Name: Rogel R. Gerodiaz  
Grade&Section: BSIT-32E1

**1. Techniques Used in Computer Forensics to Extract & Analyze Digital Evidence**

Computer forensics employs various techniques to extract and analyze digital evidence. Some of the key techniques include:

1. Disk Imaging:

* Creating an exact, bit-by-bit copy of a storage device to preserve the original evidence.

2. Data Recovery:

* Retrieving deleted, hidden, or corrupted data from storage devices.

3. File Carving:

* Extracting files from unallocated space or fragmented files without relying on file system metadata.

4. Memory Forensics:

* Analyzing volatile data in RAM to uncover running processes, network connections, and other transient data.

5. Network Forensics:

Capturing and analyzing network traffic to identify suspicious activities and data breaches.

6. Log File Analysis:

* Examining system and application logs to trace activities and identify anomalies.

7. Email Analysis:

* Investigating email headers, content, and attachments to uncover fraud, phishing, or other malicious activities.

8. Mobile Device Forensics:

* Extracting and analyzing data from smartphones, tablets, and other mobile devices.

9. Forensic Software Tools:

* Utilizing specialized software (e.g., EnCase, FTK, Sleuth Kit) to automate and facilitate the forensic analysis.

10. Hashing:

* Using cryptographic hash functions to verify the integrity of digital evidence by comparing hash values before and after analysis.

11. Timeline Analysis:

* Constructing timelines of digital events to understand the sequence and context of activities.

**2. Types of Computer Forensics**

Computer forensics can be categorized into several types, each focusing on different aspects of digital evidence:

1. Disk Forensics:

* Analysis of hard drives and other storage media to recover files, analyze file systems, and examine metadata.

2. Network Forensics:

* Investigation of network traffic and logs to detect intrusions, data exfiltration, and network-based attacks.

3. Wireless Forensics:

* Examination of wireless network communications, including Wi-Fi and Bluetooth, to uncover unauthorized access and other wireless-specific issues.

4. Database Forensics:

* Analysis of databases to recover data, analyze transactions, and identify unauthorized modifications.

5. Email Forensics:

* Investigating email systems to uncover fraud, phishing, and other email-related crimes.

6. Malware Forensics:

* Study of malicious software to understand its behavior, origin, and impact on systems.

7. Mobile Device Forensics:

* Extraction and analysis of data from mobile devices, including smartphones and tablets.

**3. Challenges Faced by Experts in Computer Forensics**

Experts in computer forensics encounter several challenges, including:

1. Data Volume:

* Managing and analyzing vast amounts of data from various sources.

2. Data Encryption:

* Overcoming encryption and secure deletion methods that hinder access to evidence.

3. Technological Advances:

* Keeping up with rapidly evolving technology and new types of devices and software.

4. Anti-Forensic Techniques:

* Detecting and counteracting methods used to obscure or destroy digital evidence.

5. Legal Issues:

* Navigating complex legal frameworks, maintaining chain of custody, and ensuring evidence admissibility in court.

6. Privacy Concerns:

* Balancing investigative needs with privacy rights and ethical considerations.

7. Cross-Jurisdictional Challenges:

* Coordinating investigations that span multiple legal jurisdictions with different laws and procedures.

8. Resource Limitations:

* Dealing with limited tools, expertise, and funding in some forensic labs.

9. Cloud Computing:

* Addressing the challenges posed by data stored in the cloud, including issues of jurisdiction, access, and data integrity.

10. Skill Gap:

* Ensuring forensic analysts have the necessary skills and ongoing training to handle advanced and emerging threats.