

Kara proposal

by Kara Thomas

Submission date: 23-Oct-2025 11:15AM (UTC+0100)

Submission ID: 265892333

File name: 50547_Kara_Thomas_Kara_proposal_695044_2097994824.docx (106.92K)

Word count: 1628

Character count: 9159



TO CARRY OUT A FORENSIC ANALYSIS ON MALWARE INFECTED VIRTUAL MACHINES.



Kara Thomas (2304862)

UNIVERSITY OF WALES TRINITY SAINT DAVID [Company address]

Contents

1. Introduction	1
2. Background to the Proposed Research	1
3. Research Problem statement	2
4. Research Aim & Objectives	3
5. Methodology.....	3
5.1 Methods.....	3
5.2 Materials	3
6 Project Plan	3
7.References.....	4

1. Introduction

The project is to execute a forensic analysis on malware infected systems which are simulated on a virtual machine. The analysis will be carried out using digital forensic tools with the purpose of identifying different attack methods, points of entry and recovering evidence. The reason for choosing a project in the digital forensics field is due to it being a current and developing field. There is constant ongoing research with upcoming developments such as the look into ongoing research in IoT (Internet of Everything) Forensics. Furthermore, this specific scenario of malware infecting computer systems and data needing to be recovered is not an uncommon one and affects organisations no matter the size. A well-known example of this is the WannaCry attack. The WannaCry attack was a ransomware attack that happened in May 2017 which caused a worldwide cyber-attack on Windows computer systems that were missing a year-old security patch. Over 200,000 computer systems were affected across 150 countries. One of the victims of the attack was the UK's NHS which is the biggest cyber-attack it has faced. It caused severe disruption to both staff and patients in England alone it caused 6,912 appointments to be cancelled. [1] [2]

This project would allow for better understanding on what tools could effectively recover data from the malware's attack. In addition, it would allow for insight into its attack vectors allowing for additional new and relevant security measures to be implemented.

2. Background to the Proposed Research

The area of study this project is taking place in is with digital forensics. Digital forensics has become an integral part of the response to security breaches; it allows for any data to be recovered and analysed which can help identify the method and point of entry of the attack. This in turn is used to further improve the system's security infrastructure. Within the field there are many different specialties such as mobile forensics which entails investigating smart phones and tablets, file system forensics which focuses on investigating files and folders on a device such as computers and servers for evidence and, network forensics which has investigators looking at packet traffic. [3]

There are different specialist tools used regularly within the field, one of which is FTK imager. Set up by Access Data Group, FTK imager has multiple different uses one of which is it is able to create a copy of the data on the hard drives, USB thumb drives, CDs etc allowing for the evidence to be looked

through without any risk of it being accidentally tampered with. A benefit of this is it keeps the integrity of the original data. Another feature it has is that it can capture data from the system's RAM allowing for another opportunity for data to be extracted. There two types of FTK imager the free and pro version, the previously stated features are in both. An extra feature that FTK imager pro has is it allows for drives that are encrypted with McAfee, Symantec, BitLocker etc to be decrypted instantly, allowing for files on the drive to be accessed a lot quicker. [4] [5] [6]

Another digital forensic tool most commonly used with network forensics is Wireshark which is an open-source software that allows network administrators to monitor and analyse network packets. It has multiple different features one of them is that the network traffic can be looked at live showing in real time what packets are coming in and out of the network. Another feature is that the packets in the network traffic can be filtered by multiple types of criteria allowing for a more tailored experience. [7] [8]

An additional example of a popular digital forensic tool is the free software Autopsy. Autopsy acts as a GUI(Graphical User Interface) version to command line tools used in the Sleuthkit. It has other features too such as allowing multiple investigations on the go at once and having the option to search for keywords in the data. It is quite flexible as it is available on Linux, MacOS and Windows. [9] [10]

The final example of a digital forensic tool is Volatility which focuses specifically on carrying out forensics and analysis on the system's temporary memory. It was first released by the company Black Hat DC and it was one of the first digital forensic tools to focus on memory forensics. [11]

One of the main developments recently in digital forensics is the incorporation of using artificial intelligence and machine learning. A use of AI in the field includes it being used to automate different tasks allowing for investigators time to be allocated elsewhere. One specific example of this is for it helping with identifying pattern recognition in the data being analysed to become an automated process. Another example is it being used in Natural Language Processing (NLP) which combs through and analyses emails, text messages and social media messages. From there it will pick out what parts of the text are relevant and important pieces of information. [12]

An area that is getting further development is IoT (the Internet of Things) forensics. This is due to the rise in everyday devices that have the software to connect to the internet to exchange or retrieve data. Some examples of IoT devices include smart watches, smart fridges, and smart lights. As the creation of these devices are recent there is still developments being worked on. [13]

There is a research gap in the comparison of multiple modern malware infected operating systems such as Windows 11 having malware analysis conducted on them with the use of digital forensic tools.

