National College of Ireland

Project Submission Sheet

Student Name: Manoj Santhoju

Student ID: 23394544

Programme: MSc in Cybersecurity **Year:** 2025-2026

Module: Practicum

Lecturer: Dr. Zakaria Sabir

Submission Due Date: 15-06-2025

Project Title: MEMORY FORENSICS IN MODERN OPERATING SYSTEMS: TECHNIQUES AND TOOL COMPARISON

Word Count: 760

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 references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: Manoj Santhoju

Date: 15-06-2025

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

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

AI Acknowledgement Supplement

[Insert Module Name]

[Insert Title of your assignment]

Your Name/Student Number	Course	Date

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

[Insert Tool Name]	
[Insert Description of use]	
[Insert Sample prompt]	[Insert Sample response]

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:

[Place evidence here]

Additional Evidence:

[Place evidence here]

MEMORY FORENSICS IN MODERN OPERATING SYSTEMS: TECHNIQUES AND TOOL COMPARISON

Manoj Santhoju
23394544
Programme Code – Research in Computing CA1
National College of Ireland

1. Research Problem Background

“Memory forensic investigations” have emerged as a crucial part of digital forensics, with relevance continually increasing due to the surge in sophisticated cybercrimes that exploit “volatile memory” for stealth. Conventional forensic methods primarily focus on static data sources, such as “hard drives” and “storage devices”. A host of modern cyber threats, from “advanced persistent threats(APTs)” to “fileless malware”, linger in the system memory, giving no time to etch any trace of their existence. The forensic practitioners, hence, have taken a step toward memory forensics to extract crucial pieces of evidence such as “running processes”, “network sockets”, “cryptographic keys”, and “injected codes” that simply never make it onto disk.

Modern OS such as “Windows 11”, “latest Linux kernel distributions”, and “macOS” have made the complexity of memory forensics grow. Being equipped with some of the best protections in the memory area, these operating systems prevent the traditional memory parsing, such as “kernel data isolation”, “secure boot”, and “address space layout randomization (ASLR)”. Different tools have been made using different architectures and support plugins. Implementation is also dependent on the OS. Whatever their increased use, a systematic comparison of their effectiveness against modern OS platforms remains absent from both academic and professional research.

2. Research Question

- How do the latest memory forensics tools compare in terms of detection accuracy, performance efficiency, and OS compatibility, concerning the volatile-memory analysis of modern operating systems such as Windows, Linux, and macOS?

3. Justification

The research question is significant because it focuses on a pressing need in the cybersecurity field, which is to evaluate and improve forensic methods of analysis for modern systems. With malicious actors increasingly turning to system memory to hide their malicious activities, choosing the correct memory analysis method can be crucial for detection and mitigation.

While memory analysis tools such as “Volatility” and “Rekall” are used extensively, without a systematic comparative study, investigators cannot know which produces the fastest and accurate results for a particular OS. The proposed study is feasible due to the usage of “open-source” tools and “memory dump” samples from public sources. Controlled environments can be established with VMs running “Windows”, “Linux”, and “macOS” updated versions, respectively.

Each auto forensic tool under study can be run on the same memory dump scenarios so that it can be evaluated consistently. These questions are measurable, breaking down to metrics such as “detection accuracy (true/false positives)”, “performance (execution time, CPU/memory usage)”, and “OS support (degree to which a plugin was successful or failed)”. Minimal ethical implications exist as no real-world personal or sensitive data will be used, and there will be synthetic data sources or data generated within isolated environments. This can help in generating new knowledge in “cybersecurity and digital forensics” by providing practical toolkit usage recommendations in modern memory investigations.

4. Specific Items to Be Addressed

The study begins by establishing a fundamental understanding of “memory forensics”, explaining its importance to “digital investigation”, and contrasting “volatile” with “non-volatile” data. The internal “memory architecture” of “Windows”, “Linux”, and “macOS” can be examined to define structures and components of interest for forensic extraction, such as “process lists”, “kernel modules”, and “memory-mapped files”.

Special attention can be given to aspects of the selection and configuration of forensic tools involved in this study, such as “Volatility”, “Rekall”, and “MemProcFS”. Each tool can be installed under standard environment conditions and tested against several memory dumps from VMs simulating “malware infections” or suspicious activity. Considerations involve whether a tool detects “malicious artifacts”, its processing speed, and the scope of OS versions it supports. The results can be discussed regarding the strengths and weaknesses of each tool.

Bibliography

Daghmehchi Firoozjaei, M., Habibi Lashkari, A. and Ghorbani, A.A., 2022. Memory forensics tools: a comparative analysis. *Journal of Cyber Security Technology*, *6*(3), pp.149-173.

Javed, A.R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K. and Gadekallu, T.R., 2022. A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. *IEEE Access*, *10*, pp.11065-11089.

Kara, I., 2023. Fileless malware threats: Recent advances, analysis approach through memory forensics and research challenges. *Expert Systems with Applications*, *214*, p.119133.

Nyholm, H., Monteith, K., Lyles, S., Gallegos, M., DeSantis, M., Donaldson, J. and Taylor, C., 2022. The evolution of volatile memory forensics. *Journal of Cybersecurity and Privacy*, *2*(3), pp.556-572.

Shree, R., Shukla, A.K., Pandey, R.P., Shukla, V. and Bajpai, D., 2022. Memory forensic: Acquisition and analysis mechanism for operating systems. Materials Today: Proceedings, 51, pp.254-260.