CYBR472 Digital Forensics
Assessment One (30%)

Due Date: 9th of April 2023

Overview

This assignment has two parts:

- Lab work – the aim is to develop practical skills that will be applied in the case study
- Questions – help you engage with the theory and its application

The assignment has four main learning objectives. Students should be able to:

- Apply tools and techniques used in the identification, collection, examination and analysis phase of the digital forensics process.
- Explain the relationship between the practical work to theory covered in class.
- Explain how to apply forensics processes at a high level in a given scenario.
- Critically engage with cybercrime legal framework and relate it to the New Zealand context.
- Analyse a real-world case study as a legal exercise.

This assignment is worth 30% of your final grade - the lab work and questions are weighted equally.

Submission

Use the ECS submission system and submit your document as a single PDF file called `FullName-Report.pdf`.

You should follow these guidelines:

- Use first-person, informal style aimed at someone new to digital forensics but with a background in engineering. Make sure that your writeup is spell checked and grammatically correct.
- Use hyperlinks to link to any other sites that you want to discuss or reference.
- The lab report and question writeups **must not exceed 10 pages *(single space)*** *in total****. Anything beyond 10 pages will not be marked.***
- Please reference this piece of writing with the same rigour that you would a formal essay, including in-text references or hyperlinks to websites you refer to and include a list of references at the end of the writeup *(not each entry)*. Note that we exclude the reference list from the overall word count.

Grading

We will read your lab and question writeups and then provide some feedback (to help you improve for the next assignment) as well as an indicative letter grade, according to the Victoria University Assessment Handbook (p38). For the indicative grade, letter grades will usually be in the form of A, B, C, D, E with no +/-.

***Broadly speaking**:*

A Grade: Demonstration that lectures and readings have been considered and understood. Demonstration of independent thinking that is inspired by course content. Interesting analysis, critique or interpretation of content. Creative. Enjoyable to read. Writing includes clarity, precision, concision, and excellent spelling and grammar. Length is within guidelines.

B Grade: Demonstration that lectures and readings have been watched/read but possibly not always understood. Demonstration of some independent thinking inspired by course content but much repetition of lecture material, readings and ideas from peers. Writing quality mainly includes clarity, precision, concision, and basic spelling and grammar. Length is within guidelines.

C Grade: An understanding of lectures or readings is not conveyed. May include a basic summary of key points in the course material or repetition of contributions by peers. She has attempted contributing but does not demonstrate much deeper or critical thinking about the topic. Writing contains several errors and is sloppy. Length is mostly within guidelines.

D/E Grade: Minimal submissions, inadequate submissions or pure repetition of content. She appears to have just answered to “get a grade” with no extra critical thinking.

F Grade: No submission.

Part 1: Lab Work

This part of the assignment aims to become familiar with tools and techniques that can be applied in the case study. It is worth 50% of the overall grade for this assignment.

Instructions

Ideally, write a 1 page (max) report for each of the following labs that reflects on the following points:

- Very brief summary of what the lab was about and what was done
- Something that you have learnt or discovered by doing lab work
- Explain how this illustrates or expands upon something you learnt in the course lecture or reading
- Brief summary of the tools/systems used in the lab exercise and their capabilities

Which labs to complete

Go to **netlab.ecs.vuw.ac.nz**

Log in using your netlab username and password and completes the following labs in the given order:

Lab 21 – Chain of custody
Lab 01 – Creating a forensics image
Lab 02 – Live acquisition
Lab 07 – Data carving
Lab 06 – Keyword search and analysis

Make sure that you read everything; otherwise, you will learn nothing!

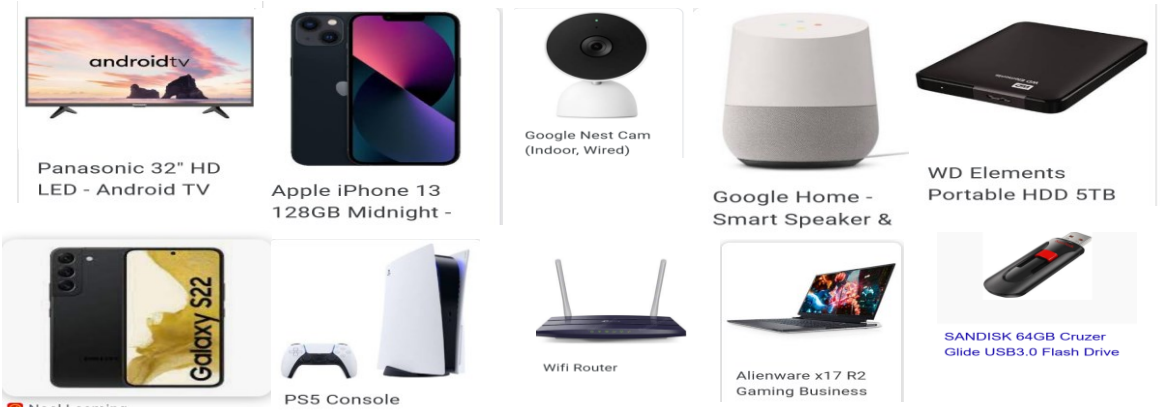
Part 2: Questions

This part of the assignment aims to help you engage with the theoretical material related to digital forensics. It is worth 50% of the overall grade for this assignment.

