Block Based Signature Detection for Forensic Triage

Student name: Karan Nihalani

Supervisor name: Robert Hegarty

Course-Specific Learning Outcomes: On successful completion of this unit, this student will be able to:

- Interpret legislation appropriate to computer professionals and also be aware of relevant ethical issues and the role of professional bodies.
- Apply the principles and operation of languages, compilers and interpreters.
- Demonstrate effective communication, decision making and creative problem solving skills, and identify appropriate practices within a professional, legal and ethical framework.
- Use knowledge, abilities and skills for further study and for a range of employment in areas related to scientific and technical computing.

Project Abstract

In today's world, digital forensics and computer science plays a very important role in solving most, if not practically all, criminal offences. The identification of mistakes and flaws certain devices or people have committed, which lead us to crimes, such as, hacking, malware installation, identity theft and more, are represented to us as a timeline of events. The US-CERT mentions Computer Forensics to be very important due to the idea that "adding the ability to practice sound computer forensics will help you ensure the overall integrity and survivability of your network infrastructure" and ignoring the critical use of digital forensics would result in risking "destroying vital evidence or having forensic evidence ruled inadmissible in a court of law" (US-CERT, 2008).The clarification of some terminologies is required, in order to fully comprehend the methodologies utilized for the analysis and detection of a crime, starting with, *'What is Digital Forensics?'*

Digital Forensics is defined as the practice of "retrieving, storing and analysing electronic data that can be useful in criminal investigations" (NIST, 2019) and diving even further into the digital forensics investigative process, we find it a fundamental aspect to be able to search and extract data that can or have caused harm to the compromised digital device.

Going further, it is necessary to have knowledge on the Digital Forensics Triage, which is the process of attempting to access data as efficiently as possible and understanding the damage caused to the harmed device, where the endgame would be providing an explanation or a solution for the crime taken place, all through the "collection, assembly, analysis, and prioritization of evidence from a crime" (N. Burton, 2018). This provides advantages to an investigation, as time can be saved, avoiding evidence from being collected in masses and therefore, being able to give importance to the relevant data or information found on the computer.

A widely used approach to digital forensics is the application of, *signature detection*. Signature detection encompasses the idea of being able to identify malicious patterns in a block or piece of data, which leads to the comparison of certain signatures with other signatures found in data of known attacks and the ability of detecting these. Although signature detection is a frequently used method in forensic investigations, it is not considered the only aspect of digital forensics. Two types of detection employed within the industry are, *file hash-based* and *block-based* signature detection,

where an example would be a rather simple one as the detection of file signatures are utilised in a simpler manner, in the case of an image viewer application, the app would “recognise the header signature as an image file and will correctly open it” (B. Shavers, J. Bair, 2016). We already have a fair idea about how these detection techniques work and therefore, this project will allow me to conduct a detailed research into these two approaches. Further on, I will be developing a tool that implements and compares these two methods determining the importance of accuracy and efficiency needed for using signature detection in a live investigation.

Project Aims and Objectives:

