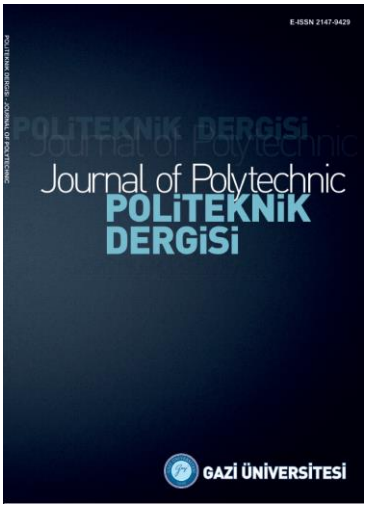


POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)
URL: http://dergipark.org.tr/politeknik

Effective management of rapid intervention, investigation, analysis and reporting processes in computer crimes with new-generation digital forensic methods

Bilgisayarla işlenen suçlara hızlı müdahale, inceleme, analiz ve raporlama süreçlerinin yeni nesil adli bilişim yöntemleri ile etkin yönetimi

***Authors (Yazarlar)**: Abdulkerim Oğuzhan ALKAN[1], İbrahim Alper DOĞRU[2], İsmail ATACAK[3]*

ORCID[1]: 0000-0003-3505-196X

ORCID[2]: 0000-0001-9324-7157

ORCID[3]: 0000-0002-6357-0073

To cite to this article: Alkan A. O., Doğru İ. A. ve Atacak İ., "Effective management of rapid intervention, investigation, analysis and reporting processes in computer crimes with new-generation digital forensic methods", ***Politeknik Dergisi***, *(*): *, (*).

Bu makaleye şu şekilde atıfta bulunabilirsiniz: Alkan A. O., Doğru İ. A. ve Atacak İ., "Effective management of rapid intervention, investigation, analysis and reporting processes in computer crimes with new-generation digital forensic methods", ***Journal of Polytechnic***, *(*): *, (*).

To link to this article (Erişim linki): http://dergipark.org.tr/politeknik/archive

DOI: **10.2339/politeknik.1255535**

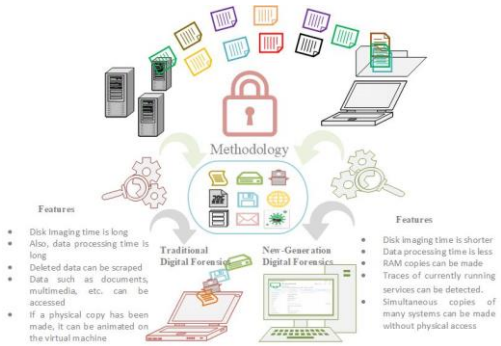
Effective Management of Rapid Intervention, Investigation, Analysis and Reporting Processes in Computer Crimes with New-Generation Digital Forensic Methods

Highlights

- *Saldırı vektörlerinin hacminde ve hızındaki büyüme / The exponential growth in volume and speed of attack vectors.*
- *Adli bilişim açısından geleneksel ve yeni nesil yaklaşımlar / Traditional and new-generation approaches in terms of digital forensics.*
- *Binalyze AIR ve Binalyze Tactical yazılımları kullanılarak yeni nesil adli bilişim teknikleri. / New-generation digital forensic methods using Binalyze AIR and Binalyze Tactical software.*

Graphical Abstract

Nowadays, the increase in cyber-attacks on personal and corporate basis has brought about an important need for rapid response to incidents, investigation, analysis and reporting processes in terms of security. In this sense, it is seen that the new-generation digital forensic approaches are quite successful compared to traditional ones.



Şekil. Metoloji / **Figure.** Methodolgy

Aim

In this study, it is aimed to reveal the effectiveness of new-generation digital forensic methods (Binalyze AIR and Binalyze Tactical software) in response to computer-based crimes in terms of fast and reliable performance of evidence collection, analysis and reporting processes.

Design & Methodology

Methodologically, both Binalyze AIR and Binalyze Tactical software, known as the new-generation digital forensic tools, and a traditional method including classical evidence collection processes on a computer are discussed. With these tools and the traditional method, a number of performance results are obtained for comparison purposes by analyzing the processes that involve collecting only evidentiary documents, taking hashes, copying and creating preliminary reports in the incident response process.

Originality

Traditional digital forensics and new-generation digital forensics are practiced, which can evaluate different types of evidence and work on the endpoint details at the same time.

Findings

The evaluation process was carried out by comparing all the statistics obtained for traditional and new-generation digital forensic methods.

Conclusion

It has been revealed that the new-generation digital forensic methods are more advantageous than traditional ones. In this context, it has been seen that the new-generation methods proposed within the scope of the study will be able to produce more effective results in the evidence gathering and reporting process in the incident response.

Declaration of Ethical Standards

The authors of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

Effective Management of Rapid Intervention, Investigation, Analysis and Reporting Processes in Computer Crimes with New-Generation Digital Forensic Methods

Research Article / Araştırma Makalesi

Abdulkerim Oğuzhan ALKAN[1*], İbrahim Alper DOĞRU[2], İsmail ATACAK[2]

[1]Department of Computer Forensics, Graduate School of Informatics, Gazi University, Ankara, Turkey
[2]Department of Computer Engineering, Faculty of Technology, Gazi University, Ankara, Turkey

(Geliş/Received : 23.02.2023 ; Kabul/Accepted : 09.04.2023 ; Erken Görünüm/Early View : 01.02.2024)

ABSTRACT

The exponential growth in attack vector volume and speed, the rapid increase in computer crimes, and huge volumes of enterprise attack surface and data to be managed have led to the recognition that 100% prevention of breaches in individual and corporate cybersecurity is no longer a realistic expectation. With traditional digital forensic approaches, the process of collecting and creating digital evidence, such as getting the disk image, examining and reporting, can be quite time-consuming and difficult to the incident response quickly, depending on the size of the data. For example, on average, getting an image of harddisk which includes 20 terabyte capacity, takes 2 days of time. As a solution, with a special digital forensic tool such as Binalyze AIR, collecting only evidentiary documents (Disk Proof, Proof of Memory, Proof of Scanner, Proof of NTFS, Proof of Log, Proof of Network, Proof of Event Logs, Proof of WMI, Proof of Process Execution, etc.), hashing all evidence and automatically generating preliminary report will allow this process to be completed in a much shorter time. It provides effective management of crime scene investigation and fast response to computer crimes, investigation, analysis and reporting processes blocked with traditional digital forensic methods and offers an innovative solution to the scientific literature. This study presents results obtained by using new-generation digital forensic methods (Binalyze AIR and Binalyze Tactical software) in comparison with traditional digital forensic methods.

