

Evaluating the Memory Footprint of Random Access Memory Acquisition Software

Christine Utz and Marcus Thompson
Purdue University

Problem Overview

Volatile Memory Forensics is the branch of Digital Forensics dealing with the acquisition and analysis of volatile memory, i.e., a computer's Random Access Memory (RAM). RAM can contain types of data not found anywhere else on the system such as encryption keys, passwords, and information about the state of the system at the time of the incident under investigation.

There is a multitude of both command line and GUI-based tools for memory acquisition. As with any other program, executing the volatile memory acquisition tool requires the tool itself to be loaded into the computer's volatile memory – at the risk of possibly overwriting valuable evidence.

Memory Dump

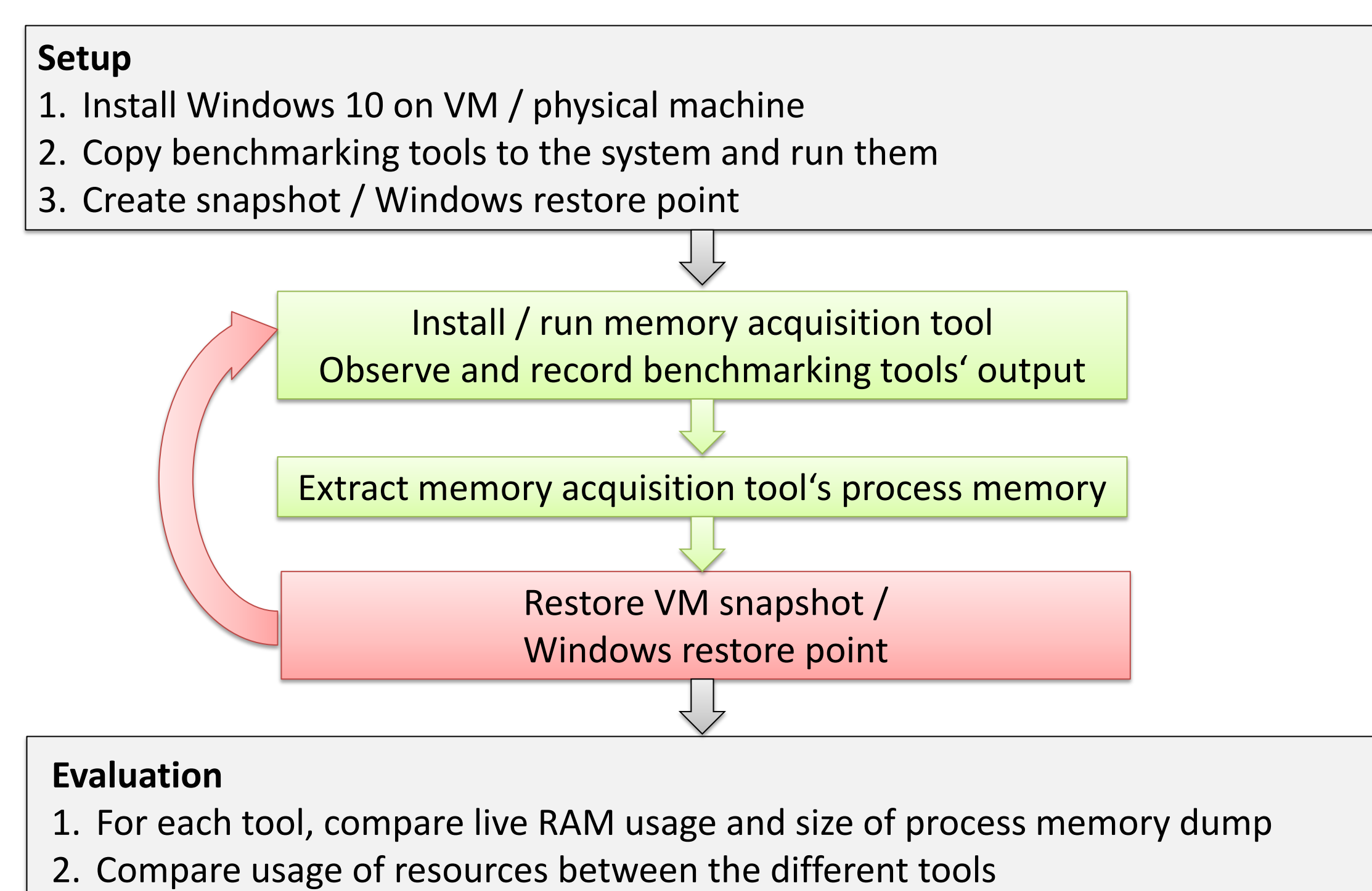
C4 8B D8 0F 8C 9A 00 00 00 4C 8B 64 24 60 44 8B	E-Mail Client Process Memory
AC 24 F0 00 00 00 4C 8D 44 24 40 4D 8B CC 48 8B	
D5 48 8B CF C7 44 24 28 01 00 00 00 41 FF C7 C7	
44 24 20 05 01 00 00 E8 88 FA FF FF 44 8B F0 85	
C0 75 42 48 8B 44 24 48 4C 8B 4C 24 40 4D 8B C4	Browser Process Memory
48 8B D6 48 8B CF 44 89 6C 24 28 48 89 44 24 20	
E8 AB 00 00 00 8B D8 3D 05 00 07 80 0F 84 67 65	
10 00 3D 02 00 07 80 0F 84 5C 65 10 00 85 C0 0F	
85 FE 64 10 00 85 DB 0F 88 81 65 10 00 49 8B CC	
FF 15 FA 10 35 00 44 8B 6C 24 50 4C 8B 74 24 48	
45 33 E4 4C 39 67 70 74 0F 48 8B 4F 70 48 8B 01	
FF 50 20 41 3B C4 7C 12 45 3B EC 0F 84 94 09 00	
00 41 3B DC 0F 8C 8B 09 00 00 4C 39 67 70 74 15	Memory Acquisition Tool Process Memory
48 8B 4F 70 48 8B 01 FF 50 20 B9 C7 04 07 80 41	
3B C4 0F 4C D9 8B C3 48 8B 4C 24 70 48 33 CC E8	
00 00 00 00 00 00 00 00 00 00 00 41 5F 41 5E 41	
5D 41 5C 5F 5E 5D 5B C3 90 90 90 90 90 90 90 90	Password Manager Process Memory
FF F3 55 56 57 41 54 41 55 48 83 EC 68 48 8B 05	
64 63 40 00 48 33 C4 48 89 44 24 50 4C 8B A4 24	
C0 00 00 00 33 DB 49 8B E9 4D 8B E8 48 8B FA 48	
8B F1 48 39 59 70 74 0C 48 8B 49 70 48 8B 01 FF	Word Processor Process Memory
50 20 8B D8 85 DB 0F 88 C6 00 00 00 48 8D 44 24	
48 4C 8D 0D D8 32 38 00 45 33 C0 48 8B D7 33 C9	
48 89 44 24 20 E8 16 D4 FB FF 8B D8 85 C0 0F 88	
9E 00 00 00 F6 46 3C 01 0F 84 5F 66 10 00 33 C0	
EB 00 48 8B 4C 24 48 48 83 64 24 30 00 48 8D 54	
24 40 4C 8B 11 48 89 54 24 28 48 83 64 24 20 00	
4D 8B CD 45 33 C0 48 8B D0 41 FF 52 18 8B D8 85	
C0 78 54 48 8B 54 24 40 48 8B CF E8 20 C3 FB FF	
48 8B D0 48 8B F8 48 F7 DA 1B DB F7 D3 81 E3 0E	
00 07 80 7C 27 8B 94 24 C8 00 00 00 4D 8B CC 4C	

