Current Trends in Forensic Investigation through Evidence based on External Storage

Abdul Khader Jilani [†] and Shirina Samreen[††]

[†] College of Computer Studies, University of Technology, Bahrain,
[††] Department of Computer Science, College of Computer and Information Sciences, Majmaah University, Al Majmaah 11952, Saudi Arabia

Summary
The proposed research employs external storage as an evidence to provide concise information with a transparent picture about forensic analysis concerns. Thereafter, the primary concern of this selected research study was to provide appropriate information on how external storage media help the forensic department to store sensitive information in a secure location. The entire study would have justified the cause and purpose of external storage in this case as the research intent described the necessity of external storage. The main contribution of the research study was employment of an appropriate research methodology for forensic analysis based on evidence through external storage. It included steps relating to data collection, drive history, and time regarding the security incident followed by creating audit trails. The next step was adequate documentation of forensic collection activities and the use of a number of tools to analyze and write findings. In this specific study, the researcher took both processes as primary and secondary in the form of qualitative research and objective analytical procedure respectively.Specifically, a computer forensics reference dataset named as hacking case was employed and the analysis and examination process was performed on a replica copy and the Autopsy tool was used to analyze the evidence. A great deal of information was extracted through forensic analysis including the information on the device like system type, device name, domain, the number of accounts registered in this computer, name of the account that used most often, and tools used for hacking.

Keywords:
Digital Forensics; Hacking; Forensics Evidence; Autopsy Tool

1. Introduction

According to the current scenario, the inclusion of the internet has played a dominant role in different aspects and services. Following that, people are getting vivid ranges of impacts across the world. With the following time, it is noteworthy the usage of internet has increased tremendously and hence, to provide or deliver appropriate service, the research developers have found two important aspects regarding this. Both of these aspects are popular as cybersecurity and cloud computing [1]. This is because the context of rapid advancement following the technological changes has been responsible for shifting the world's perspectives towards the concept of the digital domain. On the other hand, this evaluation of rapid technological advancement leads to develop an emergence of cybercrimes that in turn, reflects upon the context of security breach incidents as an outcome.

The forensic analysis is affecting by various problems as data breach, external access, data stealing and others. The forensic information is considering as the sensitive information that needs to be collected in the storage. The information is collected in the computer device and third-party access is occurring through malware, spyware and worms. The data breach and data-stealing activity is happening that are accessing the data stored in the device [2]. The problem is occurring through the computer device where malware is existing in the system and slowly accessing all the information from the system.

The pieces of evidence are highly sensitive information that is storing in the device. The pieces of evidence are representing a criminal in the court. The pandemonium situation is happening a lack of proper information. The storage media is not providing the appropriate security in this case while the hackers are accessing all the information and modifying the data. This situation is causing a huge problem where inappropriate information is submitting in the court.

A recent research reviews the existing penetration testing methods and suggests ways for the improvement so as to have greater security. The calculation of risks using the Common Vulnerability Scoring System (CVSS) scores along with the impact on confidentiality, integrity, and availability is also done. Specifically, an approach based on Kali Linux employing a Wi-Fi penetration testing is proposed [3] as the conventional methods might not be appropriate due to technological changes.

A forensics investigation approach which is a mix of qualitative and quantitative methods is proposed [4]. It involves a scenario of a virtual environment wherein browser exploitation of the victim machine occurs. A comparison of the browsing activities between victim computer and another one in the same context helps in identifying the culprit.

Manuscript received November 5, 2022
Manuscript revised November 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.11.68

A research work in the context of mobile forensics employing a qualitative and quantitative approach wherein the classification of recovered data items from the phone's memory is proposed [5]. It performs the recovery of Facebook app and the recoverable data included text messages, login information, friend lists, and user account details.

1.1 Research Aim and Objectives

The aim of the research study is to provide a discussion on the use of external storage in forensic analysis. The research is aiming to deliver the appropriate information about how external storage media is helping the forensic department to store sensitive information in a secure place. The entire study is going to justify the reason and purpose of external storage in this case where the intention of the research is describing the necessity of external storage. The forensic information is highly sensitive and the information needs to be stored in a secure device. The external devices are playing a significant role in this case as these devices are not easy to hack or getting access.

The objective of the research is:

- Getting a clear understanding of the value of forensic information. The forensic information is highly valuable in this case where the information is taking to the courtroom to identify the criminals.
- Provide a better discussion about the significance of external storage in the forensic department. The external media is playing an important role in recent times as the external storage is more secure than storing information in a computer device.
- Forensic experts are collecting sensitive information from the criminal background and match with the pieces of evidence
- Cybercrimes are trying to access sensitive information from a computer device and steal or modify the data.

The research is going to analyze the significance of external storage that is needed in forensic analysis. It involves conducting the data collection and then storing the data into pen drive, external hard disk, memory card and others. The research is also discussing the procedures of data collection and how that can be stored in an external device. The matching information is deciding the future of the culprit in the court. Hence, the purpose of the research is to discuss the need for external storage and how the organizations are using external storage in their forensic analysis. The research study is addressing the information regarding forensic analysis and how this would be conducted with external storage usage.

This may be a difficult task to store the entire data in external devices within a short period of time. To solve the problem, there is cloud storage which is transferring data into a cloud device to store sensitive information.

