolama Birimlerine İlişkin Verilerin Konum Bilgileri

Kategori	Konum
Drive Letter and Volume Name	- HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
USB Device Information	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR
Windows Portable Devices	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\PortableDevices\Devices
Mapped Network Drives	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU
USB Device Properties (First/Last Times)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_<Vendor>_Prod_<Product>_Rev_<Version>\<SerialNumber>\Properties\

Windows, kayıt defteri kovanlarına veri yazarken genellikle işlem loglarını kullanır. Her kovanın işlem logları kovanın kendisiyle aynı dizinde bir .LOG dosyası olarak depolanır. Kayıt defteri kovanı ile aynı ada sahiptir ancak uzantısı .LOG'dur. Örneğin, SAM kovanının işlem günlüğü \Windows\System32\Config dizininde SAM.LOG isimli dosyada bulunur. Bazen birden fazla işlem günlüğü de olabilir. Bu durumda dosya uzantıları .LOG1, .LOG2 vb. olur.

Kayıt defteri yedekleri, \Windows\System32\Config dizininde bulunan kayıt defteri kovanlarının yedekleridir. Bu kovanlar her on günde bir \Windows\System32\Config\RegBack dizinine kopyalanır.

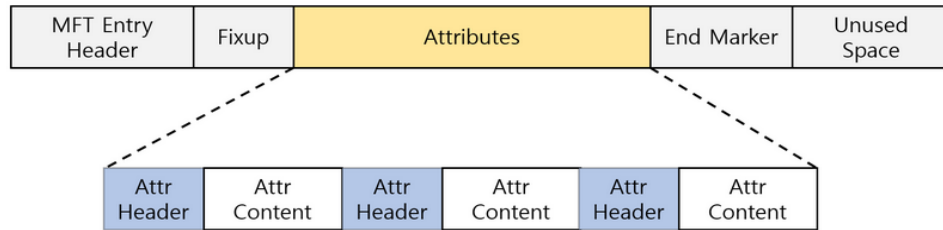
3.2. Dosya Sistemi

Dosya sistemi, verilerin depolama aygıtlarında nasıl saklanacağını ve bunlara nasıl erişileceğini belirleyen temel yapıdır. Dosya sistemi, dosyaları düzenlemek ve yönetmek için kullanılır; dosya boyutu, öznitelikler, disk konumu, oluşturulma ve değiştirilme tarihleri gibi bilgileri kaydeder. Ayrıca alan yönetimi, veri bütünlüğü, şifreleme ve dosya erişim kontrolü gibi görevler, dosya sisteminin sunduğu mekanizmalar aracılığıyla gerçekleştirilir. Bir diskte birden fazla dosya sistemi barındırılabilir. Disk bölümlenmişse bu mümkündür. Bölümleme, bir fiziksel diskin mantıksal olarak birden fazla parçaya bölünmesidir. Bu, bir disk bölümü arızalandığında diğerinin normal şekilde çalışmaya devam etmesini, dosyaların daha iyi organize edilmesini ve her bölümün başka bir depolama aygıtı gibi ayrı ayrı yönetilebilmesini sağlamak gibi çeşitli avantajlar sağlar [30].

Master File Table (MFT), NTFS dosya sisteminin temelini oluşturur. Her dosya ve klasör, NTFS dosya sisteminde MFT içinde en az bir kayıt (entry) ile temsil edilir. Her MFT kaydı varsayılan olarak 1 KB (1024 bayt) boyutundadır. Kaydın baş kısmında, genellikle ilk 42 bayt, kayıt başlığı (file record header) olarak adlandırılır ve burada kayıt türü, sıra numarası, referanslar ve temel meta veriler gibi bilgiler bulunur. Kayıt başlığından sonraki bölüm, dosyanın tüm özelliklerini (attributes) içerir; bunlar arasında dosya adı, boyutu, oluşturulma, değiştirilme ve erişilme zaman damgaları, dosya izinleri, veri akışları (data streams) ve dosya sistemine özgü diğer meta veriler yer alır [31]. NTFS, özellikle aşağıdaki bilgileri \$MFT içerisinde bulunan ilgili özniteliklerde saklar:

- Dosyanın adı,
- Boyutu,
- Yeniden adlandırma,
- Oluşturulma tarihi,
- Değiştirilme tarihi,
- Erişilme tarihi.

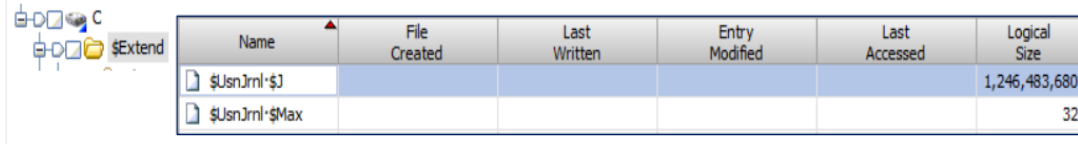
MFT mimarisi Şekil 3.2’de sunulmuştur.



Şekil 3.2. MFT Mimarisi

NTFS dosya sisteminde USN Journal (\$J), dosya ve izinlerde gerçekleşen tüm değişiklikleri kaydeden özel bir veri akışıdır ve Windows işletim sisteminde \$Extend\$UsnJrnl altında saklanır. Bu günlük, dosya oluşturma, silme, yeniden adlandırma, özellik (attribute) değişiklikleri ve bazı veri değişiklikleri gibi işlemleri içerir ve metadata değişikliklerinin izlenmesini sağlar. USN Journal verileri, öncelikle yedekleme uygulamalarının değişen dosyaları tespit etmesine olanak tanımak için kullanılır; bu sayede incremental veya differential yedeklemeler gerçekleştirilebilir.

Modern Windows sürümlerinde USN Journal varsayılan olarak aktiftir ve NTFS üzerinde gerçekleşen dosya sistemi işlemlerinin bir kısmını sürekli olarak kaydeder. Böylece adli bilişim analizlerinde, sistemdeki dosya ve izin aktivitelerinin zaman çizelgesi çıkarılmasında değerli bir veri kaynağı olarak işlev görür. USN Journal dosya yapısına ilişkin görsel Şekil 3.3'te sunulmuştur.



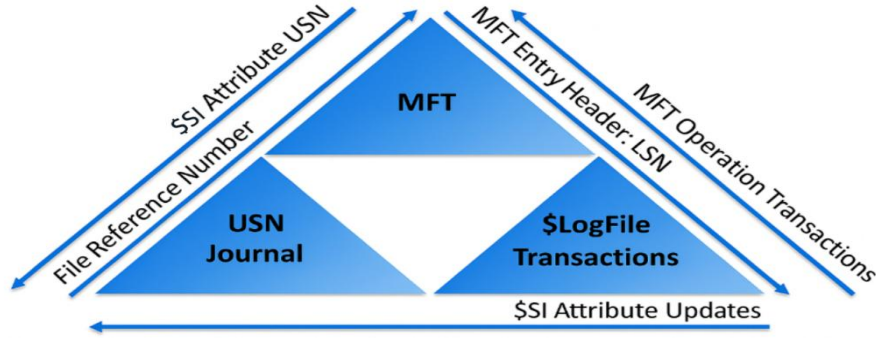
Name	File Created	Last Written	Entry Modified	Last Accessed	Logical Size
\$UsnJrnl-\$J					1,246,483,680
\$UsnJrnl-\$Max					32

Şekil 3.3. USNJournal Dosya Yapısı

Windows NTFS dosya sistemi, dosya sistemi bütünlüğünü korumak ve beklenmedik sistem kapanmalarında tutarsızlıkları onarmak amacıyla \$LogFile adlı günlük dosyasını kullanan işlem (transaction) tabanlı bir günlükleme mekanizmasına sahiptir. NTFS'te gerçekleştirilen işlemler öncelikle günlük dosyasına kaydedilir ve işlem başarıyla tamamlandığında değişiklikler taahhüt edilir. Sistem beklenmedik bir şekilde kapanır veya çökerse, NTFS yeniden başlatma sırasında \$LogFile içeriğini analiz ederek yarım kalan işlemleri geri alır ya da tamamlar ve böylece dosya sisteminin tutarlılığını yeniden sağlar.

NTFS dosya sisteminde \$LogFile, dosya sistemi işlemlerine ilişkin metadata değişikliklerini kaydeden sabit boyutlu bir log dosyasıdır. Adli bilişim analizlerinde \$LogFile incelenerek geçmiş işlem aktivitelerinin kronolojik sıralamasına yakın bir liste elde edilebilir; ancak bu kayıt yalnızca metadata işlemlerini içerir ve dosya içerik değişikliklerini kapsamaz. Dosya boyutu dolduğunda eski kayıtlar üzerine yazıldığından, kaydedilen geçmişin miktarı ve süresi, dosya sistemi aktivitesine bağlı olarak değişir. Standart NTFS uygulamalarında \$LogFile boyutu genellikle 64 MB civarındadır ve yöneticinin müdahalesiyle yeniden yapılandırılabilir. Pratikte, log dosyası genellikle birkaç saatlik sistem aktivitesini kaydedebilir, ancak yoğun aktivitelerde eski kayıtlar hızla silinebilir. \$LogFile analizi, \$MFT ve \$UsnJrnl gibi diğer NTFS kayıtları ile birlikte kullanıldığında, sistemde gerçekleşen olayların daha kapsamlı ve güvenilir bir zaman çizelgesinin çıkarılmasına olanak sağlar.

Dosya sistemine ilişkin kalıntılar, \ \$Extend \$UsnJrnl, \ \$MFT ve \ \$LogFile konumlarında bulunmaktadır. NTFS meta veri yapıları arasındaki ilişki Şekil 3.4'te sunulmuştur.



Şekil 3.4. NTFS Meta Veri Yapıları Arasındaki İlişki

3.3. Kullanıcı ve Sistem

Windows işletim sistemi, hem kullanıcı etkileşimleri hem de sistem olayları sonucu çeşitli düzeylerde kalıntılar üretir. Bu kalıntılar, kullanıcı davranışlarını ve sistemin iç işleyişini yansıtan önemli dijital izlerdir. Kullanıcı kaynaklı kalıntılar; oturum açma geçmişleri, erişilen dosyalar, kullanılan uygulamalar ve dış aygıt bağlantıları gibi eylemlerle ilişkilidir. Sistem kaynaklı kalıntılar ise işletim sisteminin kendi süreçlerine, servislerine ve güvenlik mekanizmalarına dair izleri içerir. Adli bilişim incelemelerinde, bu izlerin doğru şekilde sınıflandırılması ve yorumlanması, olayın teknik olarak aydınlatılabilmesi açısından kritik öneme sahiptir.

Amcache

Amcache, Windows 8 ve sonrası işletim sistemlerinde yürütülebilir dosyalara ait metadata bilgilerini tutan, kayıt defteri benzeri bir hive dosyasıdır. Amcache kayıtları üzerinden program adı, sürüm bilgisi, çalıştırılan veya tanımlanan dosya yolu, dosya boyutu, hash ve dijital imza bilgileri ile dosyanın sistemde ilk kez görüldüğü zamana ilişkin zaman damgaları elde edilebilir [32]. Bu bilgiler, bir uygulamanın sistemde varlığı ve çalıştırılmış olabileceği konusunda adli analizlerde güçlü göstergeler sunar. Ayrıca Amcache verileri, kötü amaçlı yazılımların veya kullanıcı aktivitelerinin izlerini takip etmek için de kullanılabilir, çünkü bazı durumlarda silinmiş dosyaların bile metadata kayıtları Amcache’te kalabilir [33]. Amcache dosyası \\Windows\\AppCompat\\Programs\\Amcache.hve konumunda bulunur.

Prefetch

Windows işletim sisteminde Prefetch, uygulamaların ve sistem bileşenlerinin daha hızlı açılmasını sağlamak amacıyla kullanılan bir önbellekleme mekanizmasıdır. Sistem, bir uygulama ilk kez çalıştırıldığında veya belirli aralıklarla, uygulamanın

çalışması sırasında eriştiği dosya ve bellek bloklarının bilgisini .pf uzantılı dosyalar halinde \Windows\Prefetch\ dizininde saklar. Bu sayede sonraki çalıştırmalarda, uygulama ihtiyaç duyduğu veriye daha hızlı erişebilir ve açılış süresi kısalmır. Prefetch kayıtları bir bilgisayarda uygulamaların çalıştırılma tarihleri ve konum bilgilerini içerir [34].

Shimcache

Shimcache, Microsoft tarafından Windows XP'den itibaren yürütülen uygulamaların kaydını tutmak amacıyla oluşturulmuştur. Shimcache verileri, eski girişlerin üzerine yeni girişler yazılarak tutulur ve kayıt sayısı işletim sistemi sürümüne bağlı olarak değişebilir. Shimcache'de kaydedilen bilgiler dosya yolu, dosya boyutu ve metadata zaman damgalarını içerir [35-36]. Shimcache verilerinin konum bilgileri Tablo 3.3'te sunulmuştur.

Tablo 3.3. Shimcache Verilerinin Konum Bilgileri

Konum
• HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatibility • HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

UserAssist

UserAssist, Windows işletim sisteminde kullanıcıların hangi uygulamaları ve dosyaları ne sıklıkla çalıştırdığını takip eden bir mekanizmadır [32]. Çalıştırılan uygulamaların sayısı, son kullanım tarihi ve kullanım sıklığı, Windows kayıt defterinde HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist altında şifrelenmiş veya kodlanmış biçimde saklanır.

SAM Database

SAM (Security Accounts Manager - Güvenlik Hesapları Yöneticisi), Windows işletim sisteminde kullanıcı hesap bilgilerini depolamak için kullanılan bir veri tabanıdır. SAM, kullanıcı adları, hesap grupları, erişim hakları ve özel ayrıcalıklar ile parola hashlerini içerir. Parolalar hashlenmiş olarak saklanır ve SAM dosyasına yalnızca yönetici ayrıcalıklarına sahip kullanıcılar erişebilir [37]. SAM verilerinin konum bilgileri Tablo 3.4'te sunulmuştur.

Tablo 3.4. SAM Verilerinin Konum Bilgileri

Kaynak	Konum
Dosya Sistemi	\Windows\System32\config\SAM
Kayıt Defteri	HKEY_LOCAL_MACHINE\SAM

SRUM

Windows 8'den itibaren kullanılan SRUM (System Resource Usage Monitor) veri tabanı, sistem kaynaklarının kullanımını izlemek için tasarlanmıştır. SRUM, ağ kullanımları, veri miktarları, uygulama kullanım süreleri, enerji tüketimi, CPU ve disk kullanım miktarları gibi çok sayıda veriyi içerir [38]. Kullanıcı ve uygulama bazlı işlem bilgileri, CPU kullanım süreleri, okunan/yazılan veri miktarları ve uygulama bazlı ağ veri miktarları, SRUM mekanizması tarafından periyodik olarak kaydedilir [39]. SRUM verilerinin konum bilgileri Tablo 3.5'te sunulmuştur.

Tablo 3.5. SRUM Verilerinin Konum Bilgileri

Kaynak	Konum
Dosya Sistemi	\Windows\System32\sru\SRUDB.dat
Kayıt Defteri	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SRUM\Extensions

Jumplist

Jumplist, kullanıcıların en son eriştiği programlara ve dosyalara daha hızlı bir şekilde ulaşmasını sağlayan ve ilgili uygulama üzerinden sıkça gerçekleştirilen işlemleri kolaylaştıran bir Windows özelliğidir. Windows 7 ile birlikte kullanılmaya başlanmıştır. Jumplist dosyalarının içeriği dosya türüne bağlı olarak değişebilir; bir uygulama üzerinden hangi dosyaların veya klasörlerin açıldığına, bunların açılma zamanlarına ve bazen dosya yollarına dair bilgiler sağlar [40]. Jumplist verileri adli bilişim analizinde kullanıcı etkinliği ve dosya erişim zamanlarını belirlemek için önemli bir kaynaktır. Jumplist verilerinin konum bilgileri Tablo 3.6'da sunulmuştur.

Tablo 3.6. Jumplist Verilerinin Konum Bilgileri

Konum
\Users\<KullanıcıAdı>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations \Users\<KullanıcıAdı>\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

Shellbag

Shellbag kayıtları, Windows işletim sisteminde kullanıcıların grafiksel kullanıcı arayüzü üzerinden gezindiği dizinlere ilişkin bilgileri tutmak amacıyla oluşturulan ve Windows Kayıt Defteri içerisinde yer alan önemli kayıtlardan birisidir. Bu kayıtlar, esas olarak Windows Explorer aracılığıyla açılan klasörlere ait konum, pencere boyutu, görünüm ayarları ve klasör hiyerarşisi gibi bilgileri saklar [41]. Shellbag verileri, kullanıcının en az bir kez görüntülediği dizinleri gösterebilir; ancak doğrudan ve kesin bir erişim zamanı bilgisi tutmaz. Bunun yerine, ilgili kayıt defteri anahtarlarının Last Write Time değerleri üzerinden dolaylı zaman analizi yapılmasına imkân tanır. Bu kayıtlar yalnızca yerel sabit disklerle sınırlı değildir; çıkarılabilir depolama aygıtları, ağ paylaşımları ve hatta silinmiş veya artık mevcut olmayan klasörler hakkında da bilgi içerebilir [42]. Shellbag verilerinin konum bilgileri Tablo 3.7’de sunulmuştur.

Tablo 3.7. Shellbag Verilerinin Konum Bilgileri

Konum	Açıklama
HKEY_USERS\<SID>\Software\Microsoft\Windows\Shell\BagMRU	Klasörlerin hiyerarşik yapısını ve geçmişte hangi klasörlerin görüntülendiğini gösterir.
HKEY_USERS\<SID>\Software\Microsoft\Windows\Shell\Bags	Her klasör için görünüm, konum ve ikon gibi detaylı ayar bilgilerini içerir.

Shortcut (Lnk)

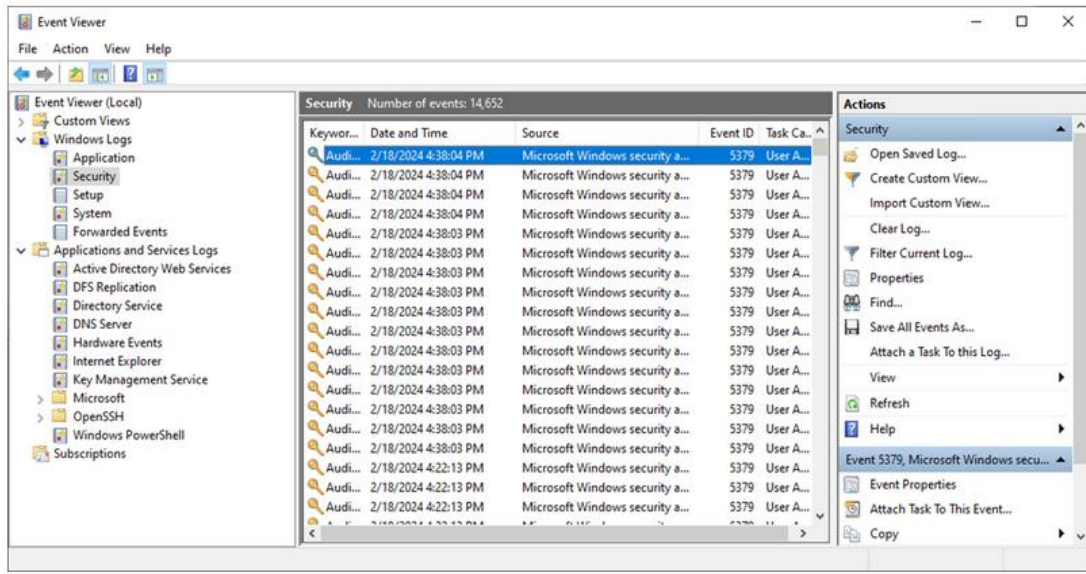
LNK (Shortcut) dosyaları, Windows işletim sisteminde kullanıcıların bir dosya, klasör veya uygulamaya erişimini kolaylaştırmak amacıyla oluşturulan kısayol dosyalarıdır. Bu dosyalar, kullanıcı tarafından erişilen dosya ve uygulamaların tespit edilmesinde önemli kayıtlar arasında yer alır. Windows ortamında, bir dosya veya uygulama Windows Explorer gibi grafiksel arayüz bileşenleri aracılığıyla açıldığında, hedef dosya daha sonra silinmiş olsa dahi ilgili LNK dosyası sistem üzerinde varlığını sürdürebilir ve silinen dosyalar veya belgeler hakkında bilgi sağlayabilir. LNK dosyaları, bir hedef dosyaya veya çalıştırılabilir programa erişildiğini gösterecek şekilde çeşitli meta veriler içerir. Bu kapsamda; hedef dosyanın orijinal yolu, boyutu, hedef dosyaya ve LNK dosyasına ait zaman damgaları, dosya öznitelikleri (sistem, gizli vb.), disk ve volume bilgileri, hedef kaynağın yerel veya ağ üzerinden erişilip erişilmediğine dair bilgiler ve bazı durumlarda ağ bağlantılarına ilişkin ek veriler elde edilebilir [43]. Lnk dosyalarına ilişkin verilerin konum bilgileri Tablo 3.8’de sunulmuştur.