Keywords: Traditional digital forensics, new-generation digital forensics, binalyze air, binalyze tactical.

Bilgisayarla İşlenen Suçlara Hızlı Müdahale, İnceleme, Analiz Ve Raporlama Süreçlerinin Yeni Nesil Adli Bilişim Yöntemleri İle Etkin Yönetimi

ÖZ

Saldırı vektör hacmi ve hızındaki üstel büyüme, bilgisayarla işlenen suçların hızlı artışı ile kurumsal saldırı yüzeyi ve yönetilecek veri miktarının çok büyük hacimlere ulaşması, bireysel ve kurumsal siber güvenlik içinde %100 ihlal önlemenin artık gerçekçi bir beklenti olmadığının kabul edilmesine yol açmıştır. Geleneksel adli bilişim yaklaşımları ile bir olaya müdahalede kullanılacak disk imajının alınması, imajın incelenmesi ve raporlanması gibi dijital delillerin toplanma ve oluşturulma süreci, veri büyüklüğüne bağlı olarak çok zaman alıcı olabilmekte ve hızlı müdahaleyi zorlaştırabilmektedir. Ortalama 20 terabaytlık bir diskin sadece imajını almak (bir elektronik delilin kopyasının oluşturulması) 2 gün sürmektedir. Binalyze AIR gibi özel bir adli bilişim aracıyla olay yeri müdahalesinde sadece delil niteliği taşıyan belgelerin (Disk Kanıtı, Hafıza Kanıtı, Tarayıcı Kanıtı, NTFS Kanıtı, Kayıt Kanıtı, Ağ Kanıtı, Olay Günlükleri Kanıtı, WMI Kanıtı, Süreç Yürütme Kanıtı vb.) toplanması, tüm delillerin hash'ının alınması ve otomatik olarak ön raporlarının oluşturulması bu sürecin çok daha kısa bir sürede tamamlanmasına olanak sağlayacaktır. Geleneksel adli tıp yöntemleriyle bloke edilen olay yeri inceleme ve bilgisayar suçlarına hızlı müdahale, soruşturma, analiz ve raporlama süreçlerinin etkin yönetimini sağlar ve bilimsel literatüre yenilikçi bir çözüm sunar. Bu çalışmada Binalyze AIR ve Binalyze Tactical yazılımları kullanılarak yeni nesil adli bilişim yöntemleri ve geleneksel adli bilişim yöntemleri üzerine çalışmalar yapılarak elde edilen sonuçlar karşılaştırmalı olarak ortaya konulmuştur.

Anahtar Kelimeler: Geleneksel adli bilişim, yeni nesil adli bilişim, binalyze air, binalyze tactical.

1. INTRODUCTION

In large networks and corporate structures, the increase in the amount of data to petabyte levels and the increase in the number of devices connected to the network make it impossible to analyze the image of the data on the network and the analysis process that comes with it with tradational digital forensic methods. Therefore, when a breach occurs in network structures with large chunks of data, organizations need tactical tools that eliminate the inadequacies of traditional digital forensics approaches in

**Sorumlu yazar (Corresponding Author)*
e-posta : aoguzhan.alkan@gazi.edu.tr

order to conduct a rapid and effective incident response. This leads us to new-generation digital forensic methods with a tendency to blend traditional cybersecurity strategies with cyber flexibility [1], [2].

In this era where everything is digitized, criminals use modern technologies to attack countries, institutions, organizations and individuals. As a result of these attacks, intense digital forensic processes emerge. This situation increases forensic cases day by day and creates an important workload for the courts[3]. Digital forensic approaches are used in civil, administrative and criminal cases. In these cases, a smart choice of tool and the use of a correct method are vital in criminal investigations. Digital forensic computing has a close connection with human behavior. Forensic medicine provides the psychological conditions and characteristics of human behavior [4]. Behavioral evidence analysis in digital forensics helps to understand psychology and behavior according to a particular situation [5]. Investigators use a variety of tools to carry out digital forensic procedures to gain inescapable evidence against them in order to hold criminals accountable in court [6].

Digital forensic information to be used as evidence in a forensic case is obtained from different technological equipments and various computer applications. Computer applications such as software, databases, web and e-mails are sources from which can be accessed digital forensic information [7], [8]. In addition to these sources, because the computer is allowed to transmit and share the necessary information, research that reveals network information can contribute significantly to the acquisition of needed forensic information [9]. However, emerging technologies such as distributed computing and cloud computing, which are referred to as virtualized systems, can cause some difficulties in this area. Hardware devices such as memory cards, smart cards, dongles, cameras, biometric scanners, routers, pagers, printers, answering machines and GPS systems are other important sources from which digital forensic evidence can be obtained [10].

