Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2021/2022

COURSE NAME	:	COMPUTER CRIME AND DIGITAL FORENSICS
COURSE CODE	:	BIS 30803
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY 2022
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER ALL QUESTIONS
		2. THIS FINAL EXAMINATION IS AN **ONLINE** ASSESSMENT AND 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 As a good forensic practice, why it is a good idea to wipe a forensic drive before using it?

A. To differentiate file and operating systems.
B. No need to wipe.
C. To prevent cross-contamination.
D. To follow chain of custody.

Q2 Which of the following is the procedure that involve imaging a disk?

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

Q3 Which of the following technique **IS NOT** Windows non-volatile data?

A. System version and patch level.
B. History of login.
C. Cached NetBIOS Name Table.
D. IIS log.

Q4 What is an 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.

Q5 Metadata for a file contains information as listed in the following **EXCEPT** _____.

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

Q6 Which of the following is a 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.

Q7 Assuming that the size and the start of sector for file test.jpg is 13,000 and 31,500 respectively. What is the offset of the starting point of this file?

A. 30,500.
B. 31,012.
C. 16,128,000.
D. 15,628,000.

Q8 The smallest area on a drive that data can be written to is a _____, while the smallest area on a drive that a file can be written to is a _____.

A. bit and byte.
B. sector and cluster.
C. volume and drive.
D. memory and disk.

Q9 You are a computer forensic examiner tasked with determining what evidence is on a seized computer. On what part of the computer system will you find data of evidentiary value?

A. Microprocessor or CPU.
B. USB controller.
C. Hard drive.
D. PCI expansion slots.

Q10 Following are the people involve in forensic accounting **EXCEPT** _____.

A. forensic accountant
B. forensic auditor
C. forensic analyst
D. investigator auditor

(20 marks)

SECTION B

Q11 (a) Differentiate between Adware and Spyware.

(4 marks)

(b) What is a zero day attack?

(2 marks)

(c) Explain **TWO (2)** conditions for a warrantless search to be legal.

(4 marks)

Q12 Consider the following scenario:

July 8, 1977. Glen Woodall was convicted of the brutal sexual assault of two women by a Cabell County, West Virginia, jury. He was sentenced to two life terms with an additional sentence of 203 to 335 years in prison after the judge convince with evidence. The forensic scientist in this case was West Virginia State serologist Fred Zain. After an investigation into Zain's work in both West Virginia and Texas, he was charged with perjury and tampering with evidence. During the investigation, it was found that Glen Woodall was innocent after serving four years in a West Virginia prison. He was released and awarded $1 million from the state for his wrongful imprisonment.

(a) In your opinion, what document West Virgina and Texas law organization used to confirm the evidence tampering. Explain **TWO (2)** importances of this document.

(4 marks)

(b) Suggest **SIX (6)** items that normally can be recovered in **Q12(a)**.

(6 marks)

(c) Propose **TWO (2)** actions that should be done by the Digital Forensics Division to ensure the competency of their forensic investigator in handling the digital evidence.

(4 marks)

(d) State **SIX (6)** minimum requirements for digital forensics certificate according to The Scientific Working Group on Digital Evidence (SWGDE).

(6 marks)

Q13 Azrul is a forensic analyst who handles 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 are hidden data in the disk. He believed that there are records contain list of company that being used to launder the money and there could be emails or other conversation channels for their communications.

Based on the above scenario, answer the following questions:

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

(6 marks)

(b) Suggest **TWO (2)** places Azrul should look for the hidden data.

(4 marks)

(c) Apply **THREE (3)** forensic techniques (other than decrypt disk and finding hiding data) that can help the investigation.

(12 marks)

Q14. 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 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.

(2 marks)

(b) Mat Hitam case. A "Mat Hitam" was suspected to lure several girls to transfer money to him through emails conversation.

(2 marks)

(c) Connie Dabate murder case in 2015. His husband told police there was an intruder who shot and killed her wife when she returned home from the gymnasium.

(2 marks)

(d) 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.

(2 marks)

- END OF QUESTIONS -