IPAR

IPAR is a detective themed adventure game in which the player assumes the role of an investigator and collects evidence, answers questions, and draws conclusions as part of a simulated investigation. Players are guided through a series of scripted steps, allowing them to gain practical experience and draw their own conclusions by answering subject related questions. Files and weblinks can be linked to each question, allowing the instructor to provide a wealth of relevant resources to the player as they need them. Originally developed for entry level digital forensics classes in community colleges, IPAR is flexible and can be used to create cases covering virtually any subject material.

PLATFORM

IPAR was developed using the Windows Presentation Foundation and is compatible with any Windows computer running Windows 7 or newer with the .NET framework installed. The .NET version 4.5 is required to run this game.

INSTALLING IPAR GAME, EDITOR and READER:

IPAR Game, Editor and Reader are portable applications and do not require installation. All three programs will run when opened (or double clicked).

After downloading and saving the IPAR Game, creating a desktop shortcut is recommended for easy access.

SETTING UP THE TOOLS:

The exercises requires imaging and analysis tools on windows operating system.

Imaging Tool:

FTK imager lite version 3.1.1 is used for imaging phase of the general forensics game. This tool can be download from the access-data website. It is available for free and does not require installation.

Link: http://accessdata.com/product-download/digital-forensics/ftk-imager-lite-version-3.1.1

Analysis Tools:

For Dishonesty Case (General Forensics):

- **Autopsy**: Autopsy 4.0 version is used for the analysis phase of the game. The tool can be downloaded from the sleuthkit website. The tool is provided for free and requires installation.

http://www.sleuthkit.org/autopsy/download.php

For Financial Case (Linux Forensics):

- **Autopsy**: Version 4.0 is used for the analysis phase of the game. The tool can be downloaded from the sleuthkit website. The tool is provided for free and requires installation.

http://www.sleuthkit.org/autopsy/download.php

For Rhino Case (Network Forensics)

- **Wireshark:** Version 2.0.2 is used for network protocol and packet analysis. The can be

downloaded from WireShark website. The tool is provided for free and requires installation.

https://www.wireshark.org/#download

For Suspicious Employee Case (Windows Registry Forensics):

- **Registry Explorer by Eric Zimmerman** : Version 0.7.1.0 is used for exploring registry keys. The tool is provided for free. It is a portable tool and does not requires installation.
    - **Dependency:** Requires at-least Microsoft .net 4.6.
    - Available at https://ericzimmerman.github.io/
- **Event Viewer:** To view and filter windows event logs. It is a built-in tool, available with Windows OS.
- **Dcode:** Version 4.02a is used to convert the windows FILETIME data to Date & Time Value.
    - It is a portable tool and does not requires installation.
    - Available at:

http://www.digital-detective.net/digital-forensic-software/free-tools/

For Linux Incident Response Forensics case:

- Linux Virtual Machine is required for performing the steps required in the case.
- The compressed VM image of Ubuntu Virtual Machine is uploaded on the google drive.
- Extract the compressed VM image.
- The extracted folder will contain VMDK and OVF files. The OVF file can be imported by VMWare workstation or VMWare Fusion to create the Virtual Machine. Refer the

following article for more details:

https://pubs.vmware.com/workstation-9/index.jsp?topic=%2Fcom.vmware.ws.using.doc%2FGUID-DDCBE9C0-0EC9-4D09-8042-18436DA62F7A.html

IMP:

Create a folder named "Toolbox" on the desktop. The folder should contain shortcuts to launch applications.

- For tools requiring installation, create a shortcut after installation and place in 'Toolbox' folder.
- For portable tools, copy the executable files in C drive and create a shortcut. Place the shortcut in 'Toolbox' folder.

RECOMMENDED:

Recommendation for the convenience of students:

- Create a desktop shortcut for the IPAR Game.

- Create a folder named "Cases" on the desktop.

- Place the folders for each case in the "Cases" folder.

- Each case folder will contain the IPAR game file and evidence files.

- The IPAR Game file shortcut, the folder containing Case files, and the toolbox folder should be on the desktop.

Starting out

• When first launching the game, you will be presented with the option to load a case file. Cases for the game are contained within .ipar type files.

- The “Cases” folder on the desktop will contain folders for each case. The .ipar game file will be inside the related case folder.

• When a case has been loaded, a screen displaying a detailed description of the case will appear. If a save file from a previous session exists, the player will be given the opportunity to confirm their identity and pick up where they left off. Otherwise they can choose to start the case from the beginning.

Playing the Game

• The game interface is made up of a conspiracy board in the center of the screen with a tray of buttons along the bottom. Navigation buttons that change the active category line the left of the tray and system buttons that allow the player to save and exit the game are allocated on the right.

• Pieces of evidence populate the conspiracy board, each representing a question implemented by the instructor. Multiple choice questions require the player to select from a list of potential responses, and justification multiple choice questions are similar but require the player to explain their answer with text. Short response questions are open ended and require the player to write a text response. Submission questions open a file browser and prompt the player to choose a file to be submitted. Finally, messages are not actually questions but appear as emails on the board that contain messages that the player reads before progressing.

• Clicking one of these opens a dynamic interface that displays the question and provides the means that the player can use to submit their response and progress.

• Correctly responding to a question will advance the game by uncovering any connected pieces

of evidence that have not yet been revealed. As the game progresses, a web of connected pieces of evidence will be revealed.

• Revealing and completing all questions on a conspiracy board will unlock the next board provided that the current board is not the last populated board. Players can move between active boards by using the navigation buttons in the tray.

• Completing all categories in a case will add a new navigation button to the tray that allows the player to “close” the case and export a file to be submitted to their instructor for evaluation and grading.

• Clicking the save button will compress the current case into a single .ipar file, replacing the original that the case was originally loaded from. Progress will load from this file exactly where it left off.

• The exit button will return to the main menu of the game after giving the player the option to save their progress.