Operating system forensics is a sub-discipline of the digital forensics domain within the software forensics discipline. In fact, it performs a function that allows the retrieval of useful information from the operating system of the computer or mobile device in question [11]. An operating system (OS) is the first application to run when the computer starts. From a technical point of view, the choice of digital forensic tools for evidence examination is decided by the investigator based on the specific nature and requirements of the case. However, the file system is highly valuable in computing because all files would be corrupted without it. On a computer without a file system, there will be no clue as to where the data is placed and where the data begins and ends. Each instance of the file system has a unique size, but the underlying structure allows the file system to be processed by any copied computer [12]. It has important programming and good product support, such as extensibility to use repetitive cells and command execution languages to automate them. In general, a forensic tool that provides more features in a single product/package and multi-platform support can be identified as the tool to be used in analyzing and evaluating this process. Careful and in-depth examination of the characteristics of each tool will help researchers choose the most appropriate tool for research. Because this will save research time and effort, case investigation groups can focus on other investigations such as case preparation, evidence gathering, maintaining the chain of custody, and reporting. Digital forensic tools are shown in Table 1.1.

Table 1.1. Forensic tools.

Tools	Summary
Autopsy Sleuthkit [13]	This Kit obtains image analysis of disk and features of file discovery. These Kits are free tools and support Unix, Linux, OS X as well as Windows platforms.
Redline [14]	It helps users to find malicious activities through memory and file analysis and locate processes and drivers.
Belkasoft Evidence Center [15]	It analyzes hard drives, drive images, cloud, memory dumps, IOS, Blackberry, Android backups, GrayKey, UFED, OFB, Elcomsoft, TWRP images (aka images), JTAG, and chip dumps to analyze digital evidence.
OS Forensics [16]	It helps users identify suspicious activities and files with hash matching techniques. Supports Windows 7, Windows 8, Windows 10.
ProDiscover Basic [17]	Using this tool, investigators can collect time zone, web browsing activities, and device information via a report as needed.
XWays Forensics [18]–[20]	Much faster, finds deleted files and search hits that competitors would miss, no hardware requirements, no dependency on setting up a complex database.
Encase [21], [22]	Key features of this toolset are large scale reports, Engraving, Memory acquisition, Disk Imaging, Password Recovery.
FTK [23], [24]	It can do research on PCs, networks and mobile phones. Some key features of FTK are Network data, Data transfer, Internal viewer, Disk Imaging, Password Recovery.
Magnet Axiom [25]	Key features of this toolkit are data recovery, review of evidence from all sources, and reporting.

This study includes areas of digital forensics, available open source and proprietary analysis tools and their feature-based comparison.

2. MATERIAL AND METHOD

2.1. Digital Forensic Analysis

Digital forensic analysis, also known as computer forensic analysis, focuses on a process from the diagnosis of the data obtained as a result of the examination of the memory element, where the information consisting of the combination of information materials such as sound, image and data is stored, to the reporting. The procedure to be followed in this process is as given below.

1. Collection
2. Examination
3. Analysis
4. Reporting

Here, after the crime scene is determined, firstly, the collection of evidence begins. For this purpose, devices such as computers, hard disks and phones are seized and data is copied and images are taken. Then, these data are examined, defined and extracted. After that, the data defined and extracted are analyzed and their relationship with the incident took place is determined. In the last process, a report on the incident is prepared by evaluating the results obtained in the light of the analyzed data.

Digital forensics can be considered in different sub-domains, depending on the analysis of the devices that have the quality of evidence. These domains are given below.

- Operating systems forensic analysis [26]
- Disk and file systems forensic analysis [27], [28]
- Live memory forensic analysis [29], [30]
- Web forensic analysis [31]
- Email forensic analysis [32]
- Network forensic analysis [33], [34]
- Multimedia forensic analysis [35]
- Other

2.1.1. Operating Systems Forensic Analysis

Operating System Forensics is the process of obtaining useful information from the operating system of the computer or mobile device in question[11]. The purpose of collecting this information is to obtain empirical evidence against the perpetrator. An operating system (OS) is an application that is the first thing to run when a computer system starts up[12]. This helps examine the operating system's configuration files and output data to determine what event may have occurred. OS Forensics allows its users to identify suspicious files and activities with hash matching, driver signature comparisons, emails, memory and binary data[11]. With advanced file search and indexing, it enables users to quickly extract forensic evidence from computers and effectively manage this data. It supports Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2000, 2003, 2008, 2012 (for 32-bit and 64-bit platforms). OS Forensics is available in trial version as well as paid version. Highlights of this tool are Misnamed file search, Drive signature comparison, and Hidden disk spaces.

2.1.2. Disk and File Systems Forensic Analysis

The file system is quite valuable in computing, because without it all the files get corrupted. There will be no clue as to where the data is placed, where a particular piece of data begins and ends. Each file system instance has a unique size, but its basic structure allows any computer that supports the file system type to process it [2]. There are different file systems. Each has a different structure, logic, speed, flexibility, security, size, etc. Some file systems are designed to be used for a particular application. For example, the ISO 9660 file system was designed specifically for optical discs [4]. Different storage devices use different media that support different file systems, such as SSDs.

Another excellent example of a file system would be Random Access Memory (RAM) as a temporary file system for short-term use. Some other file systems provide file access via a network protocol such as NSF and SMB [13]. The key features of file systems are file names, directories, meta data, and space management. Analysis of the file system depends on the data contained within a partition or disk. This typically involves processing data to extract the contents of a file or recover the contents of a deleted file. File system analysis examines data on a volume (i.e. a partition or disk) and includes listing files in a directory, recovering deleted content, and viewing the contents of a sector [11].

2.1.3. Live Memory Forensic Analysis

Live memory (RAM) is a buffer between the processor and storage. It allows accessing and processing information, associated Delay Locked Loops (DLLs), identifiers, open files, decrypted data, registry, user password and events, connection, and session details [36]. RAM allows accessing data in a way that produces transparent information that is not otherwise possible [11], [27]. Thus, it can help reveal hidden processes, malware, and toolkits that try to hide information.

