Total No. of Questions: 6 *Total No. of Printed Pages:3*

Enrollment No......................................

Faculty of Science

End Sem Examination May-2024

BC3CO57 Computer Forensics & Investigation

Programme: B.Sc. Branch/Specialisation: Computer Science / 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 a primary goal of conducting a digital forensics investigation? **1**

(a) Improving network performance
(b) Prosecuting offenders
(c) Marketing analysis
(d) Software development

ii. In digital forensics, what is the first step in preparing for an investigation? **1**

(a) Seizing digital devices
(b) Conducting interviews
(c) Developing an investigation plan
(d) Reviewing legal processes

iii. Which file system is commonly examined in windows forensic analysis? **1**

(a) ext4 (b) NTFS (c) HFS+ (d) FAT32

iv. The windows registry is crucial in forensics for: **1**

(a) Storing user passwords
(b) Managing network configurations
(c) Holding system configuration and user profiles
(d) Encrypting data files

v. Network forensics involves: **1**

(a) Designing network architecture
(b) Repairing network faults
(c) Analysing network traffic for malicious activities
(d) Increasing network speed

P.T.O.

vi. In cloud forensics, what is a major technical challenge? **1**

(a) Cloud storage limitations (b) Data acquisition

(c) High costs (d) Physical access to servers

vii. Tracing an email back to its source is crucial for: **1**

(a) Improving email server efficiency

(b) Identifying spam emails

(c) Investigating email-related crimes

(d) Marketing research

viii. Social media forensic analysis can help in: **1**

(a) Increasing followers

(b) Investigating digital crimes and misconduct

(c) Advertising products

(d) Improving post visibility

ix. Forensic reports must be: **1**

(a) Complex and technical

(b) Subjective and opinionated

(c) Clear, concise, and accurate

(d) Lengthy and detailed

x. Ethics in forensic analysis are important to ensure: **1**

(a) Faster investigation

(b) The investigator's popularity

(c) Fairness and integrity in the process

(d) High financial returns

Q.2 i. Explain the significance of maintaining professional conduct in digital forensics. **4**

ii. Describe the steps involved in preparing a digital forensics investigation plan. **6**

OR iii. Discuss the role and procedures for private-sector high-tech investigations. **6**

Q.3 Attempt any two:

i. What are the key differences between Linux validation and Windows validation methods in data acquisitions? **5**

ii. Explain the importance of understanding file systems in digital forensics investigations. **5**

iii. Describe the process of examining NTFS disk and its relevance in forensics. **5**

Q.4 i. Outline the establishment procedure for network forensic. **3**

ii. Discuss the legal and technical challenges in cloud forensic investigations. **7**

OR iii. Explain the process of collecting network traffic data and its importance in network forensics. **7**

Q.5 i. Describe the role of email servers in forensic investigations and how they can be investigated. **4**

ii. Discuss the application of digital forensic techniques to social media. **6**

OR iii. Analyse the challenges faced in email and social media forensic investigations. **6**

Q.6 Attempt any two:

i. What guidelines should be followed when writing a forensic report? Explain the importance of these guidelines. **5**

ii. Discuss ethical difficulties in expert testimony and how they can be addressed. **5**

iii. Explain how applying ethics and codes to expert witness contributes to the integrity of forensic investigations. **5**

******

Marking Scheme

BC3CO57 (T) Computer forensics & Invesigation

Q.1	i)	B	**1**
	ii)	C	**1**
	iii)	B	**1**
	iv)	C	**1**
	v)	C	**1**
	vi)	B	**1**
	vii)	C	**1**
	viii)	B	**1**
	ix)	C	**1**
	x)	C	**1**

Q.2 i. Significance of maintaining professional conduct in digital forensics (4 Marks) **4**
- Identification of key principles of professional conduct: 1 mark
- Explanation of how professional conduct impacts investigation integrity: 1.5 marks
- Examples of professional conduct in digital investigations: 1.5 marks

ii. Preparing a digital forensics investigation plan **6**
Outline of steps involved/role and procedures: 2 marks
- Detailed explanation of each step/role and procedure: 2 marks
- Relevance and importance in digital forensics: 2 marks

OR iii. Private-sector high-tech investigations **6**

Q.3 i. Linux vs. Windows validation methods 5 points **5**

ii. Understanding file systems in investigations **5**

OR iii. Examining NTFS disk **5**

Q.4 i. Establishment procedure for network forensic (1 Marks) **3**
- Step-by-step procedure: 1marks
- Significance of each step: 1 marks

ii. Legal and technical challenges in cloud investigations **7**
Detailed explanation of challenges/process: 3 marks
- Solutions to challenges/Importance of data collection: 2 marks
- Implications for forensic investigation: 2 marks

OR iii. Collecting network traffic data **7**
- Detailed explanation of challenges/process: 3 marks
- Solutions to challenges/Importance of data collection: 2 marks
- Implications for forensic investigation: 2 marks

Q.5 i. Role of email servers **4**
- Explanation of the role in investigations: 2 marks
- Investigation methods: 1 marks
- Challenges and solutions: 1 marks

ii. Digital forensic techniques in social media **6**
Techniques/challenges described: 3 marks
- Application to real-world scenarios: 3 marks

OR iii. Challenges in investigations-6 points **6**

Q.6 i. Guidelines for forensic report writing (5 Marks) **5**
- List of guidelines: 1.5 marks
- Explanation of the importance of each guideline: 2.5 marks
- Impact on the investigation and legal process: 1 mark

ii. - Identification of ethical difficulties/codes: 1.5 marks **5**
- Explanation of how they affect testimony/integrity: 2 marks
- Solutions or methods to address challenges: 1.5 marks

iii. Applying ethics to expert witness-5 points **5**

******