ITM UNIVERSITY
GWALIOR • MP • INDIA
"CELEBRATING DREAMS"

Mid Term Exam Sep2022

Class &Batch : .Tech. V Sem — Subject Name& Code: Digital Forensic Essentials CSL0521
Time 01:30 Hours — Maximum Marks:30
All Questions are Compulsory:

Q. No.	Questions	Marks	CO	BL
Q 1				
1.1	Define computer Forensic and list down the resources that are analyzed during this process.	1	CO1	L1
1.2	Discuss the objectives of computer forensic and describe why do we need to do computer forensics? OR Discuss in brief the potential resources of digital evidences and their location from where they can be found in the respective devices or interfaces.	5	CO1 CO2	L1 L2
Q 2				
2.1	State Locard's principle of evidence and elaborates it in your own words.	1	CO1	L1
2.2	Describe five basic rules of evidences with their legal significance in legal aspects of evidence presentation in the court of Law. OR Describe what do you understand by forensic readiness. Suggest at least five measures for forensic readiness for an organization with an IT infrastructure of 100 computers distributed in 3 LANs, an internet server, an high speed internet connection with DHCP setup.	5	CO2 CO2	L2 L2
Q 3				
3.1	Define forensic investigation process and write a one definition of the three stages.	1	CO1	L1
3.2	Discuss the tasks involved in pre investigation phase of forensic investigation. What should be the composition of a forensic investigation team, describe the role of each expert of the team. OR An individual has been attacked by an offender by sending a message to click on a link and sharing OTP for bank transaction received through mail. The offender was successful to withdraw money from the victim's account. List down the evidences that should be collected to solve the case along with their location and the tools required to extract or retrieve these evidences, types of experts required to do digital forensic analysis for the case. Also suggest forensic readiness to the victim for future.	5	CO2 CO3	L2 L3
Q 4				
4.1	List down the tasks involved in the forensic investigation process.	1	CO1	
4.2	What do you understand by physical and logical structure of hard disks. Explain at least three ways in which these structures can be exploited by the cyber crime offenders to perform attacks. OR Describe the structure of GPT(GUID Partition table) and describe the entires done in it. Also write the command that can be used to extract GPT details from a window's operating system.	5	CO2, CO2, CO3	L2 L2, L3
Q 5				
5.1	Define booting and its types.	1	CO1	L1
5.2	Describe the kind of artifacts that can be collected from hard disk and	5	CO2	L2

	their significance as an evidence. OR What do you understand by clusters, explain from utility in storage management point of view. Also, define lost clusters and describe how are they formed.		CO2	

.L2