7906ICT Digital Forensics Assignment Specification

Due Date: 20 September 2019
Weighting: 40%

This assignment is worth 40% of the total assessment for 7906ICT. It is individual work. While you can discuss the assignment with your peers, your submission should be your own work. You should provide evidence of your own work incorporated in your submission.

The objective of this assignment is to gain knowledge and understanding of digital forensics through research and practical experience. This understanding is to be demonstrated by submission of a formal technical report of an analysis of digital forensics artefacts and a brief essay on recent advanced in digital forensics.

Background

On his way to rendezvous with Maria Hill, the espionage agency S.H.I.E.L.D. Director, Nick Fury, is ambushed by assailants led by a mysterious assassin called the Winter Soldier who works for the evil secret society H.Y.D.R.A. Fury escapes to Steve Rogers' apartment, and warns Rogers, also known as Captain America that S.H.I.E.L.D. is compromised. Fury is gunned down by the Winter Soldier, before handing Rogers a flash drive. Fury is pronounced dead during surgery, and Hill recovers the body. [1]

Task 1

Steve Rogers has asked you to investigate an internal S.H.I.E.L.D. transmission found on the flash drive. He suspects that there is evidence of H.Y.D.R.A. double agents in the transmission. Your task as his friend and S.H.I.E.L.D. digital forensics analyst is to answer Rogers' questions.

1. Who are the agents in the transmission? When does the first communication begin?
2. What browsers are the agents using and on what operating systems?
3. Are there double agents working for H.Y.D.R.A.? Who are they?
4. What applications are running on Steve's computer? Should Steve have these open?
5. What web pages has Steve Rogers visited recently?
6. What is Steve Rogers' email address?
7. What is Steve Rogers' Password?
8. Is Steve Rogers PC infected with a virus?
9. What was sent for Daisy to collect?
10. Is Daisy a H.Y.D.R.A. agent?

[1] The story, all names, characters, and incidents portrayed in this assignment are fictitious. No identification with actual persons (fictitious, living or deceased), places, buildings, events, and motion pictures is intended or should be inferred. No person or entity associated with this assignment received payment or anything of value, or entered into any agreement, in connection with the depiction of tobacco products. No animals were harmed in the making of this assignment.

11. Create a detailed map of the network, including IP addresses, hostnames and services as well as suspected owners of each host.
12. Create a detailed timeline of the significant events that take place in the captured transmission.

As part of the answer for each of these questions you must include:

- A clear description of the evidence and reasoning for your answer.
- A detailed description of the process that you followed and the tools that you used to obtain the evidence. It is expected that you will include screenshots in your description.

Task 2

After the Winter Soldier affair and the major part your digital forensics investigation played in the outcome of that situation, Nick Fury has decided that S.H.I.E.L.D. should know more about the digital forensics field. He has asked you to review the latest research in the digital forensics area and conduct some investigations of your own either developing new findings or confirming previous work. Your task is to write a brief educational essay for S.H.I.E.L.D. forensics operatives that will be useful in improving their investigations.

Select one topic in digital forensics. This may include the following list but is not limited to:

- Acquisition Processes
- Disk Forensics
- File Carving
- Live Memory Forensics
- Network Packet Forensics
- Internet Forensics
- SDN Forensics
- Internet of Things Forensics
- Forensics Readiness
- Forensic Standards and Legal Regulations

Your essay on recent advances in digital forensics should not exceed 6 pages in the IEEE Conference A4 Template format. It should include the following main headings:

- **Introduction** – Provides motivation and background
- **Previous** Work – Describes lead up work to this area
- **New Project** – Title may vary, but should describe the digital forensics topic
- **Conclusions and Recommendations** – Describes future recommendations

Submission

Please submit your assignment via the 7906ICT Blackboard web site under the Assessment section. Reports may be submitted as two separate files in one zip file or as a single file.

The quality of the presentation of a formal technical report is as important as the quality of the technical content of the report in the profession. Your assignment will be assessed on:

1. The body text of your report for Task 1 should be no more than 14 pages in length excluding appendices;
2. The text of your report for Task 1 should be in 12-point Times New Roman or 11-point Arial font or something equivalent, and in single space;
3. Page size is A4 with 2cm in margins on all sides;
4. The Task 1 report is suggested to be organised with executive summary within one page, table of contents, body text, and appendices;
5. Task 1 report body text consists of your overall analysis of each task, description of how you went about completing each task and your conclusions.
6. The Task 2 report should follow the IEEE Conference A4 Template.
7. The Task 2 report should be a minimum 4 pages and a maximum 6 pages.