2. Literature Review

In accordance with the present scenario, the researcher has noticed that the era of the possible concept of portable digital data has played a significant role as it deals with the constant exponential expansion. Following that, the researcher has noticed that global evolution has been interlinked with the concept of consumer electronics. In addition, based on the multiple evidential research papers, it is popular that there is a presence of different components that make a sense for modern digital innovation [6]. These components include the use of mobile phones, digital cameras, and portable music system, personal digital assistant or PDAs, data storage devices and many more. All these aspects have played a significant role in the rapid growth of global digital innovation. On the other hand, the researcher has obtained that most of these evaluated devices have been responsible for the inclusion of the memory cards that in turn, allow the users to make portable digital storage in an easy way as much as possible. Besides, it is known that all these evaluated components have the capabilities to incorporate a huge amount of data in accordance with the concept of non-voltaic way.

From the context of several pieces of those evidential research papers, the researcher has observed that the development, especially of the information technology infrastructure has created top-notch priority in accordance with the concept of artificial intelligence [7]. This is because the chosen component which includes the information technology infrastructure has been responsible for the inclusion of vivid ranges of elements. Based on the global concept of the digital innovation, it is noteworthy that the elements of the information technology infrastructure include the involvement of faster networking system, advanced virtualization technology and the wider distribution of the free software and many more. Consequently, all these aspects have played a crucial role in accordance with the concept of the cloud computing system.

In accordance with the present scenario, it is noted that the log of the respective cloud server has the capability to reveal different types of information about the history and the action of the potential users [8]. Therefore, the artificial intelligence team has given their immense focus on the respective security system in accordance with the concept of cloud computing and digital innovation. Besides, through the inclusion of other evidential research papers, the researcher has noticed that the through the uses of the cloud storage system, the artificial intelligence team has been responsible for gaining deep understanding of the traces that in turn, assist them in the field of forensic analysis based on the concept of digital innovation.

3. Digital Forensics Model

The given research study needs to incorporate specific models or frameworks that in turn, help the researcher to deliver an excellency with this respective study. Figure 1 depicts the digital forensic model employed. Following that, the researcher has given its immense effort to observe the outcome of the research approaches that in turn, assist the researcher to gain information about the appropriate methodology. As per the evidential research papers, it is noted that the traditional method along with the concept of law enforcement has been dealing with the search and seizure procedures, especially for the computers based on the context of crime scenes [9]. In addition, the traditional approach has been representing as the evidence facility.

Besides, the first factor representation as to the inclusion of respective actions that have been taken to the investigators in order to secure the integrity of digital evidence. Following that, the next aspect relates to appropriate conduction of respective examination procedures along with the digital evidence. The last factor has inter-linked with the seizure of activity which includes documentation, preservation and availability of the digital evidence. In addition, computers are responsible for the inclusion of the appropriate operating system, which in turn, helps the computers to operate smoothly [10]. On the other hand, the investigators have been responsible for the identification of vivid ranges of aspects regarding the aspect of volatile data along with the computer system. Consequently, these aspects are called the unencrypted data, internet protocol address, instant messages, running processes, the concept of Trojan horses and many more. In addition, to the chosen context, the researcher has noticed there is presence of other aspects in the context of volatile data. However, this type of volatile data, especially for the investigation system is extracted from the Microsoft Windows Operating system [11]. These chosen components are called open ports along with the listening applications, system information followed by registry information, current running processes in association with the logging system and many more.

