Muhammad Izham Bin Norhamadi

No.: B032020039 Date:

Part A: Question 1

a) 1- Server access logs
- Contains information such as page requests and responses
- During an attack, records the direction of the attack

2- Server error logs
- The system logs suspicious activity in the network.
- Get a glimps of what we're dealing in the network

3-

b) - Identify the source of the email through ip address
- Analyze browsing activity before and after composing the email
- Identify address of the computer from which the email is originated
- Alternative in ease logs of servers aren't available.

c) 1- Identify and determine incident based on network indicators
2- Close way to the network
3- Isolate and preserve data, attempt to retrieve all volatile data with live acquisition
4- Acquire compromised drives make a forensic image
5- Examine data and compare to original instalation image using hash values
6- Analyze and investigate the data
7- Draw conclusion and presentation

Muhammad Izham Bin Norhamadi
B032020039

No.: Date:

Question 2

a) 1- Collection of too many irrelevant data and evidence to the case
2- Investigation takes a long time
3- Straining limited resources on investigation
4- Weak evidence and case when presenting to court

b) For example when investigating a case involving compromised data of a company, we would need to follow company's ethic on what data will be used as evidence without revealing sensitive data. In case of network attack, we might only need to look at the network logs to identify the case.

c) - Determine the scope of the data to collect to prevent from revealing sensitive data
- Follow company policy on the permitted location
- Requests permission before gathering evidence
- If investigation requires more evidence, request for court proceedings to investigate.

Muhammad Izham Bin Norhamadi

B032020039

No.: Date:

Part B Question 1

a) 1- Secure evidence by capturing live data on the ram then shutting down the system and collects the disk drive. ~~Secure the disk drive in anti-static bag and send to forensic lab~~

2- Secure the disk drive in anti-static bag and send it to forensic lab

3- Attach a write-blocker on the disk drive before connecting to computer to avoid manipulating data

4. Perform disk imaging on the drive using software such as ftk imager.

5 - Validate the image using hash values.

b) Let's say it is a file with png extension. Using software like Hex Editor check the headers of the file and compare it to the extension. If the header is not %PNG then the file extension was modified.

c) - Seeret.pdf has a correct pdf headers while Secret-Me.pdf does not.
- Edit the first 4 bytes of Secret-Me.pdf to 25 50 44 46 to match Secret.pdf headers.

d) 1- Brute force and dictionary attack to find the correct password. Example tools are Passper for ZIP file or PassFab for Microsof Word file.

2- Finding clues on the password using investigation tools such as Forensic Toolkit.

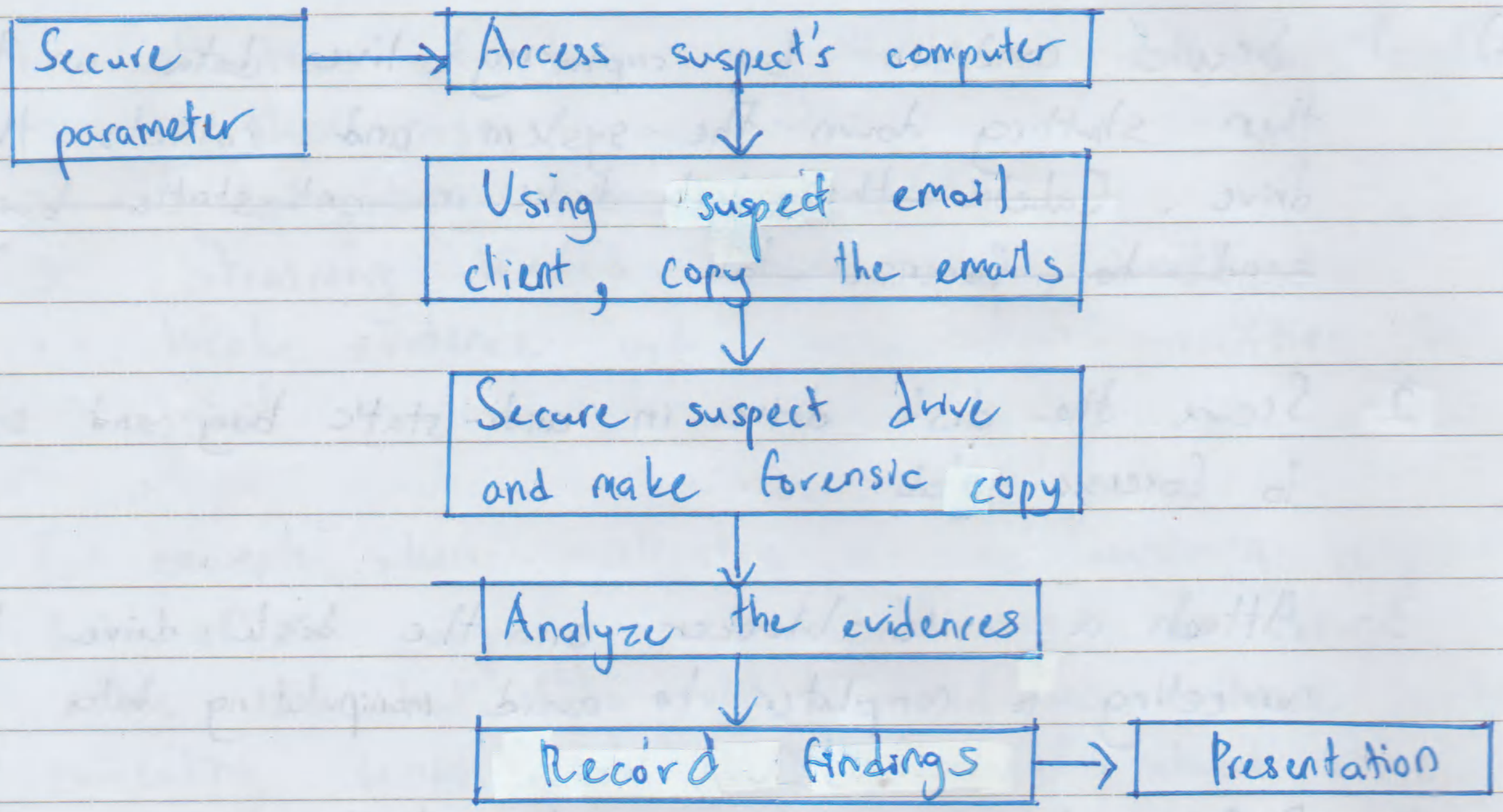
Muhammad Izham Bin Norhamadi

B032020039

No.: Date:

Question 2

a)



b) 1- First, secure the area so that the evidence won't get tampered.

2- To collect the evidence we need to access suspect's computer. Capture the ram data and copy it to removable drive. Make sure to not make any modification on evidence.

3. While suspect's session is still on, copy their emails to a removable drive.

4- Turn off the system and secure suspect's drive in anti static bag and send it to forensic lab. Then, create forensic images on all the evidences using ftk imager.

5- Analyze content of the emails. Then analyze the email headers such as Delivered-To:, Received: and Return-Path:. These will give us information on

where the emails originating from and it's destination. Example tool that can analyze email headers is MxToolBox. Then, we analyze suspect's image drive to find additional evidence such as deleted emails. We can analyze this image using Forensic Toolkit.

6- From the evidence analysis we record our findings on the case such as the reason for disclosing evidence, and the party involved in the crime.

7- Present our findings to the company.

c) - To focus the scope of the investigation on party involved in the crime and the amount of information disclosed
- To respect company's private information by collecting only the necessary data as evidence.