OR iii. Discuss the main features of the Indian IT Act 2008 (Amendment) and its significance in the digital landscape. Describe the structure and format of a well-organized forensic report. **6**

Q.6 Attempt any two:

i. What tools and techniques are used in network analysis to identify a web server compromise? Explain the process of tracking an attacker's movement within a network after a web server compromise. **5**

ii. Describe the types of information that can be found in web server logs and access logs. How do you perform log analysis to determine the origin and nature of web server attacks? **5**

iii. What is a code injection attack, and why is it a common threat to web applications? Explain the steps to conduct forensic analysis for code injection attacks. **5**

******

*Total No. of Questions: 6* *Total No. of Printed Pages:4*

**Enrollment No.....**

Faculty of Engineering

End Sem Examination Dec-2023

CS3EY07 Cyber Forensics & Investigation

Programme: B.Tech. Branch/Specialisation: CSE All

**Duration: 3 Hrs.** **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d. Assume suitable data if necessary. Notations and symbols have their usual meaning.

Q.1 i. Which of the following is an example of a cybercrime involving unauthorized access to computer systems or data? **1**

(a) Digital piracy (b) Phishing

(c) Online harassment (d) E-commerce fraud

ii. Who is typically responsible for immediately securing the scene and ensuring the physical safety of personnel when responding to a computer-related incident? **1**

(a) Non-technical staff (b) Technical staff

(c) Forensics expert (d) Local law enforcement

iii. What is the function of the spindle motor in a hard disk drive (HDD)? **1**

(a) It reads data from the platters.

(b) It writes data to the platters.

(c) It controls the movement of the read/write heads.

(d) It spins the platters at a constant speed.

iv. Which of the following methods is commonly used for data recovery in digital forensics when data has been accidentally deleted? **1**

(a) Overwriting the data with random characters

(b) Running a virus scan on the storage device

(c) Scanning for bad sectors on the device

(d) Using specialized data recovery software

v. In Windows forensics, the Windows Registry is a crucial source of information. Which part of the Windows Registry contains user-specific settings and configurations? **1**
(a) HKEY_LOCAL_MACHINE
(b) HKEY_USERS
(c) HKEY_CURRENT_CONFIG
(d) HKEY_CLASSES_ROOT

vi. In mobile forensics, what does the process of "rooting" or "jailbreaking" a device refer to? **1**
(a) Legally unlocking a device for use with any carrier
(b) Gaining privileged access to the device's operating system, potentially bypassing security measures
(c) Wiping all data from a mobile device
(d) Installing a custom, more secure operating system on the device

vii. The Indian IT Act of 2008 (Amendment) focuses on: **1**
(a) Promoting unrestricted internet usage
(b) Enhancing data privacy and security
(c) Tax regulations for IT companies
(d) Environmental regulations for IT businesses

viii. Corporate espionage involves: **1**
(a) Ethical practices in business.
(b) Legal competition between companies.
(c) Unlawful activities aimed at gaining a competitive advantage.
(d) Cybersecurity awareness programs.

ix. What is a primary objective in the forensic analysis of a compromised web server? **1**
(a) Determining the server's physical location
(b) Isolating the server from the network
(c) Patching the server immediately
(d) Preserving the integrity of digital evidence

x. In web server log analysis, what is the purpose of analysing access logs? **1**
(a) To determine the server's physical location
(b) To assess the server's hardware performance
(c) To identify patterns of suspicious activity and potential breaches
(d) To monitor network traffic in real-time



Q.2 i. What are computer forensics, and why is it important in today's digital age? **2**
ii. Describe the basic steps involved in a typical computer forensics investigation. **3**
iii. What are the challenges and best practices for first responders when dealing with cybercrime incidents? **5**
OR iv. How does a forensics expert handle evidence to maintain its integrity throughout the investigation process? **5**

