2203890

Guru Nanak Dev Engineering College, Ludhiana			
Department of Information Technology			
Program	B.Tech.(IT-A/B)	**Semester**	6
Subject Code	: PEIT- 112	**Subject Title**	Digital Forensics
Mid Semester Test (MST) No.	1	**Course Coordinator(s)**	Dr. Amit Kamra
Max. Marks	24	**Time Duration**	1 hour 30 minutes
Date of MST	March 2025	**Roll Number**	

Note: Attempt all questions

Q. No.	**Question**	**COs, RBT level**	**Marks**
Q1	List the names of various hardware and software tools for CF.	CO1, L2	2
Q2	Outline the steps required to prepare a computer investigation	CO2, L2	2
Q3	Discuss the procedure used for handling E mail abuse investigations.	CO3, L3	4
Q4	Elaborate the typical computer supported crimes that occur in corporate? How can these be prevented?	CO2, L3	4
Q5	John deposits a stolen third-party check into his account. No problems are detected during check clearance, and two days later cleared funds are available in john account. Subsequently an ATM camera records John making cash withdrawal. The bank's forensics system analyzes the video image and a match is found against the latest police records of john, wanted in connection with illegal drug activities. How would your forensic system continue to handle this analysis?	CO2, L5	4
Q6	When senior officials of a Top company found out that certain employees were operating internal slush funds totaling about 100 crores, they called in a computer forensics professional to find out why and how to assess the impact. Explain in the form of forensic report, how the computer forensics professional went about resolving the problem.	CO5, L6	8

Course Outcomes (CO)

Students will be able to

1	Understand the concepts and vocabulary of digital forensics
2	To understand how to examine digital evidences such as the data acquisition, identification analysis
3	Understand what open source tools exist for use when performing Digital Forensics
4	Document their findings when performing a digital forensic analysis.
5	Write a basic report based on digital forensics findings
6	To understand the basic digital forensics and techniques for conducting the forensic examination

RBT Classification	**Lower Order Thinking Levels (LOTS)**			**Higher Order Thinking Levels (HOTS)**		
RBT Level Number	L1	L2	L3	L4	L5	L6
RBT Level Name	Remembering	Understanding	Applying	Analyzing	Evaluating	Creating

Guru Nanak Dev Engineering College, Ludhiana

Department of Information Technology (Jan- May 2025)

Program	B.Tech.(IT-A/B)	**Semester**	6
Subject Code	PEIT- 112	**Subject Title**	Digital Forensics
Mid Semester Test (MST) No.	2	**Course Coordinator(s)**	Dr. Amit Kamra
Max. Marks	24	**Time Duration**	1 hour 30 minutes
Date of MST		**Roll Number**	

Note: Attempt all questions

Q. No.	**Question**	**COs, RBT level**	**Marks**
Q1	List the benefits of professional forensic methodology.	CO1, L2	2
Q2	Write the difference between safeback and snapback.	CO2, L2	2
Q3	What are basic rules for collecting evidence? Discuss the types of evidence.	CO3, L3	4
Q4	How e-mail forensics works?	CO2, L3	4
Q5	A computer was seized during a routine drug arrest. What did the CFS do to prove that the computer was involved in other crimes?	CO5, L5	4
Q6	An accounting firm was conducting an audit of a publicly owned company when they came upon some accounting irregularities. The irregularities were serious enough to potentially necessitate a re-stating of earnings. Considering the many scandals currently blighting the corporate sector, the accounting firm wished to confirm their findings before sounding any public alarms. They retained a CFST to conduct large-scale data mining to get to the bottom of the irregularities. How would a CFST go about conducting a forensics data mining operation?	CO5, L6	8

Course Outcomes (CO)

Students will be able to

1	Understand the concepts and vocabulary of digital forensics
2	To understand how to examine digital evidences such as the data acquisition, identification analysis
3	Understand what open source tools exist for use when performing Digital Forensics
4	Document their findings when performing a digital forensic analysis.
5	Write a basic report based on digital forensics findings
6	To understand the basic digital forensics and techniques for conducting the forensic examinaticn

RBT Classification	**Lower Order Thinking Levels (LOTS)**			**Higher Order Thinking Levels (HOTS)**		
RBT Level Number	L1	L2	L3	L4	L5	L6
RBT Level Name	Remembering	Understanding	Applying	Analyzing	Evaluating	Creating

Please check that this question paper contains 09 questions and 02 printed pages within first ten minutes.

[Total No. of Questions:09] [Total No. of Pages: 02]

Uni. Roll No. 2203890......

Program: B.Tech. (Batch 2018 onward)
Semester: 6
Name of Subject: Digital Forensics
Subject Code: PEIT-112
Paper ID: 17212

Time Allowed: 03 Hours **Max. Marks: 60**

NOTE:

1) Parts A and B are compulsory
2) Part-C has Two Questions Q8 and Q9. Both are compulsory, but with internal choice
3) Any missing data may be assumed appropriately

Part – A **[Marks: 02 each]**

Q1.

a) List the various problems associated with computer forensics evidence.

b) Write the benefits of having professional forensic methodology.

c) Distinguish between safeback and snapback.

d) Write the steps to prepare computer evidence.

e) Name some remote network acquisition and data recovery tools.

f) Point out the things to be examined during investigation of media leak.

Part – B **[Marks: 04 each]**

Q2. How does e-mail forensics work? List some tools used in this analysis.

Q3. What do we need to conduct as forensic specialist when some internet abuse is being investigated?

Q4. Discuss the various types of business computer forensic technologies.

Q5. An accounting company needed to review approximately 10 million pages of client internal documents in the context of an audit. The data resided in email, text documents, and file attachments. The original plan was to deploy a team of professionals at the

P.T.O.

client site for a three-month document review. How would your advanced document management services center (DMSC) handle this document review?

Q6. Explain various steps involved in forensics investigation that can identify and attempt to retrieve possible evidence.

Q7. Elaborate the various types of RAID data acquisition levels.

Part – C **[Marks: 12 each]**

Q8. Discuss the employer safeguard program. Also describe the services provide by computer Forensics.

OR

With reference to evidence, discuss its types, rules and procedure for collection and their archiving.

Q9. After two former employees left a high-quality large-format imaging firm to work for a competitor, the defendants emailed the firm's customer database to their home computer in an attempt to steal intellectual property from the firm and provide it to their new employer. They firmly denied the allegations put forth by the firm, believing that no one would find out since they had deleted the email and the attachment containing the customer database from their home computer. How would the firm's Forensic team go about investigating this case?

OR

Ram enters a bank branch in the Ludhiana and deposits a check for her brother. The bank video camera captures an image of Ram entering the branch and matches it against its database of customers. The image is time and date stamped. Later that day, Ram savings account is accessed via Internet banking from an IP address located in Jalandhar. During a routine correlation of data, the apparent discrepancy is detected by the bank's forensics system. How you would as a computer forensics specialist, go about investigating this incident?

****