Assignment 4: RAM
Digital Forensics

Elisa Pioldi
ID 12305812

January 17, 2024

1 Background

This analysis is divided into two parts:

1. Acquisition and analysis of a choosen RAM dump
2. Analysis of a RAM dump sent by an unknown source

2 Factual part

2.0.1 Software and hardware specifications

For this analysis, I utilized the following software:

- **Volatility** [1] to analyze the RAM dump.
- **???** [???] to acquire the RAM dump.

2.1 Acquisition

First of all, I had to acquire a RAM dump.

2.2 Analysis of the unknown RAM dump

I received a RAM dump from an unknown source. The SHA-256 of `physmem.raw` is: `fee4a87527509ed8a67c51a2b3e21a74ae52739e0d69020312180339cfd79e3b`

2.2.1 Basic information

First of all, I checked the basic information about the RAM dump, such as the operating system, the architecture, the profile, the time of the dump, etc. The results are shown in Table 1.

Property	Value
layer_name	0 WindowsIntel32e
memory_layer	1 FileLayer
KdVersionBlock	0xf804216099a0
Major/Minor	15.22621
MachineType	34404
KeNumberProcessors	2
SystemTime	2023-01-09 22:17:11
NtSystemRoot	C:\Windows
NtProductType	NtProductWinNt
NtMajorVersion	10
NtMinorVersion	0
PE MajorOperatingSystemVersion	10
PE MinorOperatingSystemVersion	0
PE Machine	34404
PE TimeDateStamp	Mon Jul 5 20:20:35 2100

Table 1: Checksums of important files.

2.2.2 Processes

I looked for the processes running at the time of the dump:

1. **System** (PID 4)
2. **Registry** (PID 88)
3. **smss.exe** (PID 384)
4. **csrss.exe** (PID 576, 652)
5. **wininit.exe** (PID 644)
6. **winlogon.exe** (PID 736)
7. **services.exe** (PID 772)
8. **lsass.exe** (PID 804)
9. **svchost.exe** (PID 908, 424, 536, 1088, 1100, 1208, 1252, 1300, 1324, 1336, 1420, 1452, 1496, 1540, 1752, 1856, 1916, 1924, 1936, 2036, 296, 1484, 2060, 2132, 2156, 2196, 2204, 2240, 2348, 2464, 2484, 2604, 2636, 2784, 2900, 2908, 2916, 2980, 2992, 3016, 3032, 3064)
10. **LogonUI.exe** (PID 852)
11. **dwm.exe** (PID 920)
12. **MemCompression** (PID 2020)
13. **Fontdrvhost.exe** (PID 924, 932)

14. **AggregatorHost** (PID 3456)
15. **sihost.exe** (PID 3584)
16. **SearchIndexer.exe** (PID 6076)
17. **explorer.exe** (PID 4108)
18. **VBoxTray.exe** (PID 6972)
19. **OneDrive.exe** (PID 7056)
20. **SecurityHealth** (PID 6908, 6924)
21. **VBoxService.exe** (PID 1784)
22. **spoolsv.exe** (PID 2484)
23. **msedge.exe** (PID 4800, 6212, 5288, 5260, 2760)
24. **msteams.exe** (PID 7324)
25. **msedgewebview2** (PID 7492, 7508, 7636, 7788, 7800, 7816, 7920)
26. **dllhost.exe** (PID 8108, 9096)
27. **firefox.exe** (PID 7252, 6548, 8244, 8444, 8708, 9112, 9160, 9196, 3940, 4796, 4140, 2508)
28. **Notepad.exe** (PID 8944)
29. **NisSrv.exe** (PID 6004)
30. **ctfmon.exe** (PID 4828)
31. **SearchHost.exe** (PID 4588)
32. **LockApp.exe** (PID 5880)
33. **RuntimeBroker.exe** (PID 7492, 6924, 5012)
34. **taskhostw.exe** (PID 3908, 5184)
35. **userinit.exe** (PID 3820)
36. **RuntimeBroker.exe** (PID 5928)
37. **Widgets.exe** (PID 4684)

2.2.3 Network connections

2.2.4 SID

3 Expert testimony

Observing the information about the RAM dump, we can retrieve the time of the dump, which is **2023-01-09 22:17:11**.

Taking a closer look to the running processes, we see that not all the browsers are the same. In fact, we have **msedge.exe** and **firefox.exe**. This means that the user was using two different browsers at the time of the dump.

I could also find the SID of the user, which is **S-1-5-21-2607170198-3457296929-47938352-1001**. This SID is associated to the user **Spongebob**.

3.1 User password

To retrieve the user password, I first got the hashes contained in the memory dump, then I used an online tool (hashes.com [2]) to crack the hash: this tool searches for the hash in a database of already cracked hashes.

The hash is `bcf8548eae42900beda0f150e16504b5` and the associated password is: `ThisIsPatrick`.

Given this, we can assume that who sent the RAM dump is **Patrick**.

References

[1] Volatility Foundation. *Volatility*. URL: `https://github.com/volatilityfoundation/volatility` (visited on 01/2023).

[2] *Hashes*. URL: `https://hashes.com/en/decrypt/hash` (visited on 01/2023).