Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 5, No. 2, May 2020, Pp. 155-160

Detection of metasploit attacks using RAM Forensic on proprietary operating systems

Danar Cahyo Prakoso*[1], Imam Riadi[2], Yudi Prayudi[3]
Department of Informatics, Universitas Islam Indonesia, Indonesia[1,3]
Department of Information System, Universitas Ahmad Dahlan, Indonesia[2]

Article Info
Keywords:
Digital Forensics, RAM Forensics, Live Forensics, Metasploit, Digital Evidence

Article history:
Received 05 January 2020
Revised 30 April 2020
Accepted 22 May 2020
Available 22 May 2020

Cite:
Prakoso, D., Riadi, I., & Prayudi, Y. (2020). Detection of Metasploit Attacks Using RAM Forensic on Proprietary Operating Systems. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 5(2). doi:https://doi.org/10.22219/kinetik.v5i2.1037

*Corresponding author.
Danar Cahyo Prakoso
E-mail address:
danarcahyop@gmail.com

Abstract
Information technology has become an essential thing in the digital era as it is today. With the support of computer networks, information technology is used as a medium for exchanging data and information. Much information is confidential. Therefore, security is also essential. Metasploit is one of the frameworks commonly used by penetration testers to audit or test the security of a computer system legally, but it does not rule out the possibility that Metasploit can also be used for crime. For this reason, it is necessary to carry out a digital forensic process to uncover these crimes. In this study, a simulation of attacks on Windows 10 will be carried out with Metasploit. Then the digital forensics process uses live forensics techniques on computer RAM, where the computer RAM contains information about the processes running on the computer. The live forensic technique is important because information on RAM will be lost if the computer is off. This research will use FTK Imager, Dumpit, and Magnet RAM Capture as the RAM acquisition tool and Volatility as the analysis tool. The results of the research have successfully shown that the live forensics technique in RAM is able to obtain digital evidence in the form of an attacker's IP, evidence of exploits/Trojans, processes running on RAM, operating system profiles used and the location of the exploits/Trojan when executed by the victim.

1. Introduction

Crime does not only occur in the real world. In the era of advancement in information technology, criminal acts can also be committed in cyberspace [1]. Many criminal activities can occur in cyberspace, such as illegal access, theft of personal data, robbery of confidential data, and others. Crime in cyberspace by using computers as media or targets is called cybercrime [2]. Metasploit is a tool that is often used by professional penetration testers to carry out testing and audits on a computer system. Still, on the other hand, some parties are not responsible for using Metasploit to carry out illegal hacking [3][4]. On a computer, there is a Random Access Memory (RAM) in which there is a lot of data and information related to the processes running on a computer [5][6].

Handling of data and information contained in computer RAM needs to be done quickly and adequately so that the data and information can be used as digital evidence before the law [7][8]. Digital forensics processes need to be carried out to expose these crimes. Digital forensics is a science that aims to obtain evidence related to criminal cases and can be accounted for before the law [5][9][10].

RAM is volatile, where data will be lost if the computer is dead [11][12]. For this reason, a live forensic technique is needed to save potential digital evidence on RAM when it is on [13][14][15]. This research will discuss how to explore digital evidence on computer RAM by simulating an attack on Windows 10 using Metasploit with the aim of exploring digital evidence left on the RAM of a computer affected by an attack using Metasploit.

In the digital forensic process, the acquisition process is vital because the investigator will duplicate digital evidence on the storage media or RAM and will influence the results of further investigations [16]. For this reason, this study will use three different RAM acquisition tools, namely FTK Imager, Magnet RAM Capture, and Dumpit, with the aim of increasing knowledge about the digital evidence characteristics of the results of each of these tools. In this study the analysis process will use Volatility. This tool is a tool that is used by investigators to identify and analyze an image file that was acquired by the command line on a Linux-based computer [17].

Research on forensic RAM has been widely carried out, such as research conducted by Yudhistira, et al. in this study focused on finding digital evidence on RAM in the form of e-mails, user IDs and passwords related to internet activity [18]. Hausknecht, et al. conducted research and exploration of RAM which in their research stated that RAM contained much information that could potentially be used as digital evidence such as processes, open files and "registry handling", general files, information in network traffic, internet data, passwords, and cryptographic keys, decrypted content, and others [19].

