Comparative Analysis of Open-Source Forensics
Tools to Efficiently Conduct Memory Forensics

MSc Research Project
MSc Cybersecurity

Ashley Sunny George
Student ID: 21218714

School of Computing
National College of Ireland

Supervisor: Mr. Eugene McLaughlin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:……. …Ashley Sunny George……………………………………………………………………

Student ID: …………21218714..……………………………………………………………………………..……

Programme: …………MSc Cybersecurity……………………… **Year:** …………1………………..

Module: …………MSc Research Project…………………………………………………………….………

Supervisor: …………Mr. Eugene McLaughlin………..…………………………………………….………

Submission Due Date: …………14-12-2023.……………………………………………………………….………

Project Title: ………… Comparative Analysis of Open-Source Forensics Tools to Efficiently Conduct Memory Forensics

Word Count: ……………219…………………… **Page Count**………………2………….……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

Date: …………………………14-12-2023……………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Ashley Sunny George
Student ID: 21218714

1 System Requirements

Minimum System Requirements:

CPU	Intel(R) Core(TM) i3
RAM	8.0 GB
Clock Speed	2.50 GHz
Operating System	Windows 10
Architecture	x64
Hard Disk	256 GB

Recommended System Requirements:

CPU	Intel(R) Core(TM) i7
RAM	16.0 GB
Clock Speed	2.50 GHz
Operating System	Windows 11 Pro
Architecture	x64
Hard Disk (SSD)	1 TB

2 Acquisition tools required

Tool Name	**Version**	**Link**
DumpIt	3.1.0.0	https://www.magnetforensics.com/resources/magnet-dumpit-for-windows/
Magnet RAM Capturer	1.2.0.0	https://www.magnetforensics.com/resources/magnet-ram-capture/
Belkasoft RAM Capturer	1.0	https://belkasoft.com/ram-capturer
FTK Imager	4.7.1.2	https://www.exterro.com/ftk-imager
Redline	2.0.1	https://fireeye.market/apps/211364

3 Analysis tools required

Tool Name	Version	Download Link
Volatility	2.6	https://www.volatilityfoundation.org/releases
Redline	2.0.1	https://fireeye.market/apps/211364

4 Other tools and resources required

Windows tools:

- Task Manager
- Resource Monitor

Other files required:

- Trusted crash dump sample files for memory analysis

References

Volatilityfoundation (2019) Memory Samples, GitHub. Available at: https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples (Accessed: 14 December 2023).

Volatilityfoundation (2020) volatilityfoundation/volatility: An advanced memory forensics framework, GitHub. Available at: https://github.com/volatilityfoundation/volatility (Accessed: 14 December 2023).

MAGNET DumpIt for Windows (2023) Magnet Forensics. Available at: https://www.magnetforensics.com/resources/magnet-dumpit-for-windows/ (Accessed: 14 December 2023).

MAGNET RAM Capture (2022) Magnet Forensics. Available at: https://www.magnetforensics.com/resources/magnet-ram-capture/ (Accessed: 14 December 2023).

Belkasoft RAM Capturer: Volatile Memory Acquisition Tool. Available at: https://belkasoft.com/ram-capturer (Accessed: 14 December 2023).

FTK® Imager (no date) Exterro. Available at: https://www.exterro.com/ftk-imager (Accessed: 14 December 2023).

Redline FireEye Market. Available at: https://fireeye.market/apps/211364 (Accessed: 14 December 2023).