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: 60021

B.E. / B.Tech. DEGREE END-SEMESTER EXAMINATIONS – NOV. / DEC. 2024
Fifth Semester
Information Technology
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.	Why is professional conduct important?	2	K2	CO1
2.	Why should evidence media be write protected?	2	K2	CO1
3.	Mention the most critical aspect of digital evidence?	2	K2	CO2
4.	Name the three formats for digital forensics data acquisitions.	2	K1	CO2
5.	Write the rules for a forensic hash.	2	K1	CO3
6.	What does commingling evidence mean?	2	K1	CO3
7.	List three subfunctions of the extraction function.	2	K1	CO4
8.	In testing tools, what does the term "reproducible results" mean?	2	K1	CO4
9.	What is the main piece of information you look for in an email message you're investigating?	2	K2	CO5
10.	Router logs can be used to verify what types of email data?	2	K2	CO5

PART – B

(5 x 13 = 65 Marks)

Q.No.		Questions	Marks	KL	CO
11.	a)	Examine the requirement for a standard risk assessment to prepare for an investigation?	13	K3	CO1

(OR)

	b)	Describe the ways to determine the resources needed for an investigation.	13	K3	CO1
12.	a)	Discuss about logical acquisition and sparse acquisition for an investigation.	13	K4	CO2
		(OR)			
	b)	How the acquired data are validated? Discuss in detail.	13	K2	CO2
13.	a)	When you arrive at the scene, why should you extract only those items you need to acquire evidence?	13	K3	CO3
		(OR)			
	b)	Describe what should be videotaped or sketched at a digital crime scene.	13	K3	CO3
14.	a)	Discuss about the validation and testing of forensic software.	13	K3	CO4
		(OR)			
	b)	Determine what data to analyze in a digital forensics investigation and explain the tools used to validate data.	13	K3	CO4
15.	a)	Examine how to identify an unknown graphics file format that your digital forensics tool doesn't recognize?	13	K3	CO5
		(OR)			
	b)	When confronted with an e-mail server that no longer contains a log with the date information you need for your investigation and the clint has deleted the e-mail, explain what should you do?	13	K3	CO5

PART – C

(1 x 15 = 15 Marks)

Q.No.		Questions	Marks	KL	CO
16.	a)	As part of the duties of a digital forensic examiner, creating an investigation plan is a standard practice. Describe how you would organize an investigation for a potential fraud case. In addition, list methods you plan to use to validate the data collected from drives and files, such as Word and Excel with hashes and specify the hash algorithm you plan to use, such as MD5 or SHA1.	(7+8 = 15)	K6	CO4
		(OR)			
	b)	You need to acquire an image of a disk on a computer that can't be removed from the scene and you discover that it's a Linux computer. What are your options for acquiring the image? Write a brief report specifying the hardware and software you would use.	(7+8 = 15)	K4	CO2