On the other hand, Rochmadi, et al. conducted research on the theme of the live forensics method in RAM for anti-forensic analysis in portable web browser private mode [20]. Other research on RAM extraction in Windows 7 was conducted by Thomas, et al. The research explained the methodology for listing running processes, loading DLLs, and extracting memory processes from running processes [21]. In addition, Riadi, et al. explored RAM forensics using Live forensic techniques in chat line applications on the Windows 8.1 operating system with online shop fraud cases [5].

Ranul Thantilage and Neera Jeyamohan conducted research focusing on developing a framework for memory volatility for digital evidence on social media based on Windows 10 workstations [22]. On the other hand, research on RAM forensics in malware attacks was also carried out by Podile, et al. They researched the Man In The Browser Trojan malware attack, which was developed with the aim of carrying out attacks on banks and the financial industry [23]. In his research, Kiel Wadner conducted a study on Windows 7 RAM to explore the Metasploit attack to look for digital evidence characteristics on Windows 7 RAM after exploitation [24].

Based on previous research, the exploration of forensic RAM, which was attacked using Metasploit, is still little done. Even if there is, it is still limited to Windows 7 and not yet on Windows 10 and in previous studies also have not been done using comparative research with various variants of acquisition tools. This study aimed to provide additional knowledge regarding digital evidence that can be found when a Metasploit attack occurs so that it is expected to help Investigators to uncover cybercrime perpetrators. The results of this study showed that RAM acquisition tools such as Magnet RAM capture, FTK Imager and Dumpit were successful get digital evidence artifacts such as attacker's IP, evidence of exploits/trojans, processes running on RAM, operating system profiles used and the location of the exploit/trojan when executed by the victim so that with the digital evidence that can be obtained in the computer RAM can be used as additional evidence to help uncover the case of cybercrime.

2. Research Method

2.1 Method

This study will use several methods, referring to research that has been done [25] in the scientific journal mentioned there are four stages, including Preservation, Collection, Examination, and Analysis [25].

1. Preservation
   This stage is an attempt to maintain and protect the integrity of the evidence so that there is no change or loss of evidence.
2. Collection
   This stage involves collecting evidence related to cases that have occurred to help uncover cases that are being investigated
3. Examination
   This stage is carried out processing of evidence that has been collected previously, so that data will be found relating to the case being investigated.
4. Analysis
   The last step is an analysis of the available evidence so that information can be obtained from the identification of digital evidence contained and left behind on computer RAM.

2.2 Scenario

In this research, an attack scenario will be performed on a Windows 10 computer using Metasploit on the local network. The attack scenarios are as follows:

1. The attacker generates a Trojan using Metasploit, named explorer.exe then stores it on a USB drive
2. The victim executes explorer.exe on the USB drive on his computer
3. The attacker who has been listening will get a session and can control the victim's computer remotely.

The simulation is carried out on a local network, using two computers. After the attacker gets a session, he can access the victim's computer, such as camera access, access files on the computer, and can turn off the computer remotely.

Live forensic technique is used to acquire the RAM of the victim's computer using FTK Imager, Magnet RAM Capture, and Dumpit when the victim's computer is on and still in remote control by the attacker

The purpose of this study is to look for digital evidence that is focused on five digital evidence in the form of an attacker's IP, evidence of exploits/trojans, processes running on RAM, operating system profiles used and the location of the exploit / trojan when executed by the victim.

3. Result and Discussion

In this section, an analysis of RAM acquisition files will be analyzed with live forensic techniques from the three tools used in this study, namely FTK Imager, Dumpit, and Magnet RAM Capture. The purpose of using these various tools is as a comparison of how the characteristics of digital evidence result from the acquisition of each tool used in

this study. This research will focus on searching digital evidence in the form of attacker IP, evidence of exploits / Trojans, processes that run on RAM, operating system profiles used, and the location of exploits / Trojans when executed by the victim. This section will explain the stages of analysis in each file acquisition or capture RAM results from the three tools used in this study, namely FTK Imager, Magnet RAM Capture, and Dumpit. First is analyzing the victim operating system, analyzing the process, then analyzing the dump exploit / Trojan, followed by analyzing the location of the exploit/trojan when the victim is executed and finally analyzing the network.

