**A close-up of a logo

Description automatically generated**

**Course: CYB304**

**IT Security Forensics  
(Canadian Context)**

**Lab 3: Data Acquisition**

**Instructor:**

**Muhamma Saleem**

**Student Name: Olushola Enoch Bayode**

**Student ID: 23077087**

**Section: 3rd Semester**

A screenshot of a computer

AI-generated content may be incorrect.

**A screenshot of a computer program

AI-generated content may be incorrect.**

**A screenshot of a computer

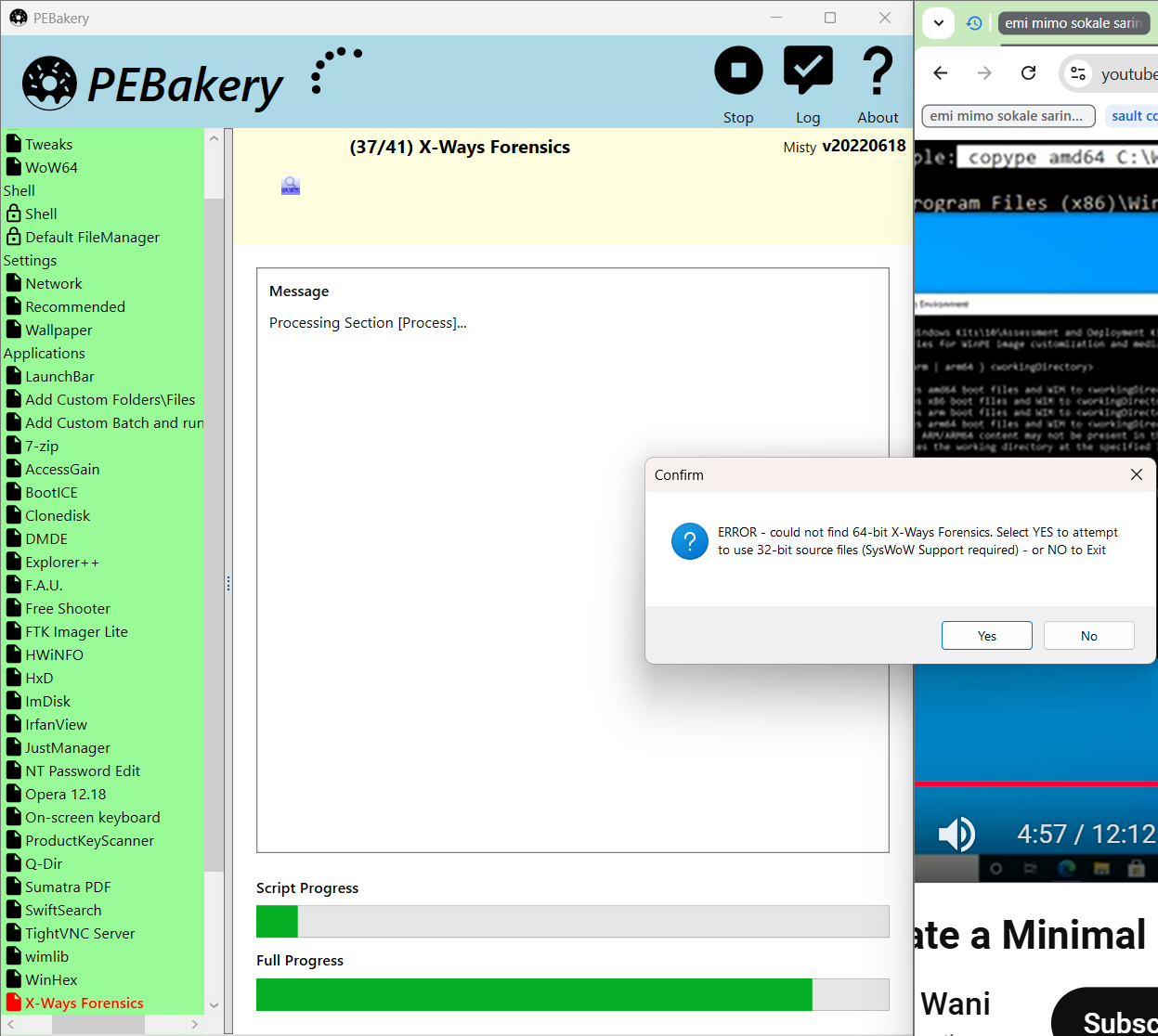
AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