2.1.4. Web Forensic Analysis

Web activities are performed in a web browser, which provides an interface between the user and the Internet [37], [38]. Forensic information can be obtained from web storage log sessions, searches, and a history where all user activity is located [39]–[41]. Every OS and Browser has this method of keeping logs that can be analyzed to track down a crime [41].

2.1.5. E-mail Forensic Analysis

Communication over the internet uses e-mails as the mainstream for communication. When an e-mail is transmitted, it contains the source, content, actual sender and recipient information, date/time, protocols, and server information. E-mail forensics is the process of collecting evidence from e-mails, as e-mail is an electronic communication over the internet that carries messages to deliver files, documents, and other transaction items [42]. It can be an e-mail service, a webmail, or a local mailbox [43], [44].

2.1.6. Network Forensic Analysis

Network forensic analysis focuses on monitoring network traffic and investigating the source of the attack. The purpose of this analysis is to implement plans before a security breach occurs [4], [11], [45]. The methods used for this purpose are 'Catch if you can' and 'Stop, look and listen'. It covers identity threat, the main line that includes collecting evidence, examining data, analyzing and finalizing data, presenting analysis, and responding to attacks. Network packets can be examined using the Open Systems Interconnection (OSI) model to interpret raw data as an application-level stream.

2.1.7. Multimedia Forensic Analysis

Today users benefit from smartphones, high-bandwidth connectivity, rich media, and inexpensive storage. People use visuals, audios, videos and text on social sites. They share huge multimedia content in the form of digital formats [46]. In this contex, digital visual media is one of the most important communication tools today. Digital image analysis is the latest digital forensics trend as it confirms the history of an image by discovering, analyzing, and retrieving information about the image [47]. In addition, two more important areas in image forensics are identifying the imaging device that captured the image and detecting traces of forgery. Digital images are the target of many digital studies [48], [49]. This type of analysis looks for information about where the picture was taken and who is in the picture. Image analysis also includes examining images for shorthand evidence. Video analysis can automatically analyze video to detect and identify temporal and spatial events, while video forensic analysis compares and evaluates video on legal issues [50].

2.2. Methodology Used in Study

In today's world, storing large amounts of data on digital devices has brought about an increase in cyber attacks against them. As a result, many digital forensic methods was proposed to detect cybercriminals. In this study, we discussed two different methods among the related approaches: traditional digital forensics and new-generation digital forensics. A 1 TB hard disk drive for the traditional digital forensic method was dismounted from a computer and the hash values were obtained by taking its image on copying hardware. The digital forensic tools were used for new-generation digital forensic method.

Here, Binalyze AIR and Binalyze Tactical softwares, which are known to provide effective examination, analysis and pre-reporting against cyber threats, were preferred as new generation digital forensic tools. The both tools can create a preliminary report by taking the hash of all the evidence (Disk Evidence, Memory Evidence, Browser Evidence, NTFS Evidence, Log Evidence, Network Evidence, Event Log Evidence, WMI Evidence, Process Execution Evidence and so on), copying it, without shutting down the computer during the crime scene intervention. In addition, it can complete this process in a very short time and provides an effective management of crime scene investigation and fast response to computer crimes, investigation, analysis and reporting processes that are blocked with traditional forensic methods, and offers an innovative solution to the scientific literature. The methods used in this study were tested in the laboratory enviorement with an expert.

3. RESULTS AND DISCUSSION

In this section, the findings obtained within the scope of the laboratory study are given. The actions taken are:

- Evidence collection,
- Dismounting and imaging the disk,
- Reconciliation evaluation,
- Triage with YARA,
- Establishment of the investigation timeline,
- Removing the test computer disk and taking its image with the traditional forensic method,
- Disassembling the test computer disk and analyzing the image taken with the traditional forensic method with forensic analysis software,
- Data collection with modern forensic method on the test computer,
- Analyzing the data collected with modern forensic method on the test computer with forensic analysis software,
- Comparison of the analysis results of the image obtained with the traditional forensic method and the analysis results of the data collected with the modern forensic method,
- Correlation of obtained comparison results.

It provides a solution by hashing, copying and generating a preliminary report of all evidence (Disk Evidence, Memory Evidence, Browser Evidence, NTFS Evidence, Log Evidence, Network Evidence, Event Log Evidence, WMI Evidence, Process Execution Evidence, etc.) and completing this process in a very short time. In this study, over a computer provided, evidence was collected using the Ditto DX Fieldstation hardware for collecting

evidence with traditional forensic methods, and Binalyze AIR and Binalyze Tactical softwares for collecting evidence with new-generation digital forensic approaches. Then, the correlation process was carried out by comparing all the statistics obtained for both methods.

3.1. Image Acquisition with Traditional Digital Forensic Method

The case of the supplied computer was removed and it was seen that there was a 1 TB SATA hard disk inside. Then, in order to take images with the traditional forensic method, SATA was removed from the hard case and connected to Ditto DX Fieldstation, Tableau TD3, Tableau TD2, Tableau TD1, and EZDupe Holmes forensic copy hardware, respectively, and its physical image was taken in E01 format. The size of the image file formed as a result of the image acquisition process was found to be 417 GB in total. The screenshot of the image acquisition process using the Ditto DX Fieldstation forensic copying hardware is shown in Figure 3.1, the statistics of all the operations performed in Table 3.1 and the HASH values calculated as a result of the image acquisition process are shown in Figure 3.2.

