Reg. No.															

Question Paper Code	13500

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2025

Sixth Semester

Computer Science and Engineering

20CSEL602 - DIGITAL FORENSICS

Regulations - 2020

Duration: 3 Hours Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	What is considered Digital Evidence in a forensic investigation? (a) Physical evidence such as fingerprints (b) Any data that is stored digitally, including files, emails, and logs (c) Witness testimony (d) Crime scene photos	1	K1	CO1
2.	Computers can be used in crimes in the following ways, EXCEPT: (a) As a tool (b) As a storage device (c) As a witness (d) As a target	1	K2	CO1
3.	The main duty of an expert witness in digital forensics is to: (a) Represent one side of the case (b) Manipulate evidence (c) Provide unbiased, expert analysis (d) Make personal opinions	1	K2	CO2
4.	Scaffolding in digital investigations refers to: (a) Physical scaffolds for data centers (b) A step-by-step support framework (c) Software for hackers (d) Network protocols	1	K1	CO2
5.	Which tool is widely used for file analysis in digital forensics? (a) WinRAR (b) Fiwalk (c) MS Excel (d) PowerPoint	1	K1	CO3
6.	Fingerprint recognition systems rely on: (a) Hair colo (b) Skin tone (c) Ridge and minutiae patterns (d) Retinal blood vessels	1	K2	CO3
7.	In digital forensics, the term "chain of custody" refers to: (a) A method for encrypting data (b) The process of transferring digital evidence from one device to another (c) A documented process showing who handled the evidence at every stage (d) A way to erase evidence securely	1	K2	CO4
8.	Which of the following is a primary control in handling digital evidence? (a) Ensuring the evidence is erased (b) Ensuring evidence is not tampered with during analysis (c) Only analyzing evidence after it is corrupted (d) Ignoring the documentation of evidence	1	K1	CO4
9.	In network forensics, the primary goal is to: (a) Encrypt network traffic (b) Recover lost data (c) Identify and analyze network traffic to uncover evidence of illegal activities (d) Increase the speed of data transmission	1	K2	CO5
10.	Which of the following tools is commonly used in network forensics to capture and analyze packets? (a) Wireshark (b) MS Word (c) Adobe Acrobat (d) VLC Media Player	1	K1	CO6

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

11.	List two fundamental principles of digital forensics.	2	K1	CO1
12.	Explain what a cyber trail refers to in a digital forensics investigation.	2	K2	CO1

13.	List two types of digital investigation process models.	*2*	*K1*	*CO2*
14.	Define the term "security breach."	*2*	*K1*	*CO2*
15.	Illustrate the usage of Fiwalk .	*2*	*K2*	*CO3*
16.	Show the two types of internet artifacts.	*2*	*K1*	*CO3*
17.	Mention one key provision of the Indian Evidence Act related to digital data.	*2*	*K1*	*CO4*
18.	State one objective of the Electronic Communication Privacy Act.	*2*	*K1*	*CO4*
19.	Name any one forensic science principle applied to networks.	*2*	*K1*	*CO5*
20.	Name any one tool used in network forensic investigations.	*2*	*K1*	*CO5*
21.	Illustrate the primary goal of digital forensic analysis.	*2*	*K2*	*CO6*
22.	Explain metadata play in Network Forensic investigations.	*2*	*K2*	*CO6*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a)	Explain the evolution of digital forensics from its inception to the present. Discuss how advancements in technology have shaped its methodologies.	*11*	*K2*	*CO1*
		OR			
	b)	Discuss the role of digital evidence in cybercrime investigations. Analyze the challenges involved in obtaining, preserving, and presenting digital evidence in court.	*11*	*K2*	*CO1*
24.	a)	Summarize the process of presenting digital evidence in court. What are the key challenges involved?	*11*	*K2*	*CO2*
		OR			
	b)	Explain the admissibility of digital evidence in a courtroom. What factors influence its acceptance or rejection?	*11*	*K2*	*CO2*
25.	a)	Explain the procedure for analyzing files such as images, audio, video, and documents during an investigation.	*11*	*K2*	*CO3*
		OR			
	b)	Discuss how graphical investigation environments assist in forensic analysis with examples.	*11*	*K2*	*CO3*
26.	a)	Identify a case study that illustrates a failure in following digital evidence control procedures and propose how legal consequences could have been avoided.	*11*	*K3*	*CO4*
		OR			
	b)	Develop a training module outline for law enforcement officers on ethical digital investigation practices under IPC and CrPC.	*11*	*K3*	*CO4*
27.	a)	Explain the role of forensic science principles in investigating network intrusions.	*11*	*K2*	*CO5*
		OR			
	b)	Discuss the challenges of preserving digital evidence on the internet and suggest best practices.	*11*	*K2*	*CO5*
28.	a)	Develop a scenario in which digital evidence from the internet is crucial to solving a cybercrime.	*11*	*K3*	*CO6*
		OR			
	b)	Identify the admissibility and reliability of network-captured evidence in court.	*11*	*K3*	*CO6*