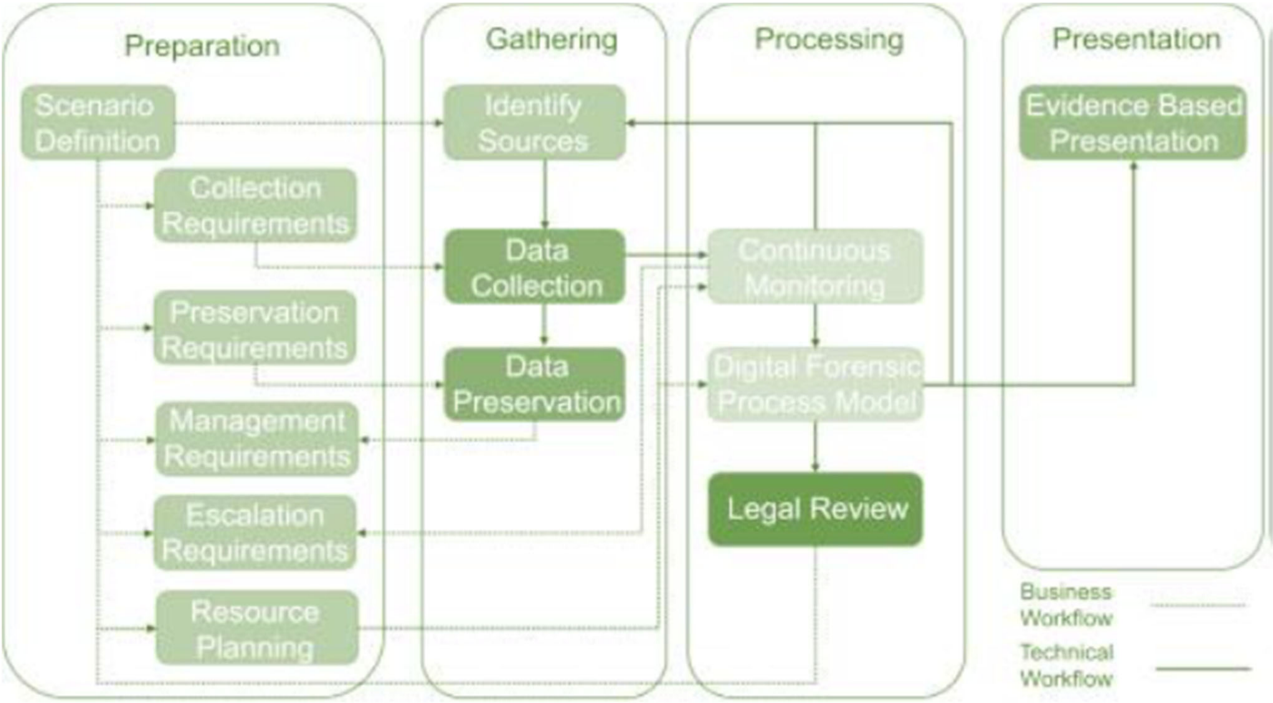


Figure 1 Digital Forensics Model

In addition, the researcher has noticed that the investigation of forensic analysis through the traditional approach has been responsible for providing its effect on law enforcement applications. Following that the raised circumstances in association with the global evaluation of digital techniques have been responsible for discovering its potential uses in a more frequent way [12]. Henceforth, it can be said that the advancement of home networking technology plays a crucial part in pushing the respect of law enforcement applications. In addition, the researcher has noticed that the evaluation of the digital crime scenes is treated trough traditional approaches during the initial times.

However, later on, the computer forensic personnel have been reported with inadequacy due to the rapid growth of digital evidence [13]. Besides, the investigators have tried to increase their crime scene investigation skills to deal with the modern challenges of electronic crimes. As per the digital innovation for forensic analysis, it is noted that there are presences of different tools based on the volatile data. In order to gain a deep understanding of the forensic analysis through the uses of volatile data, the researcher has noticed that the possible methodology, especially for this field has

been associating with the CERT training [14]. This selected training procedure has been responsible for the inclusion of a few steps which include preparation of incident along with documentation, verification of appropriate policy along a collection of proper strategy regarding the volatile data and set up of the chosen volatile data.

Based on the above section's discussion, it is noteworthy that the volatile data has played a major role, especially for forensic analysis. Consequently, there are presences of a few steps regarding the collection of volatile data for this chosen context. The first step associates with the collection of data, command history and time regarding the security incident followed by the establishment of audit trails. The next step is proper documentation of forensic collection activities in association with the network information and volatile system [15]. In the alternative method, the first aspect relates to the maintenance of all actions that are operated in a running machine, recognition of appropriate operating system, especially on the suspect machine followed by the proper collection of volatile data and stored into a removable storage device [16]. After that, the determination of evidence seizure methods holds an important place as it deals with the collection of additional information from the artefacts followed by appropriate documentation. These above-stated basic steps provide evidence for forensic analysis.

Apart from the traditional approaches for the forensic analysis, the researcher has tried to incorporate current processes in this regard. Following that, current practices of forensic analysis require jurisdiction in two ways. The first way needs one search jurisdiction to seizure the computer and subsequent forensic examination. The second way associates with two search warrants. This first search warrant is used for the seizure of the computer whereas the second search warrant inter-links with the forensic examination [17]. In accordance with the raised circumstances, the investigators have applied for the search warrant that in turn, help them to conduct the live analysis. However, regarding the jurisdiction system, especially for the forensic analysis, it is noteworthy that the search warrant has been considering with a few factors. In addition, the first factor has been associating with the presence of an electronic document in association with the electronic storage media and computer network. Besides this, the second factor has been implying the conduction processes of preview the screening based on the computer data storage media that in turn, assist the investigators to gain a deep understanding of the fact of data recovery software [18]. Therefore, it can be said that the live analysis is always seeking trained personnel as it deals with the complex procedure of the jurisdiction system.

Moreover, the core concept of the live analysis has been associating with numerous important components such as capture, preserve and proper collection of record evidence. All these selected components provide enough strength for the forensic analysis and electronic crime scene. In order to give the best limelight on this respective research study, the researcher has identified that sometimes the investigators do not need a search warrant. Therefore, this selected aspect needs to involve legal considerations in accordance with the relevance. On the other hand, the researcher has observed an important factor regarding forensic analysis and electronic crime scenes [19]. Consequently, it is noted that the respective investigators have the capability for effective conduction of the chosen aspect which includes forensic analysis in association with digital crime scenes.

Furthermore, the conduction of live analysis through the establishment of the respective probable cause prior. This aspect is relying upon time consent in association with the forensic analysis revokes the overall concept. Following that, the revoke of probable cause prior along with the time consent helps the authority in association with the forensic investigators to conduct the full phase of forensic examination [20]. On the contrary, the researcher has noticed that if the probable cause prior has not been evaluated, then the proves of data may be lost. In addition, as per the forensic analysis in association with the digital crime scenes, the researcher has observed that the accuracy along with the reliability has played a significant role. This is because both these aspects such as accuracy and reliability have helped to collect the necessary evidence. Therefore, it can be said that the potential issues or challenging factors of the forensic analysis have been associating with different types of aspects [21]. However, to conduct the research study with more efficiency, the researcher has observed that the most important two factors, especially for the forensic analysis been called the corporate network along with the capture of content, especially for the real-time scope.

