UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2017/2018

COURSE NAME	:	COMPUTER CRIME AND DIGITAL FORENSICS
COURSE CODE	:	BIS 30803
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JUNE / JULY 2018
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 Forensic analysis procedure should be done on _________ of the digital storage.

A. the image
B. the original
C. the suspicious file
D. the remote desktop

Q2 Which of the following describe non-volatile data?

i. Information lost when the cable is unplugged.
ii. Information retain even when cable is unplugged.
iii. Current networks connections.
iv. System event logs.

A. i, ii and iii
B. i and iii
C. i, iii and iv
D. ii and iv

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 statements is **FALSE?**

A. Cyber war is motivated by military or political dominance.
B. Cybercrime is motivated by economic gain.
C. Hacktivism is motivated by ego and personal intention.
D. Cyber terrorism is motivated by political change.

Q5 A well-known commercial software used for forensic analysis is________.

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

Q6 Following are the people involve in forensic accounting **EXCEPT** __________.

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

Q7 The evidence custodian should ____________________.

A. give the evidence to the secretary
B. place evidence in the storage place
C. keep logs of who has the evidence, when was it check out, etc
D. use the evidence for personal use

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. To make it organized.
C. To differentiate file and operating systems.
D. To follow chain of custody.

Q9 To verify the original drive with the forensic copy, you use __________.

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

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

Instruction: Choose either **TRUE** or **FALSE** for each of the following statements.

Q11 Computer memory files written to the hard drive are called spool files.

Q12 New Technology File System (NTFS) is the file system for Apple computer.

Q13 The reason of the existence of probable cause is to allow law enforcement to make an arrest, search or seize without a warrant.

Q14 For digital evidence, an evidence bag is typically made of anti static material.

Q15 The American Society of Crime Laboratory Directors/ Laboratory Accreditation Board (ASCLD) mandates the procedures established for a computer forensics lab.

(10 marks)

SECTION C

Q16 (a) Suggest **FIVE (5)** crimes that can be committed through computer systems.

(10 marks)

(b) Propose **THREE (3)** ways to fight the crimes.

(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.

(3 marks)

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

(1 mark)

Q17 Consider the following scenario:

Mr. WX worked at Borland International, Inc., a software manufacturer, when he used email to allegedly send trade secrets from his current employer to his new employer. Mr. WX was caught when someone read his email. Besides that, there are a number of suspicious files in his computer. The company try to build a case against him. You are assigned as a team leader of forensic investigation team to serve this purpose.

(a) Outline procedures to be done by the team according to Forensic Investigation Life Cycle (FILC) 6'R Policy.

(20 marks)

(b) Determine either inculpatory evidence or exculpatory evidence for the following possible cases of Mr. WX:

(i) Call log showing Mr. WX contact his new employer before he quit his job.

(2 marks)

(ii) Global Positioning System (GPS) log file showing Mr. WX was out of country at the time email sent from his computer.

(2 marks)

Q18 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 -