UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2018/2019

COURSE NAME	:	COMPUTER CRIME AND DIGITAL FORENSICS
COURSE CODE	:	BIS 30803
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JUNE 2019
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **SIX (6)** PAGES

SECTION A

Instruction: Choose the BEST answer for each of the following questions

Q1 A file header is which of the following?

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.

Q2 Assuming that the size and the start of sector for file test.jpg is 12,000 and 30,500 respectively. What is the offset of the starting point of this file?

A. 30,500.
B. 31,012.
C. 15,616,000.
D. 15,628,000.

Q3 Which of the following is the file system for Apple computer?

A. New Technology File System (NTFS).
B. Hierarchical File System (HFS +).
C. File Allocation Table (FAT 32).
D. Command line.

Q4 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.

Q5 One very well-known commercial software used for forensic analysis is_____.

A. SIFT (SANS Investigative Forensic Toolkit).
B. Autopsy.
C. FTK Imager.
D. Dossier.

Q6 Which of the following statement is **FALSE**?

A. Digital signature protects both metadata and data.
B. Hashing protects the image data only.
C. Digital signature binding identity to integrity operation.
D. Hashing can bind time with data.

Q7 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.

Q8 Following are the people involve in forensic accounting **EXCEPT** _____.

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

Q9 To verify the integrity of the forensic copy, you use _____.

A. hash analysis
B. a password
C. disk to disk verification
D. none of the above

Q10 _____ is a malicious software that appears to be legit but executes a hidden harmful malware.

A. Trojan horse
B. Virus
C. Backdoor exploits
D. Rootkits

(20 marks)

SECTION B

Q11 (a) Differentiate between Adware and Scareware.

(4 marks)

(b) What is a zero day attack?

(2 marks)

(c) Discuss **TWO (2)** types of warfare.

(4 marks)

Q12 Consider the following scenario:

Company ABC is suspected to do online gambling. You are the person that is responsible to assist the law enforcement in collecting digital evidence on the premise. You are responsible to handle the scene before the invetigator arrive and process the evidence if necessary. On the premise, there are 5 gambling machines put inside computer CPUs' cases, one computer on the reception and two unit of CCTV.

Propose **TWO (2)** footprints or artifacts that you have to examine during the investigation process.

(5 marks)

Q13 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 is the document that West Virgina and Texas law organization used to confirm the evidence tampering?

(2 marks)

(b) Suggest **FOUR (4)** items/information that normally can be recovered in **Q13(a)**.

(4 marks)

(c) Propose **TWO (2)** methods to ensure the competency of the 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)

(e) Differentiate between inculpatory and exculpatory evidence.

(4 marks)

Q14 Azrul is a forensic 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 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 should be email or other conversation channel to connect their organizations.

Based on the above scenario, answer the following questions:

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

(9 marks)

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

(4 marks)

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

(12 marks)

- END OF QUESTION -