UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2014/2015

COURSE NAME	:	COMPUTER CRIME AND DIGITAL FORENSICS
COURSE CODE	:	BIS 30803
PROGRAMME	:	3 BIS
EXAMINATION DATE	:	JUNE 2015 / JULY 2015
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **THREE (3)** PAGES

Q1 (a) Discuss **THREE (3)** roles of computer in cybercrimes.

(6 marks)

(b) Describe how a computer can be considered as a target of crime.

(4 marks)

(c) For each category of computer facilitated-crime, provide **THREE (3)** possible cases. (Notes: There are three categories of computer facilitated-crime)

(15 marks)

Q2 Consider the following scenario:

An annonymous person has called Mr A, tipped that his employee, Mr X was trying to sell his company's trade secret. The tipper also mentioned that MR X had already received the deposit of RM10,000 to secure the deal. Before any action (legal or otherwise) can be brought against the suspected Mr X, and to stop the potential loss of any further trade secrets, Mr A wishes to determine conclusively the innocence or guilt of Mr X. Mr A's call launches an internal cyber forensic investigation into the activities of Mr X. You as the examiner assigned to the case are required to investigate and report the finding.

Based on the case study above, answer the questions below.

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

(4 marks)

(b) Carry out steps in evidence acquiring process.

(12 marks)

(c) Propose **THREE (3)** forensic tools to take with you during the investigation at the crime scene.

(3 marks)

(d) Justify the need of the **THREE (3)** forensic tools you prepare.

(6 marks)

Q3 (a) Explain your understanding of forensic accounting.

(3 marks)

(b) List **SIX (6)** conditions of digital evidence that make evidence analysis a challenging process.

(6 marks)

(c) Contrast **FOUR (4)** types of data hiding places.

(12 marks)

(d) Contrast between hash code and digital signature.

(4 marks)

Q4 (a) Explain antiforensic with **TWO (2)** examples of the antiforensic activities.

(5 marks)

(b) Following the 'best evidence rule', the Judge Azri requires the original to prove the content of a hard disk found at a crime scene.

In your opinion, can a print out of a photograph acquired from the hard disk be accepted in the court? Justify your answer.

(4 marks)

(c) Describe how a Botnet can disrupt a network.

(4 marks)

(d) Illustrate **FOUR (4)** types of Botnets attack.

(12 marks)

- END OF QUESTION -