Roll No. | | | | | | | | | | |

ANNA UNIVERSITY (UNIVERSITY DEPARTMENTS)

B.E. / B. Tech / B. Arch (Full Time) - END SEMESTER EXAMINATIONS, NOV / DEC 2023

MINOR DEGREE IN CYBER SECURITY
V Semester
CSM505 & CYBER FORENSICS
(Regulation 2019)

Time: 3hrs | Max. Marks: 100

CO 1	Understand the fundamentals of computer forensics
CO 2	Identify and apply smart practices for investigation
CO 3	Recognize the legal underpinnings and critical was affecting forensics
CO 4	Apply tools and methods to uncover hidden information in digital systems
CO 5	Learn the issues of cyber forensics

BL – Bloom's Taxonomy Levels
(L1 - Remembering, L2 - Understanding, L3 - Applying, L4 - Analysing, L5 - Evaluating, L6 - Creating)

PART- A (10 x 2 = 20 Marks)
(Answer all Questions)

Q. No	Questions	Marks	CO	BL
1	What are the roles played by a computer in a crime?	2	1	L1
2	What is spyware and adware?	2	1	L1
3	What are the obstacles to data backup and recovery?	2	2	L2
4	What is slack space? Why is it considered in forensics?	2	3	L1
5	What is honeypotting?	2	2	L1
6	What is chain of custody?	2	3	L1
7	List the hacker typologies.	2	4	L2
8	What is cyber extortion?	2	4	L1
9	Distinguish identity theft and identity fraud.	2	5	L2
10	What is meant by dumpster diving?	2	5	L1

PART- B (5 x 13 = 65 Marks)
(Restrict to a maximum of 2 subdivisions)

Q. No	Questions	Marks	CO	BL
11 (a) (i)	Explain the various computer forensic services.	8	1	L3
(ii)	List the benefits of professional forensic methodology.	5	1	L3
	OR			
11 (b) (i)	Give an account on the Intrusion Detection Systems.	8	1	L3
(ii)	An IT manager reviews a detection tool report that indicates a company employee is accessing restricted Internet sites and downloading objectionable material. After discovering the activity, the IT manager remotely accesses the employee's personal computer to obtain evidence. The employee is then dismissed, based on the evidence located and obtained. Can it be proved that the objectionable material was viewed on a particular PC? If so, How? Who else had access to that PC?	5	2	L4
12 (a) (i)	Explain the evidence collection procedure and its archiving.	8	2	L3
(ii)	As a forensic examiner you are asked to obtain the history records from a browser? How will you do it?	5	2	L3

	OR			
12 (b) (i)	Explain the legal aspects of collecting and preserving the computer forensic evidence.	8	3	L3
(ii)	A popular company where employee A was working witnessed an internal threat - confidential data from the company had been leaked. The mode of leakage may have been either confidential data copied to a removable storage or sent via email. As a forensic examiner you are entrusted with the task of gathering evidence about the data being copied from the system that contained the confidential data. The hard disk containing the confidential data has to be examined after data acquisition and analysis for any deleted files, email sent with date and time, etc. In addition, any access to the system over a network should be ruled out. Suggest the forensic tools you would use for this scenario as well as the reason for choosing the specific tool.	5	3	L4
13 (a) (i)	Discuss the evidence processing steps in detail.	8	2	L3
(ii)	Explain the rules of digital evidence.	5	3	L3
	OR			
13 (b) (i)	Imagine that you are the forensic examiner for a crime reported as 'theft of intellectual property' by an organization, say, X. The IO had reported after a thorough investigation that an employee, say, Y had become disgruntled in recent months and left the organization. On the day Y left the organization, he was spotted by co-workers as downloading some data from the computer to a removable storage media which is against the organization's security policy. Employee Y was associated with a research team in organization X where the research findings were on the production line and was worth huge money. The IO had already confirmed with employee Y about the usage of removable storage on the day he left the organization, for which he had given a justification to the effect that he had copied only the personal content which he didn't want to leave behind with the organization. He also added that most of the content on the removable storage had already been deleted. The removable storage has now been seized for forensic examination. Answer the following questions from the given context: (a) Explain in detail the documentation that has to be done for the seizure and acquisition of evidence. (b) How will you describe the physical characteristics of the evidence in the report? (c) What will you do to secure and preserve the crime scene?	13	4	L5
14 (a) (i)	What are the three categories of computer crime? What are some of the individual crimes included in each?	8	1	L2
(ii)	Compare virus, worm and Trojan Horse.	5	1	L2
	OR			
14 (b) (i)	Explain the toolkit of a cyber-criminal.	8	1	L2
(ii)	Categorize and five cybercrimes of your choice according to their impact as high, medium or low financial loss with justification for each.	5	1	L4
15 (a) (i)	Explain the on-scene activities while searching and seizing computer related evidence.	8	2	L3
(ii)	How will educate the public to protect themselves in the physical world and in the online world?	5	5	L4
	OR			
15 (b) (i)	Briefly describe each of the physical methods of identity theft.	8	5	L3
(ii)	Do you think using a public Wi-Fi is a crime? What are the risks associated with it?	5	2	L4

PART- C (1 x 15 = 15 Marks)

(Q.No.16 is compulsory)

Q. No	Questions	Marks	CO	BL
16.	The Subject, who was a reputed apparels merchant, had in place an e-commerce payment gateway of a reputed merchant service, facilitated through the Pay seal application, to allow customers make online purchases. This enabled the merchant to accept cards for payments. The cybercrime involved came to light when the merchant received chargeback (Chargeback is a form of customer protection provided by the banks issuing credit cards, so as to allow cardholders to file a complaint regarding fraudulent transactions when discrepancies are noticed in the accounts statement. If the transaction is known to be fraudulent on investigation, the bank would have to refund the original value to the cardholder. If the cardholder cannot prove the transaction to be legitimate, the entire amount of the transaction, along with an additional fee, will be debited from his/her account.) for many transactions worth `17,71,464 during a six-month period from October 2010. The bank had debited the merchant account for the chargeback received from various issuing banks. The most common reason for chargeback involves fraudulent transactions, where the credit card is used without the authorization and consent of the cardholder. In such a case, the merchant is held solely responsible. Hence, a case was registered based on a complaint from the Subject. Prepare an Investigation Report and Cyber Forensic Analysis Report for this case brief.	**15**	4,5	L6