IFS4102 (Digital Forensics)
Group Project - Investigation Time!

Due Dates: Tuesday, 9 April 2024, 12:59 SGT (for Case 1 Report & Slides)
Tuesday, 16 April 2024, 12:59 SGT (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 is ***one*** **forensics case** considered. However, the forensics case has been divided into **two sub-cases/parts**: **Case 1 and Case 2**. Each team needs to work on and solve ***both Case 1 and Case 2***. 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: Narcos (Part 1)

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. ***Please use the case resources (evidence files) given in Case 1 as listed below only***!

Case 1 Resources:

The evidence files delivered to you for **Case 1** consists of the only 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/. (***Note***: You can try using Volatility 2.6.1 or 3 to analyze the given dump files as shown in this screenshot: https://digitalcorpora.org/wp-content/uploads/2023/11/narcos-vol-261.jpg)

2.2. Case 2: Narcos (Part 2)

Problem Description and Tasks:

Suppose after the ***completion*** of your reporting and presentation of Case 1 above, you are then given **extra evidence** by Customs officers: the images and memory dumps of **2 seized laptops**.

Your task is to carry out an **additional forensic examination** on John Fredricksen, Jane Esteban and the unknown suspect to **further understand** their motives, goals and objectives. (It should be noted that all three devices contain different Windows 10 builds and resulting artefacts may not be located in the same location or even be present.)

Case Resources:

The **additional** evidence files delivered to you consists of the following:

- The **second drive image**: http://downloads.digitalcorpora.org/corpora/scenarios/2019-narcos/Narcos-2.zip.
- The **third drive image**: http://downloads.digitalcorpora.org/corpora/scenarios/2019-narcos/Narcos-3.zip.
- The **second set of memory dump files**, which can be downloaded from: http://downloads.digitalcorpora.org/corpora/scenarios/2019-narcos/Narcos-2/Memory%20Dump/.
- The **third set of memory dump files**, which can be downloaded from: http://downloads.digitalcorpora.org/corpora/scenarios/2019-narcos/Narcos-3/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 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?

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.

For Case 2, your team's report must describe more about the identity of John Fredrickson, Jane Esteban and the suspect as well as the relationship among them. You additionally want to further understand their respective motives, goals and objectives. 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 Jane actually?
2. What did John think of Jane, and what did he want from her?
3. Who were the guilty parties in the overall case based on the extra evidence given?
4. What were the guilty parties' future plans and intentions based on the extra evidence given?

3.2. Submission Instructions

You will work in a team to solve the two cases given above. For your team number information, you can check the finalised team list posted in our course's discussion thread. Please prepare each of your reports in **a self-contained PDF** file, and **name** it as follows (do replace "*X*" with your team no, and replace "*Y*" with the case no): Team-*X*-Case-*Y*-Report.PDF. Submit **one PDF per team 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: Tuesday, 9 April 2024, 12:59 SGT.**
- **Case 2 Report: Tuesday, 16 April 2024, 12:59 SGT.**

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!

3.3. Presentations

In addition to your submitted reports, your team will also need to present your findings in one of the two following presentation sessions during our regular course hours:

- **Tuesday, 9 April 2024, 1:00-4:00PM: Case 1 Presentation *(6 selected teams)***
- **Tuesday, 16 April 2024, 1:00-3:30PM: Case 2 Presentation *(5 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. Please submit your team's slide-deck file on the assigned case by **naming** it as follows: Team-*X*-Case-*Y*-Slides.PDF. The 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. Extra Notes for Your Reporting & Presentation

Please find below some extra notes that can be useful for your team's reporting and presentation.

Your team's position:

You can consider your team as **a team of Customs forensics investigators.** Hence, in the report, you can use "we" instead of "I" when addressing yourselves as a team of forensic investigators.

Case presentation & target audience:

Again, we won't be simulating an actual court proceeding in our course. For the given 2 cases, you can assume that the audience consists of **the Customs' IT people** who already know **basic forensics techniques**. As such, you don't need to explain standard forensic techniques in layman's terms. Yet, you still need conclude the case clearly so that the Customs' management can know the answer to the asked questions.

Evidence coverage in your analysis:

Note that you need to identify, analyze, and report all important events contained in **the shared evidence files of the respective two cases *only***.

As described in the problem descriptions above, the case actually has sub-cases/parts: the **incomplete version (Case 1)** and **the full/complete version (Case 2)**. For your reporting & presentation of Case 1, you must cite evidence and answer the questions ***only from*** the memory dump and image files given in Case 1. That is, for your Case 1 analysis, your team can't argue using the extra files given in Case 2. In fact, your team's marks *will be deducted* if you do so!

6. Queries and Contacts

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

Thanks, good luck, and have fun!