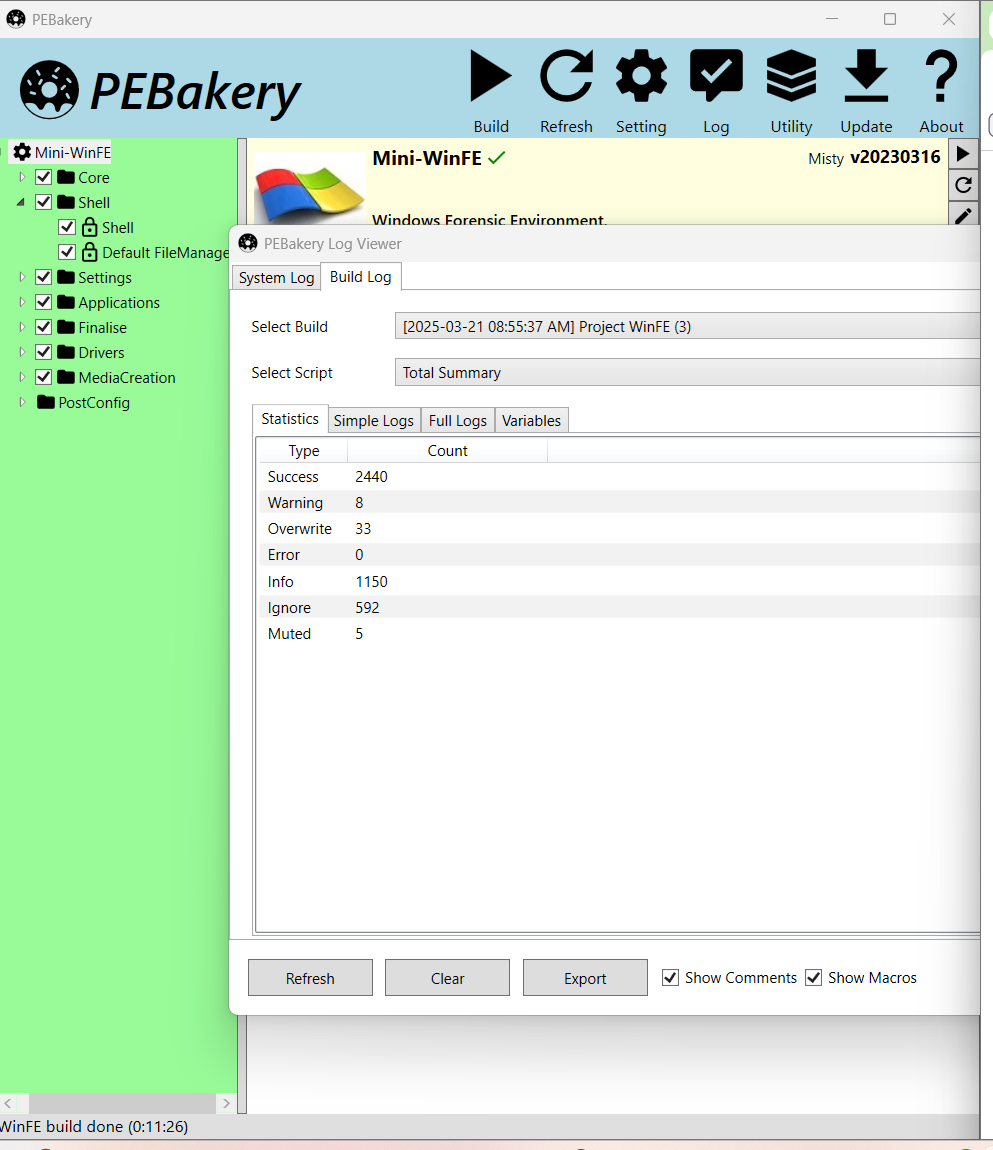
****

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

****