Running the tool can also leave behind other artifacts: It can load additional libraries into memory, write files to the computer's hard disk, or modify the Windows Registry. Ideally, the amount of such artifacts the forensic tool leaves behind is as small as possible to minimize the probability of potential evidence being changed. Forensic examiners thus need to know how many resources each tool uses to determine which is least likely to render their evidence collection inadmissible in court.

Previous research about the artifacts left behind by memory acquisition tools is limited to older tools that do not support current operating systems (1) or does not reveal how the benchmarks were determined (2), which makes the results difficult to compare with the performance of future tools. This research project analyzes the memory, hard disk, DLL, and Windows Registry usage of selected tools for the Windows 10 platform.

Methodology

Every memory acquisition tool is evaluated on both a physical computer and a virtual machine. Snapshots and Windows restore points are used to ensure each tool is tested using the same baseline as depicted below.



The following memory acquisition tools are analyzed:

- Volatility Surge Collect Pro 17.03.13
- Access Data Forensic Toolkit (FTK) Imager 3.1.1
- Access Data Forensic Toolkit (FTK) Imager Lite 3.1.1
- Belkasoft Live RAM Capturer
- Mandiant Memoryze 3.0
- MoonSols / Comae Technologies DumpIt 3.0.109.20161007
- osTriage 2.0.0.3
- CyberTriage 2.0.0

Analysis is performed using the Windows Sysinternals Suite (3) and comparing these benchmarks with the size of the memory acquisition tool's process memory extracted from the resulting memory dump.

Challenges

- Benchmarking can only be performed with a finite set of test cases and evaluation methods. How many runs and readings are enough to create reliable results?
- How much resource usage is considered "too much", thus rendering the memory acquisition process forensically unsound and the collected data inadmissible in court?

References

- (1) Sutherland, I., Evans, J., Tryfonas, T., & Blyth, A. (2008). Acquiring Volatile Operating System Data Tools and Techniques. *ACM SIGOPS Operating Systems Review Volume 42 Issue 3, April 2008*, (pp. 65-73).
- (2) McDown, R. J., Varol, C., Carvajal, L., & Chen, L. (2016). In-Depth Analysis of Computer Memory Acquisition Software for Forensic Purposes. *Journal of Forensic Sciences* (61), pp. 110-116.
- (3) Russinovich, M., Margosis, A. (2016). *Troubleshooting with the Windows Sysinternals Tools*.