4. Dataset employed and Experimental Analysis

In order to perform the analysis, the data were taken from the Computer Forensic Reference Data Sets. The dataset was the hacking case [22]. The analysis was done based on the secondary data analysis using thematic data analysis comprising of the data tool using authentic information processing. The aim of the Computer Forensic Investigation is to identify the stolen data or an unauthorized access. The detection of unauthorized access through system artifacts or logging capabilities. With the help of the forensic analysis the experts can determine the root cause of behind the unauthorized access. In addition to this, data analysis might be considered as one of the most important aspects for the successful completion of the research. The entire research is based on the final findings of the data collection. Therefore, it is the responsibility of the researchers to take time and analyses the collected data to arrive at an effective conclusion

In this hacking case, the analysis and examination process was performed on a replica copy and the Autopsy tool was used to analyze the evidence. The hacking case consists of one evidence, disk image taken from the suspect laptop. Evidence acquisition is not shown as it's assumed the first responder has done it properly. Analysis will start by verifying evidence integrity. 4.1 Context of the forensic evidence.

4.1 Context of the forensic evidence.

As per the given case, on 09/20/04 the investigating team has found an abandoned device a Dell CPi notebook computer, serial # VLQLW along with a wireless PCMCIA card and an external homemade 802.11b antennae. In addition to the several documents have also been found with the device. With the help of several types of methodologies such as dynamic. It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect, also goes by the online nickname of "Mr. Evil" and some of his associates have said that he would park his vehicle within range of Wireless Access Points where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords.

4.2 Findings of the forensic analysis

The investigation started with the objective to know what was run in the system. The homemade antennae raised the suspicion activity hence an investigation is required. The company wants to know if the user has accessed their network or performed any kind of hacking activity. All legal measures and permission is granted to handle the evidence and store it securely. A copy of the acquired image is sent to the forensics lab for analysis. The digital forensic investigator must verify the authenticity and integrity of the image of evidence to be analyzed. The received image is in Encase format, hence ewfverify is used to check the integrity of the image. In figure 2, information on the device, system type, device name, domain, time zone, last system shutdown time, and computer account name are shown.

In figure 3, it can be seen that the number of accounts registered in this computer is 5 accounts, and the name of the account that uses the computer most often is Mr. Evil, which was determined based on the number of times that the system was logged in with the name of this user. The rest of the accounts come directly with the computer system.

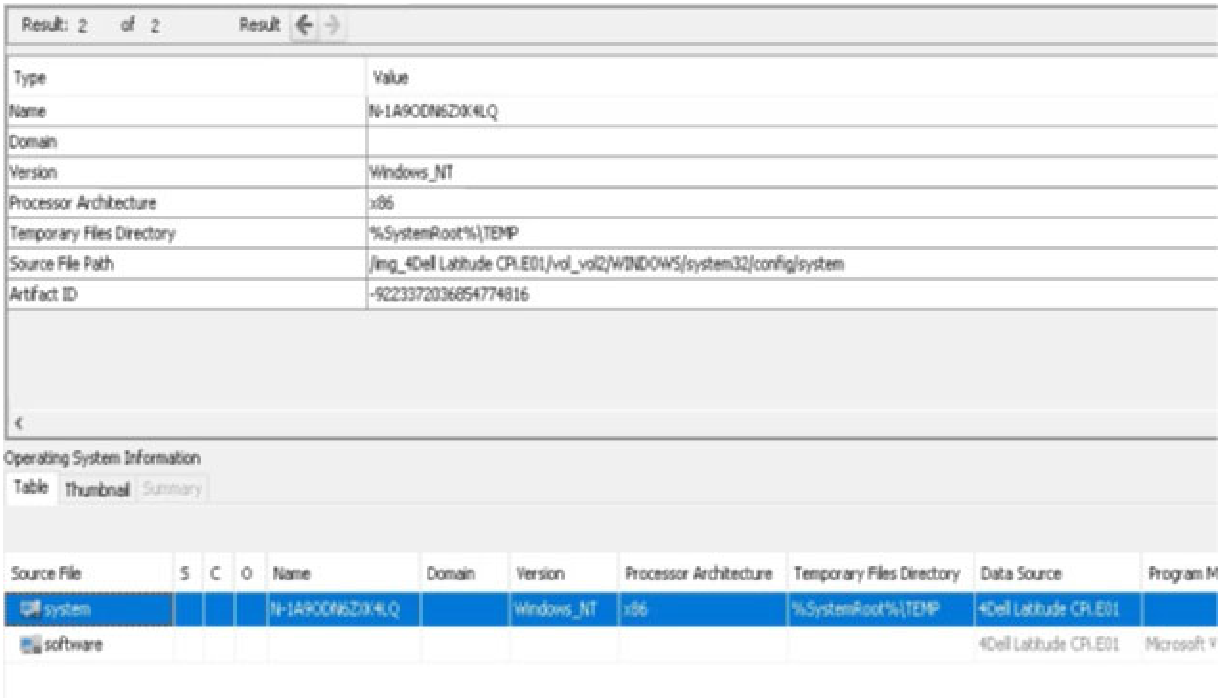
In figure 4, it can be seen that the names of some programs that can be used for hacking such as Cain & Abel v2.5 beta45, Ethereal, 123 Type all stored passwords, Anonymous, CuteFTP, LOOK Network. Above image analyzed prefetch artifacts in windows which is a data source to know what program were run and how many times. Prefetch artifact is a strong evidence to confirm whether a certain executable is run or no. It's used widely by incident responder or forensics examiners to scope malware infections of verify a user has opened and used a software.

