16

UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION (ONLINE) SEMESTER II SESSION 2019/2020

COURSE NAME	:	COMPUTER CRIME AND DIGITAL FORENSICS
COURSE CODE	:	BIS 30803
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY 2020
DURATION	:	2 HOURS 30 MINUTES
INSTRUCTION	:	1. ANSWER ALL QUESTIONS 2. STUDENT SHOULD UPLOAD ANSWER BOOKLET (PDF/ WORD FORMAT) WITHIN 30 MINUTES AFTER EXAMINATION PERIOD.

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

SECTION A

Q1 (a) Describe how metadata of a file (timestamp and date) may not be accurate. (2 marks)

(b) Explain the use of `thumbs.db` and `thumbcache.db` files. (2 marks)

(c) Why registry is important to be used as digital evidence? (4 marks)

Q2 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 (4 marks)

(b) Mat Hitam case (4 marks)

(c) Nurin Jazri murder case (4 marks)

(d) Connie Dabate murder case in 2015 (4 marks)

(e) Xiaolang Zhang stole Apple's trade secrets case in 2018 (4 marks)

Q3 Consider the following scenario:

Ali is a new digital forensics employee of DF Sdn Bhd (DSB). He is currently assigned to handle Swindle Sdn Bhd (SSB) money laundering case. He has to handle the job from First Responder and all other tasks until hearings in the court because DSB is short of staff. He came along with the police in a raid to the SSB office. Ali managed to obtain one notebook as evidence.

Based on the above scenario, answer the following questions:

(a) Draw a DF Framework that Ali can use for the case

(4 marks)

(b) Discuss how the DF Framework in **Q3(a)** is applied to solve this case

(15 marks)

Q4 MyCo Sdn Bhd (MSB) has the policy that all important files (for example bonus allocation for staff, promotion letter) must be uploaded into the shared folder in the company's server via MyCo Admin System (MAS). Mr X is a disgruntled employee who has been fired last week due to his disagreement about his 2019 bonus. Mr X manage to do unauthorized download of files related to the company's bonus allocation via MAS by exploiting some vulnerabilities.

Based on the above scenario, answer the following questions:

(a) What is the principle used in digital forensics (DF)?

(1 mark)

(b) Define the DF principle in **Q4(a)**.

(2 marks)

(c) Apply the DF principle in **Q4(b)** for solving this case by giving **FIVE (5)** examples. Explain each example.

(10 marks)

- END OF QUESTIONS –