UNIVERSITI TEKNOLOGI PETRONAS

FINAL EXAMINATION
MAY 2024 SEMESTER

COURSE	:	TEB3213/TFB2143 - COMPUTER FORENSIC
DATE	:	12 AUGUST 2024 (MONDAY)
TIME	:	9:00 AM - 12:00 NOON (3 HOURS)

INSTRUCTIONS TO CANDIDATES

1. Answer **ALL** questions in the Answer Booklet.
2. Begin **EACH** answer on a new page in the Answer Booklet.
3. Indicate clearly answers that are cancelled, if any.
4. Where applicable, show clearly steps taken in arriving at the solutions and indicate **ALL** assumptions, if any.
5. **DO NOT** open this Question Booklet until instructed.

Note :

i. There are **SIX (6)** pages in this Question Booklet including the cover page

ii. **DOUBLE-SIDED** Question Booklet.

1. a. List **FIVE (5)** major types of digital forensics.

[5 marks]

b. Define the **FIVE (5)** major roles of digital forensics investigators.

[5 marks]

c. Explain the importance of computer forensics in discovering cybercrimes.

[6 marks]

d. Show the difference between Volatile and Nonvolatile artifacts.

[4 marks]

2. a. Identify **THREE (3)** causes of losing or deleting of graphics files.

[3 marks]

b. Consider **FIGURE Q2** and compare the investigation processes of the mobile forensics and computer forensics.

[15 marks]

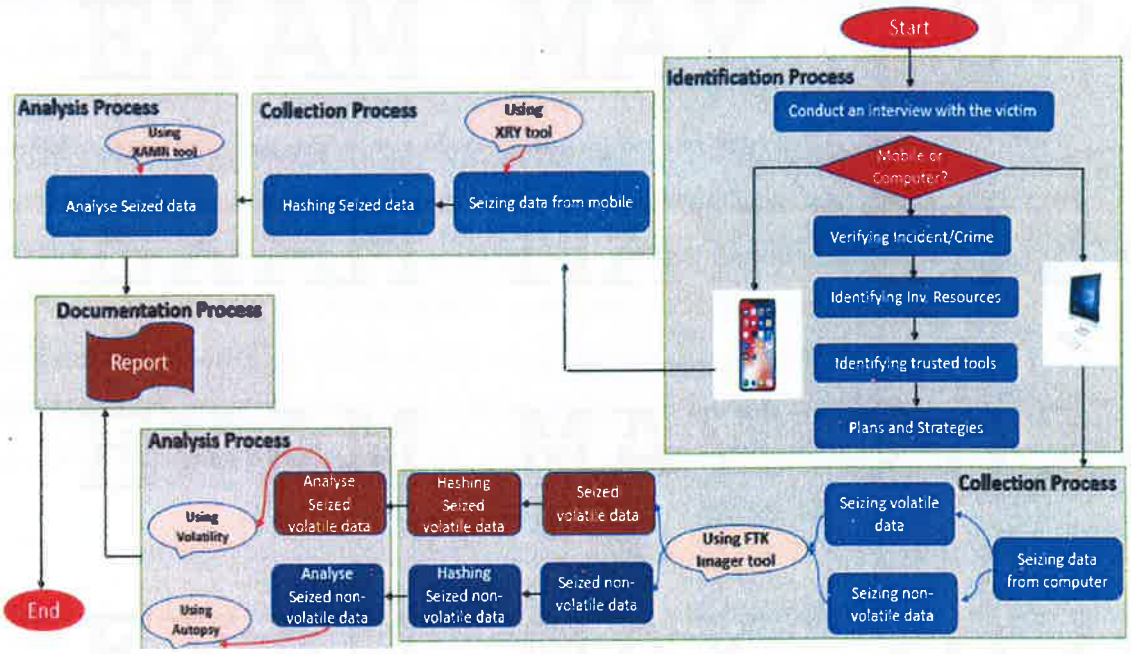

FIGURE Q2

c. List **TWO (2)** advantages of Forensic Toolkit (FTK) Imager forensics tool.

[2 marks]

3. a. Identify **FIVE (5)** main contents of the Go-Bag incident response.

[5 marks]

b. Consider this scenario: "The installation of a state-of-the-art smart home system was performed by a family in a suburb of Kuala Lumpur to simplify their lives and improve home security. A central hub controlled all the appliances remotely via interconnected devices, such as smart locks, and security cameras. Sadly, cybercriminals soon took advantage of their seemingly perfect home. A sophisticated cybercriminal breached the security system of the smart home one evening while the family was on vacation. By targeting the central hub with various attacks, the perpetrator gained unauthorized access. This gave them control over the entire house's connected devices. The cybercriminal began exploiting the vulnerabilities of interconnected devices as soon as he gained control over the smart home system. To avoid detection, they disabled the security cameras. As a result, they were able to move freely throughout the house undetected."

i. Construct in detail the main steps of the digital forensics investigation to investigate the crime.

[5 marks]

ii. Analyze the main reasons for the attack's success.

[5 marks]

iii. Discuss the possible solutions to avoid repeating this type of attack.

[5 marks]

4. a. Analyze why the needs of live acquisition of the evidence is essential for a successful digital forensic investigation task.

[5 marks]

b. Show the difference between cloud forensics and network forensics.

[5 marks]

c. List **FIVE (5)** branches of database forensics.

[5 marks]

d. Explain the importance of the of mobile logs for digital forensics investigation.

[5 marks]

5. a. Justify the importance of File Allocation Table (FAT) and New Technology File System (NTFS) for digital forensic investigators.

[4 marks]

b. Choose **FIVE (5)** major forensic areas in Windows environment.

[5 marks]

c. Discuss in detail the main steps for capturing volatile data from the laptop/computer memory using FTK Imager tool.

[8 marks]

d. Compare digital forensics to digital forensics readiness.

[3 marks]

– END OF PAPER –