Tablo 3.8. Lnk Dosyalarına İlişkin Verilerin Konum Bilgileri

Kategori	Konum
Recent (Otomatik oluşturulan LNK dosyaları)	• \Documents and Settings\<KullanıcıAdı>\Recent\ • \Users\<KullanıcıAdı>\AppData\Roaming\Microsoft\Windows\Recent\
Masaüstü (Desktop)	• \Documents and Settings\<KullanıcıAdı>\Desktop\ • \Users\<KullanıcıAdı>\Desktop\
Başlat Menüsü (Start Menu / Programs)	• \Documents and Settings\<KullanıcıAdı>\Start Menu\Programs\ • \Users\<KullanıcıAdı>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\
Başlangıç (Startup)	• \Documents and Settings\<KullanıcıAdı>\Start Menu\Programs\Startup\ • \Users\<KullanıcıAdı>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ • \ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\
Office Recent (Opsiyonel, Office uygulamalarına özel)	• \Documents and Settings\<KullanıcıAdı>\Application Data\Microsoft\Office\Recent\ • \Users\<KullanıcıAdı>\AppData\Roaming\Microsoft\Office\<versiyon>\Recent\

Olay Günlüğü

Windows işletim sisteminde gerçekleştirilen işlemler ve aktiviteler, olay günlüğü (Event Log) kayıtlarında tutulmaktadır. Olay günlüğü kayıtları, kullanılan servisler, uygulamalar ve yapılandırılmış denetim politikalarına bağlı olarak farklılık gösterebilir. Örneğin, bir antivirüs yazılımı tarafından karantinaya alınan dosyalara ait bilgiler; dosya adı, tarih ve zaman gibi detaylarla birlikte, ilgili antivirüs uygulamasına ait ayrı olay günlüğü dosyalarında kaydedilmektedir. Windows işletim sistemi varsayılan olarak System.evtx, Security.evtx ve Application.evtx gibi temel olay günlüğü dosyalarını oluşturur. Özellikle güvenlik olayları ve ayrıntılı kullanıcı aktivitelerinin kaydedilebilmesi için Windows denetim (audit) ve olay günlüğü politikalarının yapılandırılması gerekmektedir. Windows, kullanıcı ve sistem tarafından gerçekleştirilen farklı aksiyonlara göre farklı olay kimlik numaralı (Event ID) kayıtlar üretir. Bu kimlik numaraları (4688, 4624, 4625 gibi), gerçekleşen aksiyonların sınıflandırılması ve analiz edilmesinde kullanılmaktadır. Olay günlüğü ekran görüntüsü Şekil 3.5’te sunulmuştur.



Şekil 3.5. Olay Günlüğü Ekran Görüntüsü

Olay günlüğü verilerinin konum bilgileri Tablo 3.9’da sunulmuştur.

Tablo 3.9. Olay Günlüğü Verilerinin Konum Bilgileri

Kaynak	Konum
Dosya Sistemi	\Windows\System32\winevt\Logs\
Kayıt Defteri	HKLM\SYSTEM\CurrentControlSet\Services\EventLog

Silinmiş Dosya İzleri

Adli bilişim ve olay müdahale süreçlerinde, silinen dosyalara ilişkin deliller yüksek öneme sahiptir. Kullanıcı tarafından bir dizin içerisindeki dosyaların (resim, video vb.) küçük resim (thumbnail) formatında görüntülenmesi sonrasında, bu dosyalara ait çok küçük boyutlarda kopyalar oluşturulur. Eski Windows sürümlerinde bu küçük resimler Thumbs.db adlı dosyada saklanır. Bu sayede, orijinal dosya silinmiş olsa dahi, dosyaya ait küçük resim bilgileri elde edilebilir.

Windows Vista ve sonraki sürümlerde ise resimlerin, videoların, klasörlerin ve bazı ofis belgelerinin küçük resimleri thumbcache ön bellek veri tabanlarında (thumbcache_*.db) tutulur [44]. Bu veri tabanları, kullanıcı tarafından görüntülenmiş dosyalara ait küçük resimleri içerir ve tarayıcılar (Internet Explorer veya Edge’in IE modu gibi) aracılığıyla açılan dosyaların küçük resimleri de bu ön belleğe yansyabilir. Bu durum, kullanıcının belirli dosyaları görüntülediğine dair önemli ipuçları sağlar.

Geri Dönüşüm Kutusu (Recycle Bin) kayıtları ise, Windows dosya sisteminde silinen dosyalara ait önemli meta verileri içerir [45]. Bu kayıtlar; dosyanın orijinal konumu ve adı, silinme tarihi ve dosya boyutu gibi bilgileri barındırır. Ayrıca, dosyalar geri

dönüşüm kutusundan silinmedikçe geri kurtarılabılır. Silinmiş dosyaların izlerine ilişkin konum bilgileri Tablo 3.10'da sunulmuştur.

Tablo 3.10. Silinmiş Dosya İzleri Konum Bilgileri

Kategori	Konum
Thumbs.db	Tüm dizinler
Thumbcache	\Users\<KullanıcıAdı>\AppData\Local\Microsoft\Windows\Explorer
IE Edge	\Users\<KullanıcıAdı>\LocalSettings\History\History \Users\<KullanıcıAdı>\AppData\Local\Microsoft\WindowsHistory\History \Users\<KullanıcıAdı>\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat
Recycle Bin	\$Recycle.Bin

Bellek Yönetim Dosyaları

Bellek yönetim dosyaları, işletim sistemlerinin bellek kullanımını optimize etmek ve sistem kararlılığını sağlamak amacıyla oluşturulan özel dosyalardır. Pagefile.sys ve swapfile.sys, fiziksel RAM yetersiz kaldığında kullanılan sanal belleği temsil eder; bu dosyalar sayesinde sistem, aktif olmayan verileri geçici olarak disk belleğine aktararak RAM üzerindeki yükü azaltır. Hiberfil.sys dosyası, sistemin hazırda bekletme (hibernation) moduna geçmesi sırasında RAM'deki verilerin tamamını depolamak için kullanılır ve bu sayede bilgisayar, güç kaynağıyla bağlantısı kesilse dahi mevcut durumu koruyabilir. Küçük bellek dökümü (minidump) dosyaları ise sistem çökmesi sonrasında hata ayıklama amacıyla oluşturulan, çökme anındaki bellek içeriğinin kritik bilgilerini özetleyen dosyalardır. Bu dosyalar, özellikle sistem yöneticileri ve yazılım geliştiriciler için tanılayıcı bilgi sağlayarak sorunların kök nedenine ulaşılmasına olanak tanır.

Yazılım/Servis/Veri Tabanı Kayıtları

Adli bilişim disiplinde dijital olayların aydınlatılmasında, yazılım logları, servis kayıtları ve veri tabanı kayıtları bütüncül bir biçimde değerlendirilmesi gereken temel veri kaynakları arasında yer almaktadır. Yazılım (antivirüs, oyun, ofis, tarayıcı vb.) logları, yazılımlar tarafından gerçekleştirilen işlemlerin izlenmesine olanak tanırken; servis kayıtları, sistem düzeyinde çalışan arka plan süreçlerinin başlatılma, durdurulma, hata üretme gibi eylemlerini belgeleyerek olayın sistemsel boyutunu ortaya koyar. Bu loglar genellikle Windows işletim sisteminde Event Viewer altında Application ve System başlıkları altında toplanmakta, ancak birçok uygulama ve servis ayrıca kendi log dosyalarını ya da veri tabanı tabanlı kayıt sistemlerini kullanmaktadır. Veri tabanları ise, özellikle kullanıcı etkinlikleri, işlem geçmişleri, sistem

yapılandırmaları ve güvenlik olayları gibi verilerin saklandığı, hem doğrudan hem de dolaylı delillerin elde edilebildiği kaynaklardır. Bu kapsamda yazılım ve servis günlükleri ile veri tabanı kayıtları, olayın davranışsal ve teknik boyutlarının tespit edilmesini sağlayan veriler sunmaktadır.

Group Policy

Lokal veya etki alanı düzeyinde sistem ve kullanıcı yapılandırmalarını merkezi olarak yönetmek üzere tasarlanmış olan Group Policy (Grup İlkesi) altyapısı, adli bilişim incelemesinde ve analizinde sistemin hangi politika ve kısıtlamalara tabi olduğunu anlamak açısından kritik bir iz bırakır. Siber saldırganlar veya kötü amaçlı yazılımlar, politikaları değiştirerek güvenlik kontrollerini aşabilir; bu bağlamda Group Policy yapılandırmasına dair dosya ve kayıt kalıntıları incelenmelidir. Group Policy verilerinin konum bilgileri Tablo 3.11’de sunulmuştur.

Tablo 3.11. Group Policy Verilerinin Konum Bilgileri

Kaynak	Konum
Dosya Sistemi	• \Windows\System32\GroupPolicy\ • \Windows\System32\GroupPolicyUsers\
Kayıt Defteri	• HKLM\Software\Policies\ • HKCU\Software\Policies\

Scheduled Tasks

Scheduled Tasks (Zamanlanmış Görevler) bileşeni, belirli bir zaman, sistem olayı, kullanıcı oturumu başlangıcı gibi tetikleyicilerle otomatik şekilde görevleri çalıştırmak üzere tasarlanmıştır. Tetikleyiciler örnek olarak belirli bir saat veya tarih, sistem başlatma, kullanıcı oturumu açma veya belirli bir olayın gerçekleşmesini içerebilir. Adli bilişimde bu yapı, özellikle zararlı yazılımların kalıcılık sağlamak amacıyla otomatik tetiklenmiş görevlerini veya diğer şüpheli aktiviteleri tespit etmek açısından kritik öneme sahiptir. Scheduled Tasks verilerinin konum bilgileri Tablo 3.12’de sunulmuştur.

Tablo 3.12. Scheduled Tasks Verilerinin Konum Bilgileri

Kaynak	Konum
Dosya Sistemi	• \Windows\Tasks\ • \Windows\System32\Tasks\
Kayıt Defteri	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{GUID}

SUM

Windows işletim sisteminde, \Windows\System32\LogFiles\SUM dizini, kritik bir veri kaynağı olarak işlev görür. Bu klasör, özellikle Windows sunucu altyapısında kullanıcı erişim aktivitelerinin ve servis işlemlerinin izlenmesini sağlayan User Access Logging (UAL) mekanizması tarafından oluşturulan veri tabanlarını içerir. SUM klasörü, Extensible Storage Engine (ESE) tabanlı .mdb dosyaları aracılığıyla kullanıcıların sistem servislerine erişim zamanlarını, IP adreslerini ve erişim sayıları gibi ayrıntıları kaydeder. Bu veriler, hem sistem yönetimi hem de adli bilişim süreçlerinde, erişim denetimi ve siber güvenlik olaylarının analizi açısından değerlidir. SUM, işlevi ve içerdiği veri tabanları bağlamında, sistem servislerinin kullanım ve erişim metriklerini merkezi bir şekilde depolayan bir yapı olarak tanımlanabilir.

WER (Windows Error Reporting)

Windows Error Reporting (WER), Windows işletim sisteminde hata ve çökme durumlarını otomatik olarak raporlamak için kullanılan bir sistemdir. WER, uygulama hataları, sistem çökmeleri veya donanım arızaları gibi olayları tespit eder, bunlarla ilgili teknik bilgileri toplar ve kullanıcı onayı ile Microsoft'a gönderir. Bu bilgiler; hata kodları, bellek dökümleri, çalışan süreç bilgileri ve bazen kullanıcı eylemleri gibi detayları içerebilir. WER verileri, bir sistemde meydana gelen hataların zamanını, etkilenen süreçleri ve olası nedenlerini analiz etmek için değerli bir kaynaktır. WER verilerinin konum bilgileri Tablo 3.13'te sunulmuştur.

Tablo 3.13. WER Verilerinin Konum Bilgileri

Kaynak	Konum
Dosya Sistemi	• \ProgramData\Microsoft\Windows\WER\ • \Users\<KullanıcıAdı>\AppData\Local\Microsoft\Windows\WER\ • \Windows\Logs\CBS\
Kayıt Defteri	HKLM\Software\Microsoft\Windows\Windows Error

WBEM (Web-Based Enterprise Management)

WBEM, özellikle büyük ölçekli bilgi teknolojileri altyapılarında sistem yönetimini standartlaştırmak ve otomatikleştirmek amacıyla geliştirilmiş bir yönetim mimarisidir. WBEM, Common Information Model (CIM) standartlarını temel alarak donanım, işletim sistemi, yazılım ve ağ bileşenleri gibi sistem kaynaklarını soyut bir model üzerinden tanımlar ve bu kaynaklara erişim için platformdan bağımsız bir arayüz sağlar. Bu yapı, sistem yöneticilerinin yerel veya uzak sistemler üzerinde durum bilgisi

toplamaına, olayları izlemesine ve ynetimsel iřlemeleri otomatikleřtirmesine olanak tanır. WBEM'in sunduęu standartlařtırılmıř veri modeli ve protokoller, farklı reticilerin cihaz ve yazılımlarını tek merkezi ynetim erevesinde entegre etmeyi mmkn kılar. Windows Management Instrumentation (WMI), WBEM standartlarını Microsoft'un Windows ortamına uyarlaması ve uygulamasıdır. WMI Repository, sınıf tanımları, meta veriler ve yapılandırma bilgilerini ieren veri tabanı benzeri bir yapıdır. Repository'deki kalıntılar, hem sistem ve uygulama olaylarının izlenmesi hem de saldırganların WMI yoluyla komut alıřtırma veya servis bařlatma gibi eylemlerini analiz etmek aısından nemli kaynaktır. WBEM verilerinin konum bilgileri Tablo 3.14'te sunulmuřtur.

Tablo 3.14. WBEM Verilerinin Konum Bilgileri

Kaynak	Konum
Dosya Sistemi	• \Windows\System32\wbem\Repository\ • \Windows\System32\wbem\Logs\
Kayıt Defteri	HKLM\Software\Microsoft\WBEM

BITS (Background Intelligent Transfer Service)

Adli biliřim kapsamında Background Intelligent Transfer Service (BITS), Windows sistemlerde arka planda gerekleřtirilen dosya indirme ve ykleme iřlemlerinin analiz edilmesi aısından nemli bir inceleme alanıdır. BITS ile ilgili olay gnlkleri, iř kuyrukları ve iliřkili sistem kayıtları aracılıęıyla bir dosya transferinin zaman bilgisi, alıřtıęı servis veya sre baęlamı ve kullanılan kaynak adresleri hakkında bulgular elde edilebilir. Bu nedenle BITS, hem meřru gncelleme ve sistem iřlemlerinin doęrulanmasında hem de kt amalı yazılımlar tarafından gizli dosya indirme veya veri aktarımı amacıyla suistimal edilip edilmedięinin tespitinde nemli bir veri kaynaęıdır. BITS verilerinin konum bilgileri Tablo 3.15'te sunulmuřtur.

Tablo 3.15. BITS Verilerinin Konum Bilgileri

Kaynak	Konum
Dosya Sistemi	• \ProgramData\Microsoft\Network\Downloader\ • \Windows\System32\Winevt\Logs\Microsoft-Windows-Bits-Client%4 Operational.evtx
Kayıt Defteri	HKLM\Software\Microsoft\Windows\CurrentVersion\BackgroundAccessApplications

WindowsIndexSearch (Arama Dizini Hizmeti)

WindowsIndexSearch, Windows iřletim sisteminde dosya ve ierik aramalarını hızlandırmak iin kullanılan bir servis ve indeksleme mekanizmasıdır. Bu servis,

bilgisayardaki dosya ve klasörlerin metadata ve içerik bilgilerini tarayarak bir indeks oluşturur; böylece kullanıcı arama yaptığında sonuçlar hızlı bir şekilde döner. Adli bilişim açısından WindowsIndexSearch'in önemi, oluşturduğu indekslerin mevcut veya erişilmiş dosyalarla ilgili bilgiler, dosya erişim zamanları ve içerik bilgilerini barındırabilmesidir. Bu özellikleri sayesinde servis, olayların incelenmesinde değerli bir veri kaynağıdır. WindowsIndexSearch verilerinin konum bilgileri Tablo 3.16'da sunulmuştur.

Tablo 3.16. WindowsIndexSearch Verilerinin Konum Bilgileri

Kaynak	Konum
Dosya Sistemi	\ProgramData\Microsoft\Search\Data\Applications\Windows\
Kayıt Defteri	• HKLM\Software\Microsoft\Windows Search • HKCU\Software\Microsoft\Windows\CurrentVersion\Search

WindowsTimeline (Activity History / Timeline Database)

Windows Timeline, Windows 10 ve sonraki sürümlerde kullanıcıların geçmiş etkinliklerini izlemek ve yönetmek için kullanılan bir özelliktir. Bu özellik, kullanıcıların açtığı uygulamaları, üzerinde çalıştığı dosyaları ve ziyaret ettiği web siteleri gibi bilgileri kronolojik olarak kaydeder. Windows Timeline, bir kullanıcının sistem üzerindeki aktivitelerini zaman çizelgesi halinde ortaya koymak için değerli bir kaynaktır. WindowsTimeline verilerinin konum bilgileri Tablo 3.17'de sunulmuştur.

Tablo 3.17. WindowsTimeline Verilerinin Konum Bilgileri

Kaynak	Konum
Dosya Sistemi	\Users\<KullanıcıAdı>\AppData\Local\ConnectedDevicesPlatform\ActivitiesCache.db
Kayıt Defteri	HKCU\Software\Microsoft\Windows\CurrentVersion\ConnectedDevicesPlatform

3.4. Bellek (RAM)

RAM (Random Access Memory) alanında tutulan geçici bilgiler, disk imajından doğrudan elde edilemez. RAM'in imajı sistem açıkken edinilebilir. RAM imajı alınırken sistemin değiştirilmemesi ve delillerin korunması için özel bellek alma araçları kullanılır. RAM'de depolanan veriler, bilgisayar güç kaybettiğinde veya kapatıldığında kaybolur [46]. Bilgisayar açık olduğu sürece, kullanıcı aktiviteleri ve zamanlanmış görevler RAM'de tutulur ve bellek imajından erişilebilir. Örneğin; son kopyalanan öğeler, değiştirilen dosyalar, internet tarayıcı çerezleri gibi kullanıcının bilgisayarda yaptığı aktiviteler, diske kaydedilmeden önce RAM'de tutulan geçici verilerdir. Bellek imajlarından elde edilen bilgiler arasında çalışan işlem bilgisi,

kullanıcı bilgisi ve işlemin çalıştırılma tarihi gibi veriler bulunmaktadır. Ayrıca, çalıştırılan işlemin gerçekleştirdiği aktiviteler ve anlık ağ bağlantılarının durumu gibi bilgilere de erişilebilmektedir [47]. RAM'in farklı bölümleri, farklı türde veriler ve izler barındırmaktadır. Bu nedenle RAM imajı üzerinde yapılan incelemelerde bu bölümlere odaklanılmalıdır.

