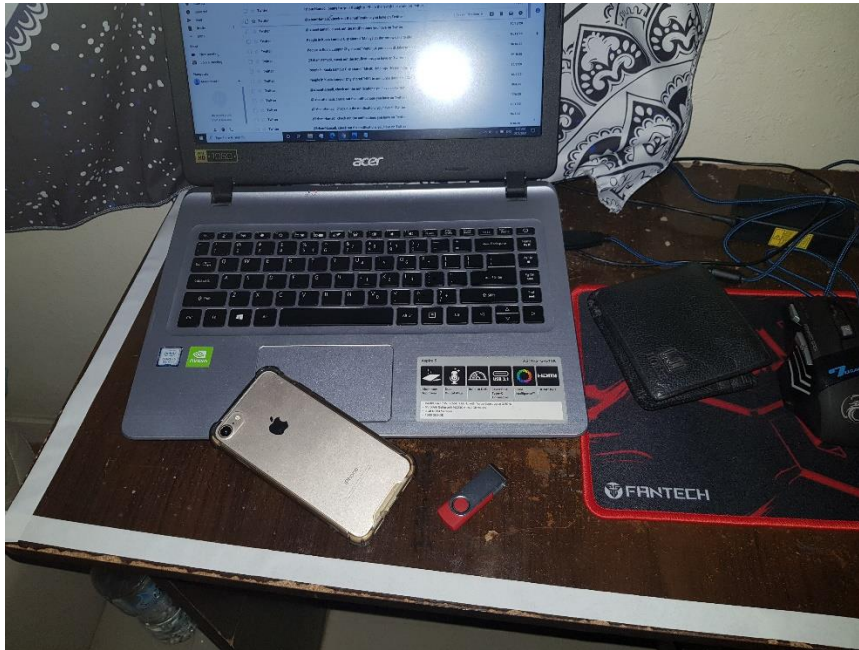


Muhammad Izham Bin Norhamadi  
B032020039  
S2G1

## Task 1: Identifying Digital Evidence

### Crime Scene

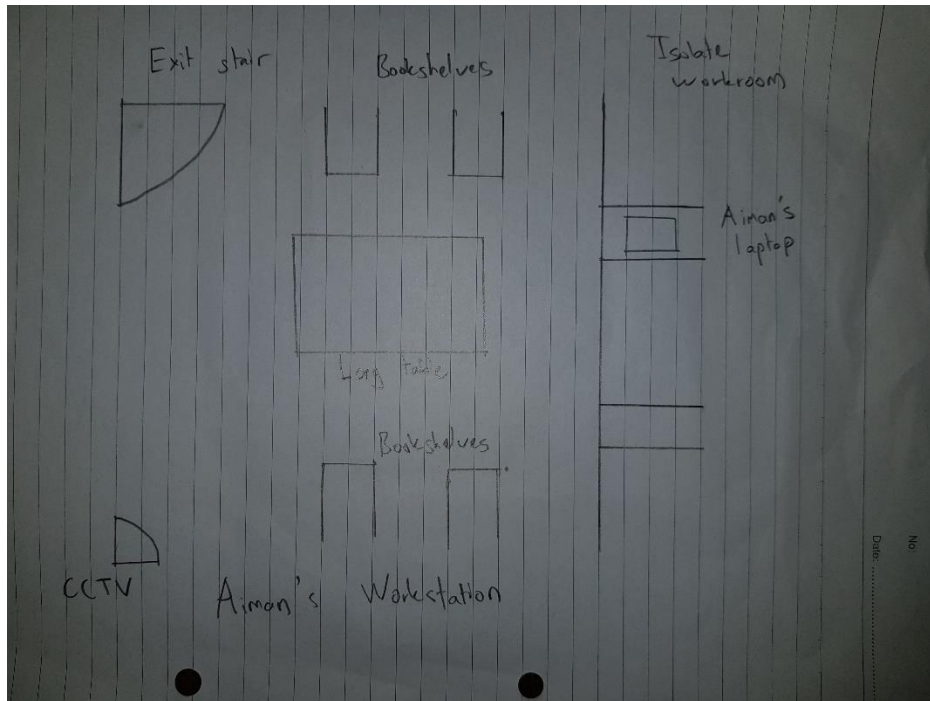


Time: 9:00 AM 26/3/2021

### 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



## 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

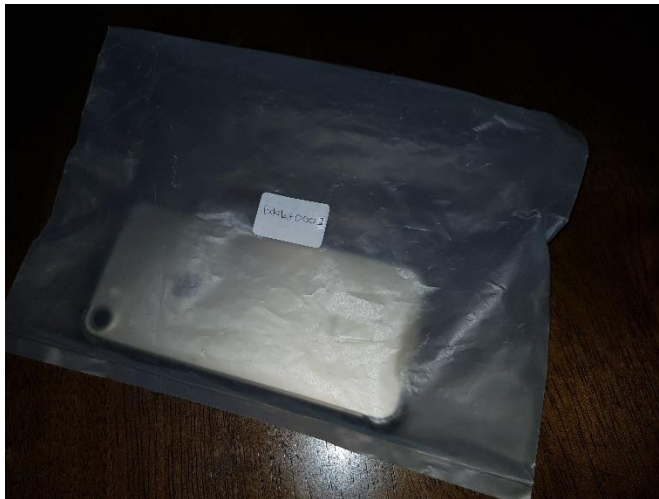
### Digital Evidence at the Crime Scene



Time: 9:05 AM 26/3/2021



Time: 9:06 AM 26/3/2021



Time: 9:07 AM 26/3/2021

Task Manager										
File Options View										
Processes Performance App history Startup Users Details Services										
Name	Status	21% CPU	70% Memory	53% Disk	0% Network	1% GPU	GPU engine	Power usage	Power usage tr...	
Runtime Broker		2.0%	3.6 MB	1.0 MB/s	0 Mbps	0%		Low	Very low	
Google Chrome (20)		1.7%	833.4 MB	0.3 MB/s	0.1 Mbps	0%	GPU 0 - 3D	Low	Very low	
Search		2.3%	138.7 MB	0.2 MB/s	0 Mbps	0%	GPU 0 - 3D	Low	Very low	
System		0.6%	0.1 MB	0.2 MB/s	0 Mbps	0%		Very low	Very low	
Lightshot (32 bit)		0.4%	2.8 MB	0.2 MB/s	0 Mbps	0%		Very low	Very low	
Antimalware Service Executable		3.5%	267.0 MB	0.1 MB/s	0 Mbps	0%		Low	Very low	
Task Manager		1.3%	25.0 MB	0.1 MB/s	0 Mbps	0%		Low	Very low	
Microsoft Content		0.2%	1.8 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low	
