SINGAPORE INSTITUTE OF TECHNOLOGY

Assignment One

Developing a Solution for a Problem in Digital Forensics, or for Anti-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, such as in media forensics, operating system forensics, mobile and IoT forensics, malware forensics and reverse engineering, network forensics, and so on.

There are many tools and solutions out there that exist to help in the digital forensics process. Disk imagers, memory dumpers, forensic toolkits, decompilers, and so on are what one may typically use when performing digital forensic work.

On the other hand, there are groups of people that engage in anti-forensics, i.e., they try to hinder, disrupt, or prevent digital forensics, be it because they need to protect incriminating evidence or activities from being discovered, or sometimes, for legitimate or other reasons.

In this assignment, you and your team will need to pick your side – will you design and develop a technical solution to solve a problem in digital forensics? Or will you design and develop a technical solution for anti-forensics?

Task

In this assignment, you and your team are required to design and develop a technical solution that can either be used for 1) solving a problem in digital forensics, or 2) engaging in anti-forensics.

You are free to decide on what your solution does and the problem statement it addresses. It is expected that your solution be of a high quality, sufficient complexity, and original. A solution can be, for example, a standalone software program, tool or utility, a plugin to a well-known or established forensics software (e.g., Volatility, Autopsy), or a hardware device.

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 and poster describing 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 must include a user manual.

SINGAPORE INSTITUTE OF TECHNOLOGY

Deciding on Your Project

You should focus your solution on accomplishing specific things that are within a reasonable problem scope, so as to allow you enough time to produce an output that is of high quality and depth. Care must be taken not to craft a problem statement or set of tasks that are trivial, of which there may be nothing much to develop for, nor too broad, for which there may be too much to possibly develop leaving insufficient time to produce work of a sufficiently high quality or rigor.

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

- What is the **problem statement**, i.e., what are you trying to address?
- Does this problem statement fall within the domain of digital forensics?
- What is your **proposed solution** to solve the problem? Is it reasonably complex?
- What are existing tools or solutions out there that can address your problem statement, 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 the knowledge required to develop the solution lies beyond the classroom?
- Can the solution and its technical implementation be developed to a reasonably high quality, tested in-depth, and validated within **ten weeks**, by a **four-person team**?
- Does the solution have the potential to be **showcased to the public**, such as through community meetups or cybersecurity conferences?

Credit will be given for strong display of technical competency in a complex topic area, the comprehensiveness of the literature review / background research[1], 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 with the subject title **"[ICT2202 Device Request]"**. Do take note however that not all requests can or will be fulfilled.

[1] This includes literature review using high-quality references such as academic journals, conference papers, and conference presentations from top tier cybersecurity conferences (e.g., Black Hat, DEF CON, etc.). Information from random websites, including Wikipedia, are generally not regarded as reputable sources.

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 **at most four (4) individuals**;
- All team members must come **from the same Practical Session group**;
- **You may form a team of less than four (4) individuals**, however your team will still have to deliver works expected of a 4-person team;

If you are unable to be part of a team by the end of Monday, September 5, 2022, 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, a member of your team must submit your team composition by the end of Monday, September 5, 2022 through the form at https://forms.microsoft.com/r/pD1ukRY9Qp.

Project Outline Document

Although you are free to decide on what you want to do, you are required to let the instructor know of your idea before embarking further on the assignment[2]. To do that, you are required to submit a one-page **project outline document** in the format of the template ***outline-template-a4.docx*** provided to you at the xSiTe Learning Management System. Your document should detail the following

- What is the **problem statement** you are trying to address?
- Why did you choose this problem statement to address, and what do you know about it?
- What are the existing solutions, tools, and / or approaches used to solve the problem, whether in part or as a whole (provide 5 to 10 references from reputable sources)?
- What is your **solution to the problem statement**? How will it work, and **what does it depend on** (e.g., list the platform, runtime, hardware, etc. that your solution needs in order to run)?
- How is your solution **different from, and why is it better** than other existing solutions?
- What are **the resources that you may require**?

This document must be submitted by the end of Sunday, September 18, 2022 through the course site. Your instructor will look at this document, and you may assume that you are on track should you not get a reply within one week of the submission deadline.

[2] This 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 teams are working on exactly the same projects.

SINGAPORE INSTITUTE OF TECHNOLOGY

Assignment Deliverables

Timeline

You are required to submit

- By the end of Monday, September 5, 2022, your team composition, submitted through a form at https://forms.microsoft.com/r/pD1ukRY9Qp.

- By the end of Sunday, September 18, 2022, a one-page project outline document, submitted through the course site

- By the end of Sunday, November 6, 2022
    - **Source codes and binaries for your solution**, plus a **user manual** uploaded to a GitHub repository;
    - A **five (5) to ten (10) minute video** demonstrating how your solution works, uploaded to YouTube (your video may be set as *Unlisted*, if so wish); and
    - A **poster** that summarizes your solution, with well-structured and clear contents, appropriate layout, and appropriate use of graphics; and
    - A **report of between five (5) to seven (7) pages**, detailing your solution in-depth and should include, but not limited to
        - An introduction describing your problem statement;
        - A comprehensive background research / literature review of the problem statement with at least 10 references;
        - Your technical solution to address the problem statement and how your solution works, including, where applicable, flowcharts, architecture diagrams, algorithms, etc.
        - Results to show the validity of your solution, and how it compares to other existing solutions;

Report Format

Your report must follow the IEEE conference proceedings template, for which a copy is provided to you in the file ***report-template-a4.docx***. Do not deviate from the format prescribed in the template (you can be penalized for doing so). You must submit two copies of your report, one in **Word** format, and another in **PDF** format.

Proper citation and referencing must be maintained, following the IEEE citation format. Credit will be given for appropriate use of high-quality references from academic journals and / or conference proceedings, and likewise penalty will be given for use of inappropriate or low-quality resources such as Wikipedia.

Poster Format

Your poster must follow the SIT poster template, for which a copy is provided to you in the file ***poster-template-a1.pptx***. You must submit two copies of your poster, one in **PowerPoint** format, and another in **PDF** format.

In designing your poster, do not alter the poster size of A1, position of the SIT logo, the color scheme or size of the red banners, or any other SIT fixtures on the template. The template prescribes a color restriction, which refer only to the font color, and not to the images and other content. Images should be at least 300dpi.

Proper citation and referencing must be maintained, following the IEEE citation format.

Video Format

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

Solution Codebase

The codes and binaries, as well a user manual for 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.

You may opt to keep your repository private, however you will need to send an invitation to the instructor to access your repository. This invitation must be sent between November 5 to 6, 2022.

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

Assignment Weightage and Further Information

This assignment shall constitute **at minimum 30%, and no more than 35% of the overall weightage** for the ICT2202 / ICT2202X Digital Forensics module.

Contact Information

Should you have any questions or queries regarding this assignment, please contact the instructor at Weihan.Goh@Singaporetech.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