# Assignment One

## Developing a Solution for a Problem in Digital Forensics

## Overview

Digital forensics can be thought of as the application of computer science in the systematic collection, processing, and study of digital data suitable for use in courts or to the just resolution of conflict, encompassing both data at rest and data in transit.

In today's context, the domain of digital forensics is typically further subdivided into different specializations, to cover both the breadth and depth of the digital domain. An example of possible specializations is shown in **Figure 1** below.

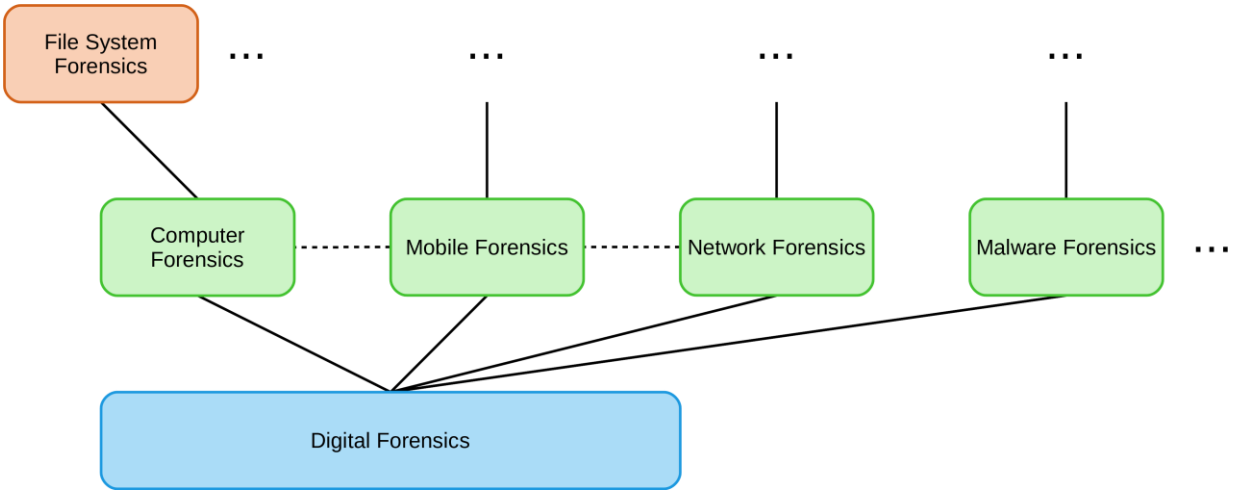


Figure 1: An example of specializations in digital forensics[1]

Given the vastness of digital forensics, the idea of knowledge and capability sharing, and learning from one another becomes imperative. In addition, the fast-changing pace of technology may introduce new things that has to be catered for, or render what was previously learnt or developed obsolete. Therefore, it is also important that a practitioner keep himself or herself up to date, and engage in continuous learning to always be in the know.

There are many tools and solutions out there that exist to help in the digital forensics process. Disk imagers, memory dumpers, decompilers and so on are what one typically uses when performing digital forensic work. In this assignment, you and your team are to design and develop a technical solution for a problem in digital forensics.

[1] Adapted from information in E. Casey, *Digital Evidence and Computer Crime*, 3rd Ed. Waltham, MA: Academic Press, 2011, p. 38.

# Task

In this assignment, you and your team are required to design and develop a technical solution for a problem in digital forensics. You are free to decide on what your solution does and the problem it addresses. It is expected that your solution be of a reasonably high quality, sufficient complexity, and novel. A solution can be a standalone software program, tool or utility, a plugin to a well-known or established forensics software (e.g., Volatility, IDA), or a hardware.

You may want to focus your solution to perform specific things, and / or within a reasonable problem scope, so as to allow you to produce an output that is of reasonably high quality and depth. Care must be taken not to choose a problem scope or set of tasks that is trivial, of which there may be nothing much to develop for, nor too broad, of which there may be too much to possibly develop leaving insufficient time to produce work of a sufficiently high quality or rigour.

As a guide, here are some questions that you may consider when deciding on what to work on

- Is your problem scope within the domain of digital forensics?
- What are the technical issues and challenges in digital forensics for the problem scope, and is there a gap for which a reasonably complex technical solution can be developed?
- What are the solutions or tools typically used to address the problem whether as a whole or in parts, and how would they compare against your proposed solution?
- Does development of your proposed solution allow for demonstration of technical competency in digital forensics?
- How much of knowledge that is required to develop the solution lies beyond the classroom?
- Can the technical solution be **developed to a reasonably high quality**, **tested in-depth** and validated **within eight weeks**, by a **five to six person team**?
- Does the solution have potential to be showcased to the public, such as through community meetups or cybersecurity conferences?

At the end of the assignment, you are required to submit 1) the codes and binaries for your solution, 2) a video demonstrating how your solution works, and 3) a report detailing your solution in-depth. Your codes are to be published to a GitHub repository, where the instructor will clone it for grading. Inside your code repository, you are expected to include a comprehensive user manual.

