Printed Page:- Subject Code:- ACSCY0601

Roll. No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA

(An Autonomous Institute Affiliated to AKTU, Lucknow)

B.Tech

SEM: VI - THEORY EXAMINATION (20 ..... - 20.....)

Subject: Digital Forensics

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-a. ____ type of data disappears when power is lost?(CO1,K2) 1

(a) Static data

(b) Persistent data

(c) Volatile data

(d) Archived data

1-b. Live forensics is performed on:(CO1,K2) 1

(a) Dead systems

(b) Backup images

(c) Running systems

(d) Virtual machines

1-c. _____ is a legal principle in forensics?(CO2,K2) 1

(a) Chain of custody

(b) Metadata hiding

(c) Data compression

(d) File shredding

1-d. Write blockers are used to:(CO2,K2) 1

(a) Prevent alteration of data during acquisition

(b) Recover deleted data

(c) Encrypt drives

(d) Copy data faster

1-e. Purpose of Using Faraday Bags(CO3,K2) 1

(a) Enhancing signal strength
(b) Preventing data transmission
(c) Charging devices securely
(d) Cooling overheated devices

1-f. File System Acquisition Provides(CO3,K1) 1

(a) Access to only user-installed applications
(b) Limited data from the device
(c) Comprehensive access to system and app files
(d) Only metadata information

1-g. Recall a key method used in capturing network traffic.(CO4,K2) 1

(a) Packet sniffing
(b) Encryption
(c) Packet flooding
(d) Data masking

1-h. Identify the OSI layer where most forensic analysis takes place.(CO4,K1) 1

(a) Layer 1
(b) Layer 7
(c) Layer 3
(d) Layer 5

1-i. Match blockchain with its primary forensic use.(CO5,K1) 1

(a) Data storage
(b) Access control
(c) Evidence verification
(d) Network analysis

1-j. List one use of AI in forensic investigations.(CO5,K1) 1

(a) Device repair
(b) Pattern recognition
(c) Malware creation
(d) Power management

2. Attempt all parts:-

2.a. State one legal consideration when seizing digital evidence(CO1,K1) 2

2.b. Define a forensic report?(CO2,K1) 2

2.c. Describe the significance of call logs in mobile forensics.(CO3,K1) 2

2.d. Define the term "network forensics" and list its key goals.(CO4,K1) 2

2.e. List the tools commonly used in IoT Forensics(CO5,K1) 2

.

SECTION-B 30

3. Answer any five of the following:-

3-a.	Explain three categories of digital evidence with examples(CO1,K2)	6
3-b.	Discuss the ethical responsibilities of a digital forensic examiner.(CO1,K2)	6
3-c.	Discuss metadata artifacts, and how can they aid an investigation?(CO2,K1)	6
3-d.	Discuss why documentation necessary at each phase of forensic investigation?(CO2,K2)	6
3.e.	Describe the process involved in mobile data acquisition.(CO3,K2)	6
3.f.	Recall two packet sniffing tools & explain them(CO4,K1)	6
3.g.	Explain the importance of securing digital evidence in Cloud environments(CO5,K2)	6

SECTION-C 50

4. Answer any one of the following:-

4-a.	Describe in detail the digital forensic process model with real-world examples.(CO1,K2)	10
4-b.	Discuss legal frameworks (e.g., GDPR, ECPA, IT Act) applicable to digital forensics.(CO1,K2)	10

5. Answer any one of the following:-

5-a.	You are forensic expert you gathered digital evidences for court.Explain the types of digital evidence, their classification, and admissibility in court(CO2,K3)	10
5-b.	You are forensic officer there is a malware in memory.What forensics you will use.Describe in detail the methods and tools used for that forensics.(CO2,K3)	10

6. Answer any one of the following:-

6-a.	As a Forensic expert explain the best practices for preserving the integrity of digital evidence in mobile forensics(CO3,K3)	10
6-b.	As a Forensic expert, discuss the role of mobile forensics in providing digital evidence for legal proceedings.(CO3,K3)	10

7. Answer any one of the following:-

7-a.	As a Forensic expert ,analyze how metadata can be used to infer user behavior in a network(CO4,K3)	10
7-b.	As a forensic expert ,categorize and describe the different phases of a network forensic investigation.(CO4,K3)	10

8. Answer any one of the following:-

8-a.	As a Forensic expert ,discuss the key challenges involved in the investigation of cloud-based crimes and how they can be addressed(CO5,K3)	10
8-b.	As a Forensic expert Analyze the legal implications of using AI and ML in Forensic investigations.(CO5,K3)	10