Reg.No.:												

VIVEKANANDHA COLLEGE OF ENGINEERING FOR WOMEN
[AUTONOMOUS INSTITUTION AFFILIATED TO ANNA UNIVERSITY, CHENNAI]
Elayampalayam – 637 205, Tiruchengode, Namakkal Dt., Tamil Nadu.

Question Paper Code: 60019

B.E. / B.Tech. DEGREE END-SEMESTER EXAMINATIONS – NOV. / DEC. 2025
Seventh Semester
Computer Science and Engineering
U19ITV23 – CYBER FORENSICS
(Regulation 2019)

Time: Three Hours | Maximum: 100 Marks

Answer ALL the questions

Knowledge Levels (KL)	K1 – Remembering	K3 – Applying	K5 - Evaluating
	K2 – Understanding	K4 – Analyzing	K6 - Creating

PART – A

(10 x 2 = 20 Marks)

Q.No.	Questions	Marks	KL	CO
1.	Recall why computer investigation is essential in digital forensics.	2	K1	CO1
2.	Mention two common areas where computer investigation is applied.	2	K1	CO1
3.	What does AFF stand for and what is its basic purpose?	2	K1	CO2
4.	State what RAID stands for and its significance in data storage systems.	2	K1	CO2
5.	Specify what a digital hash is and its use in maintaining data integrity.	2	K1	CO3
6.	Identify key operations carried out by computer forensic tools.	2	K1	CO3
7.	State the tasks performed by Computer Forensic Tools.	2	K1	CO4
8.	Mention any two common methods used to conceal digital data.	2	K1	CO4
9.	Define Bait Tactics as applied in detecting or preventing digital crimes.	2	K1	CO5
10.	What are the types of graphics file format?	2	K1	CO5

PART – B

(5 x 13 = 65 Marks)

Q.No.		Questions	Marks	KL	CO
11.	a)	Elaborate the five phases of Computer Forensic Investigation. State the main advantages and disadvantages associated with computer investigation.	13	K2	CO1

(OR)

	b)	Explain the various types of computer investigations and outline the key steps required to prepare for a computer investigation.	13	K1	CO1
12.	a)	Demonstrate the different formats for storing digital evidence. Differentiate between static acquisition & live acquisition.	8+5	K2	CO2
		(OR)			
	b)	Write down the windows validation method for data validation. Explain the contingency planning for image acquisition.	13	K2	CO2
13.	a)	Describe the Key points to consider for Private Sector Incident Scenes. State the steps of Securing a Computer Incident or Crime Scene.	7+6	K2	CO3
		(OR)			
	b)	During a digital forensic investigation, an analyst needs to verify whether a seized file has been altered. i. Explain how digital hash functions can be used to confirm the file's integrity. ii. Compare different hashing methods such as MD5, SHA-1, and SHA-256, and discuss which would be most suitable for this scenario. Support your answer with a diagram or example illustrating the hashing process.	13	K2	CO3
14.	a)	Explain the role of Command-Line Forensic Tools and Forensic Workstations in digital investigations. Discuss their key features, components, examples, and importance in ensuring accurate, secure, and efficient forensic analysis.	13	K2	CO4
		(OR)			
	b)	Explain the process of validating and testing forensic software using NIST-provided tools and frameworks. Discuss the steps involved, the evaluation criteria, and the importance of NIST standards in ensuring the accuracy, reliability, and credibility of forensic tools.	13	K2	CO4
15.	a)	Describe in detail the various techniques used for recovering graphics file formats during digital forensic investigations. Explain the steps involved in identifying, extracting, and reconstructing deleted or damaged image files, and discuss the challenges and tools commonly used in the recovery process. Support your answer with suitable examples.	13	K2	CO5
		(OR)			
	b)	Analyze the various techniques used in email forensics, explaining how emails are examined, traced, and verified during a digital investigation. Discuss the processes involved in header analysis, metadata examination, recovery of deleted emails, and detection of phishing or spoofing attempts. Support your answer with suitable examples and tools commonly used in email forensic analysis.	13	K2	CO5

PART – C

(1 x 15 = 15 Marks)

Q.No.		Questions	Marks	KL	CO
16.	a)	Describe how RAID data can be acquired using a remote network acquisition tool, explaining the steps involved in collecting and rebuilding data from multiple drives. Also, discuss the main principles and good practices that should be followed when validating and testing forensic software tools to make sure the results are accurate, reliable, and trustworthy.	15	K2	CO4
		(OR)			
	b)	Explain how forensic data can be validated using hexadecimal editors. Describe the process of analyzing and verifying data integrity at the byte level with the help of a suitable example. Discuss the significance of hex analysis in identifying data tampering, file signatures, and hidden information during forensic investigations.	15	K3	CO5