Kullanıcı Belleği (User Space Memory)

Kullanıcı belleği, işletim sisteminde her kullanıcı sürecine (process) ayrılan, korunan bellek alanıdır. Uygulamalar (örneğin Notepad, Chrome, Word) kodlarını, değişkenlerini ve açık verilerini burada tutar. Her süreç, işletim sistemi tarafından kendisine tahsis edilen izole bir sanal adres uzayında (virtual address space) çalışır; böylece doğrudan diğer süreçlerin veya kernel alanının belleğine erişemez. Bu yapı, sistemin güvenliğini ve kararlılığını sağlar. Kullanıcı belleği bölümünden elde edilebilecek kalıntılar: açık veya en son kullanılan dosya içerikleri (bufferlar), şifreler, kimlik bilgileri, geçici token bilgileri, çalışan uygulamaların geçmiş aktiviteleri, ağ bağlantı verileri, socket bufferları, runtime kayıtlarıdır (log, clipboard, kopyalanmış veriler).

Çekirdek Belleği (Kernel Space Memory)

Çekirdek belleği, işletim sisteminin çekirdeği ve sürücüler tarafından kullanılan ayrıcalıklı bellek alanıdır. Donanım erişimi, dosya sistemleri, bellek yönetimi ve işlem planlaması gibi temel işlemler burada gerçekleşir. Kullanıcı süreçleri kernel alanına doğrudan erişemez; sadece sistem çağrıları (syscalls) aracılığıyla dolaylı olarak işlem yapabilir. Bu ayırım, sistem çökmelerini ve yetkisiz erişimleri engeller. Çekirdek belleği bölümünden elde edilebilecek kalıntılar: açık dosya nesneleri (FILE_OBJECT), handle tabloları, sistem servislerinin durumları (CDP, SMB, TCP/UDP bağlantıları), yüklü sürücüler, modüller ve bellek haritaları, kullanıcı alanına ait pointerlar veya kernel önbelleklerindeki kritik bilgiler, thread, proses ve güvenlik token bilgileridir.

Pagefile / Swap

Pagefile veya swap, fiziksel RAM yetersiz kaldığında bellek sayfalarının disk üzerinde geçici olarak depolandığı alandır. İşletim sistemi, kullanılmayan veya düşük öncelikli bellek sayfalarını buraya taşır ve RAM'i aktif işlemler için boşaltır. Disk tabanlı olduğundan erişimi RAM'e göre çok daha yavaştır, ancak sistemin bellek taşmasını

önleyerek kararlılığı artırır. Pagefile / Swap bölümünden elde edilebilecek kalıntılar: RAM'deki kullanıcı verilerinin bir kısmı (şifre, metin, geçici dosya içerikleri), kapatılmış veya silinmiş işlemlere ait bellek içerikleri, uygulama önbellekleri veya oturum bilgileri, kernel ve user space verilerinin yedeklenmiş kopyaları, hata dökümü veya sistem hatası sırasında RAM'deki kritik verilerdir.





4. MATERİYAL VE METOT

Bu bölümde, Windows tabanlı sistemler üzerinden dijital delillerin elde edilmesi ve analizi kapsamında kullanılan materyaller ve metotlar ele alınacaktır.

4.1. Kopya Alma

Adli bilişimde, bir sistemden hem sabit disk hem de RAM imajı almak, dijital delil toplama sürecinin kritik adımıdır. Sabit disk için alınan bit-bit birebir kopya, diskte yer alan tüm verileri (dosyalar, silinmiş ögeler, slack-space, dosya sistemi meta verileri vb.) içerir; bu sayede orijinal materyale dokunulmadan analiz yapılabilir ve delil bütünlüğü korunur [48]. Öte yandan RAM'den alınan imaj, sistem çalışırken bellekte yer alan aktif işlemler, açık ağ bağlantıları, şifreleme anahtarları veya zararlı yazılımlar gibi yalnızca uçucu bellekte bulunan verileri ortaya çıkarabilir [49]. Elde edilen imajlara yönelik hash gibi kriptografik bütünlük kontrolleri yapılmalı ve analizler imajlar üzerinde gerçekleştirilmelidir [48]. Disk ve RAM imajları birlikte kullanıldığında, hem kalıcı hem uçucu veri bütünlüğü sağlanarak elde edilen kapsamlı bir delil seti, siber saldırı analizleri ve adli soruşturmalar açısından büyük önem taşır.

İmaj alma işlemleri FTK Imager adli bilişim aracı ve delil bütünlüğünü korumak için kullanılan bir yazma engelleyici (write blocker) aracılığıyla güvenli şekilde gerçekleştirilebilmektedir.

FTK Imager, dijital adli bilişimde kullanılan ücretsiz bir imaj alma aracıdır. Depolama aygıtlarının, belirli dosyaların ve klasörlerin, RAM'in birebir kopyasını oluşturur. Ayrıca elde edilen imajların hash değerlerini hesaplayarak doğrulama imkânı sunar.

Yazma engelleme cihazı, inceleme sırasında hedef depolama aygıtına herhangi bir veri yazılmasını engelleyen bir donanımdır. Bu sayede orijinal delilin değiştirilmesi önlenir ve inceleme süreci güvenli hale getirilir.

4.2. Dijital Delillerin Elde Edilmesi

Disk imajlarından elde edilen dijital deliller, bilgisayar sisteminde meydana gelen olayların, kullanıcı faaliyetlerinin ve sistemde gerçekleştirilen değişikliklerin geriye

dönük olarak analiz edilmesinde temel veri kaynaklarıdır. Bunlar; dosya sistemi kalıntıları, kayıt defteri girdileri, olay günlükleri, kullanıcı profilleri ve uygulama verileri gibi farklı bileşenlerden elde edilir. Her bir dijital delil, sistemin geçmiş durumu ve kullanıcı davranışları hakkında zamansal ve bağlamsal bilgiler sunar. Bu alanda kullanılan araçlar ve metodolojiler, belirli kurallar ve tanımlı veri toplama stratejileri aracılığıyla bu dijital delilleri sistematik biçimde saptar ve sınıflandırır.

Disk imajı üzerinden dijital delillerin toplanmasında SANS Enstitüsü tarafından önerilen koleksiyon kullanılmıştır [50]. SANS Enstitüsü, 1989 yılında kurulmuş, bilgi güvenliği, siber güvenlik eğitimi ve sertifika konularında uzmanlaşmış, siber güvenlik ve adli bilişim alanında dünyanın en saygın araştırma ve eğitim kuruluşlarından birisidir [51]. Windows tabanlı sistemlerin disk imajından toplanan dijital deliller Tablo 4.1’de sunulmuştur

Tablo 4.1. Disk İmajından Elde Edilen Dijital Deliller

Kategori	Konum (Genel)	Açıklama
Antivirüs	• \ProgramData\AntivirusVendor\Logs* • \Documents and Settings\All Users\Application Data\AntivirusVendor\Logs* • HKLM\SOFTWARE\AntivirusVendor* • HKLM\SOFTWARE\WOW6432Node\AntivirusVendor*	Antivirüs yazılımlarına ait loglar, karantina kayıtları ve tespit edilen tehdit raporları; sistemdeki kötü amaçlı yazılım etkinliklerinin tespiti, yanıt süreçlerinin analizi ve savunma mekanizmalarının değerlendirilmesi için birincil veri kaynağıdır.
CloudStorage_ Metadata	• \Users*\AppData\Roaming\CloudVendor* • \Users*\AppData\Local\CloudVendor* • \Users*\Documents\CloudVendor* • HKCU\Software\CloudVendor* • HKLM\Software\CloudVendor*	Bulut tabanlı depolama hizmetlerinin (ör. OneDrive, Dropbox, Google Drive) senkronizasyon, dosya erişimi ve kullanıcı etkileşimlerini belgeleyen meta veriler; veri paylaşım zincirinin ve olası dış veri aktarımının izlenmesinde kullanılır.
CombinedLogs	• \Windows\System32\winevt\Logs*.evtx • \Windows\System32\config*.evt • \Windows\Logs*	Sistem, güvenlik ve uygulama loglarının birleştirilmiş görünümünü temsil eder; olayların yeniden yapılandırılması, sistem davranışı analizi ve saldırı tespiti süreçlerinde bütünsel bir veri kaynağı sunar.
GroupPolicy	• \Windows\System32\GroupPolicy* • \Windows\System32\GroupPolicyUsers* • HKLM\Software\Policies\Microsoft*	Grup İlkesi (Group Policy - GPO) yapılandırmaları, sistem ve kullanıcı düzeyinde uygulanan güvenlik politikalarını gösterir; güvenlik uyumluluğu, erişim kısıtlamaları ve sistem konfigürasyonunun analizi için kritik öneme sahiptir.

Tablo 4.1. (Devamı) Disk İmajından Elde Edilen Dijital Deliller

Kategori	Konum (Genel)	Açıklama
EvidenceOf Execution	• \Windows\Prefetch*.pf • \Windows\AppCompat\Programs\ • \Windows\System32\Amcache.hve • \Windows\AppCompatCache* • \Users*\AppData\Local\Microsoft\Windows\ • UsrClass.dat • HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run • HKCU\Software\Microsoft\Windows\CurrentVersion\Run	Sistem üzerinde çalıştırılmış uygulamalara ilişkin kalıcı izleri içeren veri kümesidir; yürütme geçmişinin belirlenmesi, kalıcılık mekanizmalarının tespiti ve olay zaman çizelgesi oluşturulmasında kullanılır.
FileSystem	• \$MFT • \$LogFile • \$J • \$Boot • \$T	Dosya sistemi, kullanıcı ve sistem faaliyetlerine ilişkin izlerin saklandığı temel yapı taşıdır; olayların zaman temelli yeniden yapılandırılması ve veri bütünlüğü doğrulaması için başlıca kanıt kaynağıdır.
FTPClients	• \Users*\AppData\Roaming\FTPClientVendor* • \Users*\AppData\Local\FTPClientVendor* • \Program Files\FTPClientVendor* • \Program Files (x86)\FTPClientVendor* • HKCU\Software\FTPClientVendor*	FTP istemcileri ve bağlantı yapılandırılmalarına ait log ve konfigürasyon verileri; uzak sistemlere yapılan dosya transferlerinin ve olası veri sızıntılarının incelenmesinde kritik rol oynar.
LNKFilesAnd Jumplists	• \Users*\AppData\Roaming\Microsoft\Windows\Recent* • \Users*\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations* • \Users*\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations*	Windows tarafından oluşturulan LNK (kısayol) dosyaları ve Jumplist kayıtları, kullanıcı tarafından açılan dosyalar, uygulamalar ve dizinler hakkında zaman damgalı meta veriler sağlar; kullanıcı davranışlarının yeniden yapılandırılmasında kullanılır.
Messaging Clients	• \Users*\AppData\Roaming\MessagingVendor* • \Users*\AppData\Local\MessagingVendor* • HKCU\Software\MessagingVendor*	Mesajlaşma uygulamalarına (Skype, Teams, Slack vb.) ait kullanıcı profilleri, sohbet geçmişi ve medya aktarım kayıtlarını içerir; iletişim analizi ve olay bağlamı oluşturulmasında önemli bir dijital kanıt kategorisidir.
Network Scanner	• \Program Files\NetworkToolVendor* • \Program Files (x86)\NetworkToolVendor* • \Users*\AppData\Local\NetworkToolVendor*	Ağ tarama ve keşif araçlarına ait dosya ve konfigürasyon izleri; ağ yapısının haritalanması, keşif faaliyetlerinin tespiti ve tehdit analizlerinde kullanılır.
RecycleBin_ InfoFiles	• \$Recycle.Bin*\\$I* • \$Recycle.Bin*\\$R* • \Recycler*\\$I* • \Recycler*\\$R*	Silinmiş dosyaların meta verilerini içeren bilgi dosyaları (\$I ve \$R dosyaları); dosya silme zamanlarının, orijinal konumların ve kullanıcı etkileşimlerinin belirlenmesinde kullanılır.

Tablo 4.1. (Devamı) Disk İmajından Elde Edilen Dijital Deliller

Kategori	Konum (Genel)	Açıklama
RegistryHives	• \Windows\System32\config\SAM • \Windows\System32\config\SOFTWARE • \Windows\System32\config\SYSTEM • \Windows\System32\config\SECURITY • \Users*\NTUSER.DAT • \Users*\UsrClass.dat	Windows kayıt defteri (Registry) kovanları, sistem ve kullanıcı yapılandırmalarını kalıcı biçimde saklayan veri yapılarıdır; kalıcılık mekanizmalarının, yapılandırma değişikliklerinin ve kullanıcı davranışlarının analizi için temel bir kaynaktır.
RemoteAccess	• \Users*\AppData\Roaming\RemoteAccess Vendor* • \Users*\AppData\Local\RemoteAccess Vendor* • \ProgramData\RemoteAccessVendor* • HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server • HKCU\Software\Microsoft\Terminal Server Client\Servers	Uzak masaüstü (RDP), VPN veya diğer uzaktan erişim mekanizmalarına ait konfigürasyon ve bağlantı kayıtlarını içerir; yetkisiz erişim girişimlerinin ve uzak oturum faaliyetlerinin incelenmesinde kullanılır.
Scheduled Tasks	• \Windows\System32\Tasks* • \Windows\Tasks* • HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks • HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree	Zamanlanmış görevler, sistem üzerinde belirli olay veya zamanlarda otomatik olarak yürütülen işlemleri temsil eder; kalıcılık (persistence) analizleri ve kötü amaçlı görevlerin tespitinde önemli bir göstergedir.
SRUM	\Windows\System32\sru*	System Resource Usage Monitor (SRUM) veri tabanı, uygulama ve ağ kullanımıyla ilişkili istatistiksel verileri içerir; kullanıcı etkinliği, enerji tüketimi ve ağ trafiği analizlerinde faydalanılır.
SUM	\Windows\System32\LogFiles\SUM*	SUM, sunucu servislerine erişim aktiviteleri ve kullanıcı etkileşimlerine dair ayrıntılı veriler sağlar; erişim kontrolü, siber güvenlik ihlallerinin tespiti ve adli bilişim analizlerinde kullanılır.
WER	• \ProgramData\Microsoft\Windows\WER\ReportQueue* • \Users*\AppData\Local\Microsoft\Windows\WER*	Windows Error Reporting (WER) kayıtları, sistem ve uygulama çökme olaylarının ayrıntılı hata raporlarını içerir; yürütme geçmişi, bellek dökümleri ve hata bağlamı analizi için kullanılır.
ThumbCache	• \Users*\AppData\Local\Microsoft\Windows\Explorer\thumbcache_*.db • \Users*\AppData\Local\Microsoft\Windows\Explorer\iconcache_*.db • \Users*\AppData\Local\Microsoft\Windows\Explorer*.db	Windows'un küçük resim (thumbnail) önbelgesi, kullanıcı tarafından görüntülenmiş dosya ve dizinlerin görsel izlerini barındırır; görsel içerik incelemesi ve dosya erişim geçmişinin doğrulanması için kullanılır.

Tablo 4.1. (Devamı) Disk İmajından Elde Edilen Dijital Deliller

Kategori	Konum (Genel)	Açıklama
WBEM	\Windows\System32\wbem\Repository*	Windows Management Instrumentation (WMI) Repository'si, sistem yönetimi ve otomasyon süreçlerine dair olayları ve yapılandırmaları içerir; kalıcılık, komut yürütme ve sistem kontrolü analizlerinde kullanılır.
BITS	\ProgramData\Microsoft\Network\Downloader\qmgr*.dat	Background Intelligent Transfer Service (BITS) verileri, arka plan dosya aktarım süreçlerini kaydeder; güncellemelerle birlikte kötü amaçlı yüklemelerin veya veri sızıntılarının tespitinde kullanılır.
WebBrowsers	• \Users*\AppData\Local\BrowserVendor*\History • \Users*\AppData\Roaming\BrowserVendor*\Profiles*\places.sqlite • \Users*\AppData\Local\BrowserVendor*\Cache* • \Users*\AppData\Roaming\BrowserVendor*\Cache*	Web tarayıcılarına ait geçmiş, çerez, önbellek ve oturum verilerini içerir; internet etkinliklerinin, kullanıcı tercihlerinin ve veri aktarım örüntülerinin analizinde kullanılır.
WindowsIndex Search	• \ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb • \Users*\AppData\Local\Microsoft\Windows\Indexer*	Windows arama indeksleme sistemi, dosya ve içerik aramalarıyla ilgili meta verileri depolar; kullanıcı erişim örüntülerinin ve bilgiye erişim davranışlarının analizinde değerlidir.
Windows Timeline	\Users*\AppData\Local\ConnectedDevicesPlatform*	Windows Timeline bileşeni, uygulama, belge ve tarayıcı aktivitelerinin kronolojik kaydını tutar; kullanıcı davranışlarının zamana dayalı yeniden yapılandırılmasında kullanılır.
Bellek Yönetim Dosyaları	• \hiberfil.sys • \pagefile.sys • \swapfile.sys • \Windows\MEMORY.DMP • \Windows\Minidump\	Bilgisayar hazırda bekletme moduna geçtiğinde RAM içeriğini diske yazar. RAM dolduğunda, kullanılmayan bellek sayfaları pagefile.sys dosyasına taşınır. Windows 8 ve sonraki sürümlerde, modern uygulamaların bellek yönetimi için kullanılır. Sistem çökmesi (mavi ekran - BSOD) sırasında RAM'in belirli bölümleri kaydedilir.

Disk imajı üzerinden dijital delillerin toplanması Velociraptor adli bilişim aracı ile gerçekleştirilebilmektedir. Velociraptor, adli bilişim ve siber güvenlik alanlarında kullanılan açık kaynak kodlu bir araçtır. Bu araç, ağ üzerindeki uç noktalara yönelik veri toplama, izleme ve analiz etme yeteneğine sahiptir.

RAM imajı üzerinden toplanan dijital deliller ise bir sistemin çalışma anındaki durumunu yansıttığı için olay analizi ve zararlı yazılım tespitinde kritik bir kanıt kaynağı olarak kabul edilir. Bu çerçevede elde edilebilecek başlıca dijital deliller; işlem ve iş parçacığı listeleri, yüklü modüller, ağ bağlantıları, kullanıcı oturum bilgileri ve komut geçmişi gibi sistem ve kullanıcı etkinliklerine ilişkin verilerden oluşur [20]. Bu veriler genellikle işletim sisteminin çekirdek ve kullanıcı alanlarında yer alan karmaşık veri yapılarında (örneğin EPROCESS, PEB, KDBG gibi) tutulur. Bellek içerisindeki bu yapılar, farklı işletim sistemi sürümlerinde farklı adreslerde veya ofsetlerde bulunduğundan, kullanılan araçların bu adres ve yapısal bilgileri doğru biçimde eşleştirmesi gerekir. Ayrıca çekirdek düzeyindeki modüller, sürücüler ve sistem çağrıları üzerindeki olağan dışı değişiklikler, zararlı yazılım etkinliklerinin tespiti açısından önemli göstergeler sağlar [52].

Windows tabanlı sistemlerin RAM imajından toplanan dijital deliller [20, 52] Tablo 4.2’de sunulmuştur.

Tablo 4.2. RAM İmajından Elde Edilen Dijital Deliller

Kategori	Konum (Genel)	Açıklama
Aktif Prosesler	Kernel Space: PsActiveProcessHead (EPROCESS linked list)	İşletim sistemindeki aktif süreçleri listeleyerek, süreçlerin PID, PPID, başlatılma zamanı ve kullanıcı bilgilerini sunar.
RAM Taraması ile Tespit Edilen Prosesler	Kernel Space: Pool/Heap → EPROCESS	Bellek imajında sonlanmış veya gizlenmiş süreçlerin tespitine olanak sağlayarak, klasik süreç listesi taramalarının gözden kaçırdığı işlemleri ortaya çıkarır.
Proseslerin Hiyerarşik İlişkisi	Kernel Space: EPROCESS Parent/Child	Süreçler arasındaki hiyerarşik ilişkiyi görsel olarak sunarak, ebeveyn ve alt süreçlerin bağlantılarını analiz etmeye imkân tanır; süreçlerin kökenleri ve ilişkileri hakkında detaylı bilgi sağlar.
Ağ Bağlantıları	Kernel Space: TCP/IP Endpoint Structures (TCB, TCP_ENDPOINT, Socket Table)	Sistemin ağ bağlantılarını, açık portlarını, aktif bağlantı noktalarını ve ilişkili süreç bilgilerini ortaya çıkarır.
İnternet Tarayıcısı Geçmişi	User Space: IE Process Heap / VAD	İnternet Explorer tarayıcısına ait geçmiş ve çerez verilerinin çıkarılmasını sağlar.

