UNIVERSITI
TEKNOLOGI
PETRONAS

FINAL EXAMINATION
JANUARY 2025 SEMESTER

COURSE	**:**	**TEB3213/TFB2143 - COMPUTER FORENSIC**
DATE	**:**	**9 APRIL 2025 (WEDNESDAY)**
TIME	**:**	**2:30 PM - 5:30 PM (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 **SEVEN (7)** pages in this Question Booklet including the cover page .

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

1. a. List **TWO (2)** essential tools that a digital forensic workstation must have.

[2 marks]

b. With respect to your answer in **part (a)**, choose **ONE (1)** tool and explain its methods of application at the digital forensic workstation.

[6 marks]

c. Using an appropriate diagram, elaborate the **SIX (6)** digital forensic processes.

[6 marks]

d. Describe how a forensic investigator can identify whether a suspect's computer is running Redundant Array of Independent Disks (RAID).

[6 marks]

2. a. You are a computer forensic investigator in a law enforcement agency in Selangor, Malaysia. You have been assigned to a criminal investigation. A suspect worked as the director of product development for a computer software company. He was questioned about several emails sent from his office desktop computer. Further inspection of his computer revealed that he had been sending emails to institutions in Malaysia demanding their pictures and other personal information. When confronted, he stated that he would need to consult with his lawyer and had no further comment. He did not show up for work the next day. The local authorities were contacted the following day. The suspect was caught trying to board a one-way flight to a neighboring country two days after being questioned about his contact with many institutions in Malaysia.

Elaborate your digital evidence contingencies and solutions for this investigation.

[10 marks]

b. During the documentation of a forensic investigation, obtaining evidence is crucial. Explain the concept of preservation order for obtaining evidence.

[4 marks]

c. State any **TWO (2)** types of digital forensic acquisitions.

[2 marks]

d. Usman is performing a static acquisition. He is creating a physical disk-to-image, which is the most common method of acquisition and offers the most flexibility for an investigation. Determine the features that make physical disk-to-imaging method so flexible.

[4 marks]

3. a. You are a digital evidence specialist and want to make a forensic initial assessment about a new case that you are investigating. Examine the steps that you need to take for the assessment

[8 marks]

b. Compare and contrast public and private computer investigations.

[4 marks]

c. Describe the following according to computer and legal investigations:

i. Warning banner.

[2 marks]

ii. Police blotter.

[2 marks]

iii. *Voir dire*.

[2 marks]

iv. Search warrant.

[2 marks]

4. a. Maged is new to the field of computer forensics and works at a cybersecurity company. His superior has asked him to make a bit-stream copy of a disk drive for an investigation the company is working on. Maged is curious why he cannot make a backup copy instead. He then comes to you for advice.

Explain the best advice that you can provide to Maged for making a successful bit-stream copy.

[6 marks]

b. An inode is a data structure in Unix file systems that contains file and directory metadata that provides a mechanism for linking data stored in data blocks.

State any **SIX (6)** information that assigned inode contains.

[6 marks]

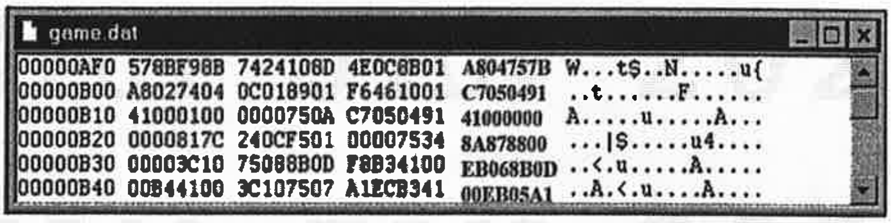
c. Explain the concept of Logical Cluster Number (LCN) with respect to computer forensic Windows OS.

[4 marks]

d. Describe the type of data stored in NTUSER.dat.

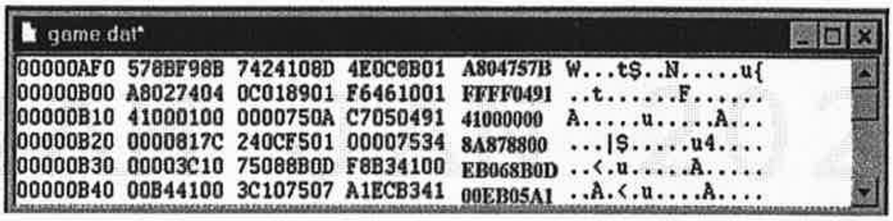
[4 marks]

5. a. **FIGURE Q5(a)** and **FIGURE Q5(b)** contain Hex tabs in content viewer of autopsy. Identify the changes and develop the process of detecting the encrypted files.



```
00000AF0 578BF98B 7424108D 4E0C8B01 A804757B W...t$..N.....u{
00000B00 A8027404 0C018901 F6461001 C7050491 ..t.......F......
00000B10 41000100 0000750A C7050491 41000000 A.....u.....A...
00000B20 0000817C 240CF501 00007534 8A878800 ...|$.....u4....
00000B30 00003C10 75088B0D F8B34100 EB068B0D ..<.u.....A.....
00000B40 00B44100 3C107507 A1ECB341 00EB05A1 ..A.<.u....A....
```

FIGURE Q5(a): hexadecimal value



```
00000AF0 578BF98B 7424108D 4E0C8B01 A804757B W...t$..N.....u{
00000B00 A8027404 0C018901 F6461001 FFFF0491 ..t.......F......
00000B10 41000100 0000750A C7050491 41000000 A.....u.....A...
00000B20 0000817C 240CF501 00007534 8A878800 ...|$.....u4....
00000B30 00003C10 75088B0D F8B34100 EB068B0D ..<.u.....A.....
00000B40 00B44100 3C107507 A1ECB341 00EB05A1 ..A.<.u....A....
```

FIGURE Q5(b): hexadecimal value

[6 marks]

b. A university graduate attended his convocation and took many pictures using his new camera. He finds a JPEG file on a hard drive and discovers that the image quality is poor. Describe other issues that can cause the image quality of a JPEG to degrade.

[4 marks]

c. Network forensic examiners must establish standard procedures for how to acquire data after an attack or intrusion. Describe the following:

i. Any **TWO (2)** modes of protection for Defense in Depth (DiD).

[2 marks]

ii. Any **TWO (2)** network forensics tools.

[2 marks]

iii. Honeypot attack.

[2 marks]

d. Explain **TWO (2)** types of cell phone log files.

[4 marks]

– END OF PAPER –