Muhammad Izham Bin Norhamadi  
B032020039  
S2G1

**Task 1: Identifying Digital Evidence**

**Crime Scene**

A computer on a table

Description automatically generated with medium confidence

Time: 9:00 AM 26/3/2021

**Crime Scenario**

Aiman was working in a library using his laptop when he took a bathroom break. When he came back to his workstation, he finds that his laptop has been unlocked and his browser is now opening his email account. Various unknown devices and things was found next to his laptop. He finds that someone has been using his email to send unknown files to his contacts.

**Crime Scene Sketch**

**A white board with writing on it

Description automatically generated with low confidence**

**Notes on the Scene**

* Aiman’s email account was opened on the laptop (aiman667@gmail.com)
* Locked Apple phone was left on the scene
* Aiman’s wallet was presumably untouched
* Kingstone’s pendrive was left on the scene

**Task 2: Collecting and Preserving Digital Evidence**

**Digital Evidence at the Crime Scene**

A picture containing text, paper, accessory

Description automatically generated

Time: 9:05 AM 26/3/2021

A plastic bag on a table

Description automatically generated with low confidence

Time: 9:06 AM 26/3/2021

A picture containing text

Description automatically generated

Time: 9:07 AM 26/3/2021

Graphical user interface, application

Description automatically generated

Processes running during the time

Time: 9:15 AM 26/3/2021

**Task 3: Gathering and Securing Digital Evidence**

**Secure Container**

A picture containing floor, indoor, wall, trash

Description automatically generated

Time: 9:20 AM 26/3/2021

**List of Evidence**

Text

Description automatically generated

**Task 4: Documenting and Reporting**

First, identify the details of the case from Aiman. From the information gathered about the case, we identify that the crime committed was email phishing using Aiman’s email. Then, we secure the parameter of the crime scene. We can get a general overview of the crime scene with a sketch. We collect all the digital evidence in antistatic bags and tag them with serial numbers and dates. Next, we put all the digital evidence in a secure container and document them in evidence form. Then, we bring them to the Forensic lab to be analyzed. We bit-stream imaged the evidence before we can run tests to replicate the crime. Then, we analyze the files contained in the digital evidence. The information gathered will then be documented until further actions for the case.

Self-Review Questions

1. What is the importance information should be collected in the evidence custody form?

- To keep track and document evidence while making sure the evidence were untampered during the extraction process

2. Why an anti-electromagnetic bag is used in securing a hard disk?

- To make sure digital evidence were not affected by outside source

3. Once the evidence is stored in a safe box, what are the safety precaution an investigator must do to make sure the evidence is securely transferred to the investigation Lab?

- Make sure the safe box is handled by a trustworthy person while it was being transported