ASSESSMENT TASK 3 - INVESTIGATION REPORT

Due: Sunday, September 27th at 11.59pm (end of week 10)
Total Marks: 50 (40 Report + 10 Interview), Weighting 50%

GENERAL REQUIREMENTS

Please use the "Assessment_Task_3_TEMPLATE" file provided in the assessments folder on the Unit Site to complete this assessment.

- 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 1-10.
- 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.
- 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 attend one of the drop-in sessions. 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

The hazardous materials team is called suddenly at 3a.m. May 10 to a warehouse behind Roma St station in Brisbane. Team member Moti identifies the scene as a drug manufacturing location, and the people there have hurriedly packaged up the loose powders they were working with, leaving traces on the floor and across many desk surfaces. Moti makes a decision not to call the forensic squad in when he sees the drug traces, because he suspects the drug is at the top of the current most dangerous list and he needs to take samples back to his lab for analysis before identifying it.

However, Moti is familiar with the protocol when there is a computer in the area, and calls his colleague Sandra, waking her at 3:17a.m. to walk him through a capture of computer data for forensic analysis. He is able to shut down the laptop and removes it from the scene along with several CDs found in the desk.

Later that day, Sandra analyses the laptop and CDs in the police forensics lab. The computer is equipped with Windows and only a basic Word document facility and Internet Explorer, a program called "OpenPuff", and has software for showing DVDs and image files. No documents appear to have been stored on the machine. Three of the CDs are actually DVDs with recent movies. The fourth contains a suspicious ZIP file.

Sandra makes three forensic copies of all the data and stores two of them safely in the lab. She then delegates the laptop and CDs to various staff members for analysis, distributing the third copies to them. As most of the staff are also involved in a large on-going investigation, she decides to ask for the help of an additional team member who is holidaying overseas.

You receive a secure e-mail from Sandra with an attachment containing two NTLM hash strings retrieved from the criminal's laptop, the ZIP file from one of the CDs along with a request to analyse it as quickly as possible for any pertinent information, and an apology for interrupting your holiday.

The two NTLM hashes are:
D6A21EA26063C42FC9876E4B0C51BC82:CA72B189F412A384D96B785A08176773
and
8282461A2BDAF626E6067B973FDDC643:5C305D4616C7571D5DDC6EEA5BA5C395

TO DOWNLOAD A COPY OF THE ZIP FILE IN THE EMAIL ATTACHMENT COPY AND PASTE THIS URL INTO A WEB BROWSER:

http://www.deakin.edu.au/~zoidberg/2019A02.zip

And you are advised that the MD5 hash value of the executable file should be
9ec1c8f62429182349f3979c39aed8fb

Analyse this file and report your findings using the outline below.

Digital Forensics Procedure

For marking purposes, it is strongly recommended that you follow this outline:

1. Explain how you downloaded the file, what precautions you took, and how you ensured its integrity. *(2 mark)*
2. Describe how you decrypt the two given NTLM hash values by using OphCrack including screen shots. *(4 marks)*
3. Describe the process that you apply to open the downloaded file. Describe whether there is a relationship between this process and the information obtained in Step 2. *(4 marks)*
4. Describe the actual content of the encrypted file that you identified in Step 3. If there are multiple files, list their file names, types and MD5 hash values. Describe the visual contents in each file. *(4 marks)*

5. What tools will you now use to proceed your investigation and why? *(2 mark)*
6. Describe how your investigation proceeded at this point, including screen shots. *(16 mark)*
7. Write a two-page report for Sandra listing your findings and recommendations. Make appropriate suggestions on how a further investigation should proceed. Construct and complete a single-item evidence form as part of your report. *(8 marks)*