

RAM Forensics for Metasploit Attack Detection on Proprietary Operating Systems

Author: Sunny Thakur

Abstract

In today's digital age, information technology is indispensable, especially in the context of data and information exchange facilitated by computer networks. With the increased transmission of sensitive data, security has become a paramount concern. Metasploit, a widely-used framework among penetration testers for security audits, is also vulnerable to misuse by malicious actors. Consequently, digital forensic methods are crucial for investigating potential cybercrimes. This study simulates an attack on a Windows 10 system using Metasploit and applies live forensics techniques to analyze computer RAM, which stores critical information about active processes. Live forensics is essential since RAM data is volatile and is lost once the computer is powered off. In this research, tools like FTK Imager, Dumpit, and Magnet RAM Capture are utilized for RAM acquisition, while Volatility is used for analysis. The findings demonstrate the effectiveness of live RAM forensics in uncovering valuable digital evidence, including the attacker's IP address, exploit/Trojan evidence, running processes, OS profiles, and exploit locations executed on the victim's system.

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

1. Introduction

Cybercrime has evolved alongside technological advancements, expanding into diverse digital spaces where malicious activities like unauthorized access, data theft, and information breaches are now common. Cybercrime involves using computers either as a tool or as a target for criminal acts. While Metasploit is often used by security professionals for legal penetration testing, it can also be exploited by unauthorized parties for illegal hacking activities. Within a computer, Random Access Memory (RAM) plays a crucial role, holding data on running processes and system activities.

Due to RAM's volatile nature, data stored is lost once the computer is turned off, making **live forensics** techniques essential for preserving potential evidence. This study simulates a Metasploit attack on a Windows 10 system, exploring the digital evidence left in RAM. During the digital forensic process, acquisition is a critical phase where investigators duplicate data from storage media or RAM to ensure evidence integrity for analysis.

This research utilizes three RAM acquisition tools—FTK Imager, Magnet RAM Capture, and Dumpit—aiming to expand understanding of how each tool captures distinct digital artifacts. The

analysis phase uses Volatility, a tool widely adopted for identifying and examining memory dumps in forensic investigations. Prior studies, such as those by Yudhistira and Hausknecht, have shown RAM can contain valuable digital evidence like emails, user IDs, passwords, process data, and cryptographic keys.

Building on these studies, this research focuses specifically on RAM forensics in the context of a Metasploit attack on Windows 10, a relatively unexplored area. Additionally, this study compares multiple RAM acquisition tools to better understand their respective efficacy in capturing critical forensic evidence. The research results indicate that tools like Magnet RAM Capture, FTK Imager, and Dumpit effectively capture artifacts such as the attacker's IP address, exploit evidence, running processes, OS profiles, and locations of executed Trojans, contributing valuable insights to the field of cybercrime investigation.

2. Research Methodology

2.1 Method Overview

This study employs a forensic investigation framework adapted from prior scientific research, comprising the following four stages:

1. **Preservation**
This stage focuses on preserving the integrity of evidence, ensuring no changes or losses occur throughout the investigation.
2. **Collection**
This involves gathering evidence relevant to the case, aiming to uncover actionable information that can assist in resolving the investigation.
3. **Examination**
During this phase, the collected evidence is processed to extract data that may hold relevance to the investigated incident.
4. **Analysis**
The final stage involves analyzing identified digital evidence from the RAM to gain insights and compile information left by malicious activity.

2.2 Attack Simulation Scenario

In this study, an attack is simulated on a Windows 10 computer using Metasploit within a local network. The attack scenario unfolds as follows:

1. The attacker creates a Trojan executable named `explorer.exe` using Metasploit and stores it on a USB drive.
2. The victim executes `explorer.exe` from the USB on their computer.
3. Once the executable is run, the attacker gains a session and can remotely control the victim's computer.

The simulation occurs within a controlled network environment using two computers. With an active session, the attacker can perform actions like accessing the victim's camera, managing files, and remotely shutting down the system.