LocalServiceNoNetworkFirewall ...		0%	4.0 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low	
Windows Explorer		0.6%	42.0 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low	
Start		2.6%	24.1 MB	0.1 MB/s	0 Mbps	0%	GPU 0 - 3D	Low	Very low	
Desktop Window Manager		1.8%	60.1 MB	0.1 MB/s	0 Mbps	0.3%	GPU 0 - 3D	Low	Very low	
Service Host: UtcSvc		0.1%	10.3 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low	
Runtime Broker		0.4%	3.4 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low	
Service Host: ContentIndexing Ser...		0%	3.0 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low	

Processes running during the time

Time: 9:15 AM 26/3/2021

### Task 3: Gathering and Securing Digital Evidence

#### Secure Container



Time: 9:20 AM 26/3/2021

#### List of Evidence

EVIDENCE SEIZURE LIST					
CASE DETAILS					
CASE NUMBER	C0091				
PREMISE ADDRESS	Amans Workstation				
PREMISE OWNER / DEVICE OWNER NAME	Amans				
DATE & TIME	9:00 AM 26/3/2021				
DEVICE DETAILS					
NO	LABEL	TYPE	MANUFACTURER & MODEL	SIZE	HASH VALUE
1-	AS14514514K-P001	Laptop	Aspire 5		
2-	Exhibit0001	Perdrive	Kingsbone		
3-	Exhibit0002	Wallet			
4-	Exhibit0003	iPhone	iPhone 12 mini		
PREMISE OWNER/DEVICE OWNER			OFFICER		
IC NUMBER	000401-14-0574		NAME	Izham	
DATE & TIME	9:00 AM 26/3/2021		DATE & TIME	10:00 AM 26/3/2021	

#### **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