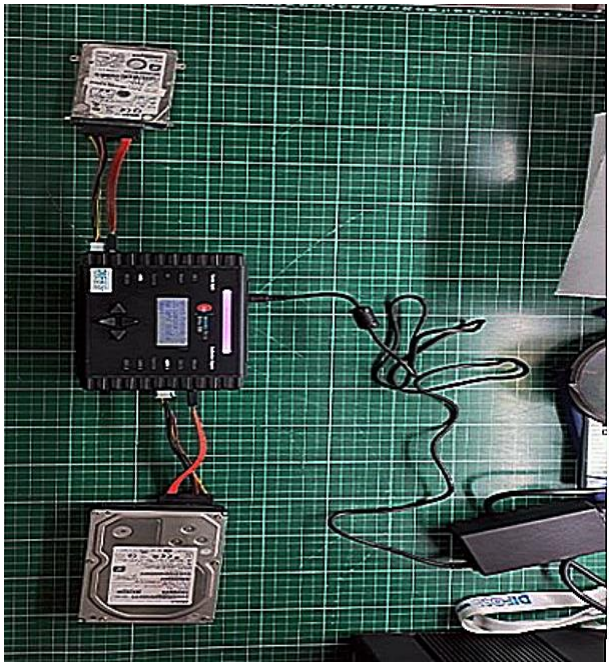


Figure 3.1. Image acquisition with traditional digital forensic method.

As explained in the previous section, Binalyze software can be run on Windows and Linux operating systems. Within the scope of this study, studies were carried out on the Windows operating system. The screenshot of the computer used for evidence collection is given in Figure 3.1.

Table 3.1. Image acquisition with traditional digital forensic method statistics.

Forensic Copy Machine	Start Time	Finish Time	Elapsed Time	MD5 HASH Value
Ditto DX FieldStation	22.03.2022 09:39	22.03.2022 11:00	1 h 21 min	1E607935E33E78AA36F9496B1BC197D5
Tableau TD3	22.03.2022 11:09	22.03.2022 12:32	1 h 23 min	1E607935E33E78AA36F9496B1BC197D5
Tableau TD2	22.03.2022 12:42	22.03.2022 14:03	1 h 21 min	1E607935E33E78AA36F9496B1BC197D5
Tableau TD1	23.03.2022 10:15	23.03.2022 11:37	1 h 22 min	1E607935E33E78AA36F9496B1BC197D5
EZ Dupe Holmes	23.03.2022 12:00	23.03.2022 13:22	1 h 22 min	1E607935E33E78AA36F9496B1BC197D5
	417 GB			

Timestamp (EET)	Type	User	Message
Mar 22, 2022 09:38:58	Physical Image	panel	Starting Physical Image E01 action from eSATA to eSATA-A, partition 1.
Mar 22, 2022 11:00:35	Physical Image	panel	Finished Physical Image E01 action.
Mar 22, 2022 11:00:35	Physical Image	panel	md5 hash value: 1E607935E33E78AA36F9496B1BC197D5
Mar 22, 2022 11:00:35	Physical Image	panel	sha1 hash value: 7730C185EA32F6CACE2256D74C9AF12A3E3529F7

Figure 3.2. Hash values of the image obtained by the traditional digital forensic method.

3.2. Data Collection with New-Generation Digital Forensic Methods

While it is powered on, an external storage disk containing the Binalyze Tactical software that can be run without installation is connected to the supplied computer. More than 150 artifact files were collected by running the file in it in order to collect data with new-generation digital forensic methods. It has been observed that the data formed as a result of the collection process is 145 MB in total.

Later, the same process was performed using Binalyze AIR software. As a result of the collection made with Binalyze AIR, it was seen that a total of 145 MB of data was collected. The screenshot of the computer used for evidence collection is given in Figure 3.3.

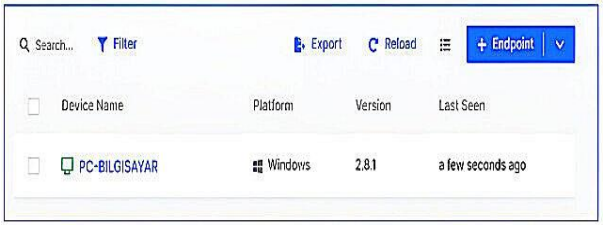


Figure 3.3. Evidence collection computer screenshot.

The screen with the information about the system and the related details is shown in Figure 3.4.

Figure 3.4. Details about the system.

The screenshot of the evidence list obtained during the evidence collection process is shown in Figure 3.5. The case summary is shown in Figure 3.6. The endpoint details are in Figure 3.7.

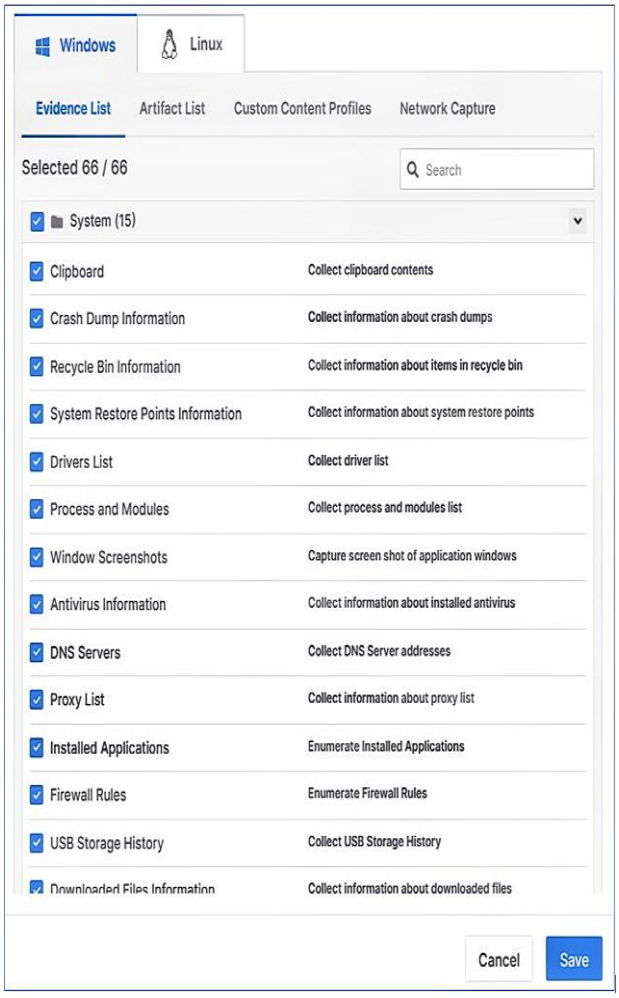


Figure 3.5. Evidence list.

