Forin Application Installation & Usage

All files can be found on the GitHub Repository.

Installation:

Download Virtual Machine (Recommended: VM Workstation Player v16 64-bit Windows)

Link: https://my.vmware.com/en/web/vmware/downloads/details?downloadGroup=WKST-PLAYER-1611&productId=1039&rPId=63655

Download Kali Linux 64-bit (Live)

Link: https://www.kali.org/downloads/

Setup Virtual Machine and Install Kali Linux (Using Workstation Player):

- Go To: Player > File > New Virtual Machine...
- Select Installer disc image file (iso) and select the Kali Live .iso image that was downloaded, Next.
- Select Linux (Debian 10.x 64-bit), Next.
- Specify a name and save directory, Next.
- Select the disk space you wish to set (recommended 20GB), Next.
- Select Finish.

This .iso *IS NOT* persistent. Please suspend the VM as shutting down will reset the state of the .iso back to default, losing all data.

- Once booted select 'Live (amd64)'
- Open terminal by right clicking the desktop and selecting 'Open Terminal Here '.
- Clone the GitHub with the following command:
  - *git clone https://github.com/Jiskey/Raspberry-Pi4-Forensics*
  - Note: do not use 'sudo' here as you may from problems navigating the folder through the GUI. (super user protection)
  - Note: This could also take a while as the repo contains 50Mb of test files.
- Navigate to Raspberry-Pi4-Forensics/ForinApp/ in the terminal.
  - *cd Rasperry-Pi4-Forensics/ForinApp*
- Run the Python 'build.py' file (all python commands are run in python3).
  - *sudo python3 build.py*
  - Note: Some tools are no longer installed as of Kali v2021.1. because of this, it could take a while to complete.

Trouble Shooting:

Though the app can work on other distributions of Linux, Kali has most of the tools installed and is a much easier deployment option. The 'build.py' file contains the commands to install the required packages and tools (refer to that file for command list), but still requires python3 to run. Kali comes with most of the packages and tools preinstalled including pyhton3 but if not, you can install it with the following command.

- *sudo apt-get install python3.7*

Usage:

Flowcharts of how the application is used can be found on GitHub under (/Docs/Usage FlowCharts):

Link: https://github.com/Jiskey/Raspberry-Pi4-Forensics/tree/main/Docs/Usage%20FlowCharts

Screenshots of the application can be found on GitHub (/Docs/Application Screenshots):

Link: https://github.com/Jiskey/Raspberry-Pi4-Forensics/tree/main/Docs/Application%20Screenshots

For help on what each of the tools do, you can refer to the help page within the application.

Test Files:

Test files unfortunately due to their size cannot be uploaded to GitHub. Because of this, google drive will have to be used.

Google drive link:
https://drive.google.com/drive/folders/1oRPjlfK6eSkUVrn9P_bo57VEbHDV1lm3?usp=sharing