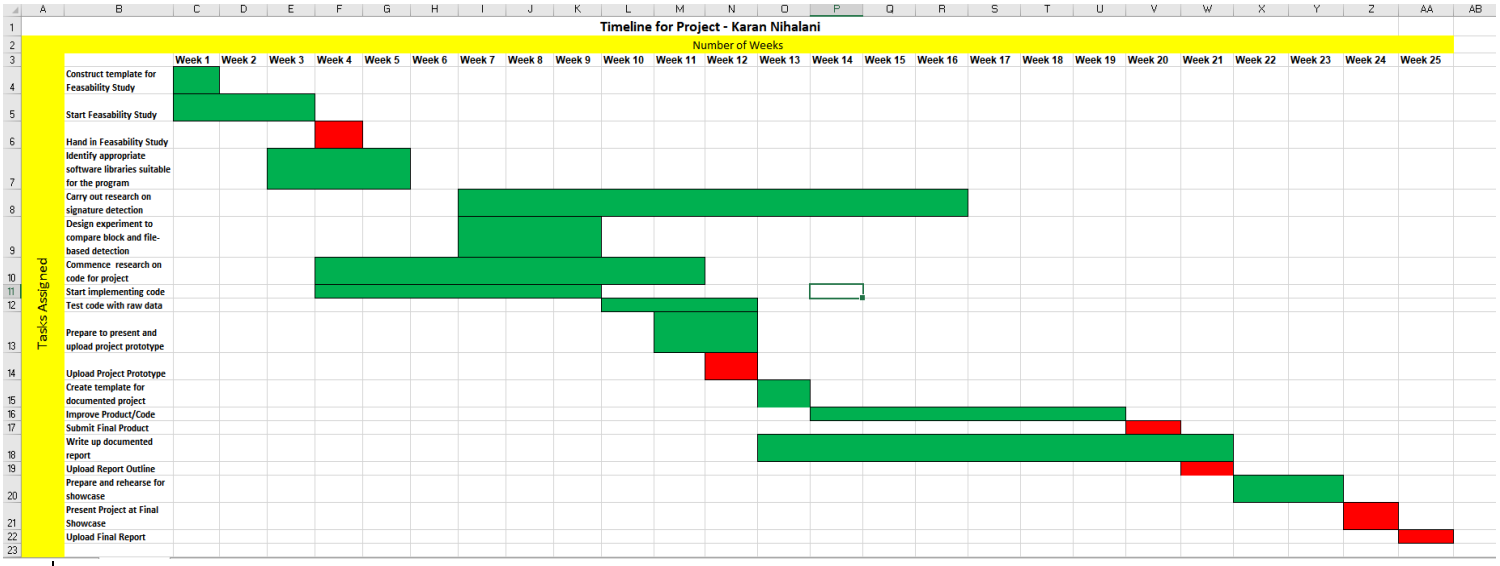
Aims:

- I will research how signature detection is employed during forensic triage
- Identify the key requirements of the triage process
- Evaluate different approaches to signature detection (Block and file based)
- Recommend the most appropriate approach based on the results of my evaluation.

Objectives: To achieve the aim of the project, I must

- Carry out research and read about signature detection and its uses in today’s world.
- Also, I will explain key concepts and different types of signatures that can be detected in the early stages of an investigation.
- Design an experiment to compare block and file based
- Identify appropriate software libraries to develop the experiment/software
- Identify the requirements for signature detection in digital forensics
- Design an experiment to evaluate and compare file and block based approaches to signature detection for digital forensic triage.
- To able to implement the appropriate and correct software to be able to conduct my experiment.
- Test the software to ensure it functions correctly
- Evaluate your software using a standardised data set, perform comparison between block and file-based approaches to demonstrate the benefits of block-based triage
- To be able to evaluate my project against the aims and objectives presented above.
- To document any future work I will have identified from working during this project.

Project Timeline:



Challenges and Potential Issues

A potential issue I might face during this project would be an issue with the software libraries imported into my program's code. This could be due to the fact that some libraries wouldn't be installed properly because of a network or system error, during the installation process. I could also face the issue where certain libraries might not work, as they would only be implemented on a certain version of Python.

Another potential issue I can face during the timeframe of the project, is an issue with hardware failure, where a problem would involve the constant requirement for a high amount of memory, which can cause the device to slow down and cause unwanted errors, e.g. lags, freezing pages and programs crashing. In addition, a device can be physically damaged anytime throughout the time the project is being completed, where broken screens or broken keyboards or internal circuit damage can result in a delay concerning the completion of project tasks.

Invasive attacks on the computing device can also be considered as a potential challenge within this project. The laptop can suffer some invasive attacks, like viruses, malware or hacking attacks. This can occur due to the unwanted downloads of unwanted files from the Internet.

Mitigation of these issues

In order to have software libraries be perfectly functional, I will ensure to have a test-run conducted for each of the libraries implemented, ensuring that they are able to work with data input and also, I will make sure that the Python software being used is compatible with all the libraries being imported or installed.

Further on, to prevent a slowed down laptop, I will make sure not to overheat and overwork the device by decreasing the amount of time spent on a section of the program which requires a lot of memory, for example, not providing the program with an increased load of data that can slow down its computation time. In terms of preventing any physical damage to the digital device, the situation

is mitigated simply, as I will make sure to perfectly secure it in a laptop case at all times to prevent any casualties.

A mitigation technique I will utilise to prevent invasive cyberattacks would be conducting a security scan to ensure a clean laptop and also make sure to have security defences, such as firewalls and anti-virus software, set up. Furthermore, online ad-blockers will be installed as add-ons to browser engines, to prevent unwanted pop-ups or pop-unders causing the unwanted downloads of files that would be able to corrupt files on my computer.

