ADAMA SCIENCE AND TECHNOLOGY UNIVERSITY

SCHOOL OF ELECTRICAL ENGINEERING AND COMPUTING

DEPARTMENT OF SOFTWARE ENGINEERING

INDIVIDUAL ASSIGNMENT

COURSE TITLE: Digital Forensics

COURSE CODE: SEng4302

PREPARED BY: ABDI SILESHI WORKU

ID.NO UGR/25299/14

SECTION 3

GROUP 6

Chapter 3: Cybercrime Law

Answer the following

• Describe the following in your own terms:

- ✓ Organized Criminal Group
- ✓ Offenses against the confidentiality, Integrity, and Availability of Computer data and systems
- ✓ Legal provision of illegal access, illegal interpretation,
- ✓ Data Interference, system interference, misuse of Devices.
- ✓ Password intrusion and Vulnerability Attack
- ✓ Legal provision of Computer-related forgery and computer-related fraud.
- ✓ Identity theft in relation to fraud

1. Organized Criminal Group:

An organized criminal group refers to a structured association of individuals who collaborate to commit serious crimes, often for financial gain or power. These groups typically operate across borders and use sophisticated methods, including cybercrime, to carry out illegal activities such as fraud, money laundering, and hacking. They are characterized by hierarchy, planning, and coordination among members.

2. Offenses against the Confidentiality, Integrity, and Availability of Computer Data and Systems:

These offenses involve unauthorized actions that compromise the security of computer systems and data.

- **Confidentiality** refers to protecting data from unauthorized access.
- **Integrity** ensures that data is not altered or tampered with by unauthorized parties.
- **Availability** ensures that data and systems are accessible to authorized users when needed.

Examples of such offenses include hacking, data breaches, and denial-of-service attacks.

3. Legal Provisions of Illegal Access, Illegal Interception, Data Interference, System Interference, Misuse of Devices:

- **Illegal Access**: Unauthorized access to computer systems or data, often through hacking or password cracking.
- **Illegal Interception**: Unauthorized interception of data transmissions, such as eavesdropping on network communications.
- **Data Interference**: Unauthorized alteration, deletion, or damage to computer data.
- **System Interference**: Unauthorized actions that disrupt the functioning of computer systems, such as denial-of-service attacks.
- **Misuse of Devices**: Using tools or software (e.g., hacking tools) to commit cybercrimes.

4. Password Intrusion and Vulnerability Attack:

- **Password Intrusion**: Unauthorized access to a system or account by cracking or stealing passwords.
- **Vulnerability Attack**: Exploiting weaknesses or flaws in a system's software or hardware to gain unauthorized access or cause damage.

5. Legal Provisions of Computer-Related Forgery and Computer-Related Fraud:

- **Computer-Related Forgery**: Creating, altering, or deleting digital documents or data with the intent to deceive, such as forging digital signatures or falsifying electronic records.
- **Computer-Related Fraud**: Using computers or digital systems to deceive others for financial or personal gain, such as phishing scams or online fraud schemes.

6. Identity Theft in Relation to Fraud:

Identity theft involves stealing someone's personal information (e.g., Social Security number, credit card details) to commit fraud, such as making unauthorized purchases, opening accounts, or accessing financial resources in the victim's name. It is a form of cybercrime that often leads to financial loss and damage to the victim's reputation.

Chapter 4: Digital Forensic Readiness

1. Name the two main objectives of forensic readiness. Why are these objectives important for digital investigations?

The two main objectives of forensic readiness are:

- **Maximizing the usefulness of evidence**: Ensuring that collected digital evidence is well-organized, reliable, and legally admissible in investigations.
- **Minimizing the cost of forensic response**: Reducing the time, effort, and resources required for forensic investigations.

Importance: These objectives are crucial as they allow organizations and law enforcement to efficiently handle digital incidents while maintaining business continuity, complying with legal requirements, and ensuring a cost-effective approach to forensic investigations.

2. What should you consider when identifying potential sources of evidence?

When identifying potential sources of evidence, the following factors should be considered:

- **Relevance and reliability**: The evidence must be pertinent to the case and credible.
- **Legal and regulatory compliance**: Ensure that the collection and handling of evidence follow established laws and regulations.
- **Type of incident**: Different cases (e.g., cyberattacks, fraud, insider threats) require different sources of evidence.
- **Format and accessibility**: Identify whether the data is stored in structured or unstructured formats and how easily it can be retrieved.
- **Integrity and authenticity**: Ensure that the evidence remains unaltered and can be verified for accuracy.

3. What is the purpose of forensic tool testing? Describe the advantages and disadvantages of function-driven testing methodology.

Purpose of forensic tool testing: Forensic tool testing ensures that the tools used for digital investigations are reliable, accurate, and capable of processing evidence without modification or corruption.

Advantages of function-driven testing methodology:

- Focuses on specific forensic capabilities, ensuring tools meet required functions.
- Validates the accuracy and efficiency of forensic tools.
- Ensures compliance with legal and industry standards.

Disadvantages:

- May not test how tools perform in real-world forensic scenarios.
- Can overlook the interaction between different forensic processes and systems.

4. You are hired as a network security architect at an enterprise. Your task is to implement a set of controls to get the infrastructure digital forensics ready. Describe what steps you would take.

As a network security architect, I would implement the following steps to ensure digital forensic readiness:

1. **Define forensic readiness policies and procedures**: Establish clear guidelines for handling digital forensic cases.
2. **Identify and classify critical digital assets**: Prioritize key data sources for forensic analysis.
3. **Implement logging and monitoring mechanisms**: Set up real-time logging to capture relevant forensic data.
4. **Ensure secure data storage and evidence preservation**: Protect evidence with encryption and controlled access.
5. **Train staff on forensic principles and incident response**: Ensure that personnel are aware of forensic best practices.
6. **Regularly test forensic tools and processes**: Conduct mock investigations to validate forensic readiness.

5. Give examples of procedures to support a digital investigation process.

Examples of procedures that support digital investigations include:

- **Incident response protocols**: Define actions to be taken when a digital incident occurs.
- **Chain of custody documentation**: Maintain records of evidence handling to ensure integrity.
- **Secure evidence collection and storage**: Follow best practices for acquiring and preserving digital evidence.
- **Log analysis and monitoring**: Continuously track and analyze system logs for anomalies.
- **Forensic tool validation and testing**: Regularly verify forensic tools for accuracy and reliability.

6. A security breach was identified in a system supporting a critical business process. The system has a 99.97% availability requirement. Describe the challenges in performing a forensic investigation under these conditions. Consider how you would resolve these challenges.

Challenges:

- **Limited downtime for forensic data collection**: A system with a 99.97% uptime requirement allows minimal service interruptions.
- **Risk of disrupting critical business operations**: Investigations must not interfere with essential business processes.
- **Ensuring evidence integrity**: Live forensic methods must be used without altering or corrupting data.

Solutions:

- **Use live forensic techniques**: Collect volatile data while the system remains operational.
- **Implement forensic readiness strategies**: Pre-configure forensic logging and monitoring to streamline evidence collection.

- **Conduct investigations during maintenance windows**: Perform major forensic tasks during scheduled downtime.
- **Use non-intrusive forensic tools**: Leverage tools designed to extract data without impacting system performance.