Tablo 4.2. (Devamı) RAM İmajından Elde Edilen Dijital Deliller

Kategori	Konum (Genel)	Açıklama
RAM Taraması ile Tespit Edilen Dosyalar	Kernel Space: FILE_OBJECT / Object Manager / Pool	Bellek imajındaki dosya nesnelerini tarayarak sistemdeki aktif dosya referanslarını listeler; ayrıca bazı silinmiş veya gizlenmiş dosya nesnelerinin tespitine de olanak sağlayarak adli bilişim incelemelerinde ve analizlerinde önemli bir kaynak oluşturur.
Yüklü DLL Listesi	User Space: Process PEB → LDR List and VAD	Süreçlere yüklenmiş dinamik bağlantı kütüphanelerini (DLL) listeler ve süreçlerin davranış analizi ile kötü amaçlı yüklemelerin tespitinde kullanılır.
Kayıt Defteri Hive Listesi	Kernel Space: Loaded Registry Hive Blocks (Kernel Hive Cache)	Bellek imajındaki Windows Kayıt Defteri (Registry) hücrelerini listeler ve kayıt defteri yapılarının konum ve durum bilgilerini ortaya çıkarır.
Proseslerin Komut Satırı	User Space: EPROCESS/PEB → ProcessParameters → CommandLine	Süreçlerin komut satırı argümanlarını listeleyerek, süreç davranışlarının detaylı incelenmesine olanak verir.
Oturum Listesi	Kernel Space: WinStation and SessionInfo and EPROCESS linked list and EPROCESS → Token	Sistemdeki kullanıcı oturumlarını listeler. Her oturum için Session ID, oturuma ait PID ve süreç adı, kullanıcı adı, domain, logon ID ve oturum durumu (Active, Disconnected) bilgilerini sunar.
Kullanıcı Hesaplarının Parola Hash Değerleri	Kernel Space: SAM and SYSTEM Hive	Sistemdeki yerel kullanıcı hesabı parolalarının hash değerlerini ortaya çıkarır.
Zararlı Prosesler	User Space: Process VAD / Anonymous and Mapped Executable Regions / Thread Contexts	Bellek imajındaki şüpheli ve kötü amaçlı kod segmentlerini tespit ederek, rootkit ve diğer zararlı yazılımların tespitinde ve analizinde kritik bir rol oynar.

RAM imajı üzerinden dijital delillerin elde edilmesi Volatility adli bilişim aracı ile gerçekleştirilebilmektedir. Volatility, adli bilişim ve siber güvenlik alanlarında kullanılan açık kaynak kodlu bir araçtır. RAM'deki veriler üzerinden sistemdeki aktif süreçler, şifreli veriler, ağ bağlantıları, kullanıcı etkinlikleri gibi izleri ortaya çıkarır.

4.3. Zaman Çizelgesinin Oluşturulması

Adli bilişimde zaman çizelgesi, bir bilgisayar sistemi veya dijital cihazda gerçekleşen olayların, belirli bir zaman dilimi içinde kronolojik sırayla düzenlendiği bir veridir [53]. Zaman çizelgesi, adli bilişim incelemesinde önemli bir role sahiptir, çünkü olayların sırasını ve ilişkisini ortaya koyarak şüpheli etkinliklerin izini sürmeyi

kolaylaştırır. Adli bilişimde zaman çizelgesi oluşturmak, dijital delilleri (dosyalar, kayıtlar, olay günlükleri, tarayıcı geçmişi, sistem etkinlikleri vb.) analiz etmek ve bu kanıtların zamanla nasıl birbirini takip ettiğini görmek için kullanılır. Elde edilen dijital deliller standart bir formatta normalize edilir, zaman damgaları tek bir referans zaman dilimine (genellikle UTC) dönüştürülür ve kaynak bilgisi de standart alan olarak eklenir. Ardından dijital deliller zaman damgasına göre sıralanır ve zaman çizelgesi oluşturulur. Bu yaklaşım, aktivitelerin zamansal ilişkilerinin incelenmesini kolaylaştırır.

Zaman çizelgesinin oluşturulması Log2timeline/Plaso adli bilişim aracı ile gerçekleştirilebilmektedir. Log2timeline/Plaso, açık kaynak kodlu bir araçtır. Temel olarak zaman çizelgesi oluşturma amacıyla tasarlanmış olan bu araç, çeşitli sistem ve dosya kaynaklarından toplanan verileri zaman dilimlerine göre düzenleyerek, dijital olayların sırasını ve ilişkilerini analiz etmeye olanak tanır.

4.4. Silinmiş Dosyaların Kurtarılması

Silinmiş dosyaların kurtarılması için dosya sistemi yapısı analiz edilir ve dosya verileri mevcutsa erişim sağlanır. Dosya silindiğinde, genellikle izin girişleri ve meta veriler işaretlenirken, veri blokları disk üzerinde kalır. Bu meta veriler ve dosya sistemi tabloları incelenerek silinmiş dosyaların başlangıç blokları, boyutları ve diğer ilgili bilgileri tespit edilir. Ardından veri blokları okunarak dosyanın içeriği yeniden birleştirir ve kurtarılabilir hale getirilir. Bu yöntem, silinen dosyanın veri blokları üzerine yeni veri yazılmadığı sürece içeriğin büyük ölçüde geri getirilmesini mümkün kılar.

Silinmiş dosyaların kurtarılması The Sleuth Kit adli bilişim aracı ile gerçekleştirilebilmektedir. The Sleuth Kit, dijital adli bilişim alanında kullanılan açık kaynak kodlu bir araçtır. Disk ve dosya sistemlerini (NTFS, FAT, Ext vb.) inceleyerek silinmiş dosyaların kurtarılmasına olanak tanır.

4.5. Analiz

Adli bilişim ve siber olay müdahale süreçlerinde önceden tanımlanmış tehdit göstergeleri ve davranış kalıpları temel alınarak zararlı, şüpheli veya anormal faaliyetlerin belirlenmesi sağlanır.

4.5.1. Kural tabanlı analiz

Adli bilişimde kural tabanlı analiz, önceden tanımlanmış kriterler, imzalar veya mantıksal kurallar doğrultusunda dijital delillerin sistematik şekilde incelenmesini ifade eder. Bu yöntem, büyük veri kümelerinde şüpheli ve kötü amaçlı aktivitelerin, yazılımların veya sistem yapılandırmalarındaki anormalliklerin hızlı bir şekilde tespit edilmesini sağlar. Bu yaklaşımda, bilinen saldırı teknikleri, dosya hash bilgileri, şüpheli IP adresleri, sıra dışı komut çalıştırmaları veya belirli kayıt defteri değişiklikleri gibi kriterler üzerinden kurallar oluşturulur. Bu kurallar elde edilen dijital delillere uygulanarak sistematik bir şekilde olası güvenlik ihlalleri taranır.

Kural tabanlı analiz kapsamında otomatik gerçekleştirilen zararlı/şüpheli işlem tespitlerine ilişkin bilgiler Tablo 4.3'te sunulmuştur. Tablo 4.3'te belirtilen kural tabanlı analizler sayesinde tespit edilen aktiviteler MITRE ATT&CK çerçevesindeki saldırgan davranışları ile ilişkilendirilir.

Tablo 4.3. Kural Tabanlı Analiz

Zararlı/Şüpheli İşlem	Veri	Veri Kaynağı	MITRE ATT&CK Çerçevesi
Zararlı Powershell Komutu Çalıştırma	"downloadstring", "downloadfile", "iex", ifadelerinden birisini içeren komutun veya scriptin powershell kullanılarak çalıştırıldığını gösteren kayıtlar	Disk Kopyası	T1059.001 Command and Scripting Interpreter: PowerShell
Pass the Hash Saldırısı	SID'si "S-1-0-0" olan bir kullanıcı hesabı ile ağ üzerinden başarılı kimlik doğrulama yapıldığını gösteren kayıtlar	Disk Kopyası	T1550.002 Use Alternate Authentication Material: Pass the Hash
Zararlı Servis Kurulumu	"PSEXEC", "paexe", "anydesk", "mssecsvc", "pwdump", "gsecdump", "cachedump", "smbexec" ifadelerinden birisini içeren yeni bir servisin başlatıldığını veya kurulduğunu gösteren kayıtlar	Disk Kopyası	T1133 External Remote Services
Psexec Çalıştırılması	"PSEXESVC" ifadesini içeren yeni bir servisin başlatıldığını ve ağ üzerinden başarılı kimlik doğrulama yapıldığını gösteren kayıtlar	Disk Kopyası	T1021.002 Remote Services: SMB/Windows Admin Shares
Windows Eventlog Silinmesi	Windows olay günlüklerinin silindiğini gösteren kayıtlar	Disk Kopyası	T1070.001 Indicator Removal: Clear Windows Event Logs
Yerel Alan Ağına Dış Ağdan RDP Bağlantısı	"10.10.", "192.168.", "172.16.-172.31." ile başlayan IP adreslerine yapılan uzak masaüstü oturum açma işlemlerini gösteren kayıtlar	Disk Kopyası	T1021.001 Remote Services: Remote Desktop Protocol

Tablo 4.3. (Devamı) Kural Tabanlı Analiz

Zararlı/Şüpheli İşlem	Veri	Veri Kaynağı	MITRE ATT&CK Çerçevesi
Windows Olay Günlüğü Denetiminin Devre Dışı Bırakılması	“removed”, “kaldırıldı” ifadelerinden birisini içeren güvenlik denetimi politikasının değiştirildiğini gösteren kayıtlar	Disk Kopyası	T1562.002 Impair Defenses: Disable Windows Event Logging
Şüpheli Zamanlanmış Görev	"AppData", "Temp", "Users", "Roaming", "powershell", "-enc", "-EncodedCommand" ifadelerinden birisini içeren zamanlanmış görev kayıtları	Disk Kopyası	T1053.005 Scheduled Task/Job: Scheduled Task
Şüpheli Başarısız Oturum Açma	“0xC0000072” (hesap süresi dolmuş), “0xC000006F” (hesap devre dışı), “0xC0000070” (hesap geçici olarak askıya alınmış), “0xC0000413” (hesap kilitlenmiş), “0xC000018C” (hesap geçici olarak kilitli), “0xC000015B” (hesap geçici olarak kilitli) ifadelerinden birisini içeren başarısız oturum açma işlemini gösteren kayıtlar	Disk Kopyası	T1110 Brute Force
Şüpheli Dosya Yazma	“System32” dizinine herhangi bir dosya yazma işlemini gösteren kayıtlar veya “AppData” ya da “Temp” dizinlerine exe uzantılı dosya yazma işlemini gösteren kayıtlar	Disk Kopyası	T1036 Masquerading
Kalıcılık Göstergesi	Kayıt defterinde yer alan başlangıç anahtarında (Run) “EncodedCommand”, “rundll32”, “cmd.exe”, “schtasks”, “appdata\roaming”, “temp”, “base64”, “invoke-expression”, “powershell.exe”, “.vbs”, “.ps1”, “.bat” ifadelerinden birisini içeren kayıtlar veya Startup klasöründe “.exe”, “.bat”, “.cmd”, “.lnk” ve “.ps1” ifadelerinden birisini içeren dosya oluşturma kayıtları	Disk Kopyası	T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
USB Depolama Cihazı Bilgileri	Kayıt defterinde usb depolama cihazlarının bilgilerini içeren kayıtlar	Disk Kopyası	-
Sistem Tarih ve Saatinin Değiştirilmesi	Sistem tarihi ve saatinde yapılan değişiklikleri gösteren kayıtlar	Disk Kopyası	-
Sistem Tarih ve Saat Ayarı Bilgisi	Kayıt defterinde yer alan zaman dilimi, UTC farkı, yaz saati durumu, saatin otomatik/manuel olması, NTP’nin açık/kapalı durumu, NTP sunucuları gibi bilgileri içeren kayıtlar	Disk ve RAM Kopyaları	-
Zararlı Proses Bilgileri	Zararlı proseslere ilişkin proses ID, proses adı, başlama zamanı, başlatan kullanıcı adı, parent proses ID, parent proses adı, ağ bağlantıları, dosya yolları gibi bilgileri gösteren kayıtlar	Disk ve RAM Kopyaları	T1055 Process Injection
Şüpheli Proses	RAM’de mevcut olup işletim sisteminin aktif proses listesinde görünmeyen proses kayıtları	RAM Kopyası	T1014 Rootkit

Tablo 4.3. (Devamı) Kural Tabanlı Analiz

Zararlı/Şüpheli İşlem	Veri	Veri Kaynağı	MITRE ATT&CK Çerçevesi
Şüpheli Ağ Bağlantısı	“powershell.exe”, “wscript.exe”, “cscript.exe”, “cmd.exe”, “python.exe”, “node.exe” ifadelerinden birisini içeren prosesler tarafından başlatılan ağ bağlantısı kayıtları	RAM Kopyası	TA0011 Command and Control
Şüpheli DLL	Disk tabanlı bir dosya yolu ile ilişkilendirilemeyen dll kayıtları	RAM Kopyası	T1055.001 Process Injection: Dynamic-link Library Injection

4.5.2. Yapay zekâ destekli analiz

Yapay zekâ destekli anomali tespiti, özellikle büyük ve karmaşık veri kümelerinde sıra dışı davranışları tespit etmek amacıyla kullanılan etkili bir yöntemdir. Bu teknikler sayesinde, veri setindeki olağan dışı örnekler otomatik olarak belirlenebilir.

Makine öğrenmesi, günümüzde yapay zekâ alanının en hızlı gelişen alt dallarından biri haline gelmiş olup, özellikle veriye dayalı karar destek sistemlerinde etkin rol oynamaktadır. Bu bağlamda, öğrenme algoritmaları temel olarak denetimli öğrenme (supervised learning) ve denetimsiz öğrenme (unsupervised learning) olmak üzere iki ana gruba ayrılmaktadır. Bu iki yaklaşım arasındaki temel fark, modelin eğitileceği verinin içerdiği bilgilere, özellikle de etiketlerin (labels) varlığına dayanır.

Denetimli öğrenme, girdi verileri ile birlikte doğru çıktıların (etiketlerin) da sunulduğu durumlarda kullanılmaktadır. Amaç, modelin bu eşleşmeleri öğrenerek daha sonra sunulacak yeni örnekler için doğru çıktılar üretmesini sağlamaktır. Bu öğrenme türü, sınıflandırma (örneğin, e-postaların spam olup olmadığını belirleme) ve regresyon (örneğin, konut fiyatlarını tahmin etme) gibi görevlerde sıklıkla kullanılmaktadır [54]. Denetimli öğrenmenin temel avantajı, sonuçların yorumlanabilir ve doğrulanabilir olmasıdır. Ancak en büyük dezavantajı, yüksek kaliteli ve kapsamlı etiketli veri ihtiyacıdır. Etiketleme süreci zaman alıcı ve maliyetli olmasının yanı sıra, insan kaynaklı hataları da içerebilir [55].

Denetimsiz öğrenme, veriler üzerinde herhangi bir önceden tanımlı etiket olmaksızın gerçekleştirilir. Bu yöntem, modelin verideki gizli kalıpları, yapıları veya kümeleri kendiliğinden keşfetmesini amaçlar. En yaygın denetimsiz öğrenme yöntemleri arasında kümeleme (clustering) ve boyut indirgeme (dimensionality reduction) yer alır [56]. Bu yaklaşım, etiketli veri gerektirmemesi nedeniyle maliyet açısından avantajlıdır ve büyük veri kümeleri üzerinde anlamlı yapılar keşfetmeye olanak tanır.

Isolation Forest, anomali tespitinde yaygın kullanılan denetimsiz bir makine öğrenme algoritmasıdır. Algoritma, veri noktalarını rastgele seçilen özellikler ve eşiklere göre izole eden ağaç yapıları oluşturarak çalışır. Veri noktalarının ne kadar hızlı izole edilebildiği, o noktanın ne derece anormal olduğunu belirler. Bu nedenle, anormal veriler genellikle daha kısa izolasyon yollarına sahiptir. Isolation Forest algoritması, rastgele oluşturulan ağaç yapıları aracılığıyla her bir gözlemin izolasyon derinliğini hesaplamayı temel alan bir öğrenme mekanizması kullanır [57-58].

Bu algoritma, eğitim aşamasında etiketli verilere ihtiyaç duymaz ve klasik anlamda bir test veri kümesi zorunlu değildir. Model, aynı veri kümesi üzerinde hem eğitimini tamamlayabilir hem de anomali skorları hesaplayabilir. Bu durum, denetimsiz öğrenmenin temel prensiplerinden kaynaklanmaktadır. Yani Isolation Forest, tek bir veri seti ile hem model yapısını oluşturabilir hem de aynı veri üzerinde anomalileri belirleyebilir [57].

Yapay zekâ destekli anomali tespiti süreçlerinde isolation forest algoritması ve decision_function fonksiyonunun birlikte kullanılması, sadece hangi gözlemlerin anormal olduklarının değil, aynı zamanda ne kadar anormal olduklarının anlaşılmasına yardımcı olur. Bu fonksiyon, her bir veri noktasına bir anomali skoru atar ve bu skora göre gözlemlerin ne kadar olağan dışı olduğunu sayısal olarak ifade eder. Skorlar genellikle -1 ile 0 arasında yer alır; 0'a yakın değerler normal, -1'e yakın değerler ise anormal kabul edilir. Bu metrik, sadece "anomali/normal" ayrımı yapmakla kalmaz, aynı zamanda anomalileri skorlarına göre sıralayarak daha ayrıntılı analiz yapılmasına olanak tanır. Bu da karar verme süreçlerinde daha doğru ve güvenilir adımlar atılmasını sağlar.

Isolation Forest, test verisine ihtiyaç duymamasına rağmen, modelin başarısını ölçmek için çıktıların etiketli veya sentetik verilerle karşılaştırılması yaygın bir yöntemdir. Böylelikle, anomali tespit performansı doğruluk, precision, recall ve F1 skoru gibi metriklerle nicel olarak değerlendirilebilir. Yapılan bir çalışmada, federated learning (dağıtık öğrenme) ile desteklenen Isolation Forest modeli yüksek performans göstermiştir [59]. Bu tür performans değerlendirmeleri, algoritmanın kullanım bağlamını ve pratik etkinliğini anlamak için önemlidir.

Isolation forest algoritması ve decision_function fonksiyonu birlikte kullanılarak registry anahtarlarının değişim sıklığı, uzunluğu ve yapısı, başarılı ve başarısız oturum açma ve kapatma işlemlerinin zamanları ile kullanıcı adları, dosya silme işlemlerinin

zamanları, sıklığı ve kullanıcı adları gibi verilerden olağan dışı işlemlerin tespit edilebilmesi için yapay zekâ destekli analiz yöntemi uygulanmıştır. Bu kapsamda gerçekleştirilen yapay zekâ destekli analize ilişkin bilgiler Tablo 4.4’te sunulmuştur.

Tablo 4.4. Yapay Zekâ Destekli Analiz

Veri	MITRE ATT&CK Çerçevesi
Registry anahtarlarının değişim sıklığı, uzunluğu ve yapısı	T1112 Modify Registry
Başarılı ve başarısız oturum açma ve kapatma işlemlerinin zamanları ile kullanıcı adları	T1110 Brute Force
Dosya silme işlemlerinin zamanları, sıklığı ve kullanıcı adları	T1485 Data Destruction

Kural tabanlı sistemler, yapay zekâ ile birlikte kullanıldığında çok daha güçlü ve esnek bir mekanizma ortaya çıkar. Bu iki yaklaşımın birlikte kullanımı, bilinen ve bilinmeyen tehditlerin ve olayların erken aşamada tespit edilmesini mümkün kılar.



