Course title: Digital Investigation

Submission date 27/05/2020 08:00- 28/05/2020 08:00

When ready to begin the analysis click start and you will be given the details for the assignment.

* Five (5) hour time limit.
* Only 1 attempt is allowed.
* Once started you cannot restart.
* You must upload your briefing statement and contemporaneous notes before the end of the time - otherwise this will be an automatic fail.
* You can submit your documents in the two questions in this quiz.

**Assignment Details** This assignment brings together all your learning, and developed skills, from throughout the course. You will be required to undertake a time constrained examination of digital media. This will cover aspects throughout the course, but will include:

• User Activity

• System Restore Point

• Windows Registry

You will produce contemporaneous notes documenting your methods and findings. You will each be provided with forensic images in the E01 format, from a system, or systems. These will be provided through Google Drive. Within the same folder will be a contemporaneous log document and a briefing note document. You must record all your actions, methods and thoughts within the cotemporaneous notes document. After you have concluded your investigation, finish by writing a short briefing note, explaining the key findings of your examination, and provide information which will be useful to the Senior Investigating Officer (SIO) in their subsequent enquiries.

This assignment is looking for a mix of accuracy, technical and professional skills. Whilst we know what data should be recovered, you can still achieve a high mark through professional documentation and clear and detailed thought process showing appropriate application of skills and knowledge.

The assessment will be available for a 24-hour period. **27/05/2020 08:00 – 28/05/2020 08:00.** Submissions after this time will be deemed as late and not marked.

At any point in this 24-hour period you will have **five (5) hours** to complete the test. All students will undertake the assessment on the same day.

We have created a “quiz” on Moodle to provide the details of the assessment and to provide the details of the data you will need to analyse. There are also two questions which are file uploads, one for your contemporaneous notes and one for your briefing statement. You are expected to upload your documents as PDF’s, DOCX or DOC. This must be within the five (5) hour period.

The quiz has a time limit of five (5) hours this gives you time to download the data and undertake the analysis:

• This is an individual assessment. Therefore, no communication with any other person is permitted, verbal, written or digital.

• Sharing is not allowed – it will be evident if this is the case and all students involved will be taken through the relevant unfair practice process and receive the penalties and records for this.

• You must ensure they have a reliable internet connection, and a quiet place to work, and time in which to complete the assessment in one sitting. You should allow five (5) hours, this will allow you to setup, download the relevant data and begin the test.

There are two aspects to the submission:

**• Contemporaneous Notes:**

o Detailed actions should be recorded

o Highlight of the significance of findings

o Justification of the reasons for conducting a certain action

o Chronological order

o Detailed enough to allow replication, but not an essay

o Use of screenshots and tables

o Clear identification of tools, with justification

o Clear identification of the data under examination

o Integrity confirmation of the exhibit

**• Briefing Statement:**

o Focus on summarising existing evidence/leads and promoting further lines of enquiry.

o Consider the format, tone and structure of what you write – this is intended for a professional audience, there should be few grammatical and spelling errors

o Accuracy is the key, your results should be accurate, justified and relevant

o Explain technical terms

o Ensure you have a balanced perspective on what is there

**Toolsets:**

• You may use any tool introduced during the course, in earlier courses or identified through your own research

• Your “main” tool must be capable of opening an E01 file

• You will need to: o Identify hash’s

o Look for keywords

o Review images

o Export and report on data

o Review dates and times

o Look at the Registry

o Look at Windows artefacts

o Access restore points

o Identify cloud-based accounts

o Identify and analyse web history

**General Guidelines for each submission**

**Word Count**: There is no explicit word count for this assignment.

**Intended Audience:** Professionals within the Digital Forensics field. Therefore, you must write in third person using a professional tone and correct use of English.

**MARKING SCHEME / CRITERIA**

Allocation of marks are described below. Marking will be conducted using a spreadsheet that generates marks based on performance in each of the marking scheme areas. For example, each requirement will have a number of comments describing possible outcomes (such as “Correct Harvard referencing style”, or “Harvard referencing style contains errors”, or “No referencing”).

Marking will involve selecting or creating appropriate feedback. Consequently, you can expect detailed feedback once your assignment has been marked.

Marks for the assignment are gained for the work you complete in terms of its depth. This is not designed to be a superficial assignment (you must submit all the requirements).

Marks will be allocated on the following basis:

**• Contemporaneous Notes: 40%**

o Chronological

o Few steps missing

o Appropriate level of detail

o Technically accurate

o Utilisation of figures and tables to support statements

o Clear identification of the location of data for repeatability

o Utilisation of appropriate technologies to confirm the integrity and accuracy of data

**• Briefing Statement: 40%**

o Technically accurate

o Identified and justified evidence and its weight towards the investigation

o Utilisation of figures and tables to support statements

o Clear identification of the location of data for repeatability

o Utilisation of appropriate technologies to confirm the integrity and accuracy of data

o Nothing additional to contemporaneous notes

**• Overall Quality: 20%**

o Correct grammar and few spelling mistakes

o Template utilised

o Correct professional tone and consideration of the reader

As a general guidance of expectations (keeping in mind the weightings provided above):

● Work that is awarded an A will precisely follow the above guidance to clearly document an outstandingly detailed analysis and practical work, including a detailed technical description that is free of errors, and will make extensive use of figures and screenshots to illustrate the use of practical testing.

● Work that is awarded a B/C will follow the above guidance to clearly document a very detailed analysis of practical work, containing few (if any) errors or inaccuracies, and will make good use of figures and screenshots to illustrate the use of work undertaken.

● Work that is awarded a D will mostly follow the above guidance to document a detailed analysis of practical work, containing few errors or inaccuracies, and will make use of figures and screenshots to illustrate work undertaken, although some sections may be lacking supporting evidence or description.

● Work that is awarded a D will more or less follow the above guidance to document a detailed technical analysis, although it will contain errors or inaccuracies or lack detailed technical discussion, it will make some use of screenshots to illustrate the use of software, although some sections may be lacking supporting evidence.

● Work that does not pass will generally not follow the above guidance, be of a poor standard, will not demonstrate an understanding of the technical goings, and/or will not provide adequate evidence of practical engagement.