Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2016/2017

COURSE NAME	:	COMPUTER CRIME AND DIGITAL FORENSICS
COURSE CODE	:	BIS 30803
PROGRAMME CODE	:	3 BIS
EXAMINATION DATE	:	JUNE 2017
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 Fraud investigation includes the following activities **EXCEPT** _____.

A. public record search
B. legal prosecution
C. computer forensics
D. suspect interrogation

Q2 Following are the people involve in forensic accounting **EXCEPT** _____.

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

Q3 Forensic accounting is the specialty practice area specialized in the following **EXCEPT** _____.

A. insurance claims
B. murder investigation
C. personal injury
D. royalty audit

Q4 Which of the following crime targets a computer?

A. Denial of service.
B. Money laundering.
C. Theft of service.
D. Child exploitation.

Q5 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. Digital signature can bind time with data.

Q6 Which of the following technique **DOES NOT** help preventing computer crime?

A. Backup.
B. Firewall.
C. Digital Forensic Analysis.
D. Encryption.

Q7 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.

Q8 As a good forensic practice, why it is a good idea to wipe a forensic drive before using it?

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

Q9 Computer memory files written to the hard drive are called _____.

A. spool files
B. swap files
C. drive slack
D. slack space

Q10 _____is some method of modifying data so that it is meaningless and unreadable.

A. Data hiding
B. Data Mining
C. Encryption
D. Digital Watermarking

(20 marks)

SECTION B

Q11 Identify keywords listed with computer crime's categories in Table **Q11**.

- Terrorism
- Gambling
- Hate crime
- Economic espionage
- Credit card fraud
- Import export human organ
- Embezzlement
- Identity theft
- Black mail
- Defamation

TABLE Q11

Against person	Against Property	Against public order & public interest

(10 marks)

Q12 Cybercrime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cybercrime also includes traditional crimes conducted through the Internet.

Based on the definition above, answer the questions below.

(a) Discuss **THREE (3)** types traditional crimes by new technologies including the related act for each type.

(9 marks)

(b) Discover **FIVE (5)** types of cyber attacks related to Internet.

(10 marks)

Q13 (a) 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.

(i) Propose **TWO (2)** methods to ensure the competency of the forensic investigator in handling the digital evidence.

(4 marks)

(ii) Differentiate between inculpatory and exculpatory evidence.

(4 marks)

(iii) Determine either inculpatory evidence or exculpatory evidence for the following cases:

- Call log showing the suspect has relationship with the victim.

(2 marks)

- GPS log file showing the suspect was out of country at the time of murder.

(2 marks)

- Email found in the victim's computer showing the argumnets between the suspect and the victim.

(2 marks)

(b) Determine **THREE (3)** common targets for warfare attacks?

(6 marks)

(c) For more than 50 years, Frye has been used as a standard to determine the admissibility of evidence. In 1973, the congress adopt the Federal Rule Evidence (FRE) standard.

(i) Differentiate both standards that may affected the admissibility of digital evidence.

(4 marks)

(ii) Name the decision that make the stand to solve the conflict between Frye and FRE.

(1 mark)

Q14 Write an algorithm to carve the following files:

(a) JPEG File Interchange Format (JFIF) file.

(3 marks)

(b) Exchangeable Image File Format (Exif) file.

(3 marks)

- END OF QUESTION -