# Cybrary Investigation Game

## Synopsis

The game will help the player get a general idea on the flow of investigation from start to finish. The game will provide a simplified process for data processing and analysis.

## Game Flow

The game will have three phases: Pre-Investigation, Investigation, Post-Investigation.

### Pre-Investigation Phase

The game begins with having the player type in a name and initials. This information is used when displaying the log of the player’s activities during the investigation.

Once the player has typed in a name and initials, the game will display the briefing: client/company, location, objectives, initial details from the company’s I.T., devices to investigate, tools provided, legal info, search warrant.

### Investigation Phase

#### Photography

The player can look around the workstation, and take photos. Points are awarded based on the visibility of the devices.

When the player is finish, they can click on the next button to proceed to the next activity. A log of the activity is displayed.

#### Check the Computer Power/Network State

For the purpose of demonstrating how to acquire volatile information, the computer’s power state will always be on.

The monitor’s power indicator will be blinking to indicate that it is in sleep mode.

The player can look around the workstation, and interact with the mouse. Interacting with the mouse (by moving it) will awake the monitor, verifying that the computer is on.

Once the monitor is active, the OS desktop is displayed indicating that the computer is not locked.

From here, the player can interact with the network cable (visible from the screen) to unplug it from the computer.

The player can also click on the camera icon to photograph the monitor.

The player can click on the next button to proceed. Points are awarded for the actions taken: checking power state, unplugging network cable, photographing monitor.

#### Volatile Acquisition

The display changes to the OS desktop display of the computer. This is a mock version of Windows OS.

The game will show the type of device the player will use to store the data.

The player is given several options to extract various volatile information. They will need to determine the order of operations based on their volatility.

Each option will demonstrate how it is collecting the data via an execution of a software or through a secured command shell.

Each action is documented on a list that the player can review.

Points are awarded based on the correct order of operations.

The following are the order of volatile information from highest to lowest:

* System time
* Process information, RAM, opened files, service/driver info
* Network info
* Logged-on users
* Command history, clipboard, print spool files

#### Acquisition of Devices

The player is now tasked to list out the items to secure and transfer to the lab.

The player can look around the workstation, and interact with all the computer peripherals displayed.

Clicking on each component will display it with further detail. The player can confirm to acquire it, or back out to select another peripheral.

Acquiring the peripheral will display its exhibit numbering on a list.

The player can click on the next button to further the progress.

Points are awarded based on the relevant peripherals gathered. Penalties for items unnecessary and/or not warranted (e.g. personal items).

The following are the list of peripherals:

* Desktop PC
* 2 Monitors
* 2 Monitor cables
* Network cable
* 3 Power cables
* Keyboard
* Mouse
* USB stick
* Speakers

The chain of custody info is shown: The person responsible for securing and transferring the peripherals.

#### Image Duplication

The chain of custody info is shown: The player is now in possession of the peripherals.

The display shows the player’s OS desktop with options to generate an image of the following storage device: hdd, usb stick.

Selecting either of the storage device, and clicking on the “copy” button will generate an image. A log of the activity is displayed.

The player can click on the next button to proceed.

#### Data Investigation