Forensic Assignment

General

Deadline: March 4th – 23:59.

Submission: Please upload to Moodle by deadline. If you're one minute late your work will be marked as late – so please upload in plenty of time. If you have extenuating circumstances please contact me and your tutor and go through the proper procedure – only if your circumstances are upheld as valid will I consider them.

Plagiarism: You may discuss with other students your general approaches and techniques for undertaking this coursework but you may not discuss specific solutions. For example, you may discuss how to use fdisk generally, but you may not discuss how to use it specifically on this work. I reserve the right to employ anti-plagiarism techniques on this coursework designed at catching such behaviour – this may include using techniques such as steganographic watermarking.

References: Your report should be your own and you should use appropriate citation and referencing formats. All sources that you use as supporting material to your reports must be referenced according to convention. Failure to do so will result in loss of marks! You should use the APA as a referencing style.

Formatting:

1. Paragraph text: Font size 12 with Calibri or Times New Roman font. 1.5 line spacing. J*ustified* alignment (ctrl+j in word).
2. Use Word (or equivalent) styles for headings, paragraphs, etc. to ensure consistency.
3. Number chapters (1, 2, etc.) and sub-chapters (e.g. 1.1, 2.1, 2.2) – and consistently.
4. Figures should have a figure number and a caption (right click and insert caption in Word).
5. Write in the third person.
6. Word limit: **3500 words**

WARNING: This coursework is worth 70% of your overall mark. Hence you cannot afford to treat this assignment as optional.

Description - Background

It's early 2010, and you're a Forensic Investigator given the following case…

Founded by Pat McGoo, m57.biz is a patent search company that researches patent information for their clients. Specifically, the business of patent search is to generally verify the novelty of a patent (before the patent is granted), or to invalidate an existing patent by finding prior art (proof that the idea existed before the patent). At the start of the scenario, the firm has four employees: CEO (Pat McGoo), IT Administrator (Terry), and two patent researchers (Jo, Charlie). The firm is planning to hire additional employees at a later date once further clients are booked. Since the company is looking to hire additional employees, they have an abundant amount of technology in the inventory that is not being used.

Employees work onsite, and conduct most business exchanges over email. All of the employees work in Windows environments, although each employee prefers different software (e.g. Outlook vs. Thunderbird).

Description - Case: Illegal Materials (Methamphetamine)

A functioning workstation originally belonging to m57.biz was purchased on the second-hand market in early December, 2009. The buyer (Mr. Aaron Greene) realizes that the previous owner of the computer had not erased the drive, and finds suspicious documents and videos related to drug use (specifically Methamphetamine) when looking through the folders and opening the various applications. Mr. Greene reports this to the police, who take possession of the computer.

Police forensics investigators determine the following:

- The computer originally belonged to m57.biz
- The computer was used in 2009 by Jo, an M57 employee, as a work machine.
- The computer was sold as-is to Mr. Aaron Greene on December 1st.

The police provide you with a disk image from the computer purchased by Mr. Aaron Greene, as created on December 2nd, 2009. The image has the extension "dd". It has been shared with you that Mr. Aaron is considered to have acted suspiciously and answered questions inconsistently throughout all interactions with the detectives.

Materials – Drive Image

The materials you will use for your investigations are:

- Hard drive image 2009-12-02.dd (of the sold computer)

Deliverable – Report

Task Description:

You should follow forensics procedures, such as taking a hash of the image before using it and checking regularly to ensure you have not modified it. You can select and use any proprietary or open source tools that you have been introduced to or find yourselves to perform the analysis and extract any evidence present.

Your report should detail the investigation process and the findings (including copies of relevant evidence), including obstacles and problems that you encountered and how you overcame them. You can assume that the reader has a light understanding of digital forensics, so any complicated terms/techniques/etc should be explained.

You must include *some* screenshots in your reports with the output of the tools or the process as and when necessary to support/show how you reached your conclusions. Screenshots should not be used to excess – they merely serve to demonstrate your understanding of the tools/processes and should be used to support written explanations (not in place of).

You will be marked based on the evidence you extract, the use of appropriate tools, the detail of the process, the explanation on its relevance to the case and documentation. Remember, your report should present the information in an unbiased way. Improper handling/validation of evidence would result in loss of marks except where accurately identified and corrected.

Deliverable – Report (continued)

Outline: Use the following as a starting-point to structure your report

Cover Page

- Title
- Date
- Student Name / Student Number

Table of Contents

- Main contents listed with page number
- Be sure to include visible page numbers on all pages

Executive summary

- Brief Description of the event
- Brief methodology of the investigation
- Brief evidence collection and preservation methods
- Conclusion with short, generalized reasons (like bullet-points)

Methodology details

- Investigation
- Evidence collection and preservation

Finding 1 - Description

- Discussion (e.g. Inculpatory or Exculpatory)
- Supporting evidence

Finding *n* - Description

- Discussion (e.g. Inculpatory or Exculpatory)
- Supporting evidence

Summary and Conclusion

- Discuss if there is there any evidence of illegal drug activity (Methamphetamine).
- How sound / reliable do you believe your evidence collection to be?
- Is the person innocent or guilty - Explain your position on this.

Appendix

- Description of persons of interest (often shown in table format)
- Association Diagram of persons of interest
- Evidence listing
- Evidence Timeline (present any evidence in a time line format, signposting the points where you believe any offence may have occurred and other significant dates/times in the case).
- Software and tools used in the investigation
- Other important listings and information as needed