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

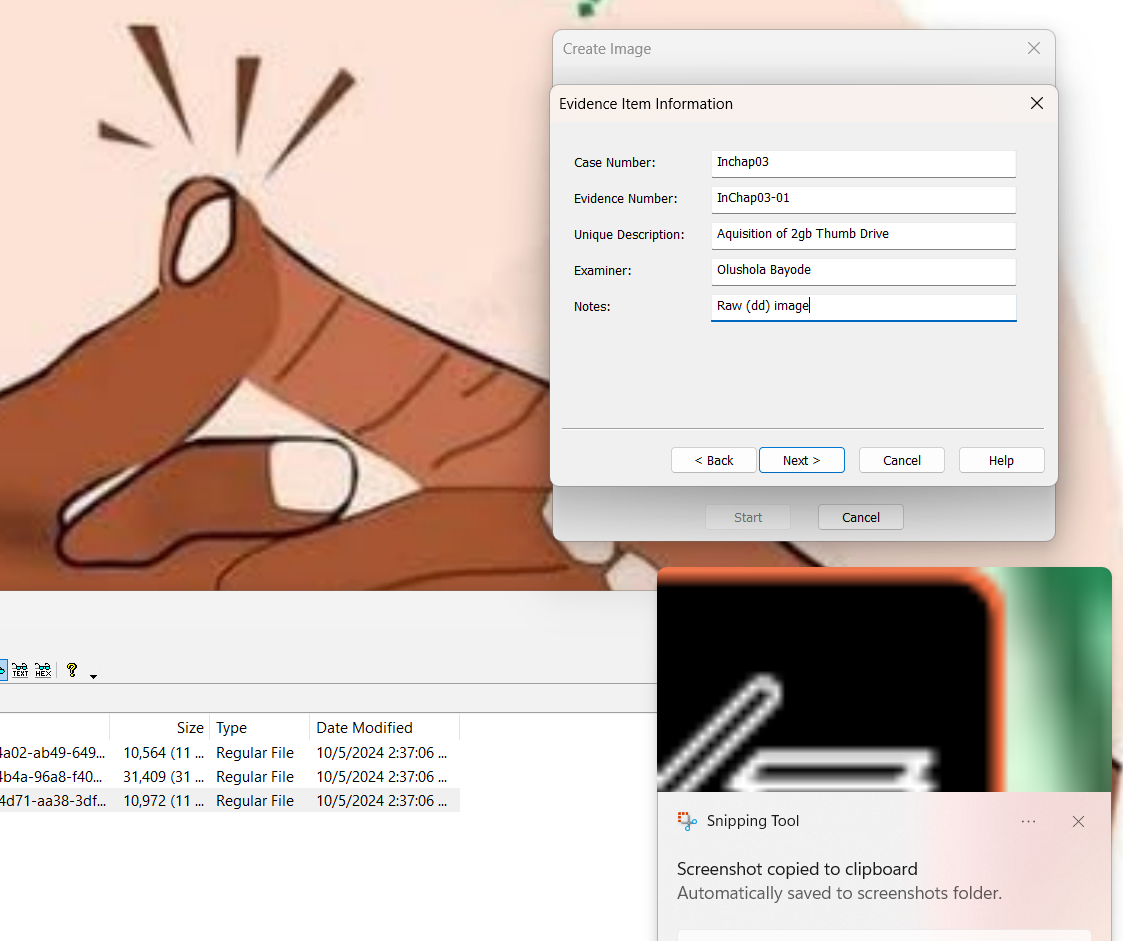
AI-generated content may be incorrect.**

