**Assessment item 3 - Tasks and Forensics Report**

**Value: 25%**

 **TASK**

**Task 1: Recovering scrambled bits (5%) (5 marks)**

For this task I will upload a text file with scrambled bits on the subject interact2 site closer to the assignment due date. You will be required to restore the scrambled bits to their original order and copy the plain text in your assignment.

Deliverable: Describe the process used in restoring the scrambled bits and insert plain text in the assignment.

**Task 2: Digital Forensics Report (20%) (20 marks)**

In this major task you are asked to prepare a digital forensic report for the following scenario after carefully reading the scenario and looking at textbook figures as referred below: You are investigating a possible intellectual property theft by a new employee of Superior Bicycles, Inc. This employee, Tom Johnson, is the cousin of Jim Shu, an employee who had been terminated. Bob Aspen is an external contractor and investor who gets a strange e mail from Terry Sadler about Jim Shu's new project (shown in Figure 8-5 of the textbook on p. 350).

Bob forwards the e-mail to Chris Robinson (the president of Superior Bicycles) to inquire about any special projects that might need capital investments. Chris forwards the e-mail to the general counsel, Ralph Benson, asking him to look into it. He also forwards it to Bob Swartz, asking him to have IT look for any e-mails with attachments. After a little investigation, Bob Swartz forwards an e-mail IT found to Chris Robinson (shown in Figure 8 - 6 of the textbook on p. 350).

Chris also found a USB drive on the desk Tom Johnson was assigned to. Your task is to search for and determine whether the drive contains any proprietary Superior Bicycles, Inc. data in the form of any digital photograph as an evidence. In particular, you may look for graphic files such as JPEG on the USB drive hidden with different format. Note for the USB drive image, you need to download the "C08InChp.exe" file from the download section of Chapter 8 on the student companion site of the textbook (Nelson, Phillips, & Steuart, 6/e, 2019).

Your task is to search all possible places data might be hidden (e-mails and USB drive) and recover and present any digital evidence in the report.

**Deliverable: For this forensic examination, you need to provide a report of 1800-2000 words** (approximately 5 A4 pages) in the format described in presentation section below.

**RATIONALE**

This assessment task will assess the following learning outcome/s:

be able to determine and explain the legal and ethical considerations for investigating

and prosecuting digital crimes.

• be able to formulate a digital forensics process.

• be able to evaluate the technology in digital forensics to detect, prevent and recover

from digital crimes.

• be able to analyse data on storage media and various file systems.

• be able to collect electronic evidence without compromising the original data.

• be able to critique and compose technical tactics in digital crimes and assess the steps

involved in a digital forensics investigation.

• be able to prepare and defend reports on the results of an investigation.

 

  

**PRESENTATION**

The following should be included as minimum requirements in the report structure:

Executive Summary or Abstract

This section provides a brief overview of the case, your involvement as an examiner, authorisation, major findings and conclusion

• **Table of Contents**

• **Introduction**

Background, scope of engagement, forensics tools used and summary of potential findings

• **Analysis Conducted**

o Description of relevant programs on the examined items

o Techniques used to hide or mask data, such as encryption, steganography, hidden

attributes, hidden partitions etc

o Graphic image analysis

• **Findings**

This section should describe in greater detail the results of the examinations and may include:

o Specific files related to the request

o Other files, including any deleted files that support the findings

o String searches, keyword searches, and text string searches

o Internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity

o Indicators of ownership, which could include program registration data.

 **• Conclusion**

Summary of the report and results obtained

**• References**

You must cite references to all material you have used as sources for the content of your work