3. Research Problem statement

The problem that my project aims to cover is if an attacker was to plant malware onto the computer system what would be the best method to extract any saveable data. The impact of malware infecting a company's systems could lead to data breaches and money being lost so it is important to

understand how these attacks occur to improve security and prevent similar attacks from taking place in the same entry points.

4. Research Aim & Objectives

AIM: Look at the impact of a virtual machine contaminated with malware and retrieve any recoverable data with the use of digital forensic tools.

Objectives:

- Research digital forensic tools that will be efficient to recover malware systems.
- Simulate two malware infected virtual machines.
- Extract any information that can be recovered.
- Analyse the data recovered from the infected system.
- Produce a forensic report to showcase my findings.

5. Methodology

5.1 Methods

For this the project the research method that will be used is mixed methods as there will be different types of data being analysed. The research strategy that will be used for this project will be an experiment. This is the most appropriate for the project as it is practical focused with minor background research. It does not fall into the software development category as no software is being created for this project, only preexisting software is being used. Any evidence recovered from the systems will be analysed using different digital forensic tools.

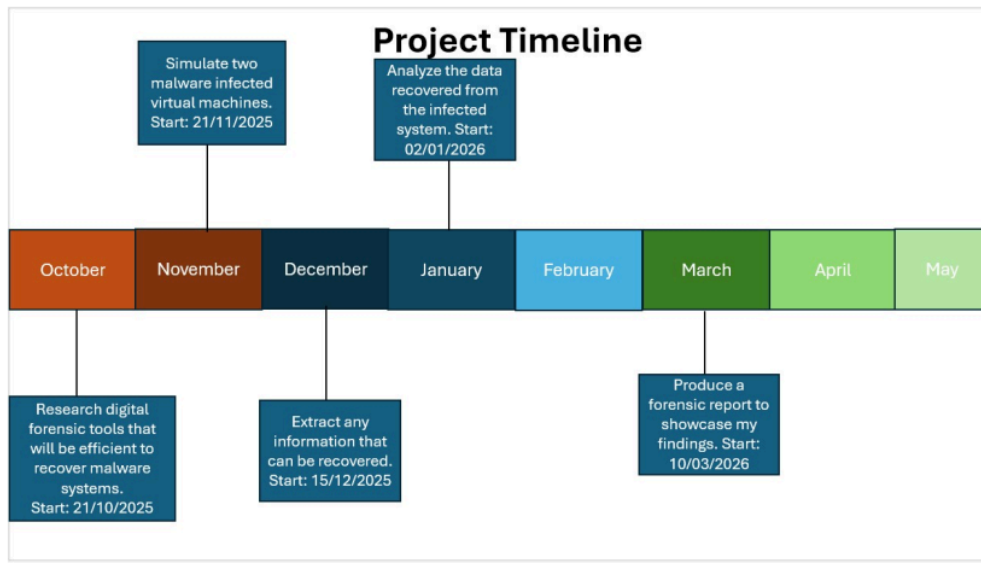
5.2 Materials

An ethical consideration is that the data that will need to be recovered and used in the experiment needs to be sample data and not personal or other people's data.

The use of Windows and Linux and virtual machines on Oracle VirtualBox. The hardware requirements for this project are 30MB free to install Oracle VirtualBox and a further an estimated 70 GB to install both Windows and Linux virtual machines. [14] [15]

6 Project Plan

Below showcases the rough timeline of when I want to carry out each of the projects main objects leading up to the submission deadline in May.