The **live forensic technique** is applied to acquire the RAM on the victim's computer while it is still under remote control. RAM acquisition is conducted using FTK Imager, Magnet RAM Capture, and Dumpit to assess how each tool performs in preserving digital evidence, focusing on the following five critical elements:

1. **Attacker's IP Address**
2. **Evidence of Exploits or Trojans**
3. **Processes Active in RAM**
4. **Operating System Profile**
5. **Location of Exploits/Trojans Executed on the Victim's System**

Through this research, the study aims to provide forensic investigators with valuable insights into identifying and preserving key digital evidence within RAM, which can significantly contribute to cybercrime investigations and prosecutions.

3. Results and Discussion

This section presents the analysis of RAM acquisition files obtained through live forensic techniques using three tools: FTK Imager, Dumpit, and Magnet RAM Capture. The use of these varied tools aims to compare the characteristics of digital evidence captured by each. The focus of this research is to uncover critical evidence, including the attacker's IP address, exploit/Trojan indicators, active RAM processes, operating system profiles, and the location where the exploit/Trojan was executed on the victim's system. Below are the stages of analysis conducted on each acquisition file and the findings from FTK Imager, Magnet RAM Capture, and Dumpit.

3.1 Stages of Analysis

3.1.1 Victim Operating System Analysis

The initial stage in RAM acquisition analysis is identifying the operating system profile using Volatility's `imageinfo` plugin. This step provides crucial preliminary information about the OS in use, laying the groundwork for further forensic analysis.

3.1.2 Running Process Analysis

At this stage, analysis focuses on all system processes running during RAM capture, performed while the victim's system was still active. Key plugins include:

1. **Pslist**: Lists active processes during RAM capture, allowing detection of any suspicious activities.
2. **Pstree**: Provides a detailed view of processes by displaying their parent-child relationships, offering additional context.

3.1.3 Exploit/Trojan Process Analysis

If suspicious processes are identified, they are further examined using the **procdump** plugin to dump executable files. This step aims to retrieve binaries of suspected exploits or Trojans, which can be analyzed further to confirm malicious behavior.

3.1.4 Execution Location of Exploit/Trojan

This analysis identifies the directory path where the exploit/Trojan was executed on the victim's system. Locating this path can help trace the origin of the exploit and understand how the victim's system became compromised. The **cmdline** plugin is utilized to reveal this information.

3.1.5 Network Analysis

Network analysis inspects network activity captured on the victim's computer during RAM acquisition to identify any suspicious connections. The **netscan** plugin is used to detect active connections and find the attacker's IP address, providing insight into external interactions.

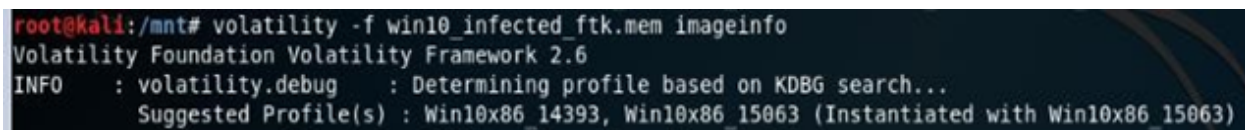
3.2 Results

The following summarizes the analysis results across FTK Imager, Magnet RAM Capture, and Dumpit.

A. OS Profile Identification

Each RAM acquisition tool provided initial OS profile suggestions through Volatility analysis:

- **FTK Imager** and **Magnet RAM Capture**: Suggested the **Win10x86_15063** profile (Figure 1).
- **Dumpit**: Recommended **Win10x86_15063** and also **WinXPS2x86**, though **WinXPS2x86** was not compatible for further analysis (Figure 3).



```
root@kali:/mnt# volatility -f win10_infected_ftk.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win10x86_14393, Win10x86_15063 (Instantiated with Win10x86_15063)
```

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

```

root@kali:/mnt# volatility -f win10_infected_magnet.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining profile based on KDBG search...
          : Suggested Profile(s) : Win10x86_14393, Win10x86_15063

```

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

```

root@kali:/mnt# volatility -f DESKTOP-2801657-20180823-033359.dmp imageinfo
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining profile based on KDBG search...
          : Suggested Profile(s) : Win10x86_14393, Win10x86_15063 (Instantiated with WinXPSP2x86)
          : AS Layer1 : IA32PagedMemoryPage (Kernel AS)

```

Figure 3. Initial Analysis of Image File Results from Dumpit

B. Running Process Identification

Two processes named **explorer.exe** appeared in each acquisition, one being a legitimate Windows process and the other a Trojan introduced during the attack simulation. Table 1 highlights the suspicious **explorer.exe** process based on differences in process IDs (PIDs).

