SIT282- Computer Crime and Digital Forensics T2 2019

Assessment Task 1 Investigation Report
Due: Sunday August 11th at 11.59pm (end of week 5).
Total Available Marks: 20, Weighting 20%

NOTE: IF YOU HAVE NOT SIGNED AND SUBMITTED YOUR ETHICS AGREEMENT, YOUR ASSIGNMENT WILL NOT BE MARKED AND YOU WILL BE DIS-ENROLLED FROM THE UNIT.

General Requirements

Please use the "Assessment_Task_1_TEMPLATE" file provided in the assessments folder on the Unit Site to complete this assessment.

- NO EXTENSIONS allowed without medical or other certification.
- LATE ASSIGNMENTS will automatically lose 5% per day up to a maximum of five days, including weekends and holidays. Assignments submitted 6 or more days late will not be marked and are given zero.
- The virtual machine used for the practicals contains all the tools required to complete this assessment task.
- Ensure you take screenshots of your work for evidence and that these are legible in your report.
- To complete this assessment you will need to have followed the theoretical material and completed the practicals for weeks 1-5. This assessment covers material up to the week ending August 9.
- Your submission must be in a form readable by Microsoft Word.
- Maximum size of your submission should be **15** pages excluding the cover page but including screenshots. The font size should be no less than 11pt.
- **No mark will be given if you fail to show the evidence of your work-out. i.e. the process carried out to produce your solution. The report should be written so the steps performed are reproducible.**
- Ensure you keep a backup copy of your work.
- Plagiarism is not tolerated. For information on Plagiarism and Collusion including penalties please refer to the link: http://www.deakin.edu.au/students/clouddeakin/help-guides/assessment/plagiarism
- The APA Referencing Style is to be used for this assignment where appropriate. https://www.deakin.edu.au/students/studying/study-support/referencing/apa-6

Help with the assessment

If you require assistance please ask your instructors (Burwood students ask your practical demonstrator; Geelong and Cloud students ask Damien Hutchinson). We will **NOT** answer questions that are requesting answers or solutions. A question MUST be substantiated with evidence that work has been attempted relating to the question being asked.

THE CASE:

Donald Price is an employee from Joachim's Art Gallery based in Melbourne, Australia. Mr. Price had been suspended from the gallery when an audit discovered that one of the pieces he was responsible for had disappeared. (This was a small watercolour of two boats.) Unfortunately, Mr. Price wiped the hard disk of his office PC before investigators could be deployed. However, a CD-ROM was found in the PC's CD-ROM drive. Although Mr. Price subsequently denied that the CD-ROM belonged to him, it was seized and entered into evidence.

A forensic image in raw format of the CD-ROM can be found here:
https://www.dropbox.com/s/ov5ksmtn7afurqw/2019Greenbook.ISO?dl=0
And its MD5 hash value can be found here:
https://www.dropbox.com/s/gu7wjpkvymhr1u0/2019Greenbook.ISO.md5?dl=0

You, an IT officer employed by Joachim's Art Gallery, are assigned to examine the image for any information relating to the case. You should keep in mind malicious codes and other means which may potentially alter the evidence. **YOU MUST CITE ALL REFERENCES INCLUDING TECHNICAL MANUALS AND LAW PARAGRAPHS.**

Your analysis should be conducted on a virtual machine (Virtual Box) and include the following information:

1. PROCEEDURE

1.1 Use an evidence form to document the evidence given to you.
(1)

1.2 Describe the environment of your forensic workstation and the access to the machine. Describe the procedure that you used to download the image file to your work directory.
(1)

1.3 Give at least two SHA-based hash function values of the ISO image.
(1)

1.4 Explain why multiple hash values are necessary to verify the validity of the image file.
(1)

1.5 Explain the procedure that you used before you could access the image file inside the virtual machine.
(1)

2. BINARY DETAILS

2.1 Use a table to document the detailed information of the files found in the root directory of the ISO image—file names, file actual sizes and their MD5 hash values

(1)

2.2 Provide a description of any programs you would like to use based on the files identified on the ISO image.

(1)

3. FORENSIC DETAILS

3.1 Describe the key words you used to search the ISO image and explain why you chose them. Detail your search result and give your conclusions. (Document your procedure including commands and screenshots.)

(9 in total)

4. LEGAL IMPLICATIONS

4.1 List one violation conducted by Mr. Price against Cybercrime Act 2001, and one violation conducted by Mr. Price against the Crimes Act 1958. Back up your answers with definitions.

(2)

4.2 Is this case best pursued as a corporate or criminal investigation? Why?

(2)