5. CAMGÖZ YAZILIMI

Adli bilişim kapsamında Windows tabanlı sistemlerden dijital delillerin otomatik olarak elde edilmesi ve analizi kapsamında CAMGÖZ isimli yazılım tasarlanmış ve gerçekleştirilmiştir. CAMGÖZ yazılımı, ismini büyük camgöz balığından almıştır. Büyük camgöz balığı deniz suyundaki planktonları filtreleyerek beslenme ihtiyacını karşılar. Bunu yaparken saatte 2000 ton deniz suyunu filtreler ve küçük deniz canlılarıyla da beslenir. Bu balık ağzını açarak gezer. Ağzı açık gezmesinin sebebi suyu solungaçlarıyla taramasıdır. Camgöz balığının görseli Şekil 5.1’de sunulmuştur.



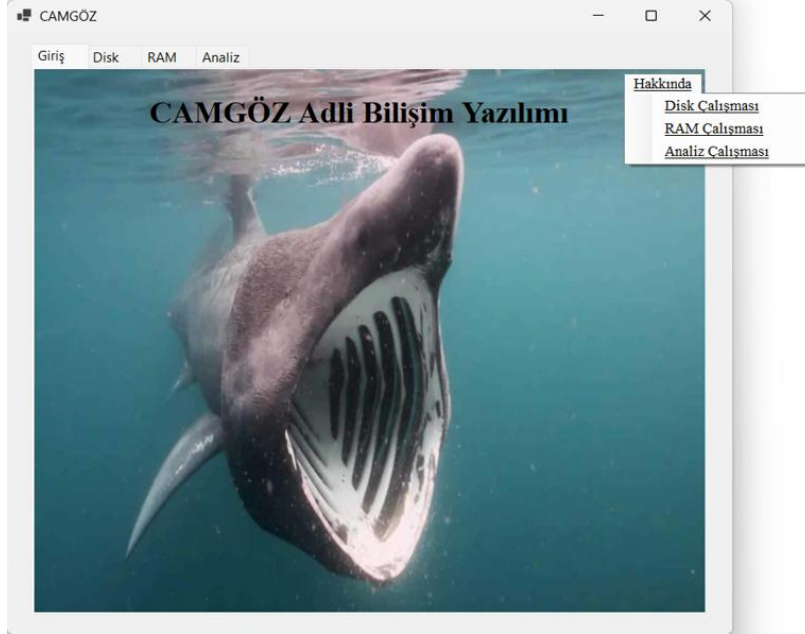
Şekil 5.1. Camgöz Balığı Görseli

CAMGÖZ yazılımı ile disk imajı ve RAM imajı üzerinden dijital deliller elde edilebilmekte ve otomatik analiz işlemleri gerçekleştirilebilmektedir. CAMGÖZ yazılımı C# programlama dilinde geliştirilmiştir. Yapay zekâ destekli analiz işlemi kapsamında Python programlama dilinde betik (script) yazılmış ve yazılıma entegre edilmiştir. Windows 10 ve üzeri ile Windows Server 2019 ve üzeri platformlarda çalışmaktadır. CAMGÖZ yazılımının açılış (giriş sekmesi) ekran görüntüsü Şekil 5.2’de sunulmuştur.



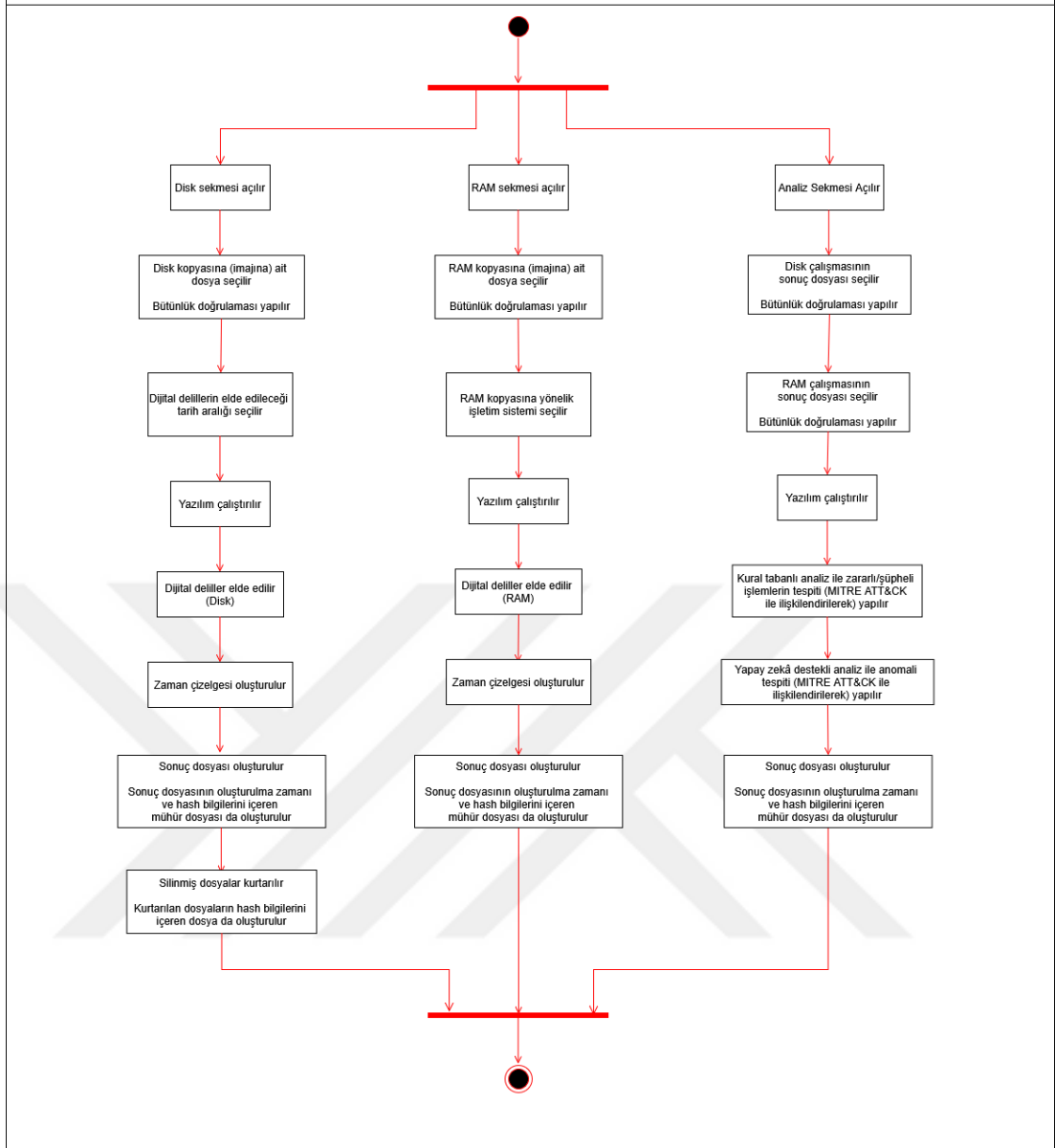
Şekil 5.2. CAMGÖZ Yazılımı Ekran Görüntüsü

Giriş sekmesinde yer alan “Hakkında” menüsündeki seçeneklerden yazılımın çalışmasına ilişkin bilgilendirme pencerelerine ulaşılmaktadır. “Hakkında” menüsünün ekran görüntüsü Şekil 5.3’te sunulmuştur.



Şekil 5.3. Hakkında Menüsü Ekran Görüntüsü

CAMGÖZ yazılımında “Disk”, “RAM” ve “Analiz” olmak üzere 3 farklı çalışma gerçekleştirilebilmektedir. Bu çalışmalara ilişkin aktivite UML diyagramı Şekil 5.4’te sunulmuştur.



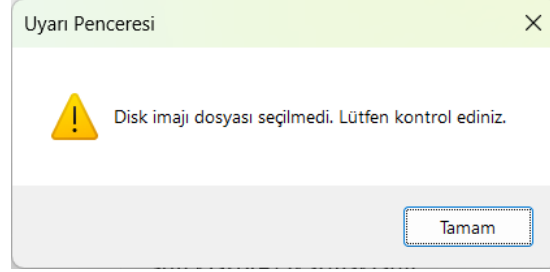
Şekil 5.4. Aktivite UML Diyagramı

CAMGÖZ yazılımı kapsamında bazı açık kaynak kodlu araçlardan faydalanılmıştır. Bunlar; disk imaj dosyasından verilerin elde edilmesi maksadıyla Velociraptor, RAM imaj dosyasından verilerin elde edilmesi maksadıyla Volatility, zaman çizelgesinin çıkarılması maksadıyla Log2timeline/Plaso, silinmiş dosyaların kurtarılması maksadıyla The Sleuth Kit araçlarıdır. Analiz bölümünde gerçekleştirilen işlemler kapsamında ise herhangi bir araçtan faydalanılmamıştır.

5.1. Disk Çalışması

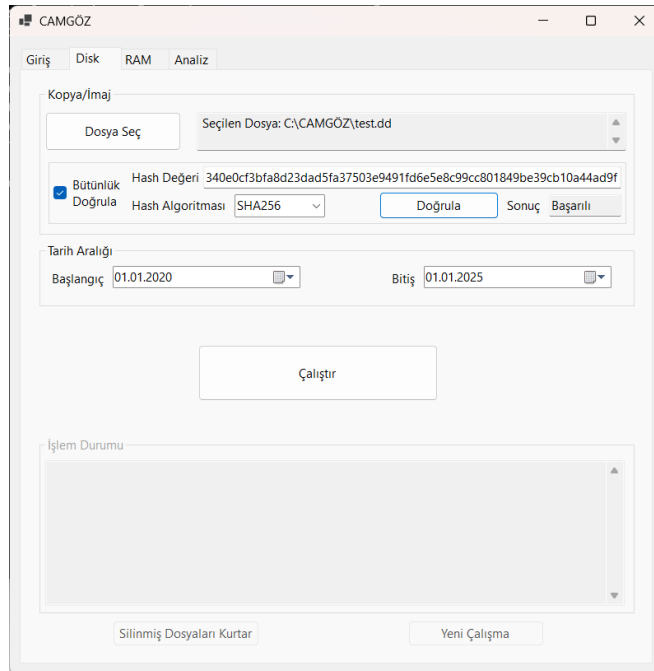
“Kopya/İmaj” bölümünde incelenmesi gereken bilgisayarın disk imaj dosyası seçilir. Disk imaj dosyası, disk imajı alma araçları ile alınan “dd”, “raw”, “img”, “vhdx”,

“vmdk”, “e01”, “001”, “ad1”, “aff” ve “bin” uzantılı dosyalardır. İmaj dosyası seçme işleminde seçilen dosyanın uzantısı kontrol edilmektedir. Seçilen dosyanın uzantısı belirtilen uzantılardan olmadığında Şekil 5.5’te yer alan uyarı alınmaktadır.



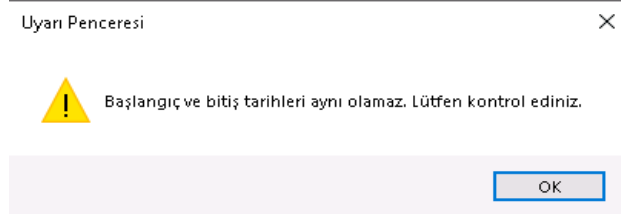
Şekil 5.5. Disk İmaj Dosyası Seçimi Uyarı Mesajı

Disk imaj dosyası seçim işleminden sonra seçilen dosyanın bütünlüğünün hash algoritmaları ile doğrulanabilmesi amacıyla “Bütünlük Doğrula” onay kutusu işaretlenir. “Bütünlük Doğrula” onay kutusunun işaretlenmesi durumunda doğrulanacak hash değerinin girilmesi, hash algoritmasının seçilmesi, “Doğrula” butonuna tıklanılması sağlanarak “Başarılı” ya da “Başarısız” sonucuna ulaşılır. Disk imaj dosyası seçme işlemi yenilenirse “Bütünlük Doğrula” onay kutusu ve bütünlük doğrulama ile ilgili bileşenler başlangıç durumuna döner. “Bütünlük Doğrula” onay kutusu işaretlenmeden de ilerlenebilir. Disk imaj dosyası işlemlerine ilişkin ekran görüntüsü Şekil 5.6’da sunulmuştur.



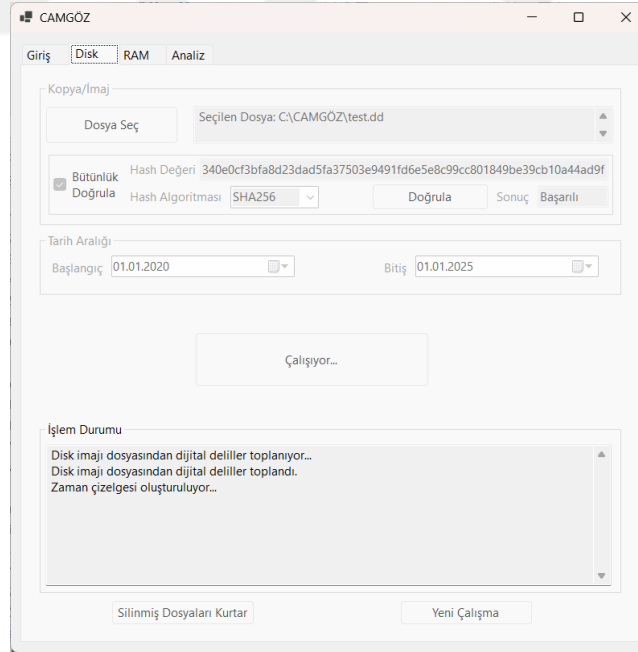
Şekil 5.6. Disk İmaj Dosyası İşlemleri

Müteakiben incelemenin yapılacağı tarih aralığı “Tarih Aralığı” bölümünden seçilir. “Tarih Aralığı” bölümündeki “Başlangıç” ve “Bitiş” alanları, CAMGÖZ yazılımının çalıştırıldığı/başlatıldığı andaki gün.ay.yıl şeklinde otomatik olarak ayarlanır. İncelemenin yapılacağı başlangıç ve bitiş tarihleri girilir. CAMGÖZ yazılımı tarafından başlangıç ve bitiş tarihlerinin aynı olması durumu kontrol edilir, aynı olması durumunda Şekil 5.7’de yer alan uyarı alınmaktadır.



Şekil 5.7. Tarih Aralığı Seçimi Uyarı Mesajı

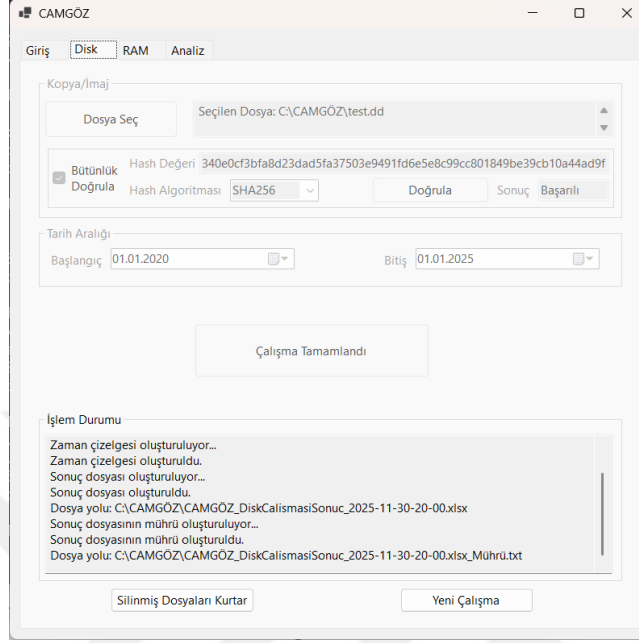
Tarih aralığı seçildikten sonra ise “Çalıştır” butonuna tıklanır ve aktif olan “İşlem Durumu” bölümünden işlemler takip edilir. “Kopya/İmaj” ve “Tarih Aralığı” bölümleri pasif olur. “Çalıştır” butonuna tıklandıktan sonra oluşan ekran görüntüsü Şekil 5.8’de sunulmuştur.



Şekil 5.8. Disk Çalışması Ekran Görüntüsü

“Çalıştır” butonuna tıklandıktan sonra butonun üzerinde işlemlerin devam ettiğini belirten “Çalışıyor...” ifadesi yer almaktadır. Ayrıca bahse konu buton pasif olmaktadır.

CAMGÖZ yazılımının çalışması esnasında “İşlem Durumu” bölümünde o anda yürütülen işleme dair bilgi verilmektedir. Çalışmanın tamamlandığını gösteren ekran görüntüsü Şekil 5.9’da sunulmuştur.



Şekil 5.9. Disk Çalışmasının Tamamlanması

Toplanan dijital deliller kronolojik olarak sıralanarak zaman çizelgesi oluşturulmaktadır. İşlem tamamlandığında csv dosya formatında zamancizelgesi.csv dosyası üretilmektedir. Olay zaman çizelgesinin çıkarıldığı zamancizelgesi.csv dosyası, Şekil 5.10’da sunulan kategorilere göre renklendirilmiş formatta bulunan excel dosyasına taşınır ve “CAMGÖZ_DiskÇalışmasıSonuç_yyyy-MM-dd-HH-mm.xlsx” isim formatında (yyyy:yıl, MM:ay, dd:gün, HH:saat, mm:dakika) sonuç dosyası ile sonuç dosyasının oluşturulma zamanını ve hash (SHA256) bilgilerini içeren “CAMGÖZ_DiskÇalışmasıSonuç_yyyy-MM-dd-HH-mm_Mührü.txt” isim formatında mühür dosyası oluşturulur.