7. References

- [1] NHS England, "NHS England business continuity management toolkit case study: WannaCry attack," NHS, 21 April 2023. [Online]. Available: <https://www.england.nhs.uk/long-read/case-study-wannacry-attack/>. [Accessed 17 October 2025].
- [2] BBC, "NHS 'could have prevented' WannaCry ransomware attack," BBC, 27 October 2017. [Online]. Available: <https://www.bbc.co.uk/news/technology-41753022>. [Accessed 19 October 2025].
- [3] V. M. S. G. K. N. M. Asheesh Tiwari, "Developing Trends and Challenges of Digital Forensics," in *International Conference on Information Systems and Computer Networks (ISCON)*, Mathura, India, 2021.
- [4] Exterro, "FTK Imager," Exterro, N/A. [Online]. Available: <https://www.exterro.com/digital-forensics-software/ftk-imager>. [Accessed 17 October 2025].
- [5] Exterro, "Introducing Exterro FTK Imager Pro: Faster, Smarter, and Built for Today's Investigations," Exterro, 24 September 2025. [Online]. Available: <https://www.exterro.com/resources/blog/introducing-exterro-ftk-imager-pro-faster-smarter-and-built-for-todays-investigations>. [Accessed 18 October 2025].
- [6] S. B. G. G. Himanshu, "Comparative analysis of acquisition methods in digital forensics," in *2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, Sonapat, India,, 2021.

- [7] L. Bock, Learn Wireshark: A definitive guide to expertly analyzing protocols and troubleshooting networks using Wireshark, Packt Publishing, 2022.
- [8] Wireshark, "Wireshark Frequently Asked Questions," Wireshark, N/A. [Online]. Available: <https://www.wireshark.org/faq>. [Accessed 18 October 2025].
- [9] Sleuthkit, "Autopsy," Sleuthkit, N/A. [Online]. Available: <https://www.sleuthkit.org/autopsy/v2/>. [Accessed 18 October 2025].
- [10] J. P. A. D. M. S. Mitchell Farnan, "Digital Forensic Tools: Comparison of Autopsy TSK and Forensic Explorer," in *2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems*, Bangalore, India, 2024.
- [11] Volatility, "About The Volatility Foundation," Volatility, N/A. [Online]. Available: <https://volatilityfoundation.org/about-volatility/>. [Accessed 18 October 2025].
- [12] T. M. K. Md Zakir Hossain Zamil, "AI-Driven Digital Evidence Triage in Digital Forensics: A Comprehensive Review," Boston, MA, USA, 2025.
- [13] IBM, "What is the Internet of Things (IoT)?," IBM, N/A. [Online]. Available: <https://www.ibm.com/think/topics/internet-of-things>. [Accessed 18 October 2025].
- [14] Debian, "2.5. Memory and Disk Space Requirements," Debian, N/A. [Online]. Available: <https://www.debian.org/releases/stable/arm64/ch02s05.en.html>. [Accessed 18 October 2025].
- [15] Microsoft, "Windows 11 requirements," Microsoft, 17 June 2025. [Online]. Available: <https://learn.microsoft.com/en-us/windows/whats-new/windows-11-requirements>. [Accessed 18 October 2025].

Kara proposal

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

60/100

PROJECT PROPOSAL – ACCA6020 INDEPENDENT PROJECT

**Student: Kara
Thomas
Mark:
60**

Intro / A&O (400 words)		
Project title; Identification of a specific problem to be investigated; Well-defined aims and SMART objectives; Explaining why this project is worth doing; Discussion of what the project needs to do in order to be a success; Description any deliverables that will be produced at the end of the project	20	11
Problem identified but need refinement. Aim and objectives need to be improved; some level of refinement. a		

Background to the Project / Literature Review (400 words)		
Description of how the work to be done by in the project relates to the work identified in the literature review; Discussion of any ethical issues raised by the project Identifying what has already been done within the field; Topic familiarity; Brief literature review using appropriate sources – 6-8 journal papers and book chapters rather than just websites; Selection of relevant models & concepts Background could articulate more the need for forensics investigation and data recovery at it relates to increase in cybercrime. This crime may require data recovery when there is a legal case that appears in court. More in-depth lit review will need to be done.	20	11
Project Design (500 words)		
Clear statement of which development methods are to be used and why they are appropriate; Clear statement of which tools are to be used and why they are appropriate; Clear description of how data collected will be analysed	30	18

This section is done very briefly. It would be good if you had used a block diagram to illustrate the design method.		
Resources / Planning (200 words)		
List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices Project timeline done. Ethics form completed.	15	10
Document Presentation		
Correct spelling, grammar and punctuation; Flow of narrative/fluency; Coherence; Word processed ; Correct use of referencing with	15	10

bibliography; Strict word limit Could do with formatting alignment. Introduction could do with paragraphing, etc. Avoid using first person tense such as “my”.		
TOTAL	100	60

PAGE 1
PAGE 2
PAGE 3
PAGE 4
PAGE 5
PAGE 6