Required Resources

Hardware:

Digital Device (Laptop)

Software:

Python

Bluefish (or other Python computable GUI)

Virtual Machine (Virtual Box – Ubuntu)

Imported Python Libraries

Internet Browsers (Firefox, Chrome, etc)

Text editor

Data Sets

References

US-CERT (2008) Computer Forensics "Why Is Computer Forensics Important?" [Online] [Accessed on 7th October 2019]
https://www.us-cert.gov/sites/default/files/publications/forensics.pdf

NIST (2019) Digital Evidence "What is Digital Forensics" [Online] [Accessed on 7th October 2019]
https://www.nist.gov/topics/digital-evidence

Brett Shavers, John Bair (2016) Hiding Behind the Keyboard – Chapter 7: Antiforensics [Online] [Accessed on 7th October 2019]
https://books.google.co.uk/books?hl=es&lr=&id=eG3eBgAAQBAJ&oi=fnd&pg=PP1&dq=hiding+behind+the+keyboard&ots=y50yC_LLxW&sig=ZWKGeeMNcTnb2LbUUtSpx_Ms7qw&redir_esc=y#v=onepage&q=hiding%20behind%20the%20keyboard&f=false

Nick Burton (2018) What is Forensic Triage? [Online] [Accessed on 15th October 2019]
https://www.adfsolutions.com/news/what-is-forensic-triage

Appendix – Ethics Form

START HERE - Basic Information

This form must be completed for all student projects.

Before you proceed

Some activities inherently involve increased risks or approval by external regulatory bodies, so a proportional ethics review is not recommended and a full ethical review may be required.

These may include:

i. Approval from an external regulatory body (including, but not limited to: NHS (HRA), HMPPS etc.);
ii. Misleading participants;
iii. Research without the participants' consent;
iv. Clinical procedures with participants;
v. The ingestion or administration of any substance to participants by any means of delivery;
vi. The use of novel techniques, even where apparently non-invasive, whose safety may be open to question;
vii. The use of ionising radiation or exposure to radioactive materials;
viii. Engaging in, witnessing, or monitoring criminal activity;
ix. Engaging with, or accessing terrorism related materials;
x. A requirement for security clearance to access participants, data or materials;
xi. Physical or psychological risk to the participants or researcher;
xii. The project activity takes place in a country outside of the UK for which there is currently an active travel warning issued by the authorities (see info button);
xiii. Animals, animal tissue, new or existing human tissue, or biological toxins and agents.

If any of these activities are fundamental to your project, please contact your supervisor to determine if a full application is required.

This form must be completed for each research project which you undertake at the University. It must be approved by your supervisor (where relevant) PRIOR to the start of any data collection.

In completing this form, please consult the University's ACADEMIC ETHICAL FRAMEWORK for ethical research.

A1 Please confirm that you will abide by the University's Academic Ethical Framework in relation to this project.

- (•) Yes
- ( ) No

A2 Are you submitting this application as a learning experience, for a unit which already has ethical approval? (please confirm with your supervisor)

- ( ) Yes
- (•) No

A3 Student details

Title	First Name	Surname
	Karan	Nihalani

Email: karan.nihalani@stu.mmu.ac.uk

A3.1 Manchester Metropolitan University ID number

17023122

A4 Supervisor

Title	First Name	Surname
Mr	Robert	Hegarty

Faculty: Science and Engineering

Telephone: +44 (0)01612471541

Email: r.hegarty@mmu.ac.uk

A5 Which Faculty is responsible for the project?

Science and Engineering

A6 Course title

Computer Forensics and Security

A7 Project title

Block Based Signature Detection for Forensic Triage

A8 What is the proposed start date of your project?

01/10/2019

A9 When do you expect to complete your project?

30/04/2020

A10 Please describe the overall aims of your project (3-4 sentences). Research questions should also be included here.

• I will research how signature detection is employed during forensic triage
• Identify the key requirements of the triage process
• Evaluate different approaches to signature detection (Block and file based)
• Recommend the most appropriate approach based on the results of my evaluation.