No.	Operating System	RAM Capture 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. Exploit/Trojan Process Dump

Using the **procdump** plugin, a process dump was successfully generated for the suspicious **explorer.exe** process across all three tools. This allowed further binary analysis of the suspected exploit/Trojan.

D. Execution Path Identification

The execution path of the exploit/Trojan was retrieved for each tool:

- **FTK Imager**: Located the file path as **G:\explorer.exe** (Figure 4).
- **Magnet RAM Capture**: Successfully identified and displayed the execution path (Figure 5).

- **Dumpit:** Also displayed the execution path, confirming it could be read by Volatility (Figure 6).

```
explorer.exe pid: 5904
Command line : "G:\explorer.exe"
.....
notepad.exe pid: 6644
Command line : "C:\Windows\system32\notepad.exe" C:\Users\korban\Documents\FILE.txt
.....
svchost.exe pid: 2424
Command line : C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
.....
FTK Imager.exe pid: 4180
Command line : "G:\AccessData\FTK Imager\FTK Imager.exe"
.....
MIADAP.exe pid: 4772
.....
```

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

```
WUDFHost.exe pid: 5760
Command line :
.....
EXPLORER.EXE pid: 2348
Command line : "G:\explorer.exe"
```

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

```
explorer.exe pid: 3612
Command line : "G:\explorer.exe"
.....
Dumpit.exe pid: 1655
Command line : "G:\Dumpit.exe"
```

Figure 6. Path Directory Suspicious Process that Captured by Dumpit

E. Network Analysis

Network analysis identified suspicious connections, including the IP address of the attacker. Table 2 consolidates the digital artifacts found during Metasploit attacks on Windows 10, confirming evidence of attacker IP, Trojan binaries, OS profiles, running processes, and execution locations across all tools.

No.	Digital Artifact	RAM Capture Tool	Status
1	Attacker IP	FTK Imager	Found
2	Exploit/Trojan Evidence	FTK Imager	Found
3	Operating System Profile	FTK Imager	Found
4	Running Processes	FTK Imager	Found
5	Exploit/Trojan Location	FTK Imager	Found
6	Attacker IP	Magnet RAM Capture	Found
7	Exploit/Trojan Evidence	Magnet RAM Capture	Found
8	Operating System Profile	Magnet RAM Capture	Found
9	Running Processes	Magnet RAM Capture	Found
10	Exploit/Trojan Location	Magnet RAM Capture	Found
11	Attacker IP	Dumpit	Found
12	Exploit/Trojan Evidence	Dumpit	Found
13	Operating System Profile	Dumpit	Found
14	Running Processes	Dumpit	Found
15	Exploit/Trojan Location	Dumpit	Found

This analysis demonstrates that each tool effectively captured essential forensic artifacts associated with a Metasploit attack on a Windows 10 computer. These findings validate the application of live forensics techniques in RAM forensics, aiding digital investigators in cybercrime detection.

4. Conclusion

The live forensics techniques used in this study, involving FTK Imager, Magnet RAM Capture, and Dumpit, effectively acquired digital evidence for analyzing Metasploit attacks on Windows 10. Volatility, as the analysis tool, successfully interpreted RAM images across all acquisition methods, with minor differences in profile suggestions. The forensic analysis identified five critical evidence types within the RAM of the victim's system, including the attacker's IP

address, exploit/Trojan binaries, active processes, OS profile, and execution path of the exploit/Trojan.

Future research could expand this work by applying live forensics techniques to other devices, such as IoT systems or Linux-based environments, and exploring additional RAM acquisition tools to broaden comparative analyses in digital forensics.

References

- 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>