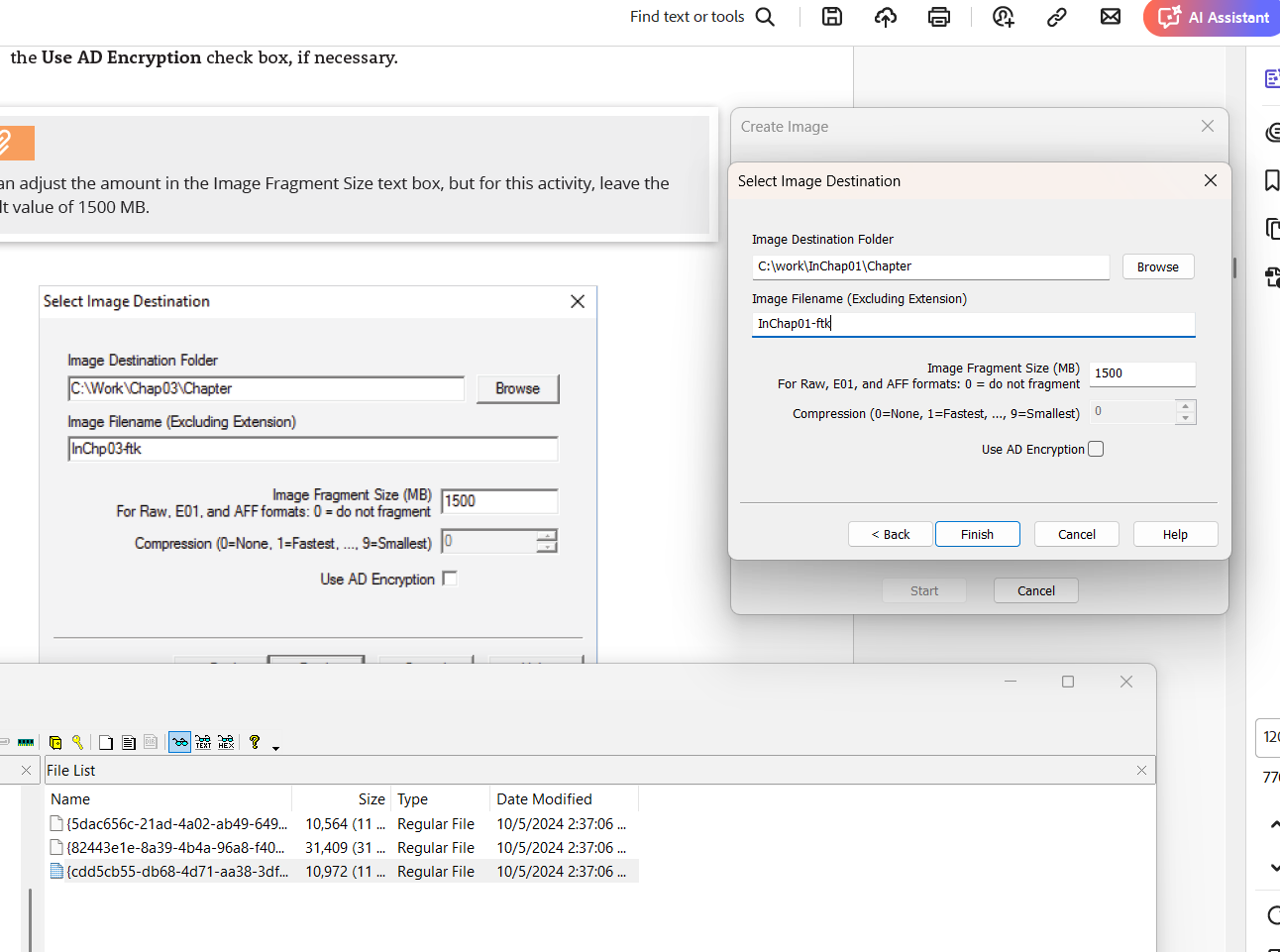
**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

