

MASTER'S PROJECT ARTIFACT

Project Title: Windows 10 Ransomware Memory Forensics: An Experimental Analysis of Acquisition Timing Using WinPmem, SIFT Workstation and Volatility 3

Student Name: Gopika Virakan Valappil

Programme: MSc Cybersecurity and Digital Forensics

1. Artifact Overview

This artifact contains the experimental materials and supporting evidence produced during the Master's Project. The project investigates the effect of volatile-memory acquisition timing on the recovery and interpretation of forensic artefacts associated with controlled ransomware-like activity.

The investigation was conducted within a controlled virtualised laboratory environment. A benign PowerShell-based ransomware-behaviour simulation was used instead of live ransomware.

2. Experimental Environment

The experimental environment consisted primarily of:

- Windows 10 victim virtual machine
- SIFT Workstation
- Kali Linux supporting environment
- Oracle VirtualBox
- WinPmem
- Volatility 3
- PowerShell
- Supporting Linux utilities for string examination and SHA-256 verification

3. Experimental Stages

T0 – Clean baseline memory acquisition.

T1 – Initial controlled experiment involving EARLY and POST memory acquisition around the benign ransomware-behaviour simulation.

T2 – Principal temporal experiment involving PRE, MID and POST memory acquisition stages.

T3 – Supporting experiment used to examine recurring forensic artefacts and acquisition-related activity.

4. Forensic Analysis

The acquired memory images were analysed primarily using Volatility 3. The principal plugins used were:

- windows.pslist
- windows.pstree
- windows.cmdline
- windows.malfind

Supporting string examination was used to identify experimental indicators including the simulator path, Rename-Item, the .locked extension and the predefined simulation marker.

SHA-256 hashing was used after memory acquisition to provide integrity reference values for the acquired evidence.

5. Artifact Folder Structure

01_README

Contains this document and provides an overview of the artifact.

02_Experiment_Design

Contains documentation relating to the experimental architecture, configuration and experimental procedure.

03_Simulator

Contains the benign PowerShell-based ransomware-behaviour simulator used during the controlled experiment.

04_Memory_Acquisition

Contains memory-acquisition information, acquisition commands, memory-image records and SHA-256 integrity information.

05_Forensic_Analysis

Contains retained forensic-analysis outputs associated with the experimental stages.

06_Results

Contains supporting comparative experimental results.

07_Supporting_Evidence

Contains screenshots and VirtualBox snapshot evidence documenting the practical investigation.

6. Safety and Ethical Statement

No live ransomware was executed during this project. The experimental activity used a controlled benign PowerShell-based simulation operating on researcher-created test files within a virtualised laboratory environment.