Assignment 2 – IT Forensics 2023

Submission instructions

Deadline: Friday, 15 September 2023 (11:55pm)

Submission format: PDF only and Moodle submissions. You can use any freely available PDF converter to make a PDF file from an editable one. *Please make sure you have submitted your assignment and it is not left in the DRAFT mode. It is also your responsibility to check if your submitted PDF is markable by our tutor. So please download your submission after finalising it to check if you can read it. If you submit a file, that is not markable by our tutors, depending on when we realise this, you may lose upto 50% your marks for that part of the submission.*

Submission platform: Upload via Turnitin assignment on Moodle.

Late submissions:

- via special consideration request
- or, without a special consideration request, you lose 10% of your mark per day that you submit late. Submissions will not be accepted more than 5 days late.

Plagiarism: It is an academic requirement that your submitted work be original. Zero marks will be awarded for the whole submission if there is any evidence of copying, collaboration, pasting from websites, or copying from textbooks. The faculty's Plagiarism Policy applies to all assessments: http://intranet.monash.edu.au/infotech/resources/students/assignments/policies.html

Further Note: When you are asked to use Internet resources to answer a question, this does not mean copy-pasting text from websites, Moodle content, and/or assignment specification. Write answers in your own words such that your understanding of the answer is evident.

Marks:

- This assignment is worth **30% of your unit marks**.
- The assignment is marked out of (part A + part B) = (40 + 80) = **100 nominal marks**.

SPECIAL NOTE:

- **FTK Imager and Autopsy are available on MoVE.**
- **FTK Toolkit is available 24/7 to all students in CG10, CG22, and CG23 at Bulding 79P (7 Innovation Walk), Clayton campus.**
- **Please do not turn off the lab machines., only log off or restart.**
- **The default username/password to access FTK is *user/user*. Please do not make changes to this default.**
- **Once you are finished with your assignment, please remove your files and**

case from the computers in the labs.

- **All assignment questions can be solved using open-source softwares. However, some students might want to use FTk for it. In that case, please start working as soon as possible, because there are only 62 computers that can run FTK at the same time. No special consideration for late submission will be given for licensing reasons. You have been warned!**

PART A - IT Forensic Criminal Case

You are required to look at a real criminal case involving a digital device. See Appendix A for a fictional example. There will be 7 different stories related to disk-based forensics:

- Story 0: Jewel Victoria GRIFFITHS - Drug Importation | Commonwealth Director of Public Prosecutions
- Story 1: Sydney man jailed for online exploitation and extortion of children | Commonwealth Director of Public Prosecutions
- Story 2: QLD man convicted for child pornography offences | Commonwealth Director of Public Prosecutions
- Story 3: Paedophile jailed for 40 years for abusing children in Australia and Thailand | Commonwealth Director of Public Prosecutions
- Story 4: Richard RAMOS - Child exploitation offences | Commonwealth Director of Public Prosecutions
- Story 5: Luca SILVERII - Medicare fraud | Commonwealth Director of Public Prosecutions
- Story 6: Record sentence for head administrator of paedophile site | Commonwealth Director of Public Prosecutions

To determine which story you are working on, do MODULO 7 OPERATION on your student ID. For example: 12345678 MOD 7 = 2. Therefore, the story that should be investigated is Story 2. Mark deduction will be applied for incorrect Story choice.

1) **Designing Questions:** After researching about your story, design *five* questions specific to the digital evidence (that a lead investigator would ask) on your case that you (as a digital forensic examiner) need to answer by using digital forensic techniques/tools/protocols. See sample questions for the sample fictitious story in Appendix A.
   (10 marks)
2) **Forensically Sound Plan Design and Forensic Tools:** In order to answer the questions you have created in Part 1, design a forensically sound plan/protocol, which will help you find the answers. The protocol should cover:
   - Preparation, e.g. how you prepare yourself before going to the crime scene.
   - Acquisition/Preservation, e.g. how would you acquire/preserve the evidence such that you will not leave any potential evidence untouched; how would you manage your time and devices.
   - Examination/Analysis, e.g. how you examine and analyse the evidence with the open-source and paid tools.

You also need to cover the following topics in your plan/protocol:

- What tools will you need to investigate the evidence?
- Describe the advantages and disadvantages of using the (non-)forensic tools of your choice, e.g. free tools vs licensed ones.
- How will you use the tools to find evidence?
- Expected time and cost to find the answers.

(30 marks)

Your answer on this (entire Part A), which should appear in the form of a report **should not exceed 800 words**. The word limit excludes tables, figures, and references. Please submit your PDF file to Assignment 2 - Part A - PDF only.

PART B - PRACTICAL EXERCISE

Please refer to “assessment” section under Moodle:
FIT3168 students:
https://lms.monash.edu/mod/quiz/view.php?id=11899266

FIT5223 students:
https://lms.monash.edu/mod/assign/view.php?id=11903866

1) Attempt the quiz in this section of Moodle. Read the quiz instructions carefully.
2) You also need to submit a short presentation of no more than 10 minutes explaining the steps you took to answer the questions of the quiz. The presentation is not marked however it serves as a reference/evidence/proof.
3) **You have only three attempts.** Each new attempt would give you a new image file different from your previous attempt. So please make sure you do not answer the questions of an attempt using a previous image. **Under no circumstances we will not open an additional attempt.**
4) The above links would take you to the quiz page. There you can download your personalised image. Download it, verify the hash, either by the CyberChef method explained there or simply right-click on your image inside a lab machine (that you would access to use FTK), then an option is shown as CRC-SHA, choose SHA256 and check the created hash output with the one provided in your quiz. Please make sure you do not miss this step as the questions will be different for each image. You may encounter a problem when using CyberChef downloaded package to check the hash of the disk image as the file may be too large for the browser-based tool to handle. An alternative way to check the hash on Windows is to use certutil command. Open a command terminal by searching cmd in Windows search bar and select "Command Prompt" app and type

```
certutil -hashfile <path to the image> SHA256
```

(80 marks)

APPENDIX

Sample Story:

The customs office tipped the local police that several strange packets crossing the border were addressed to Nilson Denny in Victoria. After several days of stakeouts the police noticed that Nilson commonly left his apartment 3 to mail a noticeable amount of envelopes every day around 15:00. After a decision from the district attorney the police intercepted some envelopes and noticed that they contained drugs of the following kind: Happy face, Sad face and Winky face. The envelopes contain addresses to three different persons that were brought in for questioning. They all said that they had ordered the stuff from Darknet, they had no idea who the seller was but stated that he or she was called something like The DD Dude.

With this information the attorney decided on a house search and a team of computer forensic experts was brought in as help. When the house search began the suspect was found sitting in front of his computer, initially they said that they found something related to the case. The forensic experts continued with their work and the suspect was arrested. During initial interrogation the suspect claims he is innocent and any possible evidence must be due to the fact that his home is open to everyone and anyone may do what they want with his computer, he rarely uses it himself. However, no one else but Nilson was present in the apartment during the arrest and the police officers that were on stakeout said that they didn't see anyone enter Nilson´s home during the stakeout that lasted for the last three days.

Sample Questions:

1. Are there any traces of the computer being involved in selling drugs?
2. Who was the user of the computer?
3. Did anyone else use it?
4. Is it possible to tie the suspect to the aliases used in the case?
5. Are there any pictures of drugs? When and where were they taken?