Digital Forensics Diploma in CSF/IT Year 2/3 (2022/23) Semester 4/6	Week 3 to 17
DF Assignment (40%)	

Objectives:

1. To assess students' ability to carry out forensic investigation on storage device;
2. To expose students to open source forensics tools;
3. To assess students' ability to prepare an examiner report.

1.0 Introduction

This assignment consists of 2 sections:

1) Research on open source forensic tools, and
2) In-class forensic investigation.

To expose students to forensics tools other than EnCase, students will research on one or more open source forensic tools and demonstrate it to the tutor.

The in-class forensic investigation is an open-book assessment using EnCase. Students will have 2 hours to carry out the investigation.

The assignment consists of both group and individual components. For group component, students are to **work in pair**.

2.0 Description of Tasks

Part 1: Research on Open Source Forensic Tools (Group & Individual)

Tasks:

You are required to research on **at least one** open source forensic tool, learn how to use the tool by performing forensic investigation on flash drive, hard drive or any other devices. You will then:

1. Do a Presentation on your approach and Demonstrate your work/investigation to your tutor and classmates, and
2. Prepare a power point presentation on your work.

The template of power point presentation will be provided in POLITEMALL.

Kali Linux provides a suite of open source forensic tools. You may make use of these tools for this assignment. However, it is not a requirement to choose from tools provided in Kali Linux, students may choose to research on other free/open source tools.

To access the tools, boot up the computer in the lab and launch VMWare Workstation Pro. Select and start Kali Linux VM. Once the VM is started, select Applications → Kali Linux → Forensics.

Note:

- You are strongly encouraged to explore on Command Line Interface (CLI) open source forensic tools.
- The team should present their work as one single demo. If more than one tool is involved, there must be some form of linkage among the tools.
- Teamwork will be assessed (refer to marking scheme for details).

Deliverables:

1. Presentation along with Demonstration of open source forensics tools will be carried out on week 16/17. Each team is given up to 15mins.
2. Submission of power point on week 17 (refer to **Deadline** section for details).
   a. You may refer to the sample power point provided in POLITEMALL Assessment link.
   b. You may change the design, colour and layout but please keep the NP and ICT logos.
   c. The content of the power point must be original and related to your demo.
   d. It is also a requirement to show the contact details of all team members.
   e. You need to acknowledge the sources for any use of Internet resources.

** Note: Students will work on Part 1 **individually on Week 5**, during whitespace week and submit an individual writeup at the end of week 5. Tutor will provide feedback on individual writeup. Students will start to work in pairs after receiving tutor's feedback.

Part 2: In-Class Forensic Investigation (Group of 2 students)

Case Scenario:

Simon recently reported an unauthorised bank transfer of SGD $2000 in his OCBC bank account history and reported it to the police. The recipient of the transaction was traced to the tenant of his apartment, Alicia.

When interrogating Alicia, she consistently denied any wrongdoings and claimed that Simon has transferred the money on his own accord. She mentioned that Simon had been sexually harassing her in the apartment, and the money was transferred as hush money to keep her quiet. She gave a possibility that Simon might be trying to frame her to get his money back and avoid any criminal indications if she reported the sexual harassment to the police. According to the bank's online banking logs, the transaction was made from Simon's apartment's public IP address. Hence, both Simon and Alicia's personal computers in the apartment has since been seized for investigation.

1) Simon's personal computer running Windows 7 (20170316-001-E01)
→ Hard Disk (20170316-001-E01HD1) [image file: Simon.Ex01]
2) Alicia's personal computer running Windows 10 (20170316-001-E02)
→ Hard Disk (20170316-001-E02HD1) [image file: Alicia.Ex01]

20170316-001-E01	20170316-001-E02
20170316-001-E01HD1	20170316-001-E02HD1

The preliminary interviews and investigation have gathered the following information:

Simon Spegman	Alicia Tan Hui Jing
● 42 years old ● Singaporean ● Male ● Single ● Chief Executive Officer of Reynholm Industries ○ Working hour: Mon - Fri, 12pm to 6pm ● Known software used: ○ Windows 7 ○ Outlook ○ Google Chrome ● Online aliases: ○ Email: “simonspegman” ○ OCBC bank account number: 7566721	● 18 years old ● Malaysian ● Female ● Single ● Student of Ngee Ann Polytechnic ● Tenant of Simon Spegman’s apartment ● Avid gamer ● Known software used: ○ Windows 10 ○ Mail (application) ○ Firefox ○ Skype client ● Online aliases: ○ Email, Skype: “aliciatanhuijing” ○ Maplestory, metasploit framework: “aliciathj”

Both Mr Thomas Chee and you work as forensics investigators in a private forensics firm, True Identity Pte Ltd. The hard disk of Simon and Alicia’s personal computers were acquired by Mr Thomas Chee and Simon’s image file (Simon.Ex01) has also been examined by him. **You have been tasked to examine Alicia’s image file (Alicia.Ex01) to solve the case.**

Tasks:

Perform extraction and analysis on the image file, Alicia.Ex01 to help to solve the case. You are expected to:

1. Recover as much relevant evidences as possible from the image file,
2. Prepare and submit the **RTF report** at the end of the investigation (within the 2 hours),
3. Prepare and submit an **Examiner report** based on the case.

Note: Exhibit Management & Image Acquisition (EMIA) report is NOT required.

The following will be helpful to you:

- It is not practical to search all folders when performing keyword searching. Search only the relevant folders. Each searching should not take more than 5 minutes.
- Ensure that the computers used for investigation has the timezone set to *(UTC +08:00) Kuala Lumpur, Singapore.*
- You are advised to use external tools for the investigation (e.g. Windows Media Player, SQLite Forensic Explorer, Windows Event Log Viewer).

RTF Report

The following are required in the RTF report:

- Case information
- Information on the Evidence seized (20170316-001-E02HD1) This include:
    - Evidence Number
    - SHA1
    - Model
    - Serial Number
    - Examiner name
- Any evidences that are relevant to the case. You should be as thorough as possible.
- Any relevant notes on the evidence recovered (base on your observation).

Examiner Report

In your examiner report, you need to state your key observations, analysis and opinions on the case based on the evidences extracted from the evidence file.

The examiner report may be of any suitable format as long as it includes the relevant sections. One suggestion is to follow the Tecbiz Frisman's *Sample Computer Forensic Report* provided. The RTF report should be included as Appendices.

3.0 Deliverables

1. In-class forensic investigation will be carried out on week 15/16 during practical lesson (2 hours). RTF report must be submitted within the 2 hours of investigation.
2. Examiner report on this case must be submitted by week 17.

Refer to **Deadline** section for details.

The following table summarizes the plan:

Week	Dates	Tutorial (2 hours)	Practical (2 hours)
5	14-18 Nov 22 **Whitespace Week**	Research work on open source forensics tool **(Individual)**	Research work on open source forensics tool **(Individual)**
14	16–20 Jan 23 **Whitespace Week**	Assignment (Students do own preparation for assignment) (Group)	Assignment (Students do own preparation for assignment) (Group)
15	23–27 Jan 23	Assignment (Students do own preparation for assignment) (Group)	Assignment – In Class Forensics Investigation (Group)
16	30 Jan – 4 Feb 23	Demo of open source Forensic tools (Group)	Assignment – In Class Forensics Investigation (Group) – For students affected by CNY only Demo of open source Forensic tools (Group)
17	6-10 Feb 23	Demo of open source Forensic tools (Group)	CA: Mel Quiz 10% (Individual)

4.0 Resources

1. Each group will be allocated with up to 2 PCs, subject to availability. The assignment is to be carried out on the same PC throughout the few weeks of assignment period.