While browsing through Evil user files, we found a file called interception after extracting and browsing this file, it turns out that the person is capturing data from a number of IP addresses. This file contains the network traffic in pcap format as shown in figure 5. From the above analysis, we confirm the user had captured the data belonging to the IP addresses listed in above picture. Those mainly were the targets of the attack.

5. Conclusion

By collecting all the data set all of cases like the hacking case, data leakage and registry forensic case this research paper has been done. It can be observed that there are Mr. Evil joined several groups which are meant for hacking. In the data analysis part, it has been shown that all the details of the device have been retrieve with the help of dynamic or static plan. Like the last login time, last shutdown, the date of last login and logout, all the time and date of these are being shown. According to the case analysis it has been observed that the person who is using this device, his name was Mr. Evil. From the data analysis it has been observed that the hacking tool has been recognize by the Autopsy suite, this could be considering as a cybersecurity situation which has been ran by under a law enforcement.at the time of data analysis several updated tools has been iced in order to collect the prominent data to diagnosis the evidences of the case.

At the time of the data analysis it has been shown that the present system is using 5 accounts and the operating system was windows XP. The install date, the time zone, the domain name has been recognized at the time of data analysis. From the analysis of the collected data all of the detail regarding the last activity, used card, last used folder, the IP address of the wireless devices, it has been detected by the investigator. After collecting all the details, the investigator was able to go ahead to this matter. In this analysis part it also has been seen that several tools are very much important in order to investigate about any cybersecurity case.

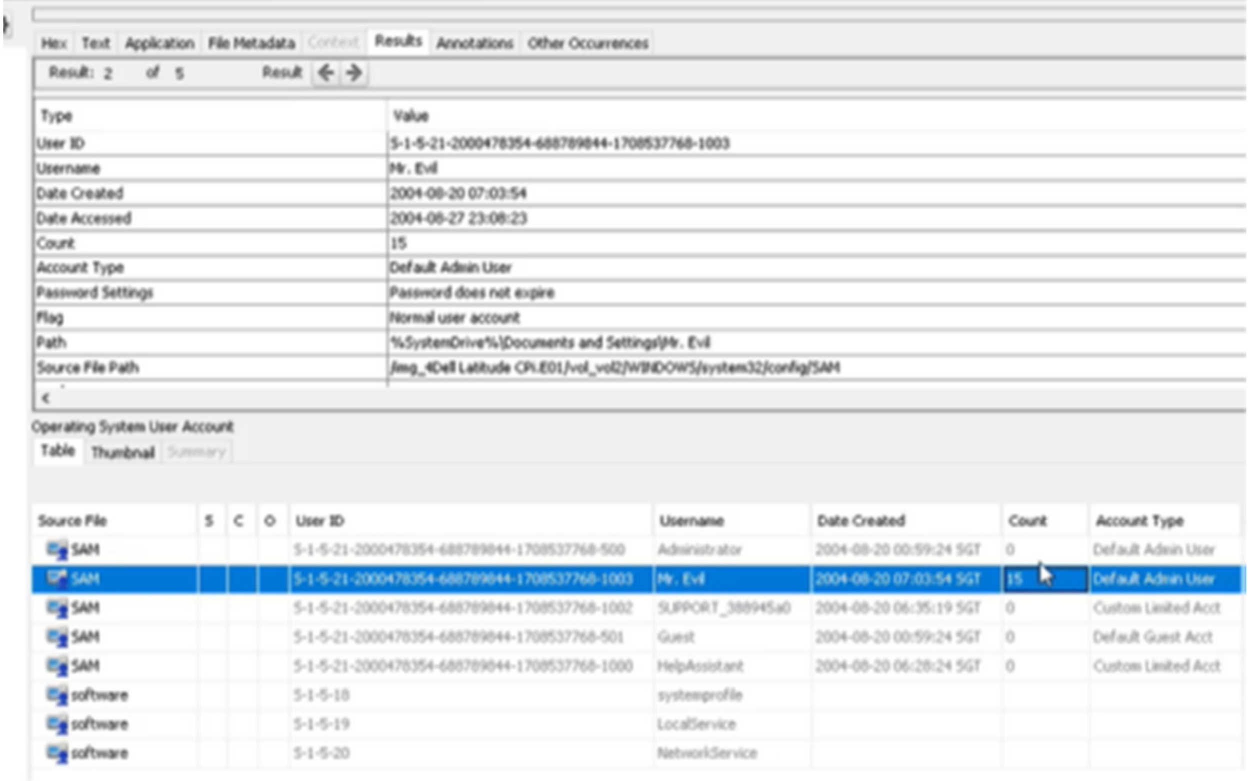


Type	Value
Name	N-1A9ODN6ZXK4LQ
Domain	
Version	Windows_NT
Processor Architecture	x86
Temporary Files Directory	%SystemRoot%\TEMP
Source File Path	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config/system
Artifact ID	-9223372036854774816

