User Manual

ForensicFacebook

This repository was made to finish a college task in the topic of Forensics. This program is used to do forensic analysis on the Facebook and Facebook Messenger app

Requirements

1. Android phone with SuperUser Access (Rooted)
2. USB Debugging is active
3. Both Facebook and Facebook Messenger are installed in the android phone
4. Python installed (preferably python ver 3.0)
5. ADB and latest USB Driver Installed (if it's not installed you can run the adbinstaller.bat while connected to the android phone)
6. Install the required modules (PySimpleGUI, pure-python-adb, and pillow. Tutorial to install are below)

Installation

If you have not installed ADB and the latest USB drivers, you can connect to your rooted android phone and run the adbinstaller.bat and follow the instructions to install it.

To install the required python modules, type these commands in the command prompt:

```
pip install PySimpleGUI
pip install pure-python-adb
pip install Pillow
```

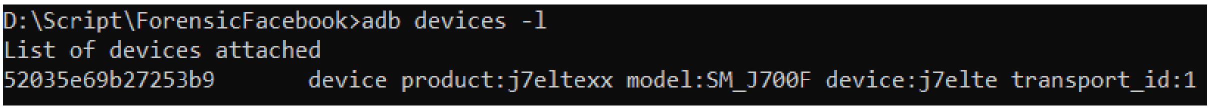
To install both Facebook and Facebook Messenger, you can find both apps in the Google Play Store in your android phone

Usage

After meeting all the requirements, you first need to connect your rooted android phone to your device. After that, make sure to allow USB Debugging on your rooted android phone after running adb on your device.

To run adb on your device, type in this command in the command prompt:

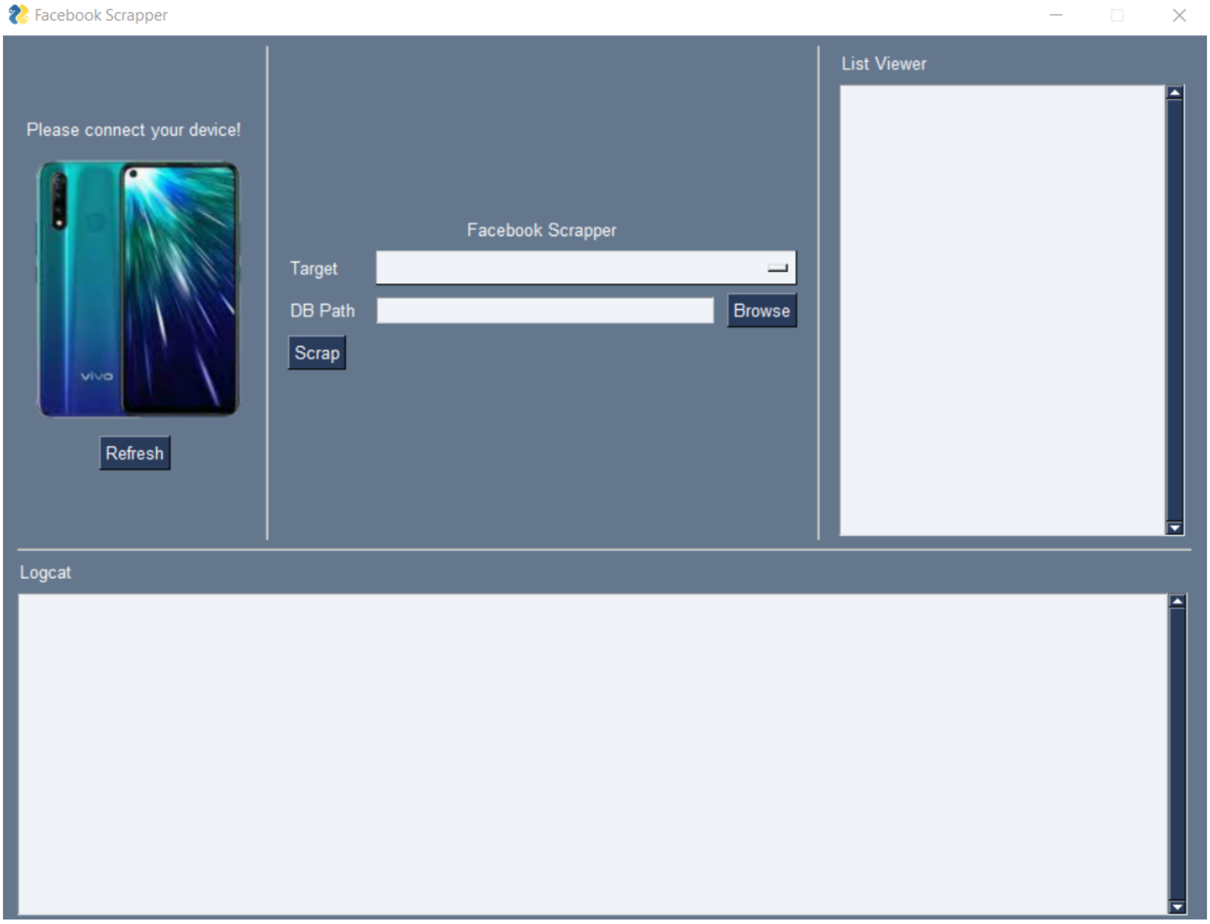
```
adb devices -l
```



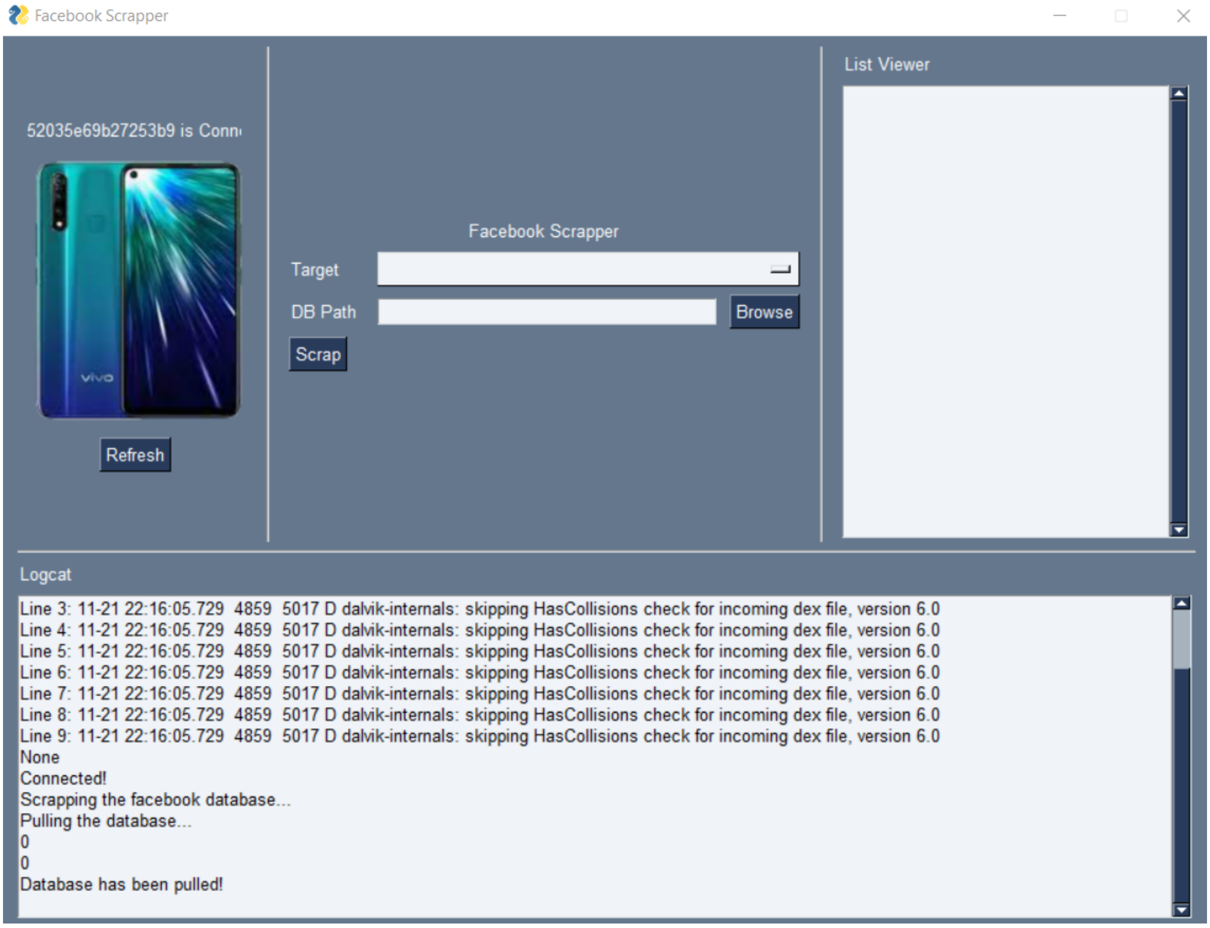
```
D:\Script\ForensicFacebook>adb devices -l
List of devices attached
52035e69b27253b9       device product:j7eltexx model:SM_J700F device:j7elte transport_id:1
```