2. Each group is required to provide own thumb drive for backing up the case file.

5.0 Deadlines

The following deliverables have to be submitted in POLITEMALL | DIGITAL FORENSICS Assessment | Assignments link:

1. **Individual** Checkpoint Submission on research work done on open source forensics tool by **11:59pm, 20 Nov 2022 (Sunday)**
2. **Group** RTF report (exported from EnCase) – **within the 2 hours** of in-class forensics investigation **in week 15/16**
3. **Group** power point (on open source tools) - by **11:59pm, 12 Feb 2023 (Sunday)**
4. **Group** Examiner report (on Simon & Alicia's case) - by **11:59pm, 12 Feb 2023 (Sunday)**

Penalty for late submission:
Late For each day past the deadline, 10% of the total possible marks will be deducted up to a maximum of 7 calendar days, after which a zero mark is given.

6.0 Marking Scheme

A) Group Components – 60 marks

1. Research on Open Source Forensic Tools (30 marks)

a. Demonstration of Forensic Tools (22 marks)

i. Workability/Completeness (10 marks)
- *Tool/s used is/are useful in conducting an appropriate forensic investigation*
- *Investigation is complete with proper steps and procedures*
- *Demonstration illustrates a complete cycle of a typical forensic investigation*

ii. The “Wow” factor (10 marks)
- *Tool/s is/are unique and not commonly demonstrated/used*
- *Simulated environment/scenario is unique and not commonly demonstrated*

iii. Teamwork (2 marks)
- *Team is able to fairly distribute work among team members*
- *Each component demonstrated by each team member compliments the entire demonstration*

b. Power Point (8 marks)

i. Content (5 marks)
- *Captures accurately essential and important information regarding the forensic investigation*
- *Information is concise and complete*

ii. Overall quality (Layout, Design etc.) (3 marks)
- *Clear, great use of visual aids with appropriate animation*
- *Use of relevant and accurate points to critically evaluate ideas/concepts*

2. In-class Forensic Investigation (30 marks)

a. RTF Report (15 marks)

i. Completeness (based on the number of relevant evidences found) (12 marks)

ii. Organization (3 marks)
- *RTF report is neatly formatted, with proper sectioning, heading and relevant comments for each section*

b. Examiner Report (15 marks)

i. Structure of report (2 marks)
- *Examiner report is properly formatted with cover page, table of contents, headings, sections and page number.*
- *Appropriate usage of tables, flow charts or diagrams*

ii. Purpose, Summary and Conclusion of report (3 marks)
- *Clearly states the essential information for each section*
- *Correctly provides reader with relevant information for each section*

iii. Analysis of evidence (10 marks)
- *Comprehensive and convincing interpretation of evidences found*
- *Analysis of evidence is complete and recommendation/suggestion is reasonable and makes relevant connections to the case*

B) Individual Components – 40 marks

1. Checkpoint (Write-up on Open Source Forensic Tools) (15 marks)

a. Content (10 marks)
- *Identify and explain the main functions of the open source tool*
- *How to simulate/setup scenarios and identify resources hardware/software) required*
- *Case description*

b. Originality of idea (5 marks)
- *Tool/s identified is/are unique*
- *Case description/scenario is unique, original and concise*
- *Description of setup is comprehensive*

2. Understanding of work (Open Source Tool Demo) (15 marks)

- *Student is able to show understanding of work presented*
- *Student is able to answer question raised by tutor*
- *Student is able to explain the purpose, function and analysis of work presented*

3. Presentation skill (10 marks)

- Presentation is lively and is able to capture audience's attention
- Articulation and pronunciation
- Voice, body language, eye contact

7.0 Plagiarism and Copyright Issues

Plagiarism means, "copying any part of a source, and then submitting it, claiming that it is your own work."

Please ensure that all the works submitted by you are not copied from other sources. Any attempt to plagiarise will be dealt with severely, and it may result in your failing the module.

If you have made any references to certain materials, make sure you cite the sources by acknowledging and providing the information necessary to find the source (e.g. Title and author of book, Internet links, etc.)

Please refer to the following URL for more details:
http://www.np.edu.sg/antiplagiarism

**** The end ****