The company's I.T. (Robert Bob) has determined that their database has been compromised, and suspects it possibly being stolen.

Looking at the network log, there have been huge amounts of traffic coming from a particular employee: John Burg.

After examining the employee’s workstation, they have determined it to be infected. Not taking any chances, they decided to call us in to further investigate the situation.

We have a full warrant to seize all devices related to the investigation for forensic purposes. We also have permission to view any information contained in the seized devices.

The pre-investigation phase shows information regarding the clients, the situation, legalities, the agents involved, and equipment.

Arrived at the workstation.

Notice that a message above shows a log of your arrival.

As an investigator, it is important to log your activities during the investigation.

These logs are needed for reviewing and evaluating the case, as well as providing consistency with the evidence.

You can review these activities at the bottom of the screen.

Now that you have arrived, first thing to do is to take pictures of the workstation.

Make sure to take a good picture of where all the devices are positioned, along with its surrounding.

The next thing to do is check if the computer’s power is on, and if so, to unplug the network cable to avoid further attack from the internet.

Simply move the mouse over items of interest, and click on it to take action.

Since the computer's power is on, we will have to acquire the volatile data.

These are data that are lost once the computer is shut down.

The following are the kind of volatile data you will want to gather: system time, RAM, process information, network log, logged-on users’ information, and cached data (command history, clipboard, print spool files).

Please ensure you gather the data in the order of most to least volatile. The most volatile data are the ones that change consistently as time goes on, and the least being the ones that rarely change.

Before transferring the items, a Chain of Custody document must be made.

Think of the Chain of Custody document as a map of who/what/when/where/why of all the items from start to finish.

The labelling of items can depend on the department, and typically has a sequential number. In this case it is: the investigator’s initials, date, sequence number, sub-sequence number if attached from another item.

The Chain of Custody helps ensure that all the evidences gathered are genuine, and can be used at the court of law.

You can review the current Chain of Custody document at the bottom. Otherwise, we are ready to move on to the lab.

Now that you are back in the lab, the first thing to do is grab the devices we need to investigate.

(chain doc)

When doing digital forensics, it is best to avoid using the evidences directly when investigating. In this case, we will simply clone the disk drives.

There are various ways to clone a disk drive, and that depends on the investigation. For our purpose, we just need to create an image file.

An image file contains a replication of all the data written on the disk. Certain software can navigate through that data as if it were an actual disk drive.

(show cloner)

Simply click on the arrow icon to copy the drive to an image file.

With the image files, we can now begin our investigation.

When it comes to analyzing data, the good approach is to look for patterns. Perhaps some initial information to use for search.

In this case, we can use our initial information from the briefing - the IP address: 240.1.2.3.

In order to simplify the investigation, our software will only allow searches on flagged items. Our initial clue is the IP address: 240.1.2.3, this can be flagged from Network Log.

Once you have the IP address flagged in Network Log, you can then search for it in File Inspector. Other flagged items can show up in the other software.

Don’t forget to identify any malware from the flagged files in Malware Identifier.

When you feel you are ready to finish the investigation, you can click on Report and proceed from there.

This type of Trojan malware will extract and execute another type of malware to the computer. They are typically under a guise of a legitimate software, and when run, will execute its malicious command invisible to the user.

A Remote Access Trojan (RAT) is a type of malware that allows hackers remote access to the user’s computer. This malware is typically injected to a user’s computer by some means, such as a Trojan, or through a website.

Now that the malware is found along with its source, we can now report back to the client, and take the necessary steps to prevent future attacks from happening.