Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2022/2023

COURSE NAME	:	COMPUTER CRIME AND DIGITAL FORENSICS
COURSE CODE	:	BIS 30803
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY / AUGUST 2023
DURATION	:	3 HOURS

INSTRUCTION

1. ANSWER ALL QUESTIONS
2. THIS FINAL EXAMINATION IS CONDUCTED VIA **CLOSED BOOK.**
3. STUDENTS ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED VIA CLOSED BOOK.

THIS QUESTION PAPER CONSISTS OF **FIVE (5)** PAGES

SECTION A
Choose the **BEST** answer for each of the following questions.

Q1 Which of the following is the procedure that involves imaging a disk?

A. Acquiring or collecting evidence.
B. Analyzing the evidence.
C. Examining the evidence.
D. Reporting.

(2 marks)

Q2 What is unallocated space?

A. Space between cluster.
B. Data that the computer is using and keeping tabs on.
C. Space that is not allocated to active files within a file system
D. Remote space

(2 marks)

Q3 Metadata for a file contains information as listed in the following **EXCEPT** _____.

A. content information
B. created information
C. modified information
D. accessed information

(2 marks)

Q4 Which of the following is the definition of a file header?

A. A unique set of characters at the beginning of a file that identifies the file type.
B. A unique set of characters following the file name that identifies the file type.
C. A 128-bit value that is unique to a specific file based on its data.
D. Synonymous with file extension.

(2 marks)

Q5 Assuming that the size and the start of sector for file test.jpg is 10,000 and 25,500 respectively. What is the offset of the starting point of this file?

A. 30,500.
B. 31,012.
C. 13,128,000.
D. 13,056,000.

(2 marks)

SECTION B

Q6 (a) Give **TWO (2)** ways to isolate wireless devices.

(3 marks)

(b) Compare the digital evidence that can be obtained between Dead Forensics and Live Forensics.

(4 marks)

(c) List **FOUR (4)** non-volatile data that can be found in UNIX environment.

(4 marks)

(d) Explain the content of Fourth Amendment Right in United States.

(2 marks)

(e) Give **TWO (2)** conditions of exigent circumstances that allow warrantless search.

(2 marks)

Q7 Naeem is a forensic accounting analyst who handle ABC money laundering case. He has received a disk image to investigate. He suspects that the image contains a record of a bank transfer of RM1,000,000 from the National bank of Country A (NBA) to The First Bank of the Country B (FBB). He believed the record is in pdf format. To make it worse, the disk is encrypted using TrueCrypt software. He also suspects that there is hidden data in the disk. He believed that there are records containing list of company that being used to launder the money and there should be email and telegram records that can connect ABC with the other organizations.

Based on the above scenario, answer the following questions:

(a) Define forensic accounting.

(2 marks)

(b) Justify **THREE (3)** hiding places that Naeem should examine in the disk.

(6 marks)

(c) Suggest **THREE (3)** ways that can be used to break the encrypted disk.

(6 marks)

(d) Justify **THREE (3)** artefacts that can help in the investigation.

(6 marks)

(e) Apply **TWO (2)** forensic techniques/ methods (other than decrypt disk and finding hiding data) that can help in the investigation.

(4 marks)

Q8 Consider the following scenario:

In 1997, Keith Cooper was wrongfully convicted of robbery in Elkhart, Indiana. The primary evidence against him was the eyewitness testimony of a victim and a jailhouse informant who claimed Cooper had confessed to the crime. However, Cooper maintained his innocence throughout the trial and was sentenced to 40 years in prison.

Years later, Cooper's lawyers learned that the digital evidence used in the case was mishandled by the police department's digital forensics investigator, Detective Michael Anderson. Anderson, who had no formal training in digital forensics at the time, had used outdated software and techniques to extract data from a computer seized from the crime scene.

The expert found that Anderson's report contained numerous errors and omissions, and he failed to follow basic protocols for the handling and analysis of digital evidence.

In 2005, Cooper's lawyers filed a motion for post-conviction relief, citing the mishandling of digital evidence as a key factor in his wrongful conviction. The motion was granted, and Cooper was released from prison in 2006, after serving nearly a decade behind bars.

(a) From your opinion, what are the steps that should be taken by Anderson in handling the digital evidence during the evidence collection procedures.

(4 marks)

(b) Explain each steps in **Q8(a)**.

(6 marks)

(c) Propose **TWO (2)** trainings that are needed to ensure the competency of the forensic investigator in handling the digital evidence.

(4 marks)

(d) Suggest **TWO (2)** forensic hardware and **TWO (2)** forensic software that should be used by Anderson during collection of digital evidence.

(4 marks)

(e) From your opinion, how a software acquisition can be vulnerable compared to hardware acquisition?

(2 marks)

Q9 Determine how the following cases are solved using digital forensics (DF) evidence(s).

(a) Allegations of Russian troops were operating in other parts of Ukraine in 2014. Alexander Sotkin (Russian Army sergeant), take few **selfies** along his journey from military base in Russia to eastern Ukraine and then back to the base. These pictures are uploaded into public Instagram.

(3 marks)

(b) Matt Baker, a Baptist preacher, was convicted of murder of his wife and was sentenced to imprisonment for 65 years. In the year 2006, his wife had apparently committed suicide by overdosing on sleeping pills. The suicide was confirmed based on the suicide note left by his wife. However, while analyzing Baker's computer, the investigator found evidence of interest at the search history of Baker's computer.

(3 marks)

(c) Xiaolang Zhang stole Apple's trade secrets case in 2018. Xiaolang Zhang who worked as an engineer for Apple's autonomous car division announced that he would be resigning and returning to China to take care of his elderly mother. He told his manager that he would be working for an electric car manufacturer in China. The conversation left the manager suspicious.

(3 marks)

- END OF QUESTIONS -