****

****

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

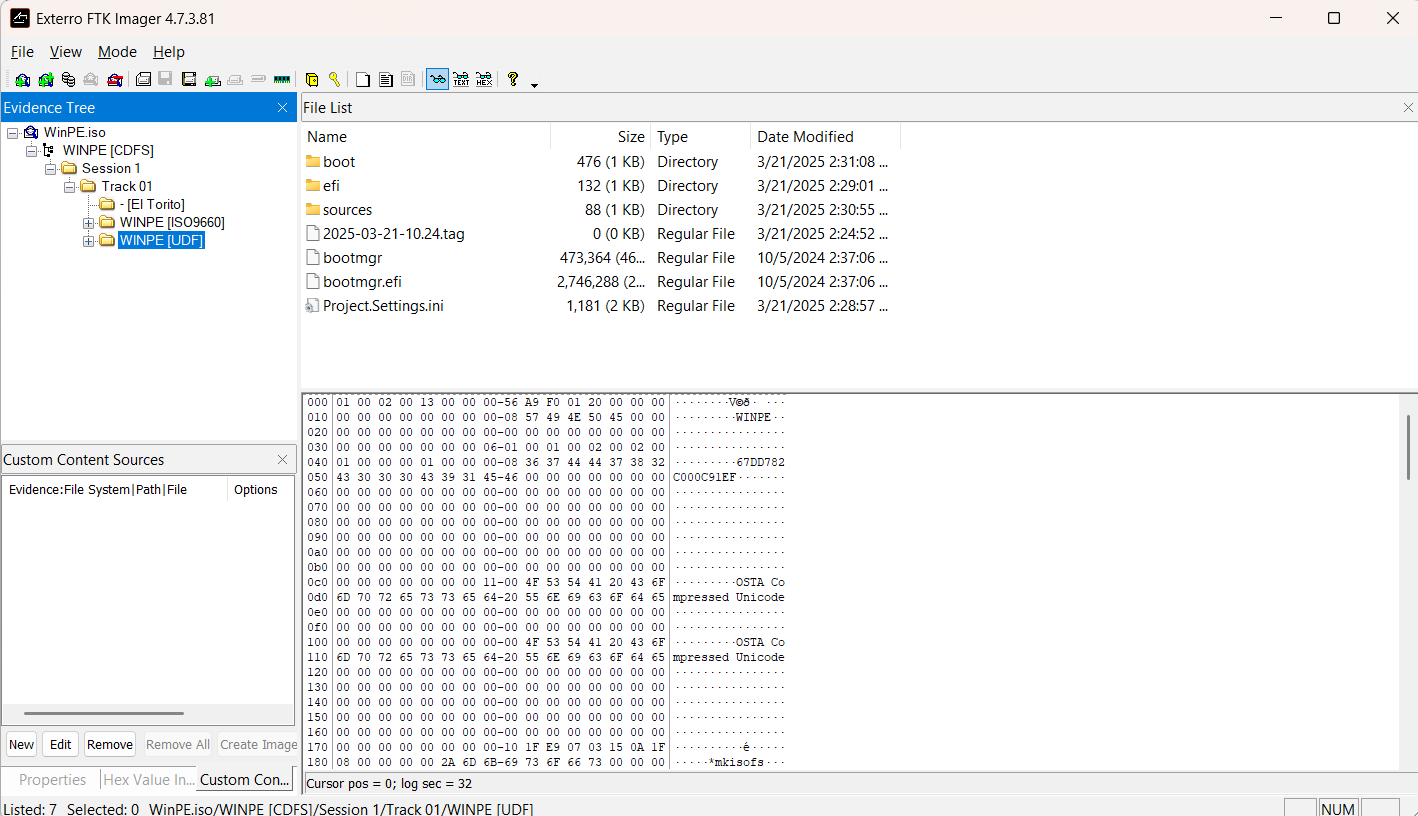
AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

****

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer program

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.**

A screenshot of a computer

AI-generated content may be incorrect.

**Activity 2-1**

Based on your requirements for two new Windows workstations and one Windows laptop, I've compiled a list of recommended hardware and software components, including estimated costs. The specifications focus on processor speeds, RAM, internal disk storage, and monitor types. Additionally, each system includes the operating system, an office suite, and two digital forensics tools.

