E/L/TX

Reg. No: 21BCI0057

VIT
Vellore Institute of Technology

Final Assessment Test – November 2024

Course: BCSE322L - Digital Forensics

Class NBR(s): 1460/1464/1467

Slot: E1

Time: Three Hours

Max. Marks: 100

- KEEPING MOBILE PHONE/ELECTRONIC DEVICES EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE
- DON'T WRITE ANYTHING ON THE QUESTION PAPER

Answer ALL Questions

(10 X 10 = 100 Marks)

1. You are an IT forensic investigator tasked with preparing for a computer investigation in a medium-sized retail company that suspects an employee of stealing sensitive customer data. Exemplify the key steps you would take to prepare for the investigation, including considerations for evidence collection, preservation, and legal compliance. Refer to a hypothetical scenario where improper preparation resulted in evidence being deemed inadmissible in court.

2. As a digital forensic investigator, maintaining professional conduct is crucial throughout the investigation process. Discuss the key ethical and professional responsibilities you must adhere to when conducting a digital forensic investigation. Also, highlight the importance of objectivity, confidentiality, and integrity. Provide your own case study where failure to maintain professional conduct compromised the investigation or led to legal consequences.

3. Investigating cyber crime requires a systematic approach to ensure the accuracy and reliability of findings. By considering the below given case study, illustrate the key stages involved in a systematic digital forensic investigation, from incident identification to reporting.

   In April 2011, Sony's PlayStation Network (PSN) suffered one of the largest data breaches in history. Hackers infiltrated Sony's servers and gained access to personal information, including names, addresses, email addresses, passwords, and possibly credit card details, affecting over 77 million user accounts. This cybercrime cost Sony approximately $171 million in damages and forced them to shut down the PSN service for over 23 days.

4. A mid-sized financial institution, XYZ Bank, experienced a security breach where sensitive customer data was accessed and possibly exfiltrated. The bank had a digital forensic team in place but lacked a robust contingency plan to address the various challenges that could arise during an investigation.

   Discuss the key components of an effective contingency plan for image acquisition in this respective digital forensic investigation. Also, elaborate the importance of validation procedures to confirm the integrity of the acquired images.

5. Redundant Array of Independent Disks (RAID) systems are often used to enhance data storage reliability and performance in digital forensics. Discuss the significance of RAID technology in the context of digital forensic investigations. Also, explain the different RAID levels, their impact on data redundancy and performance, and the challenges involved with it.

6. Discuss the significance of the Windows Registry in digital forensics. Explain the structure of the Windows Registry, including its main hives and keys. Describe how forensic investigators can utilize the Registry to uncover evidence related to user activities and system configurations. Provide examples of specific data types that can be recovered from the Windows Registry and their relevance in an investigation.

7. Demarcate the significance of file systems in an operating system. Explain the main types of file systems commonly encountered (e.g., NTFS, FAT32, HFS+) and their characteristics. Also, describe how forensic investigators analyze file systems to recover deleted files and uncover evidence related to user activities.

8. The boot process of Unix/Linux operating systems is fundamental to understanding system startup and initialization. Illustrate the stages of the boot process in a Unix/Linux environment.

Outline the key components involved in the process, including the BIOS, bootloader (such as GRUB), kernel loading, and the init process. Also, describe how understanding this process can aid forensic investigators in analyzing system startup behavior and identifying potential security incidents.

9.a) The Yahoo data breach, which occurred in 2013 and was revealed in 2016, is one of the largest known data breaches in history. It involved the theft of personal information from over 3 billion user accounts, including email addresses, passwords, and security questions. The breach not only highlighted the vulnerabilities of email systems but also underscored the significance of email forensics in cybercrime investigations.

By understanding the above given case, explain the key techniques used in email forensic analysis, including email header examination, content analysis, and attachment recovery. Describe how these techniques can help forensic investigators establish timelines, identify sender and recipient information, and uncover evidence of malicious activities.

OR

9.b) Social media forensics has become increasingly important in digital investigations, as social media platforms often contain critical evidence related to various crimes. Discuss the significance of social media forensics in the context of digital investigations. Explain the key techniques used in social media forensic analysis, including data collection, preservation, and analysis of posts, messages, and user interactions.

Describe how these techniques can assist forensic investigators in uncovering evidence of criminal activities, such as cyberbullying, fraud, or terrorism.

10.a) Acquisition procedures for mobile devices are critical in ensuring the integrity and admissibility of evidence in digital investigations. Discuss the key steps involved in the acquisition process for mobile devices. Also, outline the importance of proper handling and preservation techniques to prevent data loss or alteration.

Additionally, address the challenges that forensic investigators may encounter during the acquisition of mobile devices, such as encryption and device security measures.

OR

10.b) In November 2016, Uber Technologies, Inc. disclosed that it had suffered a significant data breach affecting the personal information of 57 million users and drivers. The breach involved unauthorized access to data stored in the cloud, raising important questions about cloud security and forensics. Hackers gained access to a private GitHub repository used by Uber software engineers. They found credentials that allowed them to access an AWS (Amazon Web Services) account where sensitive data was stored. The stolen data included the names, email addresses, and phone numbers of 57 million users, along with the driver's license information of about 600,000 drivers.

By understanding the given case, discuss the key components of cloud forensics and its significance in modern investigations. Explore the key challenges associated with conducting forensic investigations in cloud environments, including issues related to data jurisdiction, the shared responsibility model, and multi-tenancy.

Also, describe the methodologies employed in cloud forensic investigations, such as data acquisition, preservation, and analysis.

⇔⇔⇔ E/L/TX ⇔⇔⇔