CERIAS

The Center for Education and Research in Information Assurance and Security

A Benchmark of Anti-Memory Forensic Tools (WIP)

Zachary Thoreson, Marcus Thompson

Abstract

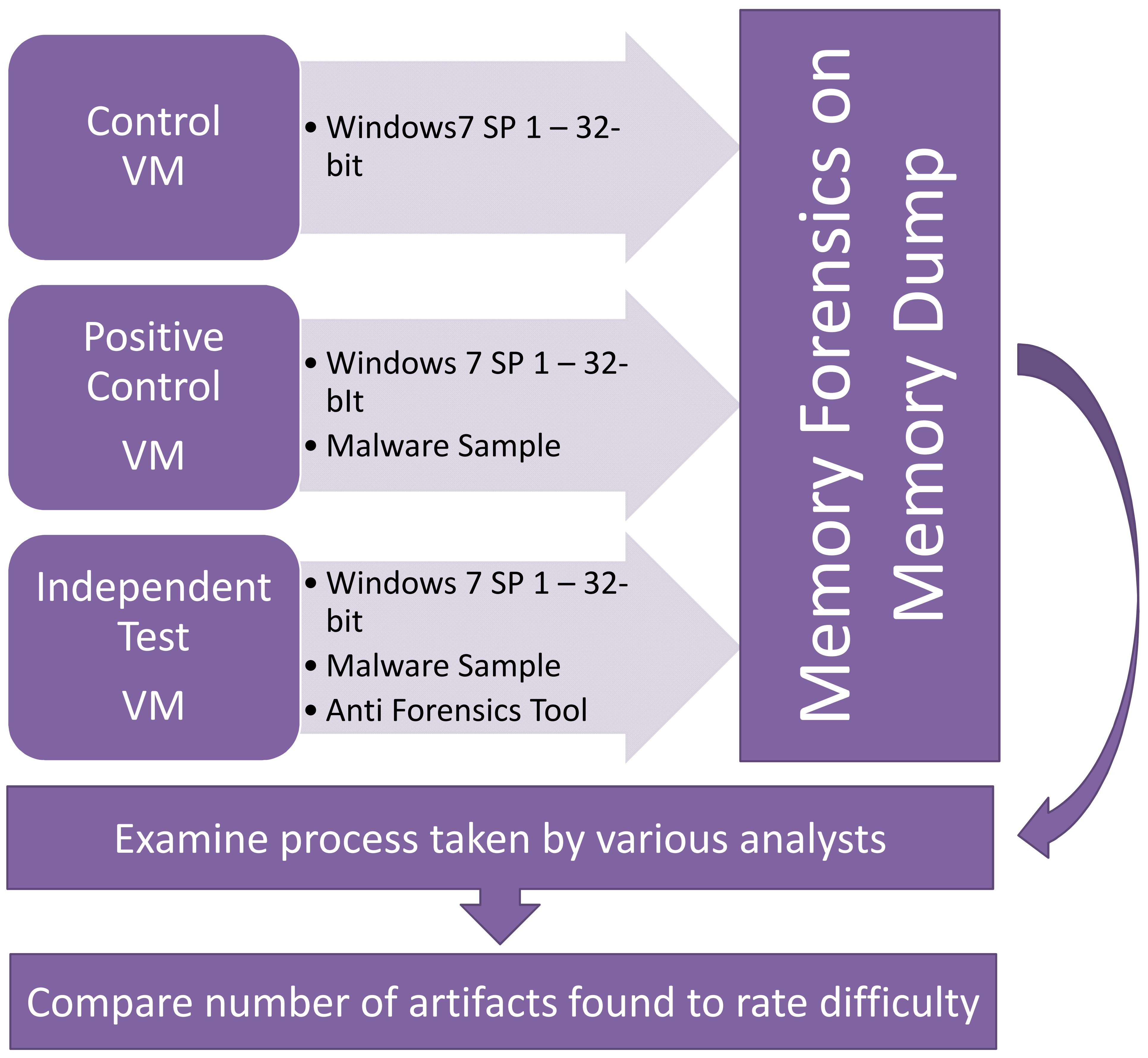
Memory forensics is a critical component in crime scene analysis, reverse engineering, and detection of malware. During the static and dynamic phases of memory forensics, an analysts tools are a critical component in the detection and investigation of artifacts that may be of interest to the analyst.

While these tools allow the processing and analysis of memory dumps taken from computers, they are not perfect. Anti-memory forensics tools seek to obfuscate the analyst's results by creating false positives and large amount of entries that make the analysts job more difficult.

This study took proof of concept anti-forensic tools, and tested effectiveness in creating false artifacts to be later investigated using Volatility. The goal of the experimentation was to establish a benchmark as to how difficult it would be to detect fake entries using memory forensic tools.

The experiment consisted of a clean Windows 7 Virtual Machine, a Windows 7 Virtual Machine with a known malware sample, and a Windows 7 Virtual Machine with the malware sample and the anti-forensic tool.

Methodology


Control VM
• Windows7 SP 1 – 32-bit
Positive Control VM
• Windows 7 SP 1 – 32-bit
• Malware Sample
Independent Test VM
• Windows 7 SP 1 – 32-bit
• Malware Sample
• Anti Forensics Tool
Memory Forensics on Memory Dump
Examine process taken by various analysts
Compare number of artifacts found to rate difficulty

Results & What to Look For (Expected – Work in Progress)

Network Traffic
- Hidden or fake IP Address Connections appear when using Netscan
- Obscure traffic or create additional connections

Processes
- Unlinking or hiding of entries normally found using psxview
- Creation of other misleading processes

Drivers & DLLs
- Prevention of dumping of drivers or DLLs for analysis in IDA Pro

Other
- Possible termination or breaking of tools such as Volatility
- One-Byte Modifications

During a forensics investigation, evidence of malicious activity can be found within memory. These artifacts can range from network activity, process injection, rouge processes, API hooking, fake or hijacked drivers, and even modification of the registry files on the system.

When a process appears out of place or a network connection looks like it should not have occurred, the analyst can then pursue those specific process IDs or memory offsets and ultimately begin to build a profile of what the malware looks like.

For an anti-forensics tool to effectively do its job, it must prevent the analyst from producing accurate results through obfuscation or attacks against the tool or investigative process. To do so, artifacts after the use of an anti-forensics tool may be either hidden or changed so they do not appear suspicious. There is also the alternative that there could be so much data that It makes it difficult to find.

The expected results of this experiment would be that the anti-forensics tool accomplishes its goal by hiding artifacts or producing fake ones that mislead the analyst. If network traffic is hidden for a specific process or processes become hidden or unlisted/unlinked, an accurate analysis is much more difficult to produce. This difficulty will be measured by the difficulty for a novice level analyst to find artifacts in memory left behind by the malware. To further understand the impact of experience, a number of students could be used to test the difficulty as well. The number of steps taken as well as the number of artifacts found could be compared to trials done by professionals in the field to rate difficulty.

CERIAS

PURDUE UNIVERSITY