1. Workstation 1

*Hardware:*

* Processor: Intel Core i9-12900K (3.2 GHz, 16 cores) – Approx. $600
* RAM: 32 GB DDR5 – Approx. $200
* Storage: 1 TB NVMe SSD – Approx. $150
* Monitor: 27-inch 4K UHD – Approx. $400

*Software:*

* Operating System: Windows 11 Pro – Approx. $200
* Office Suite: Microsoft Office 365 Business Standard – Approx. $150/year
* Digital Forensics Tools:
  + Magnet Axiom – Pricing varies; contact vendor for details
  + Wireshark – Free

2. Workstation 2

*Hardware:*

* Processor: AMD Ryzen 9 5950X (3.4 GHz, 16 cores) – Approx. $650
* RAM: 32 GB DDR4 – Approx. $170
* Storage: 1 TB NVMe SSD – Approx. $250
* Monitor: 27-inch 4K UHD – Approx. $430

*Software:*

* Operating System: Windows 11 Pro – Approx. $250
* Office Suite: Microsoft Office 365 Business Standard – Approx. $150/year
* Digital Forensics Tools:
  + X-Ways Forensics – Licenses start at $1,339
  + Velociraptor – Free

3. Laptop

*Hardware:*

* Processor: Intel Core i7-11800H (2.3 GHz, 8 cores) – Approx. $1,500 (including other components)
* RAM: 16 GB DDR4
* Storage: 512 GB NVMe SSD
* Monitor: 15.6-inch Full HD display

*Software:*

* Operating System: Windows 11 Pro – Approx. $200
* Office Suite: Microsoft Office 365 Business Standard – Approx. $150/year
* Digital Forensics Tools:
  + EnCase Forensic – Pricing varies; contact vendor for details
  + Wireshark – Free

Notes:

* Prices are estimates and may vary based on vendors and configurations.
* Some digital forensics tools offer free versions or trials; it's advisable to contact vendors for exact pricing and licensing options.
* Ensure compatibility of all hardware components before finalizing purchases.

This list provides a foundational setup for workstations and a laptop tailored for digital forensics tasks, balancing performance and cost.

**Activity 2-2**

Developments in the area of digital forensics are a constant process, with more and more certifications being introduced to keep up with all the new and emerging challenges in cybersecurity. One of the latest certifications that have been launched is the GIAC Experienced Forensics Examiner (GX-FE) which has become the standard for digital forensic examiners worldwide. It was introduced on September 17, 2024.

Certification Information: GIAC Certifications is the provider of the GX-FE certificate which is also a big name in the department making their efforts in skill sets in cybersecurity, through certification work be conspicuous and hands-on certification engagements be intensive. As one of the SANS Institute's subsidiaries, the organization is a key educational center in cybersecurity, and their most famous achievement is the courses and certifications in the field of cybersecurity. However, they also provide cybersecurity awareness content for beginners, which is the addition of the content added here.

Certification Backing: While the endorsement details for the GX-FE certification are not good enough in the given information GIAC Certifications along with the SANS Institute are well-known and respected in the cybersecurity industry. The governments of many countries are encouraging people to choose their courses and are constantly emphasizing the achievements of this institution. And also, former students of this school have always confirmed the high quality, also mentioning the strict regulations that the program adheres to.

Duration of Collaboration: The SANS Institute, the corresponding organization of GIAC Certifications, started operations in 1989. It has been an influence in the field of cybersecurity education, over time they have built such a large catalog of programs for professional skills development and knowledge improvement.

Certificate: The GX-FE certification is a course that has a special focus on advanced skills in digital forensic investigation and especially how to accurately reconstruct a system once an incident occurs. The program is an adaptation of real-world forensic examiner scenarios, and students need to handle this realistic situation well to succeed. Here, candidates need to be acquainted with process modification and how to detect anomalies that are an indication of tampering.

In conclusion: The rise of the GX-FE certification by GIAC indicates the changeability of digital forensics and the perpetual attempts to provide workers with the needed skill to beat complicated cybersecurity troubles. Considering the SANS Institute's long-standing status since 1989, the GX-FE certification will turn out to be quite a valuable asset for those looking for new knowledge and skills in digital forensic examinations.