Q.3 i. What is volatile data, and why is it important in digital forensics? **2**
ii. What are the different methods for acquiring data from a storage device during a digital investigation? Describe common techniques for secure data deletion and data sanitization. **8**
OR iii. In a hard disk drive, what is the role of the platter, and how is data stored on it? Explain the function of the head assembly in reading and writing data on a hard disk drive. What is the purpose of the spindle motor in a hard disk drive, and how does it work? **8**

Q.4 i. How does Linux forensics differ from Windows forensics in terms of challenges and tools used? What are stochastic forensics, and how is it applied in Linux forensics? **3**
ii. Describe the role of network logs, packet capture, and metadata in network forensics. How can you identify and collect evidence from network traffic? **7**
OR iii. How can SMTP, POP3, and IMAP headers provide information in an email forensic investigation? Describe the role of browser history, cache, and cookies in forensic analysis. **7**

Q.5 i. What is corporate espionage, and why is it a significant concern in the business world? Describe common methods and tactics used in corporate espionage. **4**
ii. What is the chain of custody, and why is it crucial in digital forensics? Describe the process of maintaining the chain of custody for digital evidence. **6**

# Marking Scheme
## Cyber Forensics and Investigation-CS3EY07 (T)

| | | | |
|---|---|---|---|
| Q.1 | i) | b) Phishing | **1** |
| | ii) | a) Non-technical staff | **1** |
| | iii) | d) It spins the platters at a constant speed. | **1** |
| | iv) | d) Using specialized data recovery software | **1** |
| | v) | b) HKEY_USERS | **1** |
| | vi) | b) Gaining privileged access to the device's operating system, potentially bypassing security measures. | **1** |
| | vii) | b) Enhancing data privacy and security. | **1** |
| | viii) | c) Unlawful activities aimed at gaining a competitive advantage. | **1** |
| | ix) | d) Preserving the integrity of digital evidence | **1** |
| | x) | c) To identify patterns of suspicious activity and potential breaches | **1** |

| | | | | |
|---|---|---|---|---|
| Q.2 | i. | Definition of computer forensics | 1 mark | **2** |
| | | Its importance in digital age | 1 mark | |
| | ii. | 6 Steps | 0.5 mark each | **3** |
| | iii. | 6 Challenges | 3 marks | **5** |
| | | 4 best practices | 2 marks | |
| OR | iv. | Explanation | (As per explanation) | **5** |

| | | | | |
|---|---|---|---|---|
| Q.3 | i. | Definition | 0.5 marks | **2** |
| | | Importance in digital forensics | 1.5 marks | |
| | ii. | Different methods | 4 Marks | |
| | | Techniques for secure data deletion. | 4 Marks | |
| OR | iii. | what is the role of the platter. | 2.5 Marks | |
| | | Function of the head assembly in reading | 2.5 Marks | |
| | | Purpose of the spindle | 3 Marks | |

| | | | |
|---|---|---|---|
| Q.4 | i. | Linux forensics differ from Windows forensics | 1.5 Marks |
| | | Stochastic forensics. | 1.5 Marks |
| | ii. | Role of network logs, packet capture. | 3 Marks |
| | | Identify and collect evidence from network traffic | 4 Marks |
| OR | iii. | SMTP, POP3, and IMAP | 4 Marks |
| | | Role of browser history, cache, and cookies | 3 Marks |

| | | | |
|---|---|---|---|
| Q.5 | i. | Corporate espionage and Significant concern in the business world | 2 Marks |
| | | Methods and tactics used in corporate espionage. | 2 Marks |
| | ii. | Chain of custody | 3 Marks |
| | | Process of maintaining | 3 Marks |
| OR | iii. | Main features | 3 Marks |
| | | Structure and format of a well | 3 Marks |

| | | | |
|---|---|---|---|
| Q.6 | | Attempt any two: | |
| | i. | Tools and techniques are used in network | 2 Marks |
| | | Process of tracking an attacker's movement | 3 Marks |
| | ii. | Types of information | 2 Marks |
| | | The origin and nature of web server attacks | 3 Marks |
| | iii. | Code injection attack | 3 Marks |
| | | Steps to conduct forensic analysis | 2 Marks |

******

P.T.O.