

Enrollment No.....



Faculty of Science
End Sem Examination Dec-2023

FS3SE07 Digital & Fraud Investigation

Programme: B.Sc.

Branch/Specialisation: Forensic
Science

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 not a cybercrime which used devices to participate in criminal activities? **1**
 (a) Cyberstalking (b) DoS Attack
 (c) Identity Theft (d) Phishing Emails
- ii. A VPN is a most common type of _____. **1**
 (a) DNS Spoofing (b) Email Spoofing
 (c) GPS Spoofing (d) IP Spoofing
- iii. A _____ layer creates communication channels between devices. **1**
 (a) Application (b) Presentation
 (c) Session (d) Transport
- iv. Which of the following is not a type of SQL injection? **1**
 (a) In-name SQLi (b) Inferential SQLi
 (c) Out-of-band SQLi (d) System SQLi
- v. _____ logs are like digital journals the records the events taking place at server. **1**
 (a) IP (b) Email (c) OS (d) Server
- vi. AN IMEI Stands for _____. **1**
 (a) International Mobile Equipment Identity
 (b) Internal Mobile Equipment Identity
 (c) International Mobile Establishment Identity
 (d) Internal Mobile Establishment Identity
- vii. _____ is defined as the use of technology to harass, threaten, embarrass, or target other person. **1**
 (a) Cyberstalking (b) Cyberbullying
 (c) Hacking (d) Phishing

- [2]
- viii. _____ of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages. **1**
 (a) Section 43 (b) Section 43A
 (c) Section 66 (d) Section 66E
- ix. _____ focuses on examining structured data, found in application systems and databases, in the context of financial crime. **1**
 (a) Database Forensics (b) Forensic Data Analysis
 (c) Network Forensics (d) Mobile Device Forensics
- x. _____ write blocker offer monitoring and filtering any activity that is transmitted or received between its interface connections to the computer and the storage device. **1**
 (a) Data (b) Hardware (c) Network (d) Software

- Q.2 i. What is logic bombing? Give example of it. **2**
 ii. What do you mean by vishing, mishing, and stalking? **3**
 iii. In detail, explain packet sniffing and its types. **5**
- OR iv. Which are the cybercrimes related to banking? **5**
- Q.3 i. What do you mean by NIDS? **2**
 ii. Differentiate between WEP, WPA, and WPA2 Encryption. **8**
- OR iii. With the help of diagram, illustrate OSI model. **8**
- Q.4 i. How to track mobile phone locations? **3**
 ii. List and explain various evidence present in mobile phones. **7**
- OR iii. What are the methods of extracting evidence for mobile devices? **7**
- Q.5 i. List emerging trends on social media. **4**
 ii. Which are the major threats of social media? **6**
- OR iii. What do you mean by intelligence gathering from social media? Which are the tools and techniques used for it? **6**
- Q.6 Attempt any two: **5**
 i. Elaborate various tools and techniques of computer forensic tools. **5**
 ii. List and explain different tasks performed by computer forensic tools. **5**
 iii. What do you mean by forensic workstations? Explain in detail. **5**
