VIT
Vellore Institute of Technology

Continuous Assessment Test – I

Programme Name & Branch: B.Tech

Course Name & Code: Digital Forensics CSE4004

Class Number: VL2019201001481 **Slot:** G2+TG2 **Exam Duration:** 90 mins **Maximum Marks:**50

General instruction(s):

Answer to the point and give necessary justification, if required.

Sl.No.	Question
1.	**Case Study:-** **Scenario:** An Online support agent payment company headquartered in Zurich became the victim of cyber-attack on 22nd December 2016, one week prior to Christmas, traditionally the busiest online shopping period for the company. An online sale during this period typically generates organization over 25% of its annual revenue. The company's online system alerts that the payment processing servers and the associate services were not responding began appearing on the company's monitoring services, and a large number of employees contacted the IT Service Desk. It was immediately apparent to the technical teams that the systems were offline. There was a delay in correctly identifying the outage and the reason for their service outage. Due to this, the company was very slow to implement the appropriate incident handling procedures. The company had called on several third parties both forensic and IT companies to help them and to fully restore the affected services. What were the findings by the Digital Forensics investigator? Briefly explain the problem faced by the Zurich company and list out the remedies with appropriate software tools and action steps taken by the Forensics investigator to identify and generate a report based on the collected evidences? (10)
2.	**Scenario:** Azimith LLC is one of the leading multinational Techno-Financial institutes consulting companies mostly extend their techno-consultant with the Banking Sectors. The role of the company is to provide them all sort of support to overcome issues including cybercrime, legal, and backend IT support and carter their clients or customers with 100% safety and accurate in their transactions. What are the critical steps taken by the forensic expert for preparation of search in order to achieve the above said assurance and satisfy their customers based on the modernization of Information Technology in Banking industry? (10)
3.	Scenario: During one of the digital crime evidence creation, the investigative team found that the file size is more than 1.5GB and the team has no other way to avoid any of the information from the collected evidence, due to which they have to go for optional compression. If the file size is within the limit of 2GB the team can store the file in any one of the file storage format. What are the types of file storage format used extensively for storing digital evidences? What will be your recommendation of storing the digital evidence so that the digital investigator gets maximum benefits in terms of digital investigation and what are drawbacks in adopting your recommended file storage format. Justify your answers with a proper example? (10)
4.	Explain the concept of RAID 5 data acquisition system? How is it differing from the other RAID versions? Compare RAID 5 with other RAID Versions? (10)
5.	Analysis and illustrate the different phases of digital forensics typical investigation with its goals, methodologies and policies governing the handling the incident? (10)