3.1 Stages of Analysis

3.1.1 Victim Operating System Analysis

The first stage, when analyzing file acquisition or RAM capture, is initial identification using the imageinfo plugin in Volatility. This plugin will provide initial information about the operating system used. It is crucial to find out the initial information about the operating system used because it will be used for the further analysis process.

3.1.2 Running Process Analysis

Process Stage is an analysis of all activities of the processes running in the system when RAM capture is performed using FTK Imager, Magnet RAM Capture, and Dumpit while the system is still running. There are several plugins that are used in the Process analysis stage, as follows:

1. Pslist used to see the processes that occur during the process of RAM capture by knowing the running process can be seen as suspicious processes.
2. Pstree is used to see the process in more detail by displaying the parent process.

3.1.3 Exploit/Trojan Process Analysis

Stage of Process Dump analysis is an advanced process when a suspicious process is identified from the previous stage that is Process analysis. After determining which suspicious process is possible, a dump file is performed. The dump file process will produce binary files, the purpose of the suspected exploit/Trojan dump process stage is for the purposes of further analysis of the suspicious binary file. The plugin used is Procdump.

3.1.4 The Location of *Execute* Exploit/Trojan by the Victim Analysis

This stage will find out the location or path where the victim executes the exploit/Trojan file. This is important so that the investigator gets additional information to trace where the exploit/Trojan came from so that a computer system becomes a victim of an attack. The plugin used is cmdline.

3.1.5 Network Analysis

Network analysis is carried out to find out the network activity on the computer system when the acquisition is made by knowing the activity on the computer system and will be searched for suspicious network connections. At this stage, the Netscan plugin is used.

3.2 Result

This section is the final result of the analysis process that has been done previously on the acquisition of files from the FTK Imager, Magnet RAM Capture and Dumpit. The following is a description of the results of the analysis:

A. The process of searching for profiles on image files resulting from FTK Imager, Magnet RAM capture, and Dumpit. In this experiment, Volatility, when analyzing the acquisition image file from FTK Imager and Magnet RAM capture, can suggest using the Win10x86_15063 profile directly. Figure 1 shows Volatility suggesting the OS profile used in the description image is seen in (Instantiated with Win10x86_15063).

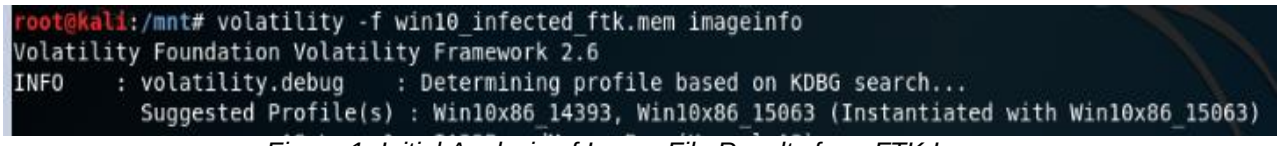

Figure 1. Initial Analysis of Image File Results from FTK Imager

The next experiment will be an analysis of the image file results from the Magnet RAM capture. Figure 2 shows the results of the Volatility analysis of the acquisition file from Magnet RAM Capture. At this stage, it is known that Volatility suggests two profiles used, namely Win10x86_14393 and Win10x86_15063.

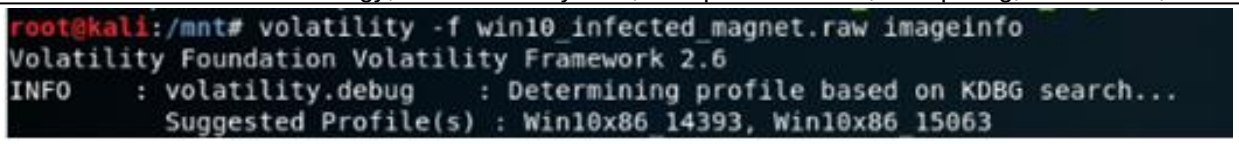

Figure 2. Initial Analysis of Image File Results from Magnet RAM Capture

The next step is to analyze the Dumpit image file. Figure 3 is the result of the analysis using Volatility in the Dumpit image file. The initial identification result of Volatility for the Dumpit image file also generates profile suggestions, namely Win10x86_14393, Win10x86_15063 (Instantiated with WinXPS2x86). Interestingly, the Dumpit image file results in a slightly different profile suggestion from the FTK Imager and Magnet RAM capture, namely WinXPS2x86, shown in Figure 3 (marked with white blocks). However, when tested using the WinXPS2x86 profile for further analysis, an error occurred, or Volatility could not use the WinXPS2x86 profile to analyze the image file.

