UNIRAZAK
UNIVERSITI TUN ABDUL RAZAK

FINAL EXAMINATION
MARCH 2024

COURSE TITLE	COMPUTER FORENSICS IMPLEMENTATION
COURSE CODE	RCIT3823
DATE/DAY	29 JUNE 2024 / SATURDAY
TIME/DURATION	01:00 PM - 03:00 PM / 02 Hour(s) 00 Minute(s)

UNIRAZAK
UNIVERSITI TUN ABDUL RAZAK
Copying, modifying or reprinting is not permitted.

INSTRUCTIONS TO CANDIDATES :

1. Please read the instruction under each section carefully.
2. Candidates are reminded not to bring into examination hall/room any form of written materials or electronic gadget except for stationery that is permitted by the Invigilator.
3. Students who are caught breaching the Examination Rules and Regulation will be charged with an academic dishonesty and if found guilty of the offence, the maximum penalty is expulsion from the University.

(This Question Paper consists of 5 Printed Pages including front page)

DO NOT OPEN THE QUESTION PAPER UNTIL YOU ARE TOLD TO DO SO

This question paper consists of TWO (2) sections. Answer ALL questions in the answer booklet provided. [100 MARKS]

SECTION A (30 Marks)

There are FIFTEEN (15) questions in this section. Answer ALL questions in the answer booklet provided.

1. What is the key factor that has led to the rise of cybercrime?

   A. Widespread adoption of ICT
   B. Lack of cybersecurity measures
   C. Increase in computer literacy rates
   D. Proliferation of mobile devices

2. Which of the following is **NOT** a factor that contributes to the difficulty in defining cybercrime?

   A. The constantly evolving nature of technology
   B. The broad spectrum of activities considered as cybercrime in different countries
   C. The borderless nature of cybercrime
   D. The universal agreement on the definition of cybercrime across the globe

3. What is the primary reason why many cybercrimes go unreported, according to the FBI?

   A. Fear of retaliation
   B. Lack of awareness
   C. Embarrassment
   D. All of the above

UNIRAZAK
UNIVERSITI TUN ABDUL RAZAK
Copying, modifying, or reprinting, is not permitted.

4. Which of the following is **NOT** an example of CJIS data?

   A. Criminal Records
   B. Fingerprint and Biometric Data
   C. Warrants and Wanted Persons
   D. Personal Banking Information

5. In the context of machine learning, what is the purpose of supervised learning?

   A. To cluster inputs into classes without existing datasets
   B. To allow the system to learn from its environment
   C. To produce outputs using pre-defined data
   D. To identify patterns in large datasets

6. What is the role of the Deputy Public Prosecutor (DPP) in the criminal justice process in Malaysia?

   A. To review the investigation paper
   B. To arrest and remand the accused person
   C. To conduct the trial and pass judgment
   D. To process and record an appeal

7. What is the difference between proactive and reactive data collection in investigations?

   A. Proactive collection is done before an incident occurs, while reactive collection is done after an incident
   B. Proactive collection is done after an incident occurs, while reactive collection is done before an incident
   C. There is no difference; both proactive and reactive terms refer to the same process
   D. Proactive collection is done during an incident, while reactive collection is done after an incident

8. Which of the following is **NOT** a principle mentioned for maintaining Electronically Stored Information (ESI) management?

   A. No action should be taken that changes data held on a digital device
   B. A competent person should access original data and explain their actions
   C. A trail of all actions taken should be created and preserved
   D. The investigator should work directly on the original data sets

9. What is the purpose of the "Preservation" stage in the Electronic Discovery Reference Model (EDRM)?

   A. To locate potential sources of Electronically Stored Information (ESI)
   B. To ensure that ESI is protected against inappropriate alteration or destruction
   C. To gather ESI for further use in the e-discovery process
   D. To reduce the volume of ESI and convert it to suitable forms

UNIRAZAK
UNIVERSITI TUN ABDUL RAZAK
Copying, modifying, or reprinting is not permitted.

10. What is the primary reason for having a custodian during the data collection process?

    A. To ensure the integrity of the collected data
    B. To comply with data protection regulations
    C. To maintain a chain of custody
    D. To coordinate with the legal team

11. What is the importance of obtaining a non-disclosure agreement (NDA) during digital forensic investigations?

    A. To protect the firm, the custodian, and the vendor
    B. To comply with data protection regulations
    C. To maintain confidentiality of the investigation
    D. All of the above

12. Which of the following is **NOT** a stage in the Electronic Discovery Reference Model (EDRM)?

    A. Identification
    B. Presentation
    C. Litigation
    D. Analysis

13. What is the purpose of the "Review" stage in the EDRM?

    A. To evaluate Electronically Stored Information (ESI) for relevance and privilege
    B. To locate potential sources of ESI
    C. To deliver ESI to others in appropriate forms
    D. To display ESI before audiences

14. Which of the following is **NOT** a key principle of data protection acts like GDPR and PDPA?

    A. Right to know
    B. Right to be forgotten
    C. Right to access personal information
    D. Right to sell personal information

15. What is the purpose of e-discovery software?

    A. To help find relevant material or evidence from large volumes of collected data
    B. To collect data from digital devices
    C. To conduct forensic analysis of digital evidence
    D. To present digital evidence in court

UNIRAZAK
UNIVERSITI TUN ABDUL RAZAK
Copying, modifying, or reprinting, is not permitted

SECTION B **(70 Marks)**

There are TWO (2) questions in this section. Answer all questions.

Question 1 **(35 marks)**

Digital triage is essential to be implemented in digital forensics.

a) What is a digital triage and its purpose?

(5 marks)

b) Discuss the benefits of implementing digital triage on computer forensics investigations.

(15 marks)

c) Digital triage comes in two forms: live and post-mortem. Explain live triage and its benefits. Provide examples of a live triage method.

(15 marks)

Question 2 **(35 marks)**

Mobile forensics, a subtype of digital forensics, is concerned with retrieving data from an electronic source.

a) What are the major sources of evidence in a module device? Explain.

(15 marks)

b) Describe the mobile forensics process.

(15 marks)

c) Discuss the challenges in acquiring evidence from a mobile device.

(5 marks)

UNIRAZAK UNIVERSITI TUN ABDUL RAZAK Copying, modifying, or reprinting, is not permitted.

***** END OF QUESTION PAPER *****