Figure 3.6. Case summary

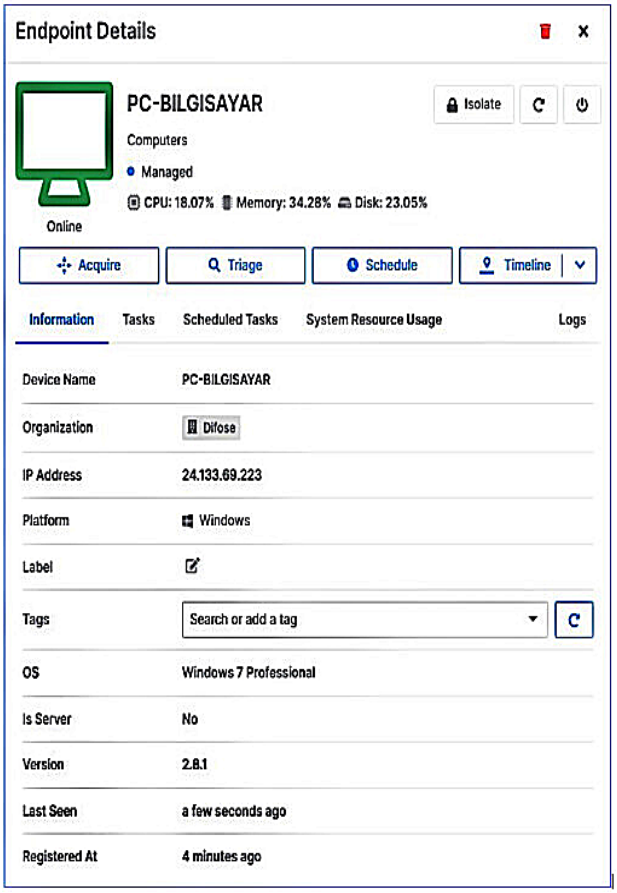


Figure 3.7. Endpoint details.

Table 3.2 shows the statistics of copies taken with the new-generation digital forensic methods.

Table 3.2. Statistics of copies taken with the new-generation digital forensic methods.

Copying Software	Start Time	Finish Time	Elapsed Time	MD5 HASH Value
Binalyze AIR	24.03.2022 10:04	24.03.2022 10:07	3min 31 sn	3718B814C051871CF5A957FA0984CB47
Binalyze Tactical	24.03.2022 10:15	24.03.2022 10:18	3min 44 sn	E0921C5284FB32EAE8AD0577BB17723C
Copy File Size (zip):			145	

3.3. Comparison of the Analysis Results of the Image Taken by the Traditional Digital Forensic Method and the Analysis Results of the Data Collected with the New-Generation Digital Forensic Methods

The E01 image taken from the computer provided for testing purposes with traditional method and the data collected by new generation methods (zip file) were analyzed using Forensic Explorer and Magnet AXIOM licensed forensic software. The number of data obtained as a result of the analysis processes and the processing times of the data is shown in Table 3.3.

Table 3.3. Analysis & process study results.

Artifact	Evidence Collected by Traditional Methods (e01)	Evidence Collected by New Generation Methods (zip)
Chrome Autofill	164	164
Chrome Cookies	1125	1125
Chrome Downloads	196	196
Chrome Keyword Search	245	245
Chrome Web History	1274	1274
Edge/Internet Explorer 10-11 Cookies	14	13
Edge/Internet Explorer 10-11 Downloads	5	5
Edge/Internet Explorer 10-11 Web History	484	202
$Logfile	7594	13416
AutoRun Items	577	577
Installed Programs	18	19
Jump Lists	333	333
Keyword Searches	18	18
LNK	1940	1932
MRU Folder Access	8	8
MRU Opened/Saved Files	67	67
MRU Recent Files & Folders	174	174
MUICache	90	78
Prefetch	472	458
Remote Desktop Records	23	23
Shellbags	206	207
Shim Cache	714	714
User Accounts	7	7
UserAssist	98	100
UsnJrnl	383938	383938
Event Logs of Windows – Firewall Events	63	63
Event Logs of Windows – Networking Events	1476	1476
Event Logs of Windows – Office Alert Events	221	221
Event Logs of Windows – Service Events	26938	26938
Event Logs of Windows – User Events	3188	3188
Total Number of Artifacts	431670	437179
Total File Size	417 GB	145 MB
Data Processing Time	1 h 45 min	1 min 43 sn

3.4 Correlation of Obtained Comparison Results

As can be seen from Table 3.3, although the image file size obtained with traditional digital forensic method is much larger, more artifacts were obtained in the analysis results from the data collected with the new-generation

digital forensic methods. The main reason for this is that with the new-generation digital forensic methods, services running in the background, processes, clipboards, and many other volatile data can be collected. In other words, while there is no difference in the number of artifacts in static data, more artifacts can be obtained from dynamic volatile data. Some of this dynamic data (especially data addressed in RAM) is lost after the computer is powered down. In conclusion, while the event being investigated in the forensic investigation is still ongoing in the system, data can be collected with new-generation digital forensic methods, enabling the ongoing process to be detected more easily and without loss.

4. CONCLUSION

New-generation digital forensics is a unique area of digital forensics that is rapid, remote, and scalable across the corporate network, pushing forensics readiness toward the center of the security stack. Since it has the ability to collect only evidentiary documents in a crime scene response, it can complete the process of hashing, copying and creating preliminary reports of this evidence in a very short time. In addition, it ensure the effective management of the processes of investigation, analysis and reporting in the rapid response to events and crimes blocked by traditional digital forensic method and, as a result, can offer an innovative solution to the scientific literature.