Figure 3. Initial Analysis of Image File Results from Dumpit

B. In the analysis process, various processes occur on a computer. There are two similar processes, namely the name explorer.exe, then determine the suspicious process that is running. In this attack simulation, the Trojan is given the name explorer.exe, so that when analyzing using pslist, two explorer.exe processes are visible, then the suspicious explorer.exe process is determined, as shown in Table 1. Determination of the explorer.exe process in Table 1 as a suspicious process is due to the explorer.exe process in Table 1 running under another explorer.exe process, which is Windows default explorer.exe

Table 1. Suspicious explorer.exe Process

No.	Operating System	RAM Capturer Tool	Process Name	PID
1	Windows 10	FTK Imager	explorer.exe	5904
2	Windows 10	Magnet RAM Capture	explorer.exe	2348
3	Windows 10	Dumpit	explorer.exe	3612

C. After determining the suspicious process, a process dump analysis is performed. In this research, a dump process using the procdump was obtained from the image file from FTK Imager, Magnet RAM capture, and Dumpit. The dump process succeeded in getting the binary file from the suspicious process for further analysis.

D. In the next process is finding out where the exploit or trojan can be executed by the victim. From the results of experiments and analysis of image files generated by FTK Imager, Magnet RAM capture and Dumpit, the path of the location of the trojan or exploit can be identified. The path of suspicious process that captured by FTK Imager is located in G:\explorer.exe as shown in Figure 4.

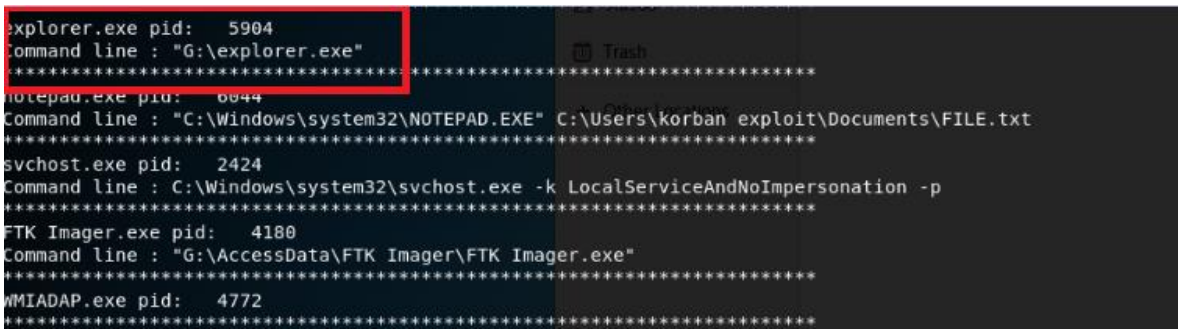

Figure 4. Path Directory Suspicious Process that Captured by FTK Imager

The next, in Figure 5 shown the path of suspicious process that captured by Magnet RAM Capture and success can be read by volatility tool.

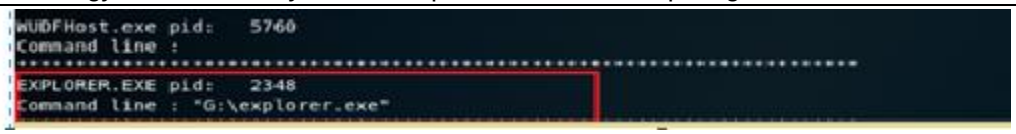

Figure 5. Path Directory Suspicious Process that Captured by Magnet RAM Capture

Based on Figure 6 we can see that the directory or path the suspicious process that can be captured by Dumpit and can be read by Volatility tool.

Figure 6. Path Directory Suspicious Process that Captured by Dumpit

E. In the network analysis process of the experimental results and analysis of image files generated by FTK Imager, Magnet RAM capture and connection dumps that occur during an attack can be found, and IPs suspected of being attackers can also be found.

