VIT

Vellore Institute of Technology

Continuous Assessment Test – II

Programme Name & Branch: B.Tech (CSE) **Course Name:** Digital Forensics

Course Code: CSE4004 **Slot:** G2

Exam Duration: 90 mins **Maximum Marks:** 50

S.No.	Question	CO
1	The Windows NT file system (NTFS) provides a combination of performance, reliability, and compatibility not found in the FAT file system. Elaborate the reasons why NTFS is designed, and if we format a volume with the NTFS file system what are the changes takes place compared to FAT. Are the NTFS file system support security features? If yes elucidate various security features and their importance.	CO4
2	**Stolen laptop leads to breach notification for 20,000 Lifespan patients:** Providence-based Lifespan, Rhode Island's largest health network, has notified about 20,000 of its patients that a laptop theft may have exposed their sensitive information contained emails with names, medical record numbers, partial address information, medications and more. The health organization said an employee's MacBook was taken after a car break-in on Feb. 25, 2017. The employee immediately contacted both law enforcement and Lifespan officials, who were able to change the employee's credentials used to access Lifespan system resources, but the data loss was happened. Find the reasons for the scenario and suggest and elaborate the suitable techniques and tools to overcome these issues.	CO4
3	In the cyber-crime huge log data, transactional data occurs which tends to plenty of data for storage and analyze them. It is difficult for forensic investigators to play plenty of time to find out clue and analyze those data. In network forensic analysis involves network traces and detection of attacks. The trace involves an Intrusion Detection System and firewall logs, logs generated by network services and applications, packet captures by sniffers. In network lots of data is generated in every event of action, so it is difficult for forensic investigators to find out clue and analyzing those data. In network forensics is deals with analysis, monitoring, capturing, recording, and analysis of network traffic for detecting intrusions and investigating them. Propose the suitable data collection and analysis techniques from the cyber system and web browser. Suggest the tools and their operations for memory forensic analysis and remote system forensic which is to be used as evidence for aiding investigation.	CO5
4	Digital forensic tools are used to unravel criminal acts and prove crime in the court of law. However, the area, task and/or functions digital forensic tools are being applied in may not be suitable hence leading to unreliable results by these tools. In many cases, forensic experts may apply a particular tool not because it is the most effective tool but because it is available, cheap and the expert is familiar with it. This has often led to use of unreliable digital forensic tools, which may yield unreliable results.	CO5

SEARCH VIT QUESTION PAPERS
ON TELEGRAM TO JOIN