Operating System Information

Source File	S	C	O	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program M
system				N-1A9ODN6ZXK4LQ		Windows_NT	x86	%SystemRoot%\TEMP	4Dell Latitude CPi.E01	
software									4Dell Latitude CPi.E01	Microsoft V

Figure 2: System Information



Type	Value
User ID	S-1-5-21-2000478354-688789844-1708537768-1003
Username	Mr. Evil
Date Created	2004-08-20 07:03:54
Date Accessed	2004-08-27 23:08:23
Count	15
Account Type	Default Admin User
Password Settings	Password does not expire
Flag	Normal user account
Path	%SystemDrive%\Documents and Settings\Mr. Evil
Source File Path	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config/SAM

Operating System User Account

Source File	S	C	O	User ID	Username	Date Created	Count	Account Type
SAM				S-1-5-21-2000478354-688789844-1708537768-500	Administrator	2004-08-20 00:59:24 SGT	0	Default Admin User
SAM				S-1-5-21-2000478354-688789844-1708537768-1003	Mr. Evil	2004-08-20 07:03:54 SGT	15	Default Admin User
SAM				S-1-5-21-2000478354-688789844-1708537768-1002	SUPPORT_388945a0	2004-08-20 06:35:19 SGT	0	Custom Limited Acct
SAM				S-1-5-21-2000478354-688789844-1708537768-501	Guest	2004-08-20 00:59:24 SGT	0	Default Guest Acct
SAM				S-1-5-21-2000478354-688789844-1708537768-1000	HelpAssistant	2004-08-20 06:28:24 SGT	0	Custom Limited Acct
software				S-1-5-18	systemprofile			
software				S-1-5-19	LocalService			
software				S-1-5-20	NetworkService			

Figure 3 Accounts Registered

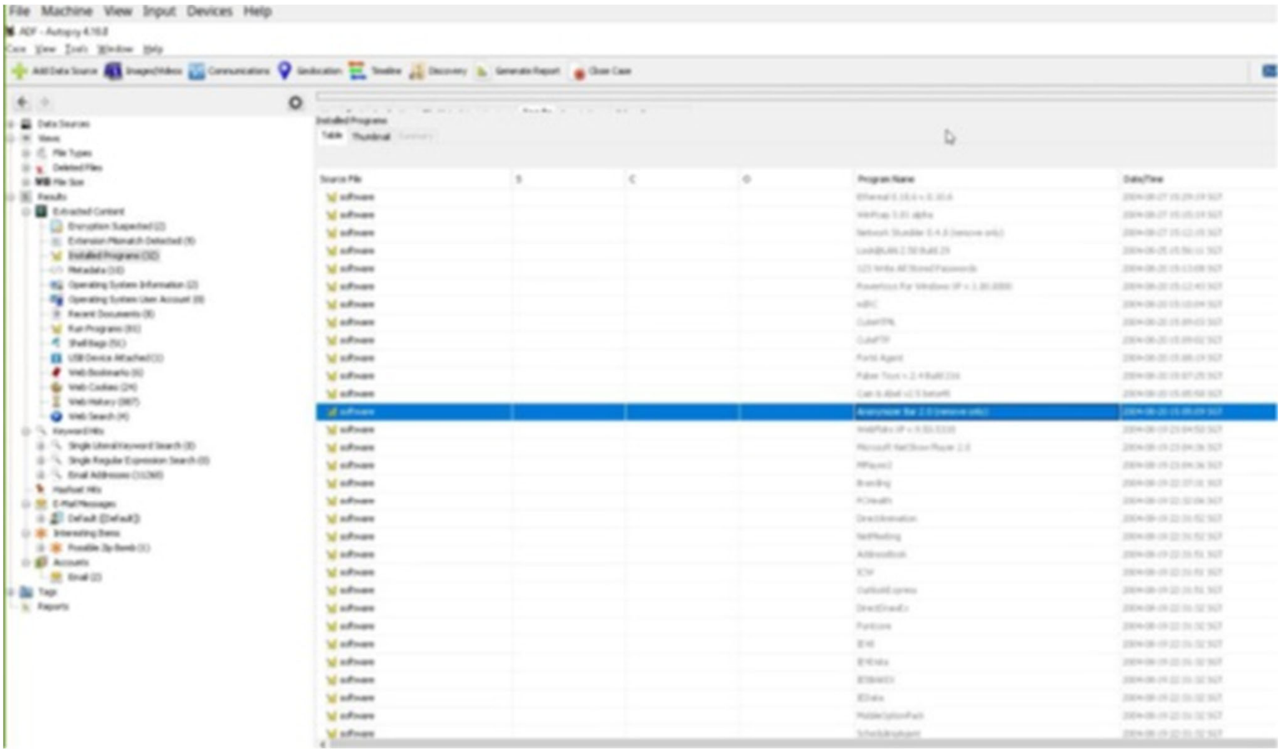
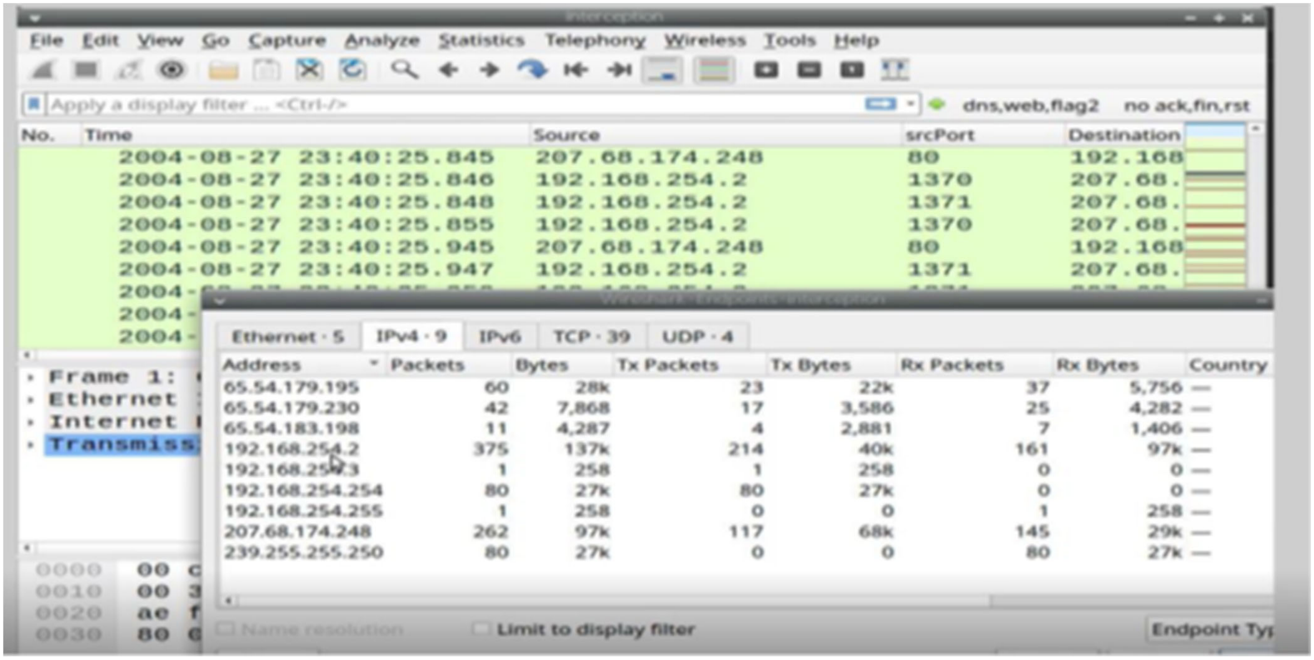


