CERIAS

The Center for Education and Research in Information Assurance and Security

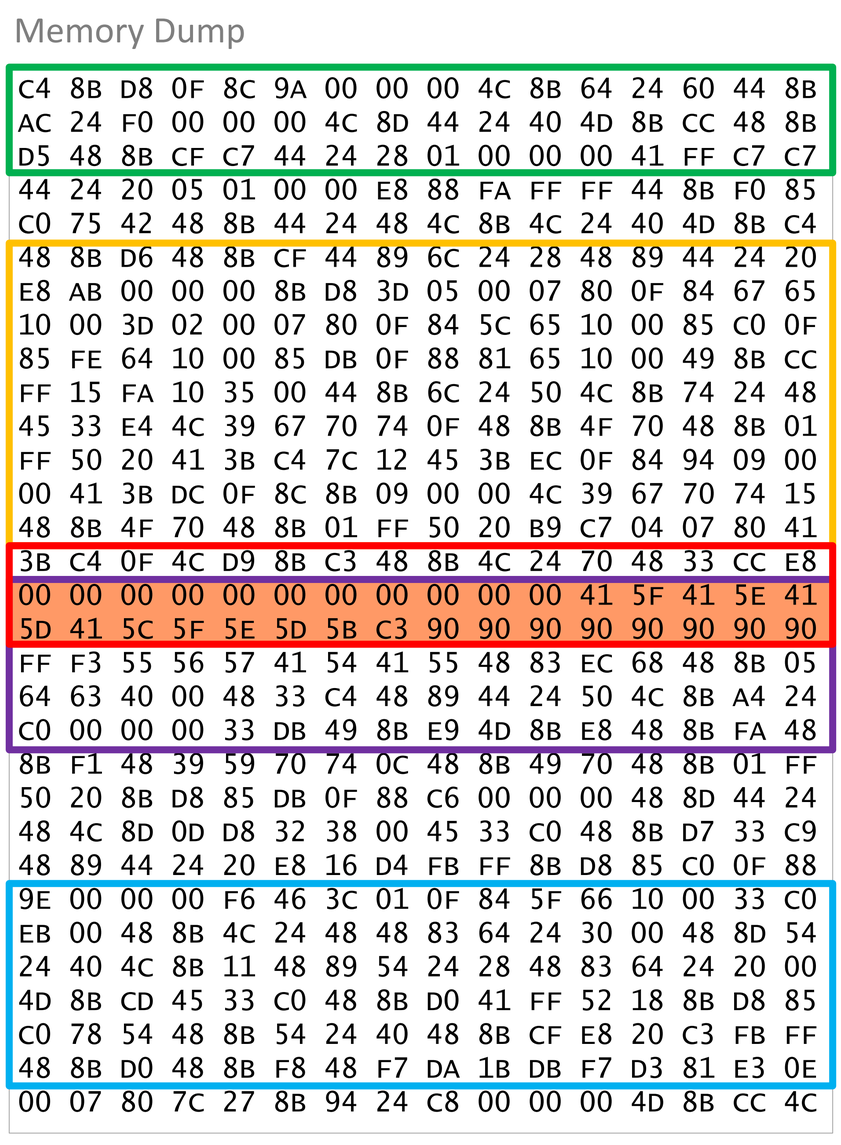
Evaluating the Memory Footprint of Random Access Memory Acquisition Software

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.

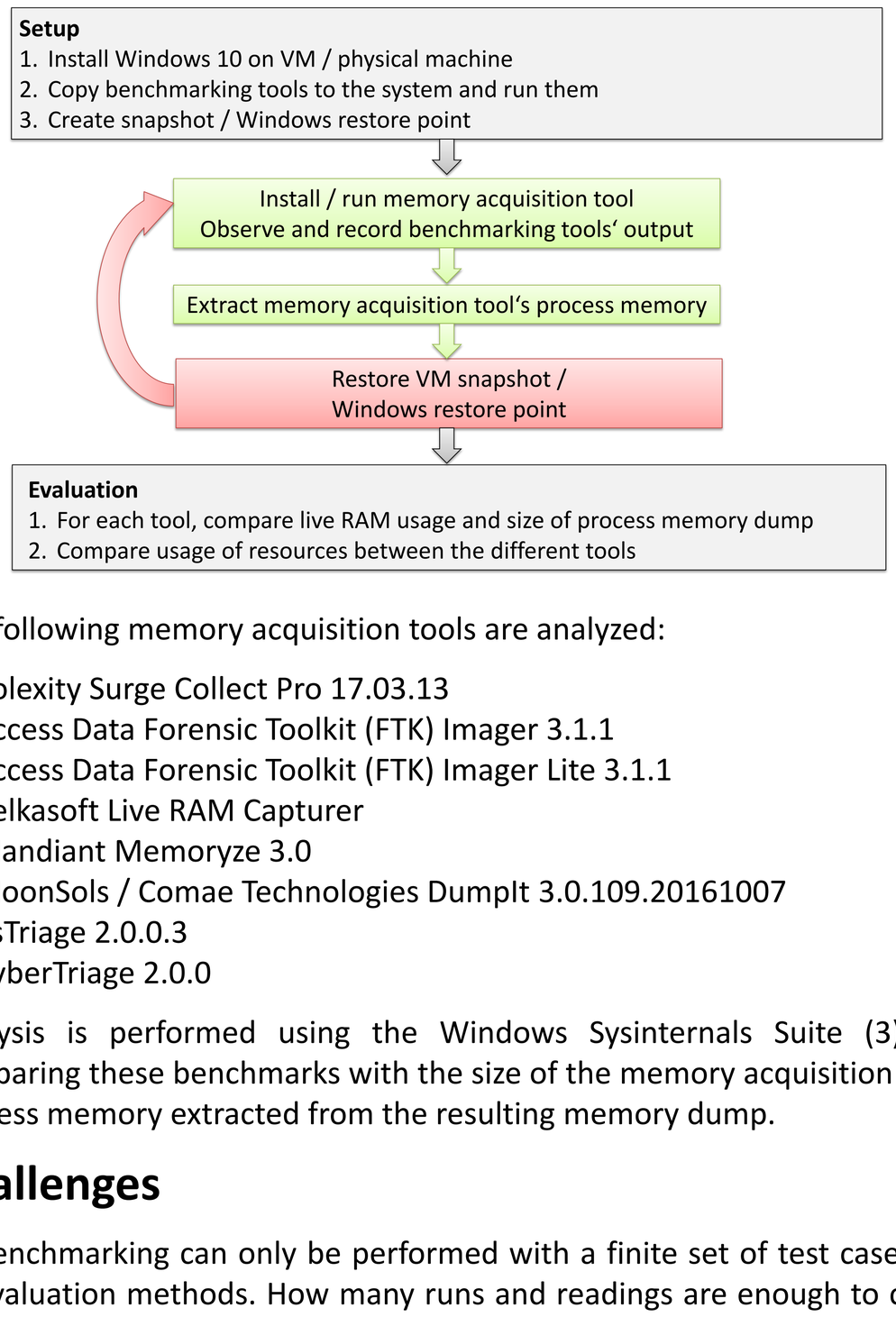


Running the tool can also leave behind other artifacts: It can load additional libraries into memory, write files to the computer's hard disk, or modify the Windows Registry. Ideally, the amount of such artifacts the forensic tool leaves behind is as small as possible to minimize the probability of potential 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:

- Volexity 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.

CERIAS

PURDUE UNIVERSITY