[**https://www.giac.org/certifications/certified-forensic-analyst-gcfa/**](https://www.giac.org/certifications/certified-forensic-analyst-gcfa/)

**Activity 2-3**

**Disaster Recovery Plan for Apex Digital Forensics Lab**

1. Introduction Apex Digital Forensics Lab is the place to visit if you are looking for a seamless digital forensic investigation for your law enforcement client or the resources for your corporate clients. The Disaster Recovery Plan (DRP) is a document that specifies the procedures for data restoration, system recovery, and operational continuity, in case of disasters such as fire, cyberattacks, hardware failure, or natural disasters.

2. Backup Strategy

Daily

Backups: Stuff like case files, forensic images, as well as logs and system configurations are constantly backed up to a secure network-attached storage (NAS) device and a cloud-based forensic repository.

Weekly

Full Backups: A full system backup is taken out on every Friday and it is then stored in an external encrypted drive at the off-site facility.

Monthly

Archive: Forensic images and completed case files are moved to long-term storage, namely tape backups kept in a fireproof safe inside the premises.

Retention

Policy: Information related to active cases is saved for six months past-case resolution, while forensic images and reports are kept for five years as per the legal compliance requirements.

3. System and Software Inventory

On the local network, every workstation and server are configured according to the stringent guidelines. The next part is about the list of OSs and forensic tools that have been installed:

Workstations (Windows 11 Pro & Ubuntu 22.04 LTS)

Autopsy

FTK Imager

EnCase Forensic

Wireshark

X-Ways Forensics

Kali Linux (VM for penetration testing and malware analysis)

Forensic Servers (Windows Server 2019 & Ubuntu Server 22.04 LTS)

Relational database (MySQL/PostgreSQL) for case management

Secure file server (SFTP-based transfer for forensic images)

Log aggregation and analysis tools (Graylog, ELK Stack)

Network Devices and Security

Cisco ASA Firewall with access control lists (ACLs)

SIEM solution for intrusion detection (Splunk Enterprise Security)

Network traffic monitoring using Zeek (formerly Bro)

4. Recovery Process

* Initial Assessment: This IT staff will examine the scale of the injury and specify how strong the accident was.
* Infrastructure Restoration: Objective the number of networking and power lines that will still be connected even after turning off the other ones (if needed). ------seems unclear.
* System Recovery: Find the forensic servers and recover the data from them if no recent full backup is found.
* Reinstall the forensic workstations from the original installation media (which are stored in a secure cabinet within the IT room).
* Check the integrity and security of the recovered systems.
* Data Restoration: Download to the main hard drives forensic data recent from NAS or cloud backup during USB synchronization. Well in the meantime, remember to keep forensic images and logs untouched.
* Testing and Validation: Perform our tests to examine if there are other problems with the forensic tools and case management systems.
* Resumption of Operations: Coolest of all forensic work and sending confirming messages to all parties in the system with information about the completion of the recovery.

5. Backup Media and Storage Locations

Original installation disks: Stored in a secure cabinet in the IT room, labeled and cataloged.

On-Site Backup: NAS device in the system room, as the server has limited access to it,

Off-Site Backup: Encrypted external drives kept in a secure place 10 miles away.

Cloud Repository: Encrypted storage hosted by a third-party provider, secured with the input of a confirmation code received by the user's email and a regular addition of the password.

6. Roles and Responsibilities

IT Team: They implement the IT system and plan ideas about their security, and periodically update the network configuration.

Lead Forensic Analyst: Responsible for the parts of the forensic tools and case files that should be accessible post-recovery.

Lab Manager: Meeting the completion of the work recover efforts or problem solving and plan it and communication of the work and status updates to the stakeholders.

Compliance Officer: His duty is to adhere to the legislative and regulatory requirements.

7. Conclusion This DRP ensures the rapid recovery of Apex

Digital Forensics Lab in the event of a disaster. Regular testing,

documentation updates, and employee training will ensure preparedness and

minimal downtime.

**References**

NIST. (2018). *Guide to Enterprise Incident Response and Recovery* (NIST SP 800-184). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-184>

ISO/IEC 27031:2011. (2011). *Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity.* International Organization for Standardization.

<https://www.iso.org/standard/44374.html?utm_source=chatgpt.com>