IFS4102 (Digital Forensics)
Group Project - Investigation Time!

Due Dates: Friday, 31 March 2023, 11:59 A.M. (for Case 1 Report & Slides)
Friday, 14 April 2023, 11:59 A.M. (for Case 2 Report & Slides)

1. Project Background & Objective

This group project is designed to give you and your team a good understanding of solving realistic digital forensics scenarios. So, it's time to show your forensic analysis skills. Apply your knowledge and skill sets to solve the given two forensic cases, which simulate real-life situations. You are welcome to use ***any*** forensic tools of your choice to analyze the cases, and there are no restrictions at all. *Hope you all have fun with the cases!* 😊

2. Case Assignments

There are **two** cases presented. Each team needs to work on and solve ***both cases***.
Your team, however, will submit the slides and present on ***one assigned case*** only.
(The case to be presented by your team will be determined later.)

2.1. Case 1: Suspicious Employee

Problem Description and Tasks:

A suspicious employee left your company. His name is **Mark**, and he was seen working on unusual hours and browsing random websites recently. A day before Mark left, another employee, **John**, reported a missing USB storage drive and was also suspicious about Mark. Human Resource decided to initiate an investigation and your team has been given the registry hives and other files from Mark's computer. You can find the evidence files under the `Evidence-files` folder in the given `Case-1-files.zip`, which has been uploaded to Canvas.

The most senior investigator in your team, however, happens to be stuck in an isolated quarantine facility somewhere. This person, nevertheless, has given some useful forensics notes/cheat-sheets, which you can find under the `Forensics-notes` folder.

Do perform a forensics investigation by analyzing the given Windows artefacts, including Windows Registry and logged event files. Please submit a report on your findings, in which you will "prove"/"disprove" the story of Mark's suspicious activities by presenting relevant evidence. The adopted procedure, findings (e.g. key extracted pieces of evidence, necessary screenshots/ diagrams) in your investigation are also expected to be included as part of your submitted report.

Case Resources:

Please refer to the `Case-1-files.zip` file, which has been uploaded to our module's Files under the `Group-Project` folder on Canvas. The following files are given:

- Four evidence files under the `Evidence-files` folder;
- Some forensics topics related notes/cheat-sheets under the `Forensics-notes` folder.

2.2. Case 2: Narcos

Problem Description and Tasks:

Due to intelligence provided by the Australian government, two passengers were intercepted by Customs upon arriving at Wellington, New Zealand from Brisbane. The Intel provided stated that **Jane Esteban** and **John Fredricksen** may be involved in illegal activity. The suspects were searched by a customs officer. John Fredricksen's baggage consisted of clothing, toiletries and a Windows laptop. Jane Esteban's baggage also consisted of clothing, toiletries and a small windows laptop.

Upon further search of the lining of John Fredricksen's suitcase, one kilogram of Methamphetamine was located. Both suspects were taken into separate interview rooms where they were interrogated. John Fredricksen refused to answer any questions.

Jane Esteban, meanwhile, stated all she knew and that she had to deliver the suitcase to the "Eastbourne library" but if all else failed then they were to deliver it to 666 Rewera Avenue, Petone as told by John Fredricksen. Customs and police subsequently raided that address. There was nobody present at the address. Customs did, however, find drugs, guns and a desktop computer in the living room of the suspect's house.

You are a Customs forensics investigator. Customs officers have delivered a **drive image** and **memory dump** of the suspect's desktop computer to you. Your task is to determine the relationship between John Fredrickson and the suspect, their future intentions and any other supporting evidence that pertains to the case.

Case Resources:

The evident files delivered to you consists of the following:

- The suspect's **drive image**: http://downloads.digitalcorpora.org/corpora/scenarios/2019-narcos/Narcos-1.zip.
- The suspect's **memory dump files**, which can be downloaded from: https://downloads.digitalcorpora.org/corpora/scenarios/2019-narcos/Narcos-1/Memory%20Dump/.