You will be marked upon the correctness of facts, your ability to apply concepts, your critical thinking and your quality of communication. Please ensure you use citations and note that ChatGPT may create random made-up citations.

When working together, please indicate this and ensure you have written your answers in your own words. You can discuss ideas but must produce the final writing independently.

Question 1 - As part of a drug cartel case, you have been asked to seize all digital devices from one of the potential drug dealers' homes and perform a forensically sound collection of potential evidence. The "dealer" was caught sitting in the living room and brought to custody. The devices pictured below were found in the living room. Assume all devices are switched on and running except for the Galaxy S22 phones and PS5. The WD elements drive connected to the laptop, and the USB stick were found down the back of the living room couch.



Consider the information above and the identification and collection phases described in lectures and the textbook (chapter 2), provide an answer for the following questions:

(a) How might these devices be relevant to the drug cartel case?
(b) What would you advise first responders to do to protect the data's integrity?
(c) When time is limited, how would you choose which devices to collect data from first?
(d) What barriers exist to collecting data from the devices?
(e) What is recommended in terms of documentation for the chain of custody?
(f) What devices could be used to ensure you do not affect the integrity of the copied data?
(g) What technical measures can be used to protect data against tampering?

Note that an excellent answer involves examples of the specific device's capabilities.

Question 2 - Answer and discuss the following questions in the given order:

(a) When is an investigation coercive according to European law? Is it only related to guarantees around privacy? What three conditions must be fulfilled for applying a coercive investigation method under European law?
(b) Discuss why secret surveillance of a drug smuggling cartel could be used, whereas secret surveillance of an opposition political party meetings might not.
(c) Consider the New Zealand context; what rights do we have concerning coercive search and what legislation defines the application of coercive investigation?

Note that an excellent answer will use case law examples from the book to illustrate their arguments.

Question 3 - Is it lawfully obtained, if digital evidence has been secretly secured from a user account on a cloud service? What would make it unlawfully obtained, and in that case, who would be the aggrieved party? Is the consequence that the evidence must be excluded from being cited as evidence at trial? Which rule (principle) is relevant in this respect, and who decides?

An excellent answer will discuss this in three contexts – the EU, the USA and New Zealand, as covered in the book.

Question 4 - Consider each of the following cases and identify whether New Zealand enforcement officials could conduct a forensic investigation as described. In your answer, cite the relevant section of the Search and Surveillance Act 2012. In the case of ambiguity, please state any additional questions that need to be answered.

(a) New Zealand police want to install a tracking device on the car of Person X. This person is suspected of mass importation of pistol carbine conversion kits. Assume that the tracking device can only be installed by coming onto private property without the owner's consent. There is no urgency in this case.
    i. Explain why a surveillance warrant would be required in the following case
    ii. What is the maximum period of time the data could be retained, assuming no criminal proceedings occur?
(b) How does your answer change when Person X is suspected to be travelling to a location to carry out a murder, and the NZ police do not have time to apply for a warrant? Justify your answer concerning the Act and discuss any restrictions that might be placed upon using a gun. Note that murder in New Zealand carried a mandatory ten-year sentence.

Question 5 - On 2 October 2014, Police searched Mr. Hager's home in Wellington and seized or cloned many items, including USB storage devices, documents, CDs, phones and computers. The search lasted for over 10 hours. While Mr. Hager was not himself a suspect, Police were seeking evidence regarding the identity of a hacker known as 'Rawshark' who had confidentially provided Mr. Hager with information for his book.

Mr. Hager sought a judicial review of the Police's search warrant. On 17 December 2015, the High Court in Wellington issued a judgment declaring the search warrant was "fundamentally unlawful" and, therefore, the search was also unlawful.

(a) What were the reasonable grounds specified in the search warrant?

(b) Summarise the argument as to why the search warrant was not specific enough in nature and what part of the Act relates to the need for a special warrant (also consider production orders)?

This resource will be useful for answering this question: https://www.ipca.govt.nz/Site/publications-and-media/2019-reports-on-investigations/2019-aug-20-unlawful-search-hager-privilege.aspx.