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.