Figure 4 Programs that can be used for hacking



No.	Time	Source	srcPort	Destination
	2004-08-27 23:40:25.845	207.68.174.248	80	192.168
	2004-08-27 23:40:25.846	192.168.254.2	1370	207.68.
	2004-08-27 23:40:25.848	192.168.254.2	1371	207.68.
	2004-08-27 23:40:25.855	192.168.254.2	1370	207.68.
	2004-08-27 23:40:25.945	207.68.174.248	80	192.168
	2004-08-27 23:40:25.947	192.168.254.2	1371	207.68.

Ethernet · 5 | IPv4 · 9 | IPv6 | TCP · 39 | UDP · 4

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country
65.54.179.195	60	28k	23	22k	37	5,756	—
65.54.179.230	42	7,868	17	3,586	25	4,282	—
65.54.183.198	11	4,287	4	2,881	7	1,406	—
192.168.254.2	375	137k	214	40k	161	97k	—
192.168.254.3	1	258	1	258	0	0	—
192.168.254.254	80	27k	80	27k	0	0	—
192.168.254.255	1	258	0	0	1	258	—
207.68.174.248	262	97k	117	68k	145	29k	—
239.255.255.250	80	27k	0	0	80	27k	—

Figure 5 Network Traffic

According to the case process it has been noticed that this identification process of this case is important to identify the hidden software's the hacker are using. From the case analysis it has been concluded that the open source tools are really helpful to cast off for a huge number of network forensics.

The future work involves extraction of detailed information about the hacker's action using various skills like the understanding of Linux system calls and networking primitives. This aids in the generation of detailed pattern of hacker's activity along with the timely detection.

Acknowledgments

The author would like to thank University of Technology, Bahrain for supporting this work.

References

[1] Choi, Jusop, Jaegwan Yu, Sangwon Hyun, and Hyoungshick Kim. "Digital forensic analysis of encrypted database files in instant messaging applications on Windows operating systems: Case study with KakaoTalk, NateOn and QQ messenger." Digital Investigation 28 (2019): S50-S59

[2] Morrison, Jack, Giles Watts, Glyn Hobbs, and Nick Dawnay. "Field-based detection of biological samples for forensic analysis: Established techniques, novel tools, and future innovations." Forensic science international 285 (2018): 147-160.