In this study, the evidence was collected on a provided computer by using Ditto DX Fieldstation hardware, which is used to collect evidence with traditional forensics method, and Binalyze AIR and Binalyze Tactical softwares, which are used to collect evidence with new-generation forensic methods. Then, the correlation process was carried out by comparing all the statistics obtained for both methods. Within the scope of this study, the results obtained from the interpretation of laboratory findings were stated as the advantages of each method.

4.1 Advantages of Forensic Copies Obtained by Traditional Digital Forensic Method

- Since there are unallocated areas in the imported copy, the deleted data can be scraped.
- The contents of data such as documents and multimedia can be accessed.
- If a physical copy has been made, it can be animated on the virtual machine.

4.2 Advantages of Forensic Copies Obtained with the New-Generation Digital Forensic Methods

- Copying time is shorter because the selected artifact list is copied.
- Data processing is completed in less time.
- It is possible to obtain more artifacts because RAM copies can be made.
- Since copies are made while the system is running, traces of currently running services can be detected.
- Simultaneous copies of many systems can be made without physical access.
- Automatic copying can be realized by integrating with the alarms generated by systems such as SIEM and Soar. In this way, volatile evidence is obtained without loss.

These results have shown us that the new-generation digital forensic methods are more advantageous than the traditional digital forensicmethod.

DECLARATION OF ETHICAL STANDARDS

The authors of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

AUTHORS' CONTRIBUTIONS

Abdulkerim Oğuzhan ALKAN: Used traditional and new-generation forensic methods in the study, performed the models, analysed the results and wrote the manuscript.

İbrahim Alper DOĞRU: Determined the softwares used in the study, checked the models used and observed the result obtained, analysed the results, and wrote the manuscript.

İsmail ATACAK: Checked the studies in the literature, determined the methods and softwares used, and took part in the creation of the model.

CONFLICT OF INTEREST

There is no conflict of interest in this study.

REFERENCES

[1] C. Karagiannis and K. Vergidis, "Digital evidence and cloud forensics: contemporary legal challenges and the power of disposal," ***Information***, 12(5): 181, (2021).

[2] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions," ***IEEE Access***, 10: 11065–11089, (2022).

[3] W. Ahmed, F. Shahzad, A. R. Javed, F. Iqbal, and L. Ali, "Whatsapp network forensics: Discovering the ip addresses of suspects," in *2021 11th IFIP International Conference on New Technologies, **Mobility and Security (NTMS)***, 1–7, (2021).

[4] A. Rehman Javed, Z. Jalil, S. Atif Moqurrab, S. Abbas, and X. Liu, "Ensemble adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles," ***Transactions on Emerging Telecommunications Technologies***, 33(10): 4088, (2022).

[5] N. Al Mutawa, J. Bryce, V. N. Franqueira, A. Marrington, and J. C. Read, "Behavioural digital forensics model: Embedding behavioural evidence analysis into the investigation of digital crimes," ***Digital Investigation***, 28: 70–82, (2019).

[6] M. Hina, M. Ali, A. R. Javed, F. Ghabban, L. A. Khan, and Z. Jalil, "Sefaced: Semantic-based forensic analysis and classification of e-mail data using deep learning," ***IEEE Access***, 9: 98398–98411, (2021).

[7] A. R. Javed, M. Usman, S. U. Rehman, M. U. Khan, and M. S. Haghighi, "Anomaly detection in automated vehicles using multistage attention-based convolutional neural network," ***IEEE Transactions on Intelligent Transportation Systems,*** 22(7): 4291–4300, (2020).

[8] O. Çıtlak, M. Dörterler, and İ. Doğru, "A hybrid spam detection framework for social networks," ***Politeknik Dergisi,*** 1–1, (2022).

[9] S. Sachdeva, B. L. Raina, and A. Sharma, "Analysis of digital forensic tools," ***Journal of Computational and Theoretical Nanoscience***, 17(6): 2459–2467, (2020).

[10] S. L. Garfinkel, "Digital forensics research: The next 10 years," ***digital investigation***, 7: S64–S73, (2010).

[11] C. M. da Silveira *et al.*, "Methodology for forensics data reconstruction on mobile devices with Android operating system applying in-system programming and combination firmware," ***Applied Sciences***, 10812): 4231, (2020).

[12] A. R. Javed, Z. Jalil, W. Zehra, T. R. Gadekallu, D. Y. Suh, and M. J. Piran, "A comprehensive survey on digital video forensics: Taxonomy, challenges, and future directions," ***Engineering Applications of Artificial Intelligence***, 106: 104456, (2021).

[13] R. K. M. Galvão, "Computer Forensics with The Sleuth Kit and The Autopsy Forensic Browser," ***The International Journal of FORENSIC COMPUTER SCIENCE***, 1: 41–44, (2006).

[14] B. V. Prasanthi, "Cyber forensic tools: a review," ***International Journal of Engineering Trends and Technology (IJETT)***, 41(5): 266–271, (2016).

[15] B. Popović, K. Kuk, and A. Kovačević, "Comprehensive forensic examination with Belkasoft evidence center," **in** ***International Scientific Conference**" Archibald Reiss Days", Belgrade, 2-3 October 2018*, 2: 419–433, (2018).

[16] R. Messier, *Operating system forensics*. Syngress, (2015).

[17] V. K. Sanap and V. Mane, "Comparative study and simulation of digital forensic tools," ***Int J Comput Appl***, 975: 8887, (2015).

[18] Y. I. N. Dan, "The Application of X-Ways Forensics in Digital Forensics," ***Chinese Journal of Forensic Sciences***, 05: 73.

[19] L. K. Lau, "The X-Ways Forensics Practitioner's Guide**," *The Journal of Digital Forensics, Security and Law: JDFSL***, 9(3): 59, (2014).

