Cybrary Investigation Game

# Concept

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.

# Story

A software company called ABC suspects a possible breach of access to their database. Their I.T. department has analyzed their network log, and determined that a huge amount of traffic is coming from one particular workstation.

The player has been called in to investigate, analyze, and identify the breach from the compromised workstation. The I.T.

# 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, initials, and click on the next button - the game will display the briefing: client/company, location, objectives, initial details from the company’s I.T. department, devices to investigate, tools provided, legal info.

The player can click on the next button to proceed to the Investigation Phase.

## Investigation Phase

During this entire phase, the following are accessible at all times:

* *AI Guide* – An “AI” guide will walk the player through the process, introducing any functionalities that need to be explained. There will be an icon for the “AI” guide that the player can click to recall the current objective, along with any hints.
* *Activity Log* – After each action the player takes, a short activity log will show as a toast pop-up. These logs can be reviewed by clicking the log icon. These logs will be similar to how an investigator documents each step they take during an investigation.
* *Chain of Custody Log* – A Chain of Custody update will display during certain parts of the game. These will occur when the peripherals in custody are moved and examined. Just like activity logs, the player can review the Chain of Custody by pressing the Chain of Custody icon.

### Photography

The game will display the workstation to investigate in the ABC company’s office.

An “AI” guide will walk the player through the process: taking photos, and checking the network state.

Afterwards, the player can proceed to taking photos by pressing the camera icon. This will go into photo mode.

During photo mode, the player can move the camera around by pressing, then dragging the virtual analog stick. Pressing the “snap” icon will take a photo.

The player can exit the photo mode by pressing the exit icon. Once they exit, they can proceed to the next objective.

Points are awarded based on the visibility of all the devices.

A log of the activity is displayed.

### Check the Computer Power/Network State

The game view orients to show: the computer, monitor, keyboard, mouse, network cable.

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

The player can interact with the following:

* *Mouse* – clicking on the mouse will make it move around, this will wake the monitor, verifying that the computer is on.
* *Network cable* – clicking on the network cable will disconnect it from the computer.
* *Camera icon* – clicking on the camera icon will take a photo of the monitor. For the photo to be effective, the monitor needs to be awake.

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 while it is awake.

### Volatile Acquisition

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

A modal interface displays a grid arrangement of mock-up software that the player can use to copy volatile data.

Double clicking on each software will “execute” it. Once execution is complete, the player can proceed by pressing the capture icon. After captured the software is closed, and its icon will be checked off. Double clicking on it again will simply display what was captured.

The following are the software:

* *System Time* – opens a mock-up shell with a command (get-time), and displays time since 1/1/1970.
* *Process Extractor* – opens a dialog that displays a list of currently running programs and processes, along with its memory/cpu/network usage.
* *Network Info* – opens a mock-up shell with a command (net-stat), and displays network information, along with network traffics.
* *User Info* – opens a display of the user log info and credentials.
* *Cache Info* – opens a display for command history, clipboard, and print spool files.

Once all software is executed, the next button will appear. The player can click on this to proceed.

Points are awarded based on the order of volatility 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 game view goes back to the display of the workstation with the entire desktop visible.

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

Hovering the mouse cursor over the peripherals will highlight it, and display a tooltip of its name.

Clicking on the peripheral will display an interface that will display its description. 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 with the format: aaa/ddmmyy/nnnn/zz where:

* aaa – initials of the investigator (player).
* ddmmyy – date of seizure.
* nnnn – sequence number.
* zz – sub sequence number.

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 (aa/ddmmyy/0001/01)
* 2 Monitors (aa/ddmmyy/0002/01, 02)
* 2 Monitor cables (aa/ddmmyy/0003/01, 02)
* Network cable (aa/ddmmyy/0004/01)
* 3 Power cables (aa/ddmmyy/0005/01, 02, 03)
* Keyboard (aa/ddmmyy/0006/01)
* Mouse (aa/ddmmyy/0007/01)
* USB stick (aa/ddmmyy/0008/01)
* Speakers (aa/ddmmyy/0009/01, 02)

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

The chain of custody info is shown: The person responsible for keeping the peripherals secured.

During this activity, the player will be looking for keywords to use for search.

Items in search/logs/registry can be tagged with a red flag. Red flag indicates that the item is a threat. Some items that are flagged will contain a keyword that can be used in Search (a pop-up will indicate if there is one). These flagged items are displayed in the report summary for review.

The game will show that the images of the devices have been mounted, and ready for inspection.

The game displays the software that manages the investigation with the following options:

* *Project* – displays investigation detail much like in pre-investigation: investigator, scenario, etc.
* *Registry Settings* – shows a tree-view of the OS software registry much like regedit in Windows. Player can click on any of the selectable items, and flag it.
* *Process/Service Info* – Shows a list of software and processes that are running with stats obtained from captured volatile data: CPU/memory/network/disk usage. Clicking on an item will show a button to inspect the item. Inspecting the item will show its file location, and a button to flag it.
* *Network Log* – Shows a list of network traffic obtained from captured volatile data (mock-up of Window’s command netstats). Player can select an item to flag.
* *Search* – From here the player can select which mounted images to search from, and search. Clicking on the search field will show a dropdown of keywords to search. Once the player has selected a keyword to search, they can click on the Search icon to proceed. Once search is complete, the player can select a file from the result list. Selecting a file will view its content much like a hex editor. The player can also flag the selected file. Within the file’s content, the player can click on certain block to flag. Certain blocks can contain new keywords to use for search.
* *Email Viewer* – shows a tree view of the emails extracted from the email cache file found from the mounted image. From here, the player can view or flag an email. Flagging an email will include the attached file associated with it.
* *Malware Identifier* – displays a list of files that are flagged. Upon selecting a file, and clicking the scan button - a progress is displayed until it is complete. The result will show if there is, and what kind of malware is associated to the file. Files that have been scanned will be marked.
* *Report* – displays the current summary of the investigation, along with the list of flagged items. From here, the player can: unflag items, or click on Submit to conclude the investigation.

Points are awarded based on the valid red-flagged items, along with identifying files that have malware through Malware Identifier. Penalty for red-flagged items that are not valid.

Player can proceed by pressing the Submit button in the report section.

## Post-Investigation Phase

The game displays a full report of the investigation with the activity logs, and discoveries from Data Investigation.

Player’s total points are tallied and displayed.

Player can click on Finish to end the game.