The result on this research shown in Table 2, the digital artifact of attacks using Metasploit on Windows 10 like an attacker IP, evidence of exploits / Trojans that were successfully dumped into binary files, Processes that run on RAM, Operating system profiles used and the location of the exploit / Trojan when it was executed by the victim. can be found.

Table 2. Artifact Digital of attacks using Metasploit on Windows 10

No.	Digital Artifact	RAM Capturer Tool	State
1	IP Attacker	FTK Imager	Found
2	Exploit/trojan	FTK Imager	Found
3	Windows 10	FTK Imager	Found
4	Running Process	FTK Imager	Found
5	Exploit/Trojan Location	FTK Imager	Found
6	IP Attacker	Magnet RAM Capture	Found
7	Exploit/trojan	Magnet RAM Capture	Found
8	Windows 10	Magnet RAM Capture	Found
9	Running Process	Magnet RAM Capture	Found
10	Exploit/Trojan Location	Magnet RAM Capture	Found
11	IP Attacker	Dumpit	Found
12	Exploit/trojan	Dumpit	Found
13	Windows 10	Dumpit	Found
14	Running Process	Dumpit	Found
15	Exploit/Trojan Location	Dumpit	Found

Based on the stages of research that have been carried out, successfully found digital evidence associated with the possibility of an attack on a Windows 10 computer. This research can be used as an initial step for further research in digital forensics, especially in the scope of RAM forensics.

4. Conclusion

Based on the research results, the live forensics technique using FTK Imager, Magnet RAM Capture, and Dumpit can be used to carry out digital evidence acquisition of attacks using Metasploit on Windows 10. Volatility as an analytical tool, in general, is able to provide information from the analysis of FTK Imager image files, Magnets RAM Capture, and Dumpit, although there are small differences when giving output in the process of giving profile suggestions. In accordance with the focus in this study, the results of forensic analysis conducted were able to find five digital evidence left in the RAM of Windows 10 computer that is in the form of an attacker IP, evidence of exploits/Trojans that were successfully dumped into binary files, Processes that run on RAM, Operating system profiles used and the location of the exploit / Trojan when it was executed by the victim.

Suggestions for further research are conducting live forensics techniques and simulating attacks on other devices such as IoT devices or on Linux and other operating systems. Besides, this research is still limited to the comparison of the acquisition tool. For this reason, future research studies can be conducted with a combination of more various

analysis tools that are expected to provide more accurate knowledge. In addition, this research can also produce binary files dumped. Therefore, further research can be carried out to investigate the binary file further.

References

[1] N. Anwar and I. Riadi, "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika,* Vol. 3, No. 1, Pp. 1–10, 2017.

[2] D. A. Arifah, "Kasus Cybercrime Di Indonesia," *Jurnal Bisnis dan Ekono*mi, Vol. 18, No. 2, Pp. 185–195, 2011.

[3] H. Gupta and R. Kumar, "Protection against penetration attacks using Metasploit," *2015 4th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2015*, Pp. 2–5, 2015. https://doi.org/10.1109/ICRITO.2015.7359226

[4] U. Timalsina and K. Gurung, "Metasploit Framework with Kali Linux," No. April 2015, Pp. 0–8, 2017.

[5] I. Riadi and M. E. Rauli, "Live forensics analysis of line app on proprietary operating system," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control. 4(4).*, Vol. 4, No. 3, 2019. https://doi.org/10.22219/kinetik.v4i4.850

[6] I. Riadi and E. Rauli, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," *Jurnal Teknik Elektro,* Vol. 10, No. 1, Pp. 18–22, 2018. https://doi.org/10.15294/jte.v10i1.14070

[7] Ruhwan, I. Riadi, and Y. Prayudi, "Evaluation of Integrated Digital Forensics Investigation Framework for the Investigation of Smartphones Using Soft System Methodology Evaluation of Integrated Digital Forensics Investigation Framework for the Investigation of Smartphones Using Soft System," *International Journal of Electrical and Computer Engineering (IJECE)*, No. October, Pp. 2806–2817, 2017. http://doi.org/10.11591/ijece.v7i5.pp2806-2817

[8] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," *Scientific Journal of Informatics,* No. November, 2018. https://doi.org/10.15294/sji.v5i2.16545