3. Deliverables

3.1. Case Analysis Reports

Your team needs to submit **written case analysis reports for *both cases***. Detailed submission instructions to Canvas are given in Section 3.2 below.

For Case 1, your report must at least analyse and answer the following questions asked by the company:

1. What websites Mark visited recently and the timing of the URL access.
2. What files he opened and what programs he ran recently on this PC.
   This is to check if he was trying to access and copy any sensitive data?
3. Did he insert any USB stick?
4. Any relation between the USB insertion time and sensitive file access time.
5. There are multiple user profiles configured on the computer that Mark was using.
   Which user was logged on at the time of suspicious activities?

Additionally, your analysis report should:

- Provide sufficient analysis and thought process of how you reached to your conclusions.
- Give counter argument(s) for every possible alternative hypothesis.

For Case 2, your team's report must determine the relationship between John Fredrickson and the suspect, as well as their future intentions. The report must thus address the following questions by providing relevant supporting evidence and sufficient analysis of how you reached to your conclusions:

1. Who was the suspect?

2. What did the suspect want from John during the latter's trip?
3. What were their future plans and intentions?
4. What was the role of Jane in the case and whether she was guilty as well?

Like in Case 1, your report must address the asked questions by providing relevant supporting evidence and sufficient analysis of how you reached to your conclusions. Also, do provide sufficient counter argument(s) for possible alternative hypotheses.

3.2. Submission Instructions

You will work in a team to solve the two cases given above. For your group number information, you can check the finalised team list posted in our module's discussion thread. Please prepare each of your reports in **a self-contained PDF** file by using your group number and case number in its filename. Submit **one PDF per group only**. Your report should also list your team members' names and matric numbers on its first page, along with brief individual contribution details.

Please upload your team's two PDF report files and presentation file to Canvas' `Group-Project-Case-1` and `Group-Project-Case-2` respectively by the following deadlines:

- **Case 1 Report: Friday, 31 March 2023, 11:59 A.M.**
- **Case 2 Report: Friday, 14 April 2023, 11:59 A.M.**

Note that the deadlines are **firm & final deadlines**. There will be no deadline extensions. After the respective case presentation session starts (at 12 noon), submitted reports and slides will **NOT** be accepted as the case solutions will already be discussed in the class. Hence, do submit well before the cut-off time so as to avoid any technical issues with Canvas or your uploading!

3.2. Presentations

In addition to your submitted reports, you team will also need to present your findings in two following separate presentation sessions during our regular lecture hours:

- **Friday, 31 March 2023, 12:00-3:00PM: Case 1 Presentation *(6 teams)***
- **Friday, 14 April 2023, 12:00-3:00PM: Case 2 Presentation *(6 remaining teams)***

In your presentation, your teams will play the role of **forensic expert witnesses**. Your team's presentation must be based on your team's submitted case report. Each team's presentation is limited to **20 minutes**, which can be followed by a **10-minute Q&A** session afterwards. The team case selection and presentation order will be fixed later.

4. Grading Scheme

This group project is worth **35%** of your final marks. The weightage distribution of all involved components is as follows:

- Case 1 analysis report: **15%**
- Case 2 analysis report: **15%**
- Case presentation: **5%**

For case analysis reports, the grading criteria are:

- Answering all the questions listed in Section 3.1 and providing strong evidence for your answers: **11%** (for case 1 report) and **11%** (for case 2 report).
- Considering and eliminating all other alternative hypotheses, as well as other interesting findings: **4%** (for case 1 report) and **4%** (for case 2 report).

For your presentations, the used grading criteria are:

- Clarity in explaining your findings.
- Clarity and correctness in answering asked questions.

5. Queries and Contacts

Please send your enquiries to the module Instructor (`dcssu@nus.edu.sg`) by using email subject title: “IFS4102 Queries - Group Project”.

Thanks, good luck, and have fun!