A11 Please describe the research activity

• Carry out research and read about signature detection and its uses in today's world.
• Also, I will explain key concepts and different types of signatures that can be detected in the early stages of an investigation.
• Design an experiment to compare block and file based
• Identify appropriate software libraries to develop the experiment/software
• Identify the requirements for signature detection in digital forensics
• Design an experiment to evaluate and compare file and block based approaches to signature detection for digital forensic triage.
• To able to implement the appropriate and correct software to be able to conduct my experiment.
• Test the software to ensure it functions correctly
• Evaluate your software using a standardised data set, perform comparison between block and file-based approaches to demonstrate the benefits of block-based triage
• To be able to evaluate my project against the aims and objectives presented above.
• To document any future work I will have identified from working during this project.

A12 Please provide details of the participants you intend to involve (please include information relating to the number involved and their demographics; the inclusion and exclusion criteria)

No participants

A13 Please upload your project protocol

Tipo	Document Name	Nombre del archivo	Version Date	Versión	Tamaño
Project Protocol	Feasibility Study Draft3	Feasibility Study Draft3.docx	17/10/2019	3	74,4 KB

Project Activity

B1 Are there any Health and Safety risks to the researcher and/or participants?

- ○ Yes
- ◉ No

B2 Please select any of the following which apply to your project

- ☐ Aspects involving human participants (including, but not limited to interviews, questionnaires, images, artefacts and social media data)
- ☐ Aspects that the researcher or participants could find embarrassing or emotionally upsetting
- ☐ Aspects that include culturally sensitive issues (e.g. age, gender, ethnicity etc.)
- ☐ Aspects involving vulnerable groups (e.g. prisoners, pregnant women, children, elderly or disabled people, people experiencing mental health problems, victims of crime etc.), but does not require special approval from external bodies (NHS, security clearance, etc.)
- ☐ Project activity which will take place in a country outside of the UK
- ☑ None of the above

B2.4 Is this project being undertaken as part of a larger research study for which a Manchester Metropolitan application for ethical approval has already been granted or submitted?

- ○ Yes
- ◉ No

Data

F1 How and where will data and documentation be stored?

Data will be stored digitally on a digital device and a USB drive for further preservation.

F2 Will you be collecting personal data or sensitive personal data as part of this project?

- ○ Yes
- ◉ No

Insurance

F3 Does your project involve:

- ☐ Pregnant persons as participants with procedures other than blood samples being taken from them? (see info button)
- ☐ Children aged five or under with procedures other than blood samples being taken from them? (see info button)
- ☐ Activities being undertaken by the lead investigator or any other member of the study team in a country outside of the UK as indicated in the info button? If 'Yes', please refer to the 'Travel Insurance' guidance on the info button
- ☐ Working with Hepatitis, Human T-Cell Lymphotropic Virus Type iii (HTLV iii), or Lymphadenopathy Associated Virus (LAV) or the mutants, derivatives or variations thereof or Acquired Immune Deficiency Syndrome (AIDS) or any syndrome or condition of a similar kind?
- ☐ Working with Transmissible Spongiform Encephalopathy (TSE), Creutzfeldt-Jakob Disease (CJD), variant Creutzfeldt-Jakob Disease (vCJD) or new variant Creutzfeldt-Jakob Disease (nvCJD)?
- ☐ Working in hazardous areas or high risk countries? (see info button)
- ☐ Working with hazardous substances outside of a controlled environment?
- ☐ Working with persons with a history of violence, substance abuse or a criminal record?
- ☑ None of the above

Additional Information

G1 Do you have any additional information or comments which have not been covered in this form?

- ○ Yes
- ◉ No

G2 Do you have any additional documentation which you want to upload?

- ○ Yes
- ◉ No

Signatures

H1 I confirm that all information in this application is accurate and true. I will not start this project until I have received Ethical Approval.

- ◉ I confirm
- ○ I do not confirm

H2 Please notify your supervisor that this application is complete and ready to be submitted by clicking "Request" below. Do not begin your project until you have received confirmation from your supervisor - it is your responsibility to ensure that they do this.

Firmado: Este formulario fue firmado por Robert Hegarty (r.hegarty@mmu.ac.uk) on 17/10/2019 13:18

H3 By signing this application you are confirming that all details included in the form have been completed accurately and truthfully.

Firmado: Este formulario fue firmado por Karan Nihalani (karan.nihalani@stu.mmu.ac.uk) on 17/10/2019 13:18