[9] M. N. Faiz and W. A. Prabowo, "Comparison of Acquisition Software for Digital Forensics Purposes," *Kinetik, Vol. 4, No. 1, Febr. 2019*, Vol. 4, No. 1, Pp. 37–44, 2019. https://doi.org/10.22219/kinetik.v4i1.687

[10] G. M. Zamroni and I. Riadi, "Instant Messaging Forensic Tools Comparison on Android Operating System," *Kinetik,* Vol. 4, No. 2, Pp. 137–148, 2019. https://doi.org/10.22219/kinetik.v4i2.735

[11] H. K. Mann and Gurpal Singh Chhabra, "Volatile Memory Forensics : A Legal Perspective," *International Journal of Computer Applications*, Vol. 155, No. 3, Pp. 11–15, 2016. http://doi.org/10.5120/ijca2016912276

[12] R. Dave, N. R. Mistry, and M. S. Dahiya, "Volatile Memory Based Forensic Artifacts & Analysis Volatile Memory Based Forensic Artifacts & Analysis," *International Journal for Research in Applied Science Engineering Technology,* 2014.

[13] A. Kurniawan and Y. Prayudi, "Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics ," *HADFEX (Hacking and Digital. Forensics Exposed)*, No. June 2014, Pp. 1–5, 2014.

[14] W. Pranoto, I. Riadi, and Y. Prayudi, "Live forensics method for acquisition on the Solid State Drive (SSD) NVMe TRIM function," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, 2020. https://doi.org/10.22219/kinetik.v0i0.1032

[15] D. Sudyana and N. Lizarti, "Digital Evidence Acquisition System on IAAS Cloud Computing Model using Live Forensic Method," *Scientific Journal of Informatics*, Vol. 6, No. 1, Pp. 125–137, 2019. https://doi.org/10.15294/sji.v6i1.18424

[16] M. Kaur, N. Kaur, and S. Khurana, "A Literature Review on Cyber Forensic and its Analysis tools," *International Journal of Advanced Research Computer and Communication Engineering*, Vol. 5, No. 1, Pp. 23–28, 2016.

[17] F. Bahtiar, N. Widiyasono, and A. P. Aldya, "Memory Volatile Forensik Untuk Deteksi Malware Menggunakan Algoritma Machine Learning," *Jurnal Teknik Informatika dan Sistem Informasi*, Vol. 4, Pp. 242–253, 2018. http://dx.doi.org/10.28932/jutisi.v4i2.776

[18] D. S. Yudhistira, I. Riadi, and Y. Prayudi, "Live Forensics Analysis Method For Random Access Memory On Laptop Devices," *International Journal of Computer Science and Information Security,* No. May, 2018.

[19] K. Hausknecht, D. Foit, and J. Burić, "RAM data significance in digital forensics," *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO - Proceedings*, No. May, Pp. 1372–1375, 2015. https://doi.org/10.1109/MIPRO.2015.7160488

[20] T. Rochmadi, I. Riadi, and Y. Prayudi, "Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser," *International Journal of Computer Aplications (IJCA)*, Vol. 164, No. 8, Pp. 31–37, 2017. https://doi.org/10.5120/ijca2017913717

[21] S. Thomas, K. K. Sherly, and S. Dija, "Extraction of memory forensic artifacts from windows 7 RAM image," *2013 IEEE Conference on Information and Communication Technologies, 2013*, No. Ict, Pp. 937–942, 2013. https://doi.org/10.1109/CICT.2013.6558230

[22] R. Thantilage and N. Jeyamohan, "A volatile memory analysis tool for retrieval of social media evidence in windows 10 OS based workstations," *2017 National Information Technology Conference (NITC)*, Pp. 86–88, 2017. https://doi.org/10.1109/NITC.2017.8285664

[23] A. Podile, K. Gottumukkala, and K. Sastry Pendyala, "Digital Forensic Analysis Of Malware Infected Machine-Case Study," *International Journal of Scientific & Technology Research,* Vol. 4, No. 09, 2015.

[24] K. Wadner, "An Analysis of Meterpreter during Post-Exploitation," 2014.

[25] R. Kaur and A. Kaur, "Digital Forensics," *International Journal of Computer Applications*, Vol. 50, No. 5, Pp. 5–9, 2012. https://doi.org/10.5120/7765-0844