You must document your solution in-detail in your report, including but not limited to a comprehensive background research on the problem, plus analysis of the issues and

challenges typically faced in solving the problem, the solutions and approaches typically used, your solution to address the problem and how it compares to other solutions, and test setup and results to show the validity of your developed solution. You must also provide in-depth details and background of the technologies that your solution relies on.

Credit will be given for strong display of technical competency in a complex topic area, the comprehensiveness of the background research, the strength, novelty, and usability of the developed solution, and the correctness of its validation.

Should you require any tools or devices that the labs may be able to provide, do drop the instructor an e-mail at Weihan.Goh@Singaporetech.edu.sg. Do take note however that not all requests can or will be fulfilled.

# Team Formation

You may form your teams based on the following conditions

- You and your peers may come together to form your **own team**;
- Your team must consist of between **five (5) to six (6) individuals**;
- You may form a team of **less than five (5) individuals**, however your team will still have to deliver works **expected of a five to six-person team**;
- If you are unable to be part of a team by **the end of Monday, September 16, 2019**, you, and others like you, may be **grouped together into teams**, or **assigned to existing teams who are willing to take you in**, subject to the other conditions governing team formation.

If you have formed a team, you, or any member of your team must submit your team composition by the **end of Monday, September 16, 2019** through the course site.

# Project Outline Document

Although you are free to decide on what your solution does and the problem it addresses, you are required to inform the instructor before embarking further on the assignment[2]. In order to do this, you and your team are required to submit a **one-page document** detailing the following

- What is the problem you are trying to address?
- Why did you choose this problem to address?

[2] The is not so much to hinder or limit your choices, but to ensure that you have thought about things in a little more detail before deciding to pursue it. Additionally, it is also to ensure that no groups are working on overlapping ideas.

- What do you currently know about this problem?
- How have others addressed the problem, whether in part or as a whole?
- What are the solutions, tools, and approaches available to solve the problem, whether in part or as a whole?
- What will your solution do, in detail?
- How will your solution work?
- How is your solution different from, and why is it better than other existing solutions?
- What are the resources you may require?

This document must be submitted by the **end of Sunday, September 22, 2019** through the course site.

# Assignment Deliverables

You are required to submit

- By the end of **Monday, September 16, 2019**
    - Your **team composition**, submitted through the course site
- By the end of **Sunday, September 22, 2019**
    - A one-page **project outline document** detailing what your solution does and the problem it addresses, submitted through the course site
- By the end of **Sunday, November 10, 2019**
    - **Source codes and binaries** for your solution, uploaded to a GitHub repository;
    - A **comprehensive user manual** for your solution, uploaded to the same GitHub repository;
    - A **five (5) to fifteen (15) minute video** demonstrating how your solution works, uploaded to YouTube; and

- A **detailed report of around ten (10) pages**, but no strict maximum page limit, submitted through the course site, detailing your solution in-depth and should include, but not limited to
  - A comprehensive background research of the problem;
  - Analysis of the issues and challenges typically faced in solving the problem;
  - Solutions, tools, and approaches typically used to solve the problem;
  - Your technical solution to address the problem and how it compares to other solutions;
  - In-depth details of the technologies that your tool relies on;
  - Detailed architecture and engineering of your solution; and
  - Test setup and results to show the validity of your developed solution.

# Report Format

There is **no specific report typesetting or layout format** for which to follow; the template used for this instruction document is uploaded for your reference should you want to use it[3]. Unless explicitly stated, all reports must be in **Word, PDF, or LaTeX**.

If you wish to have a more compact format to increase the amount of contents, you may utilize templates from major scientific journals or proceedings, such as those from the IEEE[4,5] or ACM[6].

**Proper citation and referencing** must be maintained. You may use the APA, MLA, or IEEE citation format[7], or if you are using a template from a journal or proceeding, the citation format specified for that template. Any form of academic misconduct or plagiarism **will be severely dealt with**.

# Video Format

Your video must be at least in **Full High-Definition (1920 x 1080) resolution** and subtitled. You must obtain all necessary permission for the resources that you use, such as audio clips.

[3] This document uses the default Google Docs template downloaded as a Microsoft Word document.
[4] https://www.ieee.org/conferences_events/conferences/publishing/templates.html
[5] https://www.ieee.org/publications_standards/publications/authors/author_templates.html
[6] https://www.acm.org/publications/proceedings-template
[7] A good citation helper can be found at http://www.citethisforme.com/

# Solution Codebase

The codes and binaries, as well a comprehensive user manual to your solution must be **uploaded to a GitHub repository**. Should you develop a hardware solution, a prototype will have to be submitted for grading, and the bill-of-material and schematics will have to be uploaded to the GitHub repository.

Once again, credit will be given for strong display of technical competency in a complex topic area, the comprehensiveness of the background research, the strength, novelty, and usability of the developed solution, and the correctness of its validation.

# Contact Information

Should you have any questions or queries regarding this assignment, please contact the instructor at Weihan.Goh@Singaporetch.edu.sg. Please note that the instructor may not be able to answer certain queries especially when they may give teams an unfair advantage over others.

Any academic misconduct or plagiarism will be **severely dealt with.**

**END OF DOCUMENT**