.

Printed Page:-3 **Subject Code:- BCSCY0601**

Roll. No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute Affiliated to AKTU, Lucknow)
B.Tech
SEM: VI - THEORY EXAMINATION (2025 - 2026)
Subject: Digital Forensic

Time: 3 Hours **Max. Marks: 100**

General Instructions:

IMP: *Verify that you have received the question paper with the correct course, code, branch etc.*
1. *This Question paper comprises of* ***three Sections -A, B, & C.*** *It consists of Multiple Choice Questions (MCQ's) & Subjective type questions.*
2. *Maximum marks for each question are indicated on right -hand side of each question.*
3. *Illustrate your answers with neat sketches wherever necessary.*
4. *Assume suitable data if necessary.*
5. *Preferably, write the answers in sequential order.*
6. *No sheet should be left blank. Any written material after a blank sheet will not be evaluated/checked.*

SECTION-A 20

1. Attempt all parts:-

(1.1) Forensic imaging refers to (CO1, K1) 1

(a) Copying files
(b) Exact disk copy
(c) Data deletion
(d) Compression

(1.2) Primary goal of digital forensics (CO1, K1) 1

(a) System upgrade
(b) Crime investigation
(c) Gaming
(d) Networking

(1.3) NTFS is a (CO2, K1) 1

(a) File system
(b) Protocol
(c) Tool
(d) Virus

(1.4) Bit-by-bit copy is called (CO2, K1) 1

(a) Imaging
(b) Formatting
(c) Deletion
(d) Partitioning

(1.5) Cloud acquisition collects (CO3, K1) 1

(a) Remote data
(b) Local data
(c) Virus
(d) Code

(1.6) Example of mobile tool (CO3, K1) 1

(a) Cellebrite
(b) Excel
(c) Word
(d) Paint

(1.7) Network traffic consists of (CO4, K1) 1

(a) Packets
(b) Files
(c) Images
(d) Code

(1.8) IP address identifies (CO4, K1) 1

(a) Device
(b) User
(c) App
(d) File

(1.9) SaaS stands for (CO5, K1) 1

(a) Software as a Service
(b) Storage as a Service
(c) System as a Service
(d) None

(1.10) Multi-tenancy means (CO5, K1) 1

(a) Shared resources
(b) Single user
(c) Private system
(d) Offline use

2. Attempt all parts:-

(2.1) State the purpose of maintaining chain of custody. (CO1, K2) 2

(2.2) State the purpose of disk imaging in investigation. (CO2, K2) 2

(2.3) State the difference between logical and physical acquisition. (CO3, K2) 2

(2.4) State the role of log analysis in investigation. (CO4, K2) 2

(2.5) Define PaaS and state its use in application development. (CO5, K2) 2

SECTION-B 30

Answer any one of the following:-

(3.1) Explain digital evidence and its characteristics in forensic investigation. (CO1, K2) 6

(3.2) Explain steps involved in maintaining chain of custody during investigation. (CO1, K2) 6

.

Answer any one of the following:-

(3.3) Explain process of forensic imaging in detail. (CO2, K2) 6

(3.4) Explain role of metadata in forensic investigation. (CO2, K2) 6

Answer any one of the following:-

(3.5) Describe mobile forensic tools and their applications. (CO3, K2) 6

(3.6) Explain challenges faced in mobile forensic investigation. (CO3, K4) 6

Answer any one of the following:-

(3.7) Explain DNS and its role in network communication. (CO4, K2) 6

(3.8) Describe intrusion prevention system (IPS) and its features. (CO4, K2) 6

Answer any one of the following:-

(3.9) Explain IoT forensics and its significance in investigations. (CO5, K2) 6

(3.10) Describe blockchain technology and its role in ensuring data integrity. (CO5, K2) 6

SECTION-C 50

4. Answer any one of the following:-

(4.1) Describe evidence collection techniques and preservation methods. (CO1, K3) 10

(4.2) Describe challenges faced during digital forensic investigations and suitable solutions. (CO1, K4) 10

5. Answer any one of the following:-

(5.1) Describe deleted data recovery techniques in detail. (CO2, K3) 10

(5.2) Describe hashing techniques such as MD5 and SHA for ensuring integrity. (CO2, K3) 10

6. Answer any one of the following:-

(6.1) Outline the techniques for acquiring mobile data and discuss the differences among logical, physical, and cloud acquisition. (CO3, K4) 10

(6.2) Explain the legal protocols for mobile device seizure and discuss the importance of chain of custody in digital investigations. (CO3, K4) 10

7. Answer any one of the following:-

(7.1) Explain challenges involved in analyzing encrypted network traffic. (CO4, K4) 10

(7.2) A forensic report needs to be prepared based on network investigation. Describe structure and key components. (CO4, K6) 10

8. Answer any one of the following:-

(8.1) Evaluate challenges in tracing cryptocurrency transactions. (CO5, K5) 10

(8.2) Examine digital forensics in emerging domains, including deepfake detection, cryptocurrency and blockchain forensics, and discuss future trends and research areas in digital forensics. (CO5, K5) 10