If you see your rooted android phone in the output of the command prompt after putting in the previous command, you can finally start to run the main program by typing in this command in the command prompt of the program's directory:

```
python main.py
```

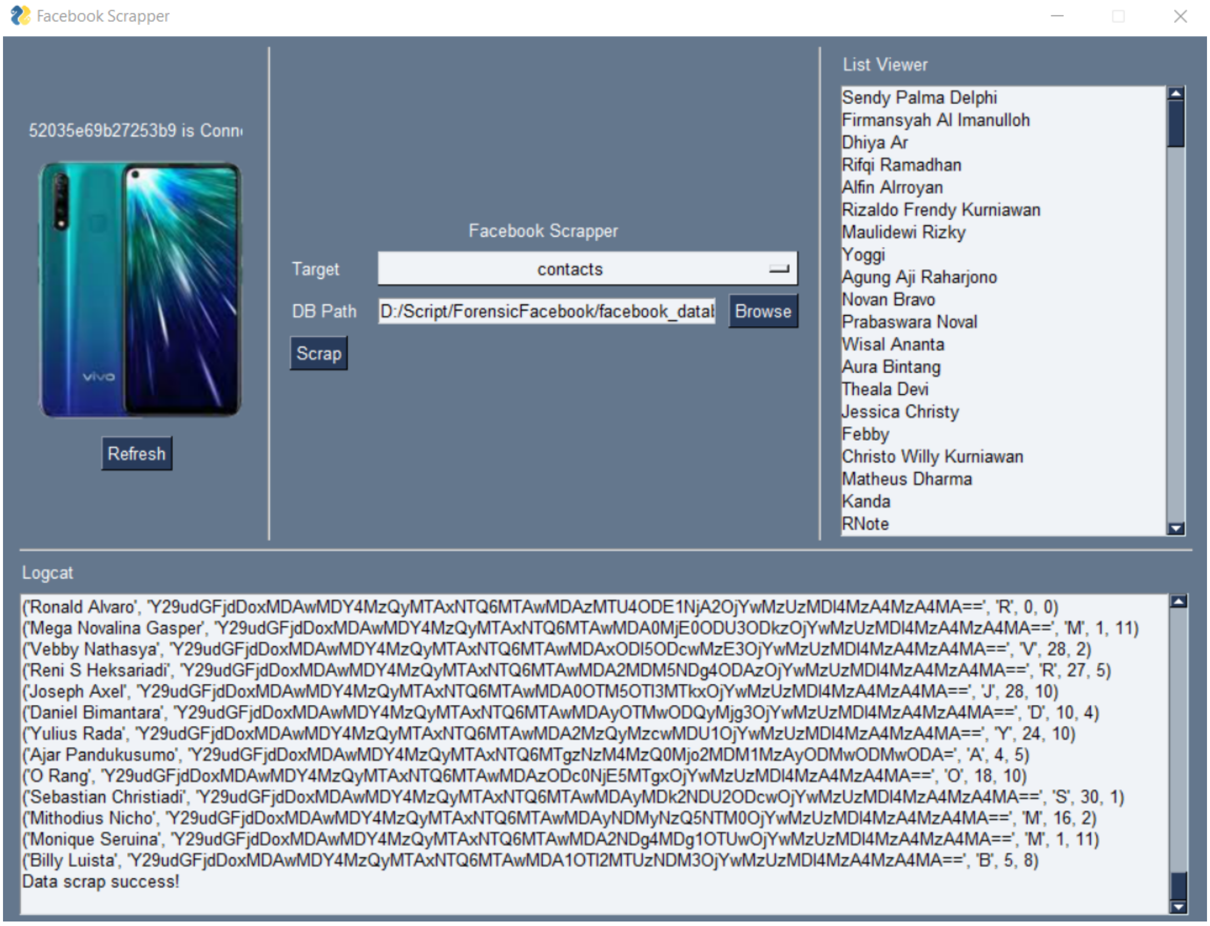


Once the program has started, you can make sure if your rooted android device has actually been connected through adb by clicking the "Refresh" button. This will also pull the facebook and facebook messenger database and put them in a folder named "facebook_databases" and "facebookM_databases" (note in order to pull the latest database folder, you need to make sure there are no folders named "facebook_databases" and "facebookM_databases" in the program directory before you click "Refresh").



```
Line 3: 11-21 22:16:05.729  4859  5017 D dalvik-internals: skipping HasCollisions check for incoming dex file, version 6.0
Line 4: 11-21 22:16:05.729  4