ADAMA SCIENCE AND TECHNOLOGY UNIVERSITY

School of Electrical Engineering and Computing

Department of Software Engineering

Course: Digital Forensic

Individual Assignment

Student Name: Ameha Seyoum

ID: UGR/22559/13

Date: March 9, 2025

Submitted to: Dr. Dereje Regassa

Table of Contents

CH4: Exercise Answers – 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:

1. **Maximizing the usefulness of digital evidence** – Digital investigations rely on strong, reliable evidence to uncover security incidents, identify attackers, and support legal cases. By ensuring readiness, organizations can collect and preserve digital evidence efficiently before incidents occur, making investigations smoother and more effective.

2. **Minimizing the cost of forensic investigations** – Without proper preparation, forensic investigations can be expensive and time-consuming, requiring extensive resources to recover and analyze data. A well-planned forensic readiness strategy reduces costs by having predefined processes, trained personnel, and appropriate tools in place.

These objectives are critical because they help organizations and law enforcement respond swiftly to cyber incidents while ensuring the integrity of the evidence. They also reduce downtime and financial losses associated with security breaches.

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

When identifying potential sources of digital evidence, several factors must be considered:

- **Relevance to the investigation** – The data must be directly related to the security incident being analyzed.

- **Integrity and reliability** – The evidence should be collected from trustworthy sources while ensuring it remains untampered.

- **Storage location** – Data can be found in different locations such as local hard drives, network storage, cloud servers, or mobile devices.

- **Log and audit trails** – System logs, firewall records, and intrusion detection system (IDS) logs can provide critical information about security incidents.

- **Legal and compliance requirements** – Organizations must follow legal guidelines on what data can be collected and how it should be handled.

- **Volatility of data** – Some evidence, such as RAM data or network traffic, is volatile and can be lost if not captured immediately.

By carefully considering these factors, forensic investigators can ensure they collect the most relevant and admissible evidence for analysis.

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

Forensic tool testing ensures that forensic software and hardware perform correctly and reliably when collecting and analyzing digital evidence. The goal is to verify that tools produce accurate, repeatable, and legally admissible results.

Function-Driven Testing Methodology:
This testing approach evaluates whether a forensic tool performs its intended functions effectively under controlled conditions.

Advantages:

- ✓ Ensures tools meet legal and technical requirements.
- ✓ Identifies bugs or vulnerabilities in forensic software.
- ✓ Provides consistency and accuracy in evidence collection.
- ✓ Helps in verifying the effectiveness of forensic processes.

Disadvantages:

- It may not fully replicate real-world scenarios.
- Focuses only on specific tool functions rather than broader system interactions.
- Time-consuming and requires specialized expertise to conduct tests.

Despite its limitations, function-driven testing is essential to maintaining the credibility of digital forensic investigations.

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, my approach would include:

1. **Establishing a Digital Forensics Policy** – Defining procedures for evidence collection, storage, and investigation processes.
2. **Implementing Logging and Monitoring** – Ensuring all critical systems generate logs that are centralized and protected from tampering.
3. **Access Controls and Authentication** – Strengthening security with role-based access control (RBAC), multi-factor authentication (MFA), and privilege management.
4. **Incident Response Integration** – Creating an incident response plan that aligns with forensic best practices.
5. **Forensic Data Storage** – Setting up secure, tamper-proof storage for evidence with encryption and access logging.
6. **Regular Testing and Training** – Conducting periodic forensic readiness drills and training staff on incident handling and forensic tools.

By following these steps, the enterprise will be better prepared to conduct forensic investigations efficiently.

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

A well-structured digital investigation process involves:

- **Evidence Collection:** Identifying, preserving, and securing relevant digital evidence without altering its integrity.

- **Chain of Custody Maintenance:** Documenting every step of evidence handling, including who accessed it and where it was stored.

- **Data Recovery:** Using forensic tools to retrieve deleted or hidden files from storage devices.

- **Log Analysis:** Examining system logs to trace unauthorized access, malware activities, or system changes.

- **Forensic Imaging:** Creating bit-by-bit copies of storage media for analysis while preserving original data.

- **Report Preparation:** Documenting findings, analysis methods, and conclusions in a legally admissible format.

- **Court Presentation:** Presenting digital evidence in a clear and concise manner if required for legal proceedings.

These procedures help maintain the integrity and credibility of a digital investigation.

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.

A system with a **99.97% availability requirement** means it can only afford **about 2.6 hours of downtime per year**, making forensic investigations extremely challenging.

Challenges:

- **Minimal Downtime Allowed:** Taking the system offline for analysis may disrupt critical business functions.

- **Volatile Evidence:** Some digital evidence, such as memory logs and network traffic, can be lost if not captured immediately.

- **Data Integrity Risks:** Live forensics increases the risk of altering evidence.

- **Legal and Compliance Concerns:** The investigation must comply with industry regulations and avoid violating privacy laws.

Solutions:

1. **Perform Live Forensics:** Use tools to collect volatile data (RAM, active connections) without shutting down the system.

2. **Use Remote Logging and Monitoring:** Enable real-time logging to capture evidence before incidents escalate.

3. **Establish a Parallel System:** If feasible, switch operations to a backup system while investigating the primary system.

4. **Automate Evidence Collection:** Deploy forensic tools that automatically log and store critical system activities.

5. **Collaborate with Incident Response Teams:** Work closely with security teams to conduct forensic investigations without disrupting operations.

By implementing these solutions, organizations can balance forensic needs with business continuity requirements.