	A	B	C	D	E	F
1	FILE OPENING					
2	WEB HISTORY					
3	DELETED DATA					
4	EXECUTION					
5	DEVICE or USB USAGE					
6	FOLDER OPENING					
7	LOG FILE					
8						

Şekil 5.10. Disk Çalışması Sonuç Dosyası Renk Kategorileri

Sonuç dosyası, dijital delillerin olay akışına göre görünürlüğünü artırmak ve araştırmacıya kolaylık sağlamak üzere tasarlanmış olup, dijital deliller kategorilerine göre renklendirilmektedir. Sonuç dosyasının ekran görüntüsü Şekil 5.11’de sunulmuştur.

date	time	timezone	MACB	source	sourcetype	type	short	desc
23.04.2020	16:01:13	UTC	M...	EVT	WinEvtX	Content Modificatic	[2820 / 0x0b04] Strings: ["Microsoft.BingTravel_8wekyb3d8bbwe\ApexTravel	[2820 / 0x0b04] Source Name: Microsoft-Windows-Immersive-Sh
23.04.2020	16:01:41	UTC	M..B	EVT	WinEvtX	Content Modificatic	[16384 / 0x4000] Strings: ["2020-04-24T16:00:40Z "RulesEngine"]	[16384 / 0x4000] Source Name: Software Protection Platform Sen
23.04.2020	16:01:41	UTC	M..B	EVT	WinEvtX	Content Modificatic	[903 / 0x0387] Strings: []	[903 / 0x0387] Source Name: Software Protection Platform Serv
23.04.2020	16:02:40	UTC	...	EVT	WinEvtX	Creation Time	[1 / 0x0001] Strings: ["{37E7572E-D68E-40E4-9DB3-595E8638955F}" "0BCB34	[1 / 0x0001] Source Name: Microsoft-Windows-Kernel-PnPConfig
23.04.2020	16:02:40	UTC	M...	EVT	WinEvtX	Content Modificatic	[1 / 0x0001] Strings: ["{37E7572E-D68E-40E4-9DB3-595E8638955F}" "0BCB34	[1 / 0x0001] Source Name: Microsoft-Windows-Kernel-PnPConfig
23.04.2020	16:02:40	UTC	M...	REG	UNKNOWN	Content Modificatic	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB\VID_04E8&P	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB\VID_
23.04.2020	16:02:40	UTC	M...	REG	UNKNOWN	Content Modificatic	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB\VID_04E8&P	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB\VID_
23.04.2020	16:02:40	UTC	..A.	REG	Registry Key : USB Entr Last Connection Tin	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB] Product: PID	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB] Prod	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB] Prod
23.04.2020	16:02:40	UTC	..A.	REG	Registry Key : USB Entr Last Connection Tin	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB] Product: PID	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB] Prod	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB] Prod
23.04.2020	16:02:40	UTC	M...	REG	UNKNOWN	Content Modificatic	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USBSTOR\Disk&V	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USBSTOR\
23.04.2020	16:02:40	UTC	M...	REG	UNKNOWN	Content Modificatic	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USBSTOR\Disk&V	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USBSTOR\
23.04.2020	16:02:40	UTC	M...	REG	UNKNOWN	Content Modificatic	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB\VID_04E8&P	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB\VID_
23.04.2020	16:02:40	UTC	M...	REG	UNKNOWN	Content Modificatic	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB\VID_04E8&P	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB\VID_
23.04.2020	16:02:41	UTC	M...	REG	UNKNOWN	Content Modificatic	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\STORAGE\Volume\{6	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\STORAGE\
23.04.2020	16:02:41	UTC	M...	REG	UNKNOWN	Content Modificatic	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\STORAGE\Volume\{6	[HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\STORAGE\

Şekil 5.11. Disk Çalışması Sonuç Dosyası Ekran Görüntüsü 1

Sonuç dosyasının Şekil 5.12’de sunulan ekran görüntüsünde belirtilen kırmızı çizgili dikdörtgen içerisinde ise toplanan dijital delillerin kronolojik olarak sıralandığı zaman çizelgesi vurgulanmaktadır.

date	time	timezone	MACB	source	sourcetype	type	short	desc
20.10.2022	18:45:59	UTC	M...	EVT	WinEvtX	Content Modificatic	[5950 / 0x173e] Strings: ["Microsoft.Reader_8wekyb3d8bbwe	[5950 / 0x173e] Source Name: Microsoft-Windows-Immersiv
20.10.2022	18:46:56	UTC	M...	REG	Registry Key : MRUList	Content Modificatic	[HKEY_CURRENT_USER\Software\Microsoft\Windows\Curre	[HKEY_CURRENT_USER\Software\Microsoft\Windows\Curre
20.10.2022	18:47:06	UTC	...	EVT	WinEvtX	Creation Time	[36887 / 0x9017] Strings: ["70"]	[36887 / 0x9017] Source Name: Schannel Strings: ["70"] Comp
20.10.2022	18:47:06	UTC	M...	EVT	WinEvtX	Content Modificatic	[36887 / 0x9017] Strings: ["70"]	[36887 / 0x9017] Source Name: Schannel Strings: ["70"] Comp
20.10.2022	18:47:06	UTC	M..B	EVT	WinEvtX	Content Modificatic	[36887 / 0x9017] Strings: ["40"]	[36887 / 0x9017] Source Name: Schannel Strings: ["40"] Comp
20.10.2022	18:47:07	UTC	..A.	WEBHIST	MSIE WebCache conta Last Access Time	URL: https://iteapps.mcafee.com/V1/app?v=S2ZDyhtVWXX0	URL: https://iteapps.mcafee.com/V1/app?v=S2ZDyhtVWXX0	URL: https://iteapps.mcafee.com/V1/app?v=S2ZDyhtVWXX0
20.10.2022	18:47:07	UTC	..A.	WEBHIST	MSIE WebCache conta Last Access Time	URL: https://iteapps.mcafee.com/V1/abt_plg_s?tr?v=k-dNj	URL: https://iteapps.mcafee.com/V1/abt_plg_s?tr?v=k-dNj	URL: https://iteapps.mcafee.com/V1/abt_plg_s?tr?v=k-dNj
20.10.2022	18:47:15	UTC		LOG	WinPrefetch	Previous Last Time f OPENWITH.EXE was run 55 time(s)		Prefetch [OPENWITH.EXE] was executed - run count 55 path:
20.10.2022	18:47:17	UTC	M..B	EVT	WinEvtX	Content Modificatic	[30800 / 0x7850] Strings: ["1" "3221226021" "1" "P"]	[30800 / 0x7850] Source Name: Microsoft-Windows-SMBClie
20.10.2022	18:47:20	UTC	MAC.	FILE	OS Content Modificatic	Content Modificatic C:\Users\Bilgisayrim\Desktop\uploads\auto\F%3A\Use...		OS-C:\Users\Bilgisayrim\Desktop\uploads\auto\F%3A\Users
20.10.2022	18:47:20	UTC		LOG	WinPrefetch	Previous Last Time f MSPAINT.EXE was run 51 time(s)		Prefetch [MSPAINT.EXE] was executed - run count 51 path: \V

Şekil 5.12. Disk Çalışması Sonuç Dosyası Ekran Görüntüsü 2

Çalıştırılan, okunan vb. dosyaların hash bilgileri dijital deliller toplanırken hesaplanarak Şekil 5.13’te gösterildiği gibi sonuç dosyasında yer almaktadır. Zararlı dosya tespit edilmesi durumunda söz konusu hash bilgileri, siber güvenlik sistemlerinde önlem alınmasına yönelik tehdit göstergesi (IoC) sağlamaktadır.

extra
sha256_hash: 5a241d571233a8388c0113fb6d8ce5078047f61c4cb85b458a28c8203ec
attribute_type: 16; file_attribute_flags: 34; file_system_type: NTFS; is_allocated: True;
attribute_type: 48; file_attribute_flags: 34; file_system_type: NTFS; is_allocated: True;
attribute_type: 48; file_attribute_flags: 34; file_system_type: NTFS; is_allocated: True;
facility: 0; message_identifier: 1073748860; recovered: False; sha256_hash: dc9c0baac
sha256_hash: 5a241d571233a8388c0113fb6d8ce5078047f61c4cb85b458a28c8203ec
sha256_hash: 5a241d571233a8388c0113fb6d8ce5078047f61c4cb85b458a28c8203ec
sha256_hash: 5a241d571233a8388c0113fb6d8ce5078047f61c4cb85b458a28c8203ec
sha256_hash: 201a9bce955ede56e3a07aff0eaf31c70d0a516691567913ead7bf38f98
attribute_type: 16; file_attribute_flags: 38; file_system_type: NTFS; is_allocated: True;
facility: 0; message_identifier: 2147489654; recovered: False; sha256_hash: dc9c0baac
sha256_hash: e761dc28d24b505a5d20ebfd971096207fee034a9ce20a9a7376eabb7ba
sha256_hash: dd72deff556db947246d7df9c1218eb851852d5de337e49c4b803a7641;
sha256_hash: dd72deff556db947246d7df9c1218eb851852d5de337e49c4b803a7641;
cache_directory_index: -2; recovered: False; sha256_hash: 1527c82103846f9beb9c704
cache_directory_index: -2; recovered: False; sha256_hash: 1527c82103846f9beb9c704
cache_directory_index: -2; recovered: False; sha256_hash: 1527c82103846f9beb9c704
cache_directory_index: -2; recovered: False; sha256_hash: 1527c82103846f9beb9c704
cache_directory_index: -2; recovered: False; sha256_hash: 1527c82103846f9beb9c704
cache_directory_index: -2; recovered: False; sha256_hash: 1527c82103846f9beb9c704

Şekil 5.13. Hash Bilgileri

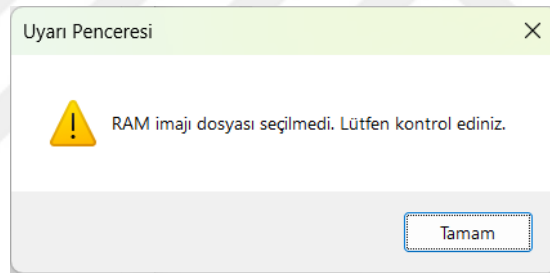
Disk çalışması neticesinde oluşturulan dosyalar Tablo 5.1’de sunulmuştur.

Tablo 5.1. Disk Çalışması Neticesinde Oluşturulan Dosyalar

Dosya Adı	Dosya Tipi
CAMGÖZ_DiskÇalışmasıSonuç_yyyy-MM-dd-HH-mm.xlsx	Excel (xlsx)
CAMGÖZ_DiskÇalışmasıSonuç_yyyy-MM-dd-HH-mm_Mührü.txt	Metin (txt)
Kurtarılan silinmiş dosyaların adları	Tümü
KurtarılanSilinmişDosyalarınHashDeğerleri.txt	Metin (txt)

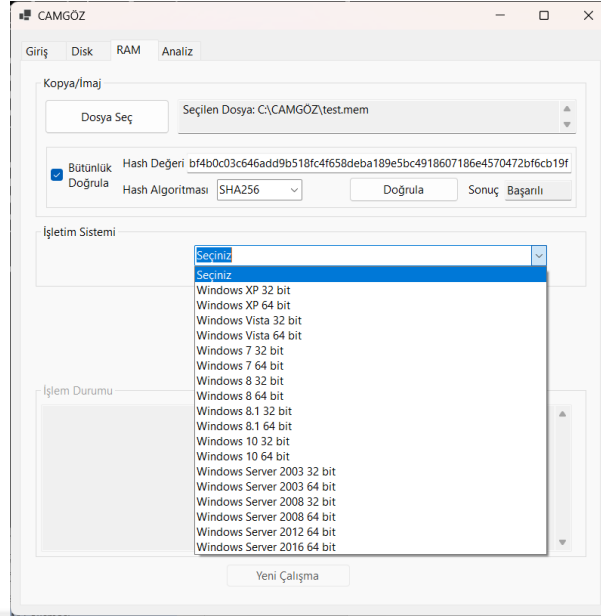
5.2. RAM Çalışması

“Kopya/İmaj” bölümünde incelenmesi gereken bilgisayarın RAM imaj dosyası seçilir. RAM imaj dosyası, RAM imajı alma araçları ile alınan “raw”, “mem”, “img”, “ram”, “dd” ve “bin” uzantılı dosyalardır. İmaj dosyası seçme işleminde seçilen dosyanın uzantısı kontrol edilmektedir. Seçilen dosyanın uzantısı belirtilen uzantılardan olmadığında Şekil 5.16’da yer alan uyarı alınmaktadır.



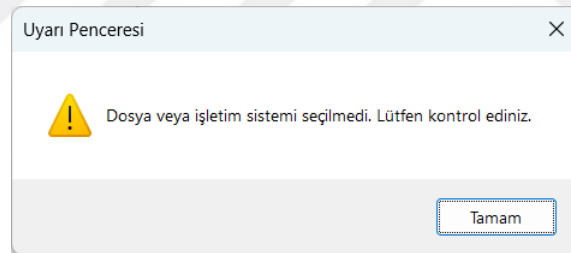
Şekil 5.16. RAM İmaj Dosyası Seçimi Uyarı Mesajı

RAM imaj dosyası seçim işleminden sonra seçilen dosyanın bütünlüğünün hash algoritmaları ile doğrulanabilmesi amacıyla “Bütünlük Doğrula” onay kutusu işaretlenir. “Bütünlük Doğrula” onay kutusunun işaretlenmesi durumunda doğrulanacak hash değerinin girilmesi, hash algoritmasının seçilmesi, “Doğrula” butonuna tıklanılması sağlanarak “Başarılı” ya da “Başarısız” sonucuna ulaşılır. RAM imaj dosyası seçme işlemi yenilenirse “Bütünlük Doğrula” onay kutusu ve bütünlük doğrulama ile ilgili bileşenler başlangıç durumuna döner. “Bütünlük Doğrula” onay kutusu işaretlenmeden de ilerlenebilir. RAM imaj dosyası işlemlerine ilişkin ekran görüntüsü Şekil 5.17’de sunulmuştur.



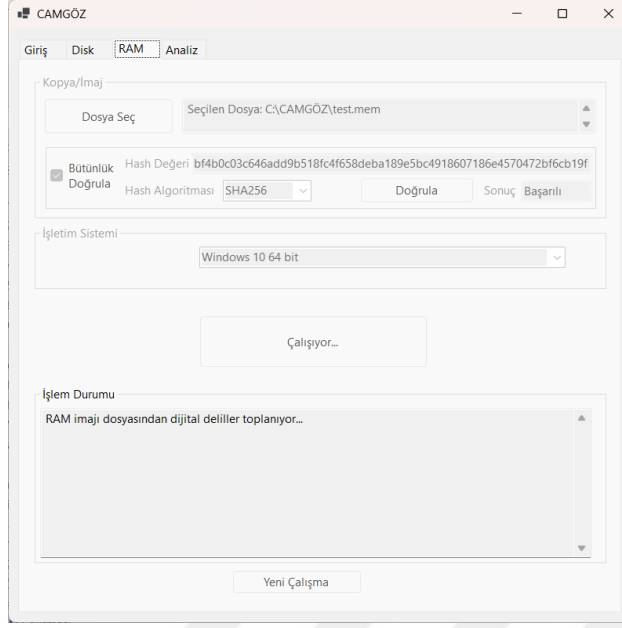
Şekil 5.17. RAM İmaj Dosyası İşlemleri

Müteakiben RAM imajının alındığı bilgisayarın işletim sistemi “İşletim Sistemi” bölümünden seçilir. İşletim sistemi seçilmemesi durumunda Şekil 5.18’de yer alan uyarı alınmaktadır.



Şekil 5.18. İşletim Sistemi Seçimi Uyarı Mesajı

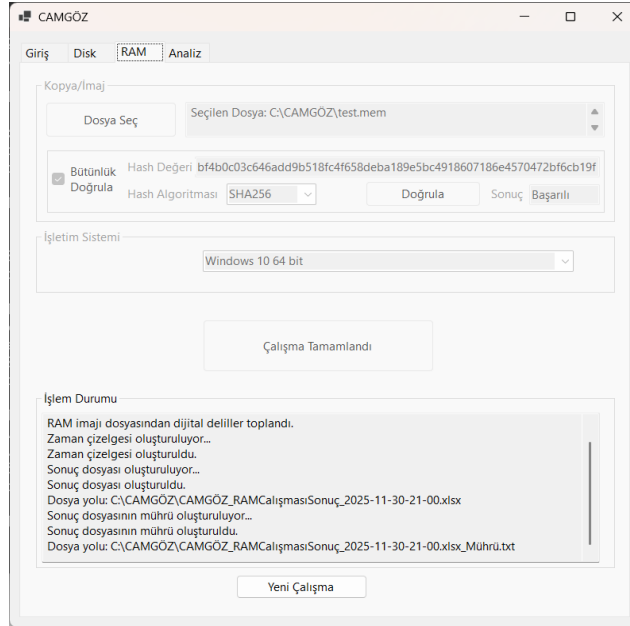
İşletim sistemi seçildikten sonra ise “Çalıştır” butonuna tıklanır ve aktif olan “İşlem Durumu” bölümünden işlemler takip edilir. “Kopya/İmaj” ve “İşletim Sistemi” bölümleri pasif olur. “Çalıştır” butonuna tıklandıktan sonra oluşan ekran görüntüsü Şekil 5.19’da sunulmuştur.



Şekil 5.19. RAM Çalışması Ekran Görüntüsü

“Çalıştır” butonuna tıklandıktan sonra butonun üzerinde işlemlerin devam ettiğini belirten “Çalışıyor...” ifadesi yer almaktadır. Ayrıca bahse konu buton pasif olmaktadır.

CAMGÖZ yazılımının çalışması esnasında “İşlem Durumu” bölümünde o anda yürütülen işleme dair bilgi verilmektedir. Çalışmanın tamamlandığını gösteren ekran görüntüsü Şekil 5.20’de sunulmuştur.



Şekil 5.20. RAM Çalışmasının Tamamlanması

Toplanan dijital delillere ilişkin csv dosyaları üretilmektedir. Söz konusu csv dosyaları bir excel dosyasında farklı sekmelerde olacak şekilde birleştirilir ve “CAMGÖZ_RAMÇalışmasıSonuç_yyyy-MM-dd-HH-mm.xlsx” isim formatında sonuç dosyası ile sonuç dosyasının oluşturulma zamanını ve hash (SHA256) bilgilerini içeren “CAMGÖZ_RAMÇalışmasıSonuç_yyyy-MM-dd-HH-mm_Mühürü.txt” isim formatında mühür dosyası oluşturulur. İşlem tamamlandığında csv dosyaları silinir. Sonuç dosyasının ekran görüntüsü Şekil 5.21’de sunulmuştur.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	*****													
2	System pid:	4												
3	Unable to read PEB for task.													
4	*****													
5	smss.exe pid:	404												
6	Command line:													
7														
8														
9	Base	Size	LoadCount	Path										
10	*****													
11	0x47610000	0x12000	0xffff											
12	0x77d00000	0x127000	0xffff	C:\Windows\system32\ntdll.dll										
13	*****													
14	csrss.exe pid:	472												
15	Command	12288	512	Windc 1	ServerDI 3	ServerDI 2	ProfileControl=Off	MaxRequestThreads=16						
16														
17														
18	Base	Size	LoadCount	Path										
19	*****													
20	0x4e130000	0x5000	0xffff	C:\Windows\system32\csrss.exe										
21	0x77d00000	0x127000	0xffff	C:\Windows\system32\ntdll.dll										
22	0x764d0000	0xf000	0xffff	C:\Windows\system32\CSRSRV.dll										
23	0x764b0000	0x13000	0x3	C:\Windows\system32\basesrv.dll										
24	0x76450000	0x60000	0x2	C:\Windows\system32\winsrv.dll										
25	0x765a0000	0x9d000	0x8	C:\Windows\system32\USER32.dll										
26	0x76bb0000	0xdb000	0x1c	C:\Windows\system32\KERNEL32.dll										
27	0x77f10000	0x4b000	0x9	C:\Windows\system32\GDI32.dll										
28	0x779d0000	0xc6000	0x12	C:\Windows\system32\ADVAPI32.dll										
29	0x77c20000	0xc3000	0x8	C:\Windows\system32\RPCRT4.dll										
30	0x76580000	0x9000	0x1	C:\Windows\system32\LPK.DLL										

Şekil 5.21. RAM Çalışması Sonuç Dosyası Ekran Görüntüsü 1

Sonuç dosyasının Şekil 5.22’de sunulan ekran görüntüsünde belirtilen kırmızı çizgili dikdörtgen içerisinde ise toplanan dijital delillerin kronolojik olarak sıralandığı zaman çizelgesi vurgulanmaktadır.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit				
2	*****													
3	0x82db0910	System	4	0	100	541	-----	0	2024-01-08 02:17:35 UTC+0000					
4	0x8454c118	smss.exe	404	4	4	28	-----	0	2024-01-08 02:17:35 UTC+0000					
5	0x84561968	csrss.exe	472	460	11	468	0	0	2024-01-08 02:17:35 UTC+0000					
6	0x84450770	csrss.exe	516	508	10	305	1	0	2024-01-08 02:17:36 UTC+0000					
7	0x84453770	wininit.exe	524	460	3	98	0	0	2024-01-08 02:17:36 UTC+0000					
8	0x84465770	winlogon.exe	552	508	3	116	1	0	2024-01-08 02:17:36 UTC+0000					
9	0x83632170	services.exe	604	524	6	250	0	0	2024-01-08 02:17:36 UTC+0000					
10	0x844bf770	lsass.exe	616	524	13	610	0	0	2024-01-08 02:17:36 UTC+0000					
11	0x844c2680	lsass.exe	624	524	10	208	0	0	2024-01-08 02:17:36 UTC+0000					
12	0x84866d50	svchost.exe	788	604	6	298	0	0	2024-01-08 02:17:42 UTC+0000					
13	0x848f53a8	svchost.exe	848	604	8	280	0	0	2024-01-08 02:17:42 UTC+0000					
14	0x848fa118	svchost.exe	884	604	15	274	0	0	2024-01-08 02:17:42 UTC+0000					
15	0x84914d90	svchost.exe	976	604	6	152	0	0	2024-01-08 02:17:42 UTC+0000					
16	0x8491bd90	svchost.exe	1000	604	45	2072	0	0	2024-01-08 02:17:42 UTC+0000					
17	0x8492a6d0	SLsvc.exe	1056	604	4	96	0	0	2024-01-08 02:17:42 UTC+0000					
18	0x84937d90	svchost.exe	1088	604	17	567	0	0	2024-01-08 02:17:42 UTC+0000					
19	0x84941d90	svchost.exe	1160	604	20	265	0	0	2024-01-08 02:17:42 UTC+0000					
20	0x84945c30	svchost.exe	1188	604	22	596	0	0	2024-01-08 02:17:42 UTC+0000					
21	0x8496e9f0	svchost.exe	1308	604	17	265	0	0	2024-01-08 02:17:43 UTC+0000					
22	0x849c18a8	spoolsv.exe	1424	604	17	291	0	0	2024-01-08 02:17:49 UTC+0000					
23	0x849d7610	armvsc.exe	1460	604	2	56	0	0	2024-01-08 02:17:49 UTC+0000					
24	0x849dc090	dns.exe	1480	604	10	164	0	0	2024-01-08 02:17:49 UTC+0000					
25	0x849e1c00	fltpbasicvsv.exe	1508	604	2	52	0	0	2024-01-08 02:17:49 UTC+0000					
26	0x849f5888	svchost.exe	1576	604	5	124	0	0	2024-01-08 02:17:49 UTC+0000					
27	0x849faad8	svchost.exe	1604	604	3	73	0	0	2024-01-08 02:17:49 UTC+0000					
28	0x849f7380	snmp.exe	1620	604	4	147	0	0	2024-01-08 02:17:49 UTC+0000					
29	0x84a0b020	vmtoolsd.exe	1640	604	7	273	0	0	2024-01-08 02:17:49 UTC+0000					
30	0x84a21d90	svchost.exe	1696	604	4	44	0	0	2024-01-08 02:17:49 UTC+0000					