[20] B. Shavers and E. Zimmerman, *X-Ways Forensics Practitioner's Guide*. **Newnes**, (2013).

[21] S. Hong *et al.*, "ENCASE: An ENsemble ClASsifiEr for ECG classification using expert features and deep neural networks," in *2017 **Computing in cardiology (cinc),*** 1–4, (2017).

[22] H. Kim, N. Bruce, S. Park, and H. Lee, "EnCase forensic technology for decrypting stenography algorithm applied in the PowerPoint file," in *2016 **18th International Conference on Advanced Communication Technology (ICACT),*** 722–725, (2016).

[23] F. Carbone, *Computer forensics with FTK***. Packt Pub**., (2014).

[24] K. J. Kuchta, "Your computer forensic toolkit," ***Inf. Secur. J. A Glob. Perspect.***, 10(4): 1–12, (2001).

[25] A. Yudhana, I. Riadi, and I. Anshori, "Identification of Digital Evidence Facebook Messenger on Mobile Phone With National Institute of Standards Technology (Nist) Method," ***Jurnal Ilmiah Kursor***, 9(3), (2018).

[26] M. R. Arshad, M. Hussain, H. Tahir, S. Qadir, F. I. A. Memon, and Y. Javed, "Forensic analysis of tor browser on windows 10 and android 10 operating systems," ***IEEE Access***, 9: 141273–141294, (2021).

[27] B. Carrier, *File system forensic analysis*. **Addison-Wesley Professional**, (2005).

[28] M. Alazab, S. Venkatraman, and P. Watters, "Effective digital forensic analysis of the NTFS disk image," ***Ubiquitous Computing and Communication Journal***, 4(1): 551–558, (2009).

[29] V. L. Thing, K.-Y. Ng, and E.-C. Chang, "Live memory forensics of mobile phones," ***digital investigation***, 7: S74–S82, (2010).

[30] S. Rahman and M. N. A. Khan, "Review of live forensic analysis techniques," ***International Journal of Hybrid Information Technology***, 8(2): 379–88, (2015).

[31] A. Rasool and Z. Jalil, "A review of web browser forensic analysis tools and techniques," ***Researchpedia Journal of Computing***, 1(1): 15–21, (2020).

[32] V. K. Devendran, H. Shahriar, and V. Clincy, "A comparative study of email forensic tools**," *Journal of Information Security***, 6(2): 111, (2015).

[33] A. Yasinsac and Y. Manzano, "Honeytraps, a network forensic tool," in ***Sixth Multi-Conference on Systemics, Cybernetics and Informatics***, (2002).

[34] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," ***digital investigation,*** 7(1–2): 14–27, (2010).

[35] M. Barni, M. C. Stamm, and B. Tondi, "Adversarial multimedia forensics: Overview and challenges ahead," in *2018 **26th European signal processing conference (EUSIPCO)***, 962–966, (2018).

[36] G. R. Panigrahi, N. K. Barpanda, and S. Mishra, "A review on: The rise in cyber forensics & innovations", (2021).

[37] Ş. Şentürk, T. Apaydın, and H. Yaşar, "Image and file system support framework for a digital mobile forensics software," in *2020 **Turkish National Software Engineering Symposium (UYMS)***, 1–3, (2020).

[38] F. Faust, A. Thierry, T. Müller, and F. Freiling, "Technical report: Selective imaging of file system data on live systems," ***arXiv preprint arXiv:2012.02573***, (2020).

[39] R. Palutke, F. Block, P. Reichenberger, and D. Stripeika, "Hiding process memory via anti-forensic techniques," ***Forensic Science International: Digital Investigation***, 33: 301012, (2020).

[40] F. Block, R. Palutke, P. Reichenberger, and D. Stripeika, "Hiding Process Memory via Anti-Forensic Techniques," ***Proceedings of Black Hat Briefings** USA*, (2020).

[41] K. Hausknecht, D. Foit, and J. Burić, “RAM data significance in digital forensics,” in *2015* ***38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)***, 1372–1375, (2015).
[42] G. Varshney, P. Iyer, P. Atrey, and M. Misra, “Evading DoH via live memory forensics for phishing detection and content filtering,” in ***2021 International Conference on COMmunication Systems & NETworkS (COMSNETS)***, 1–4, (2021).
[43] R. Chiramdasu, G. Srivastava, S. Bhattacharya, P. K. Reddy, and T. R. Gadekallu, “Malicious url detection using logistic regression,” in ***2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS)***, 1–6, (2021).
[44] O. Çıtlak, M. Dörterler, and İ. A. Doğru, “A survey on detecting spam accounts on Twitter network,” ***Social Network Analysis and Mining***, 9(1): 1–13, (2019).
[45] C. Rupa, G. Srivastava, S. Bhattacharya, P. Reddy, and T. R. Gadekallu, “A machine learning driven threat intelligence system for malicious URL detection,” in ***Proceedings of the 16th International Conference on Availability, Reliability and Security***, 1–7, (2021).
[46] R. Nelson, A. Shukla, and C. Smith, “Web browser forensics in google chrome, mozilla firefox, and the tor browser bundle,” ***Digital Forensic Education: An Experiential Learning Approach***, 219–241, (2020).
[47] S. L. Garfinkel, “Digital forensics research: The next 10 years. digital investigation, 7,”, 10: S64-S73, (2010).
[48] R. U. Rahman and D. S. Tomar, “A new web forensic framework for bot crime investigation,” Forensic Science International: Digital Investigation, 33: 300943, (2020).
[49] N. Shafqat, “Forensic investigation of user’s web activity on Google Chrome using various forensic tools,” ***IJCSNS Int. J. Comput. Sci. Netw. Secur,*** 16(9): 123–132, (2016).
[50] A. Ghafarian, “An empirical analysis of email forensics tools,” ***Available at SSRN*** *3624617*, (2020).