[3] Bin Arfaj, B. A., Mishra, S., & AlShehri, M. (2022). Efficacy of Unconventional Penetration Testing Practices. Intelligent Automation and Soft Computing, 31(1), 223-239.

[4] AlOwaimer, B. H., & Mishra, S. (2021). Analysis of web browser for digital forensics investigation. International Journal of Computer Applications in Technology, 65(2), 160-172.

[5] Thebaity, M. A., Mishra, S. ., & Shukla, M. K. . (2020). Forensic Analysis of Third-party Mobile Application. Helix, 10(04), 32-38. Retrieved from https://helixscientific.pub/index.php/home/article/view/194

[6] Umar, Rusydi, Imam Riadi, and Guntur Maulana Zamroni. "Mobile forensic tools evaluation for digital crime investigation." Int. J. Adv. Sci. Eng. Inf. Technol 8, no. 3 (2018): 949

[7] Riadi, Imam. "Forensic investigation technique on android's blackberry messenger using nist framework." International Journal of Cyber-Security and Digital Forensics 6.4 (2017): 198-206.

[8] Horsman, Graeme. "Can we continue to effectively police digital crime?." Science & justice 57.6 (2017): 448-454

[9] Wahyudi, Erfan, Imam Riadi, and Yudi Prayudi. "Virtual Machine Forensic Analysis And Recovery Method For Recovery And Analysis Digital Evidence." International Journal of Computer Science and Information Security 16 (2018).

[10] Rani, Sudesh. "Digital Forensic Models: A Comparative Analysis." International Journal of Management, IT and Engineering 8.6 (2018): 432-443

[11] Villar-Vega, H. F., L. F. Perez-Lopez, and J. Moreno-Sanchez. "Computer forensic analysis protocols review focused on digital evidence recovery in hard disks devices." Journal of Physics: Conference Series. Vol. 1418. No. 1. IOP Publishing, 2019

[12] Albanna, Faiz, and Imam Riadi. "Forensic Analysis of Frozen Hard Drive Using Static Forensics Method." International Journal of Computer Science and Information Security (IJCSIS) 15.1 (2017).

[13] Pansari, Nikunj, and Dhruwal Kushwaha. "Forensic analysis and investigation using digital forensics-An overview." International Journal of Advance Research, Ideas and Innovations in Technology 5.1 (2019): 470-475.

[14] Rasool, Aamir, and Zunera Jalil. "A review of web browser forensic analysis tools and techniques." Researchpedia Journal of Computing (2020).

[15] Sangher, Kanti Singh, and Archana Singh. "A Systematic Review– Intrusion Detection Algorithms Optimisation for Network Forensic Analysis and Investigation." 2019 International Conference on Automation, Computational and Technology Management (ICACTM). IEEE, 2019

[16] Aziz, Amira Sayed A., Mohamed Mostafa Fouad, and Aboul Ella Hassanien. "Cloud computing forensic analysis: trends and challenges." Multimedia Forensics and Security. Springer, Cham, 2017. 3-23.

[17] Chang, Ming Sang, and Chih Yen Chang. "Forensic analysis of LINE messenger on android." Journal of Computers 29.1 (2018): 11-20.

[18] Srivastava, Devesh Kumar. "Reduction of digital forensic evidence using data science." Third international congress on information and communication technology. Springer, Singapore, 2019

[19] Yuliani, Vindy Arista, and Imam Riadi. "Forensic Analysis WhatsApp Mobile Application on Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Forensic Analysis WhatsApp Mobile Application On Android Based Smartphones Using National Institute of Standard and Tec." vol 8 (2019): 223-231

[20] Zhang, Yu, Binglong Li, and Yifeng Sun. "Android Encryption Database Forensic Analysis Based on Static Analysis." Proceedings of the 4th International Conference on Computer Science and Application Engineering. 2020

[21] Sunardi, Sunardi. "Analysis of Steganographic on Digital Evidence using General Computer Forensic Investigation Model Framework." Analysis of Steganographic on Digital Evidence using General Computer Forensic Investigation Model Framework 11.11 (2020): 315-323

[22] https://cfreds.nist.gov/all/NIST/HackingCase

Dr. Abdul Khadar Jilani is working as Asst. Professor and Program Head for BSCS in College of Computer studies, University of Technology Bahrain since Jan, 2022. He graduated from Osmania University, Masters from Bharatidasan University, MTech (IT) from Punjabi University and PhD (Computer Science and Engineering) from Rayalaseema University. He has published numerous research papers in various international journals indexed by Scopus and ISI. He is also serving as a reviewer for various refereed journal. His research interest not limited to Software Engineering, Machine learning, Cyber security and software security.

Dr. Shirina Samreen is an Assistant Professor in the Department of Computer Science, College of Computer and Information Sciences, Majmaah University, Kingdom of Saudi Arabia. She is an IEEE member since 2015.She has done her PhD in Computer Science and Engineering from JNTUH, India in 2016. She has 30 research papers to her credit in various IEEE International conferences / Journals. Received Best paper awards twice for her research papers at IEEE ICCIC, a renowned international conference. She acted as a reviewer for IEEE Wireless Communication Magazine, Journal of Engineering and Applied Sciences (JEAS), Majmaah University and various IEEE International Conferences held in India and abroad.