Şekil 5.22. RAM Çalışması Sonuç Dosyası Ekran Görüntüsü 2

Sistem üzerinde çalışan zararlı prosesler tespit edilebilmektedir. Bu bilgiler analiz işlemlerinde kullanılmakla birlikte siber güvenlik sistemlerinde önlem alınmasına yönelik tehdit göstergesi (IoC) de sağlamaktadır. Zararlı proseslerin tespit edilmesine ilişkin sonucun ekran görüntüsü Şekil 5.23’te sunulmuştur.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Process: explorer.exe Pid: 2496 Address: 0x1790000													
2	Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE													
3	Flags: Con MemComr PrivateMe Protection: 6													
4														
5	0x01790000	b0 00 eb 70 b0 01 eb 6c b0 02 eb 68 b0 03 eb 64	...p...l...h...d											
6	0x01790010	b0 04 eb 60 b0 05 eb 5c b0 06 eb 58 b0 07 eb 54	...X...T											
7	0x01790020	b0 08 eb 50 b0 09 eb 4c b0 0a eb 48 b0 0b eb 44	...P...L...H...D											
8	0x01790030	b0 0c eb 40 b0 0d eb 3c b0 0e eb 38 b0 0f eb 34	...@...<...8...4											
9														
10	0x01790000	0x0												
11	0x01790002	eb70		JMP 0x1790074										
12	0x01790000	0x1												
13	0x01790006	eb6c		JMP 0x1790074										
14	0x01790000	0x2												
15	0x0179000a	eb68		JMP 0x1790074										
16	0x01790000	0x3												
17	0x0179000e	eb64		JMP 0x1790074										
18	0x01790010	0x4												
19	0x01790012	eb60		JMP 0x1790074										
20	0x01790010	0x5												
21	0x01790016	eb5c		JMP 0x1790074										
22	0x01790010	0x6												
23	0x0179001a	eb58		JMP 0x1790074										
24	0x01790010	0x7												
25	0x0179001e	eb54		JMP 0x1790074										

Şekil 5.23. Zararlı Proses Tespit Sonucu

Sonuç dosyasının ilk sekmesinde incelenen RAM imaj dosyasının adı, hash (SHA256) değeri, sistem tarih ve saat ayarı bilgisi, diğer sekmelerde ise toplanan dijital deliller yer almaktadır.

Çalışma tamamlandığında “Çalıştır” butonunun metin bölümü “Çalışma Tamamlandı” olarak güncellenir. Ayrıca “İşlem Durumu” bölümünün altında “Yeni Çalışma” butonu aktif olur. “Yeni Çalışma” butonu tıklanırsa RAM çalışmasının başlangıç durumuna dönlür. “Kopya/İmaj” ve “İşletim Sistemi” bölümleri ile “Çalıştır” butonu aktif olur, “Yeni Çalışma” butonu pasif olur, metin kutuları temizlenir, onay kutusu ve açılır listeler başlangıç durumuna döner.

RAM çalışması neticesinde oluşturulan dosyalar Tablo 5.2’de sunulmuştur.

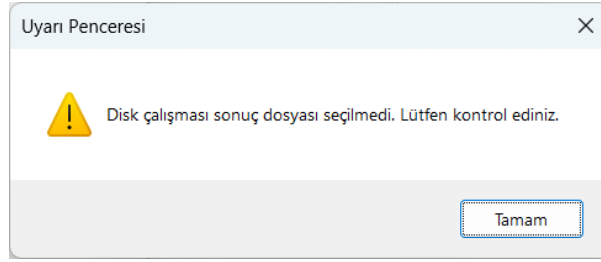
Tablo 5.2. RAM Çalışması Neticesinde Oluşturulan Dosyalar

Dosya Adı	Dosya Tipi
CAMGÖZ_RAMÇalışmasıSonuç_yyyy-MM-dd-HH-mm.xlsx	Excel (xlsx)
CAMGÖZ_RAMÇalışmasıSonuç_yyyy-MM-dd-HH-mm_Mührü.txt	Metin (txt)

5.3. Analiz Çalışması

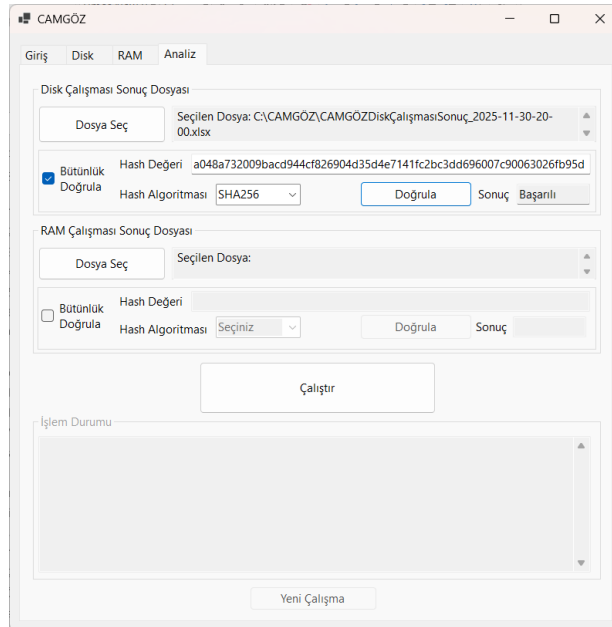
“Disk Çalışması Sonuç Dosyası” bölümünde, CAMGÖZ yazılımı tarafından disk çalışması kapsamında dijital delillerin elde edildiği dosya seçilir. Dosya seçme işleminde seçilen dosyanın uzantısının “xls” veya “xlsx” olması kontrol edilmektedir.

Seçilen dosya uzantısının belirtilen uzantılardan olmadığında Şekil 5.24'te yer alan uyarı alınmaktadır.



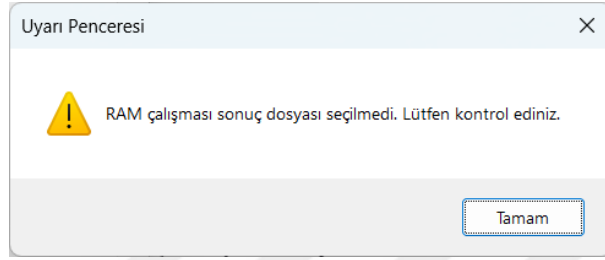
Şekil 5.24. Disk Çalışması Sonuç Dosyası Seçimi Uyarı Mesajı

Disk çalışması sonuç dosyası seçim işleminden sonra seçilen dosyanın bütünlüğünün hash algoritmaları ile doğrulanabilmesi amacıyla “Bütünlük Doğrula” onay kutusu işaretlenir. “Bütünlük Doğrula” onay kutusunun işaretlenmesi durumunda doğrulanacak hash değerinin girilmesi, hash algoritmasının seçilmesi, “Doğrula” butonuna tıklanılması sağlanarak “Başarılı” ya da “Başarısız” sonucuna ulaşılır. Disk çalışması sonuç dosyası seçme işlemi yenilenirse “Bütünlük Doğrula” onay kutusu ve bütünlük doğrulama ile ilgili bileşenler başlangıç durumuna döner. “Bütünlük Doğrula” onay kutusu işaretlenmeden de ilerlenebilir. Disk çalışması sonuç dosyası işlemlerine ilişkin ekran görüntüsü Şekil 5.25'te sunulmuştur.



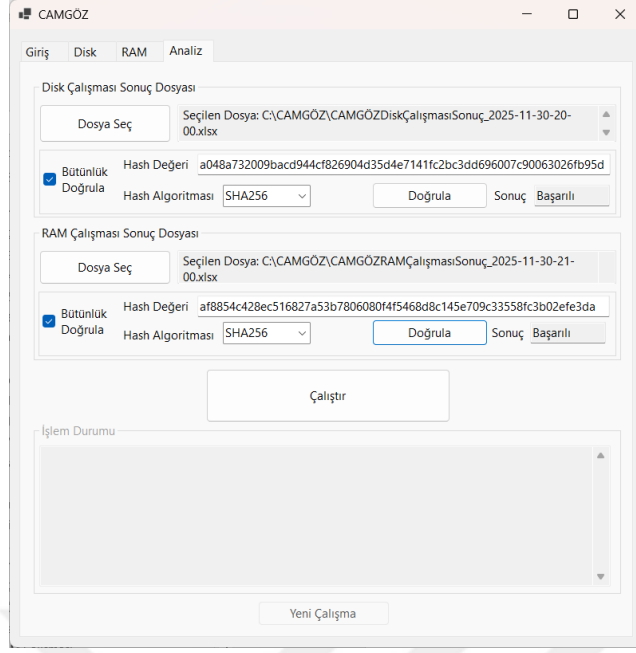
Şekil 5.25. Disk Çalışması Sonuç Dosyası İşlemleri

Analiz işlemine disk çalışması sonuç dosyası seçildikten sonra “Çalıştır” butonuna tıklanarak devam edilebilmektedir. Ancak varsa, analiz işleminde kullanılması maksadıyla “RAM Çalışması Sonuç Dosyası” bölümünde CAMGÖZ yazılımı tarafından RAM çalışması kapsamında dijital delillerin elde edildiği dosya seçilir. Dosya seçme işleminde seçilen dosyanın uzantısının “xls” veya “xlsx” olması kontrol edilmektedir. Seçilen dosya uzantısının belirtilen uzantılardan olmadığına Şekil 5.26’da yer alan uyarı alınmaktadır.



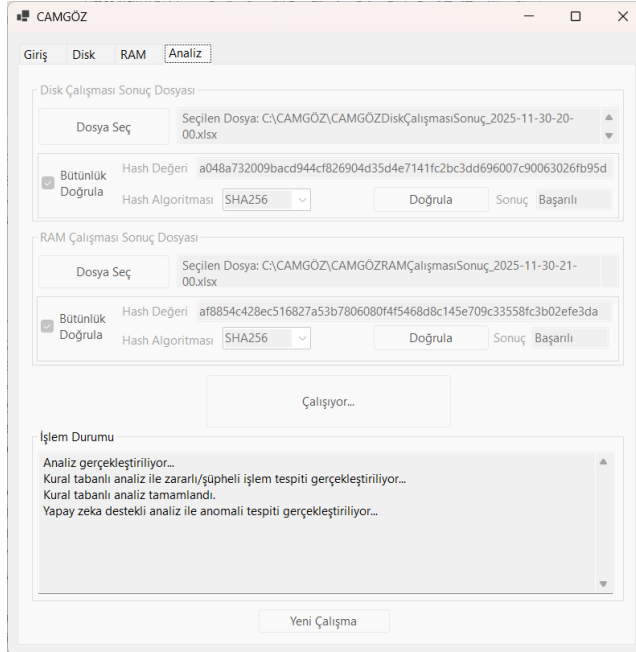
Şekil 5.26. RAM Çalışması Sonuç Dosyası Seçimi Uyarı Mesajı

RAM çalışması sonuç dosyası seçim işleminden sonra seçilen dosyanın bütünlüğünün hash algoritmaları ile doğrulanabilmesi amacıyla “Bütünlük Doğrula” onay kutusu işaretlenir. “Bütünlük Doğrula” onay kutusunun işaretlenmesi durumunda doğrulanacak hash değerinin girilmesi, hash algoritmasının seçilmesi, “Doğrula” butonuna tıklanılması sağlanarak “Başarılı” ya da “Başarısız” sonucuna ulaşılır. RAM çalışması sonuç dosyası seçme işlemi yenilenirse “Bütünlük Doğrula” onay kutusu ve bütünlük doğrulama ile ilgili bileşenler başlangıç durumuna döner. “Bütünlük Doğrula” onay kutusu işaretlenmeden de ilerlenebilir. RAM çalışması sonuç dosyası işlemlerine ilişkin ekran görüntüsü Şekil 5.27’de sunulmuştur.



Şekil 5.27. RAM Çalışması Sonuç Dosyası İşlemleri

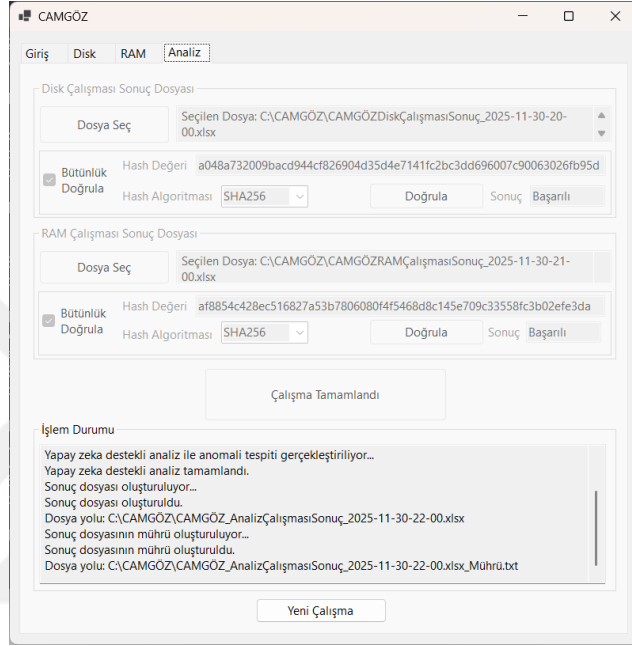
Müteakiben “Çalıştır” butonuna tıklanır ve aktif olan “İşlem Durumu” bölümünden işlemler takip edilir. “Disk Çalışması Sonuç Dosyası” ve “RAM Çalışması Sonuç Dosyası” bölümleri pasif olur. “Çalıştır” butonuna tıklandıktan sonra oluşan ekran görüntüsü Şekil 5.28’de sunulmuştur.



Şekil 5.28. Analiz Çalışması Ekran Görüntüsü

“Çalıştır” butonuna tıklandıktan sonra butonun üzerinde işlemlerin devam ettiğini belirten “Çalışıyor...” ifadesi yer almaktadır. Ayrıca bahse konu buton pasif olmaktadır.

CAMGÖZ yazılımının çalışması esnasında “İşlem Durumu” bölümünde o anda yürütülen işleme dair bilgi verilmektedir. Çalışmanın tamamlandığını gösteren ekran görüntüsü Şekil 5.29’da sunulmuştur.



Şekil 5.29. Analiz Çalışmasının Tamamlanması

Analiz çalışması kapsamında kural tabanlı analiz ile zararlı powershell komutu çalıştırma, pass the hash saldırısı, zararlı servis kurulumu, psexec çalıştırılması, Windows eventlog silinmesi, yerel alan ağına dış ağdan rdp bağlantısı, Windows olay günlüğü denetiminin devre dışı bırakılması, şüpheli zamanlanmış görev, şüpheli başarısız oturum açma, şüpheli dosya yazma, kalıcılık göstergesi, sistem tarih ve saat ayarı bilgisi, sistem tarih ve saatinin değiştirilmesi, zararlı proses bilgileri, şüpheli proses, şüpheli ağ bağlantısı, şüpheli DLL gibi hususlar; yapay zekâ destekli analiz ile registry anahtarlarının değişim sıklığı, uzunluğu ve yapısı, başarılı ve başarısız oturum açma ve kapatma işlemlerinin zamanları ile kullanıcı adları, dosya silme işlemlerinin zamanları, sıklığı ve kullanıcı adları gibi verilerden olağan dışı işlemler tespit edilmektedir.

RAM çalışması sonuç dosyası seçilmesi durumunda disk çalışmasından elde edilen dijital deliller ile RAM çalışmasından elde edilen dijital deliller ilişkilendirilerek

zararlı proseslere yönelik proses ID, proses adı, başlama zamanı, başlatan kullanıcı adı, parent proses ID, parent proses adı, ağ bağlantıları, dosya yolları gibi detaylı bilgilere ulaşılmaktadır.

Çalışma tamamlandığında, analizlere ilişkin tespitlerin farklı sekmelerde yer alacağı “CAMGÖZ_AnalizÇalışmasıSonuç_yyyy-MM-dd-HH-mm.xlsx” isim formatında sonuç dosyası ile sonuç dosyasının oluşturulma zamanını ve hash (SHA256) bilgilerini içeren “CAMGÖZ_AnalizÇalışmasıSonuç_yyyy-MM-dd-HH-mm_Mührü.txt” isim formatında mühür dosyası oluşturulur. Sonuç dosyasının ekran görüntüleri Şekil 5.30 ve Şekil 5.31’de sunulmuştur.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	MITRE ATT&CK Çerçevesi : T1059.001 Command and Scripting Interpreter: PowerShell																			
2	date	time	timezone	MACB	source	source type	type	user	host	short	desc	version	filename	inode	notes	format	extra			
3	14.01.2020	06:40:27	UTC	M..B	EVT	WinEVTX	Content M-	-	-	[4104 / 0x	[4104 / 0x2		OS:C:\Use	84442493(-		winevtx	recovered: False”; sha256_hash: 2919395f1e			
4																				
5																				
6																				
7																				
8																				
9																				
10																				
11																				
12																				
13																				
14																				
15																				
16																				
17																				
18																				
19																				
20																				
21																				
22																				
	İncelenen Dosyaların Bilgileri																			
	Zararlı Powershell Çalıştırma																			
	Pass The Hash Saldırısı																			
	Zararlı Servis Kurulumu																			
	PsEx ...																			

Şekil 5.30. Kural Tabanlı Analiz Sonucu Ekran Görüntüsü 1

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	MITRE ATT&CK Çerçevesi : T1110 Brute Force																			
2	date	time	timezone	MACB	source	source type	type	user	host	short	desc	version	filename	inode	notes	format	extra			
3	21.02.2020	17:01:37	UTC	M..B	EVT	WinEVTX	Content M-	-	-	[4625 / 0x	[4625 / 0x2		OS:C:\Use	84442493(-		winevtx	recovered: False; sha256_hash: af2853b315			
4	22.02.2020	18:01:37	UTC	M..B	EVT	WinEVTX	Content M-	-	-	[4625 / 0x	[4625 / 0x2		OS:C:\Use	84442493(-		winevtx	recovered: False; sha256_hash: af2853b315			
5	23.02.2020	19:01:37	UTC	M..B	EVT	WinEVTX	Content M-	-	-	[4625 / 0x	[4625 / 0x2		OS:C:\Use	84442493(-		winevtx	recovered: False; sha256_hash: af2853b315			
6	24.02.2020	20:01:37	UTC	M..B	EVT	WinEVTX	Content M-	-	-	[4625 / 0x	[4625 / 0x2		OS:C:\Use	84442493(-		winevtx	recovered: False; sha256_hash: af2853b315			
7	25.02.2020	21:01:37	UTC	M..B	EVT	WinEVTX	Content M-	-	-	[4625 / 0x	[4625 / 0x2		OS:C:\Use	84442493(-		winevtx	recovered: False; sha256_hash: af2853b315			
8	26.02.2020	22:01:37	UTC	M..B	EVT	WinEVTX	Content M-	-	-	[4625 / 0x	[4625 / 0x2		OS:C:\Use	84442493(-		winevtx	recovered: False; sha256_hash: af2853b315			
9																				
10																				
11																				
12																				
13																				
14																				
15																				
16																				
17																				
18																				
19																				
20																				
21																				
22																				
23																				
24																				
	Eventlog Kaydının Kapatılması																			
	Şüpheli Zamanlanmış Görev																			
	Şüpheli Başarısız Oturum Açma																			
	Şüpheli Dosya Yazma ...																			

Şekil 5.31. Kural Tabanlı Analiz Sonucu Ekran Görüntüsü 2

Yapay zekâ destekli anomali tespitine ilişkin ekran görüntüsü Şekil 5.32’de sunulmuştur.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	date	time	timezone	MACB	source	source type	type	user	host	short	desc	version	filename	inode	notes	format	extra	mitre att&ck vektörü
2	16.01.2020	22:09:48	UTC	M...	REG	UNKNOWN	Content M-	-	-	[HKEY_CU	[HKEY_CU	2	OS:C:\Use	84442493(-	winreg/wli sha256_he T1112 Modify Registry			
3	17.01.2020	21:18:23	UTC	M...	REG	UNKNOWN	Content M-	-	-	[Root\Or	[Root\Or	2	OS:C:\Use	84442493(-	winreg/wli sha256_he T1112 Modify Registry			
4	18.01.2020	21:18:23	UTC	M...	REG	UNKNOWN	Content M-	-	-	[Root\Fik	[Root\Fik	2	OS:C:\Use	84442493(-	winreg/wli sha256_he T1112 Modify Registry			
5	19.01.2020	21:27:22	UTC	M...	REG	UNKNOWN	Content M-	-	-	[Root\Fik	[Root\Fik	2	OS:C:\Use	84442493(-	winreg/wli sha256_he T1112 Modify Registry			
6	20.01.2020	21:27:22	UTC	M...	REG	UNKNOWN	Content M-	-	-	[Root\Or	[Root\Or	2	OS:C:\Use	84442493(-	winreg/wli sha256_he T1112 Modify Registry			
7	21.01.2020	08:12:35	UTC	M...	REG	UNKNOWN	Content M-	-	-	[Root\Or	[Root\Or	2	OS:C:\Use	84442493(-	winreg/wli sha256_he T1112 Modify Registry			
8	22.01.2020	15:42:37	UTC	...B	EVT	WinEVTX	Creation T-	-	-	[2005 / 0x	[2005 / 0x	2	OS:C:\Use	84442493(-	winetx recovered T1110 Brute Force			
9	23.01.2020	15:42:37	UTC	M...	EVT	WinEVTX	Content M-	-	-	[2005 / 0x	[2005 / 0x	2	OS:C:\Use	84442493(-	winetx recovered T1110 Brute Force			
10																		
11																		
12																		
13																		
14																		
15																		
16																		
17																		
18																		
19																		
20																		
21																		
22																		

Şekil 5.32. Yapay Zekâ Destekli Analiz Sonucu Ekran Görüntüsü

Sonuç dosyasının ilk sekmesinde incelenen Disk ve RAM çalışma dosyalarının adları, hash (SHA256) değerleri, sistem tarih ve saat ayarı bilgileri, diğer sekmelerde ise tespit edilen hususlar yer almaktadır.

Çalışma tamamlandığında “Çalıştır” butonunun metin bölümü “Çalışma Tamamlandı” olarak güncellenir. Ayrıca “İşlem Durumu” bölümünün altında “Yeni Çalışma” butonu aktif olur. “Yeni Çalışma” butonu tıklanırsa analiz çalışmasının başlangıç durumuna dönlür. “Disk Çalışması Sonuç Dosyası” ve “RAM Çalışması Sonuç Dosyası” bölümleri ile “Çalıştır” butonu aktif olur, “Yeni Çalışma” butonu pasif olur, metin kutuları temizlenir, onay kutuları ve açılır listeler başlangıç durumuna döner.

Analiz çalışması neticesinde oluşturulan dosyalar Tablo 5.3’te sunulmuştur.

Tablo 5.3. Analiz Çalışması Neticesinde Oluşturulan Dosyalar

Dosya Adı	Dosya Tipi
CAMGÖZ_AnalizÇalışmasıSonuç_yyyy-MM-dd-HH-mm.xlsx	Excel (xlsx)
CAMGÖZ_AnalizÇalışmasıSonuç_yyyy-MM-dd-HH-mm_Mührü.txt	Metin (txt)



6. SONUÇ VE ÖNERİLER

Adli bilişim araçlarından bazıları sistem/disk odaklı çalışırken bazıları da RAM odaklı çalışmaktadır. Özellikle açık kaynak kodlu veya ücretsiz olanlarda genellikle dijital delillerin toplanmasına ağırlık verilirken otomatik analiz hususunun arka planda kaldığı görülmektedir. Dijital delillerin toplanması, düzenlenmesi, ilişkilendirilmesi, anlamlandırılması ve analizi adli bilişim uzmanları tarafından gerçekleştirilmekte olup, uzun süreli ve maliyetli olabilmektedir. Bu çalışmada günümüzde yaygın olarak kullanılan Windows tabanlı sistemlerdeki dijital deliller/kalıntılar ve adli bilişim süreci teknik açıdan ele alınmıştır. Konuya yönelik literatür araştırması yapılmış, adli bilişim araçları incelenmiştir. Adli bilişim incelemesinin ve analizinin etkin, verimli, hızlı ve kolay bir şekilde yapılabilmesi amacıyla dijital delillerin hem disk imajı hem de RAM imajı üzerinden toplanmasını ve ilişkilendirilmesini, zaman çizelgesinin oluşturulmasını, silinmiş dosyaların kurtarılmasını, kural tabanlı analiz ile zararlı/şüpheli işlemlerin ve yapay zekâ destekli analiz ile anomalilerin tespit edilmesini otomatik olarak gerçekleştiren CAMGÖZ isimli bir yazılım geliştirilmiştir.

Adli bilişimde ve siber olay müdahalesinde Windows tabanlı sistemlere yönelik kullanılan açık kaynak kodlu ve ücretsiz araçlar ile CAMGÖZ yazılımının farkları ve benzerlikleri Tablo 6.1’de sunulmuştur.

Tablo 6.1. CAMGÖZ Yazılımının Karşılaştırılması

Kriter	KAPE	Velociraptor	Volatility	Log2timeline /Plaso	The Sleuth Kit	CAMGÖZ
Grafiksel Kullanıcı Arayüzü	+	+	-	-	-	+
Çeşitli Dijital Delillerden Zaman Çizelgesi Çıkarımı	-	+	-	+	-	+
RAM İmajından Dijital Delillerin Toplanması	-	-	+	-	-	+
Disk ve RAM İmajlarından Toplanan Dijital Delillerin İlişkilendirilmesi	-	-	-	-	-	+

Tablo 6.1. (Devamı) CAMGÖZ Yazılımının Karşılaştırılması

Kriter	KAPE	Velociraptor	Volatility	Log2timeline /Plaso	The Sleuth Kit	CAMGÖZ
Silinmiş Dosyaların Kurtarılması	-	-	-	-	+	+
Kural Tabanlı Analiz	-	+	-	-	-	+
Yapay Zekâ Destekli Analiz	-	-	-	-	-	+

Yukarıdaki tabloya göre CAMGÖZ yazılımı, belirlenen kriterlerin tamamını sağlayan başarılı bir yazılım olarak öne çıkmaktadır. CAMGÖZ ile adli bilişim incelemesinin ve analizinin etkin, verimli, hızlı ve kolay bir şekilde yapılabilmesi sağlanmıştır. Bahse konu yazılımın adli bilişim ve siber güvenlik alanında faydalı olacağı değerlendirilmektedir.

Bu çalışmada aşağıdaki sonuçlara ulaşılmıştır:

- Geliştirilen yazılım sayesinde siber olaylara müdahale ve adli bilişim açısından etkin, verimli, hızlı ve kolay bir şekilde inceleme/analiz ve aksiyon alınması sağlanmıştır.
- Geliştirilen yazılımın, grafiksel kullanıcı arayüzüne sahip olması dikkate alındığında kullanıcı dostu olduğu tespit edilmiştir.
- Windows işletim sistemi geliştikçe üzerinde bulunan dijital delillerin/kalıntıların da çeşitliliğinin arttığı görülmüştür.
- Dosya isimlerinin, hash değerlerinin ve ağ bağlantısı bilgilerinin (bağlantı kurulan IP adresleri, port numaraları) ayrıştırılarak siber tehdit istihbaratı elde edilebileceği tespit edilmiştir.
- Saldırı veya ihlalin olduğu tespit edilen bilgisayar, ağ üzerindeki bir bilgisayar ise, ağ üzerinde bulunan cihazların ve sistemlerin kayıtlarının adli bilişim incelemesine ve analizine dahil edilmesi uygun olacaktır.

Bahse konu yazılımın yetkinliğinin artırılması kapsamında:

- İşletim sistemlerine ve üzerlerinde çalışan uygulamalara ait yeni dijital delil kaynağı çıktığında geliştirilen yazılıma entegre edilmesi, yazılımın güncelliği açısından önerilmektedir.

- Geliştirilen yazılımın çalışması sonucunda zararlı veya şüpheli işlemlere ilişkin elde edilecek göstergelerin (IP adresi, hash bilgisi vb.) siber tehdit istihbaratı sistemlerine girdi olabilmesi ve diğer siber güvenlik sistemleri tarafından aksiyon alınabilmesi için siber güvenlik sistemlerine entegre edilmesi önerilmektedir.
- Geliştirilen yazılımın, güncel teknolojik gelişmeler doğrultusunda güncellenmesi etkinlik, verimlilik, performans artışı ve siber güvenlik açıklarının önlenmesi açısından önerilmektedir.





KAYNAKLAR

- [1] Lillis, D., Becker, B., O’Sullivan, T. ve Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. *Computer Law & Security Review*, 32(3), 509- 522. <https://doi.org/10.1016/j.clsr.2016.03.003>
- [2] Human Rights Center, University of California, Berkeley. (2020). *Leiden guidelines on the use of digitally derived evidence*. <https://www.law.berkeley.edu/research/hrc/leiden-guidelines/>
- [3] Allen, W. H. (2005). Computer forensics. *IEEE Security & Privacy Magazine*, 3, 59-62.
- [4] Mohammad, R. M. A. ve Alqahtani, M. (2019). A comparison of machine learning techniques for file system forensics analysis. *Journal of Information Security and Applications*, 46, 53-61. <https://doi.org/10.1016/j.jisa.2019.01.007>
- [5] Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3. baskı). Academic Press.
- [6] Albanna, F. ve Riadi, I. (2017). Forensic analysis of frozen hard drive using static forensics method. *International Journal of Computer Science and Information Security*, 15(1), 1-8.
- [7] Kolhe, M. ve Ahirao, P. (2017). Live vs dead computer forensic image acquisition. *International Journal of Computer Science and Information Technologies*, 8(3), 455–457.
- [8] Davies, S. R., Macfarlane, R. ve Buchanan, W. J. (2020). Evaluation of live forensic techniques in ransomware attack mitigation. *Forensic Science International: Digital Investigation*, 33, 300979. <https://doi.org/10.1016/j.fsidi.2020.300979>
- [9] Rahman, S. ve Khan, M. N. A. (2015). Review of live forensic analysis techniques. *International Journal of Hybrid Information Technology*, 8(2), 379-388. <https://doi.org/10.14257/ijhit.2015.8.2.35>
- [10] Henkoğlu, T. (2014). *Adli bilişim: Dijital delillerin elde edilmesi ve analizi* (2. baskı). Pusula Yayıncılık.
- [11] Shaaban, A. ve Saprionov, K. (2016). *Practical Windows forensics*. Packt Publishing Ltd.
- [12] Hassan, N. A. (2019). *Digital forensics basics: A practical guide using Windows OS*. Apress.
- [13] Easttom, C., Butler, W., Phelan, J., Bhagavatula, R. S., Steuber, S., Rodriguez, K., Balkissoon, V. I. ve Naseer, Z. (2024). *Windows forensics: Understand analysis techniques for your Windows*. Apress.
- [14] Skulkin, O. ve De Courcier, S. (2017). *Windows forensics cookbook*. Packt Publishing Ltd.

- [15] Carvey, H. (2014). *Windows forensic analysis toolkit: Advanced analysis techniques for Windows 8* (4. baskı). Syngress.
- [16] Carvey, H. (2009). *Windows forensic analysis DVD toolkit* (2. baskı). Syngress.
- [17] Pittman, R. D. ve Shaver, D. (2010). Windows forensic analysis. E. Casey (Ed.), *Handbook of digital forensics and investigation* (ss. 209-300) içinde. Academic Press.
- [18] Singh, A., Sharma, P. ve Sharma, S. (2016). A novel memory forensics technique for Windows 10. *Journal of Network and Information Security*, 4(2), 45-52.
- [19] Patil, D. N. ve Meshram, B. B. (2017). Extraction of forensic evidences from Windows volatile memory. *2017 2nd International Conference for Convergence in Technology (I2CT)* içinde (ss. 421-425). IEEE. <https://doi.org/10.1109/I2CT.2017.8075742>
- [20] Ligh, M. H., Case, A., Levy, J. ve Walters, A. (2014). *The art of memory forensics: Detecting malware and threats in Windows, Linux, and Mac memory*. John Wiley & Sons.
- [21] Dija, S. ve Fernandez, A. R. (2024). RAM forensics of various versions of Windows OS systems. *International Research Journal of Engineering and Technology*, 11(12), 1297-1303.
- [22] Baryamureeba, V. ve Tushabe, F. (2004). The enhanced digital investigation process model. *Digital Forensic Research Workshop (DFRWS 2004)*, Baltimore, ABD.
- [23] Casey, E. (2004). A model for processing and examining digital evidence. *International Journal of Digital Evidence*, 3(1).
- [24] Oğuz, R. ve Eryiğit, R. (2024). Yeni adli bilişim inceleme süreci (YABİS). *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 36(2), 717-724. <https://doi.org/10.35234/fumbd.1430113>
- [25] Nelson, B., Phillips, A. ve Enfinger, F. (2009). *Guide to computer forensics and investigations* (4. baskı). Course Technology.
- [26] Ceylan, R. ve Şirikçi, A. S. (2011). Bilişim teknolojileri incelemeleri - Veri incelemeleri. *Adli bilimler* (Cilt 2, ss. 152-174) içinde. Jandarma Kriminal Daire Başkanlığı Yayınları.
- [27] Garza, D. (2010). Data acquisition and duplication. D. Garza (Ed.), *Computer forensics: Investigating data & image files* (ss. 65-94) içinde. EC-Council.
- [28] Carvey, H. (2016). *Windows registry forensics: Advanced digital forensic analysis of the Windows registry* (2. baskı). Syngress.
- [29] Ramani, A. ve Dewangan, S. K. (2014). Auditing Windows 7 registry keys to track traces left out in copying files to external USB devices. *International Journal of Computer Science*, 5(2), 1045-1052.
- [30] freeCodeCamp. (2024, 14 Mayıs). *What is a file system? Types of computer file systems and how they work*. <https://www.freecodecamp.org/news/file-systems-architecture-explained/>

- [31] Alazab, M. ve Watters, P. (2009). Digital forensic techniques for static analysis of NTFS images. *4th International Conference on Information Technology (ICIT 2009)* içinde (ss. 1-10). IEEE.
- [32] Carvey, H. (2018). *Windows forensic analysis* (4. baskı). Syngress.
- [33] Singh, B. ve Singh, U. (2016). Leveraging the Windows Amcache.hve file in forensic investigations. *Journal of Digital Forensics, Security and Law*. <https://doi.org/10.15394/jdfsl.2016.1429>
- [34] Shashidhar, N. ve Novak, D. (2015). Digital forensic analysis on prefetch files. *International Journal of Information Security Science*, 4(2), 39-49.
- [35] Kahvedžić, D. ve Kechadi, T. (2008). Extraction of user activity through comparison of Windows restore points. *6th Australian Digital Forensics Conference* içinde (ss. 98-112). Perth, Avustralya.
- [36] Walters, A. ve Carvey, H. (2016). *Windows registry forensics* (2. baskı). Syngress.
- [37] Du, J. ve Li, J. (2016). Analysis of the structure of SAM and cracking passwords based on Windows operating system. *International Journal of Future Computer and Communication*, 5(2), 455-464. <https://doi.org/10.18178/ijfcc.2016.5.2.455>
- [38] Zhu, S. ve Ricci, F. (2018). Interaction based context aware travel recommendation. B. Stangl ve J. Pesonen (Ed.), *Information and Communication Technologies in Tourism 2018* (ss. 251-263) içinde. Springer Cham. https://doi.org/10.1007/978-3-319-72923-7_20
- [39] Google Code Archive. (2024, 20 Mayıs). *trriage-ir*. <https://code.google.com/archive/p/triage-ir/>
- [40] Singh, B. ve Singh, U. (2016). A forensic insight into Windows 10 jump lists. *Digital Investigation*, 17. <https://doi.org/10.1016/j.diin.2016.02.001>
- [41] Carvey, H. (2018). *Windows forensic analysis toolkit* (4. baskı). Syngress.
- [42] Altheide, C. ve Carvey, H. (2011). *Digital forensics with open source tools*. Syngress.
- [43] Dimitriadis, A., Ivezic, N., Kulvatunyou, B. ve Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. *Array*, 5, 100015.
- [44] Quick, D., Tassone, C. ve Choo, K. K. R. (2014). Forensic analysis of Windows thumbcache files. *20th Americas Conference on Information Systems (AMCIS 2014)* içinde (s. 990).
- [45] Leschke, T. R. (2010). *Cyber dumpster-diving: \$Recycle.Bin forensics for Windows 7 and Windows Vista*. Forensic Computer Engineer.
- [46] Carvey, H. (2007). *Windows forensic analysis DVD toolkit*. Syngress.
- [47] Kornblum, J. D. (2007). Using every part of the buffalo in Windows memory analysis. *Digital Investigation*. <https://doi.org/10.1016/j.diin.2006.12.002>
- [48] Şirikçi, A. S. ve Cantürk, N. (2013). Adli bilişim incelemelerinde birebir kopya alınmasının önemi. *Bilişim Teknolojileri Dergisi*, 5(3), 29-34.

- [49] Mehmood, R. ve Ahmad, Z. (2024). Live memory forensic: Capture and analyzing volatile data. *International Journal for Electronic Crime Investigation*, 8(3). <https://doi.org/10.54692/ijeci.2024.0803208>
- [50] Velocidex. (2025). *Rules - SANS Triage*. <https://triage.velocidex.com/docs/windows.triage.targets/rules/>
- [51] Perlroth, N. (2021, 15 Kasım). Alan Paller, a mover on cybersecurity threat, is dead at 76. *The New York Times*. <https://www.nytimes.com/2021/11/15/technology/alan-paller-dead.html>
- [52] Russinovich, M. E., Solomon, D. A. ve Ionescu, A. (2017). *Windows internals* (7. baskı). Microsoft Press.
- [53] Mandia, K., Proise, C. ve Pepe, M. (2014). *Incident response and computer forensics* (3. baskı). McGraw-Hill.
- [54] Alasu, S. ve Talu, M. F. (2024). Bilgisayarlı görüde öz-denetimli öğrenme yöntemleri üzerine bir inceleme. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 12(2), 1136-1165. <https://doi.org/10.29130/dubited.1201292>
- [55] Lifewire. (2023, 18 Temmuz). *Supervised vs. unsupervised learning: What's the difference?* <https://www.lifewire.com/supervised-vs-unsupervised-learning-7555685>
- [56] Odaibo, S. G. (2019). Is “unsupervised learning” a misconceived term? *AI & Society*. <https://doi.org/10.1007/s00146-019-00886-0>
- [57] Liu, F. T., Ting, K. M. ve Zhou, Z.-H. (2008). Isolation Forest. *2008 Eighth IEEE International Conference on Data Mining* içinde (ss. 413-422). IEEE. <https://doi.org/10.1109/ICDM.2008.17>
- [58] Cao, Y., Xiang, H., Zhang, H., Zhu, Y. ve Ting, K. M. (2025). Anomaly detection based on isolation mechanisms: A survey. *Machine Intelligence Research*, 22(5), 849-865. <https://doi.org/10.1007/s11633-025-1554-4>
- [59] Vasiljevic, P., Matic, M. ve Popovic, M. (2025). Federated isolation forest for efficient anomaly detection on edge IoT systems. *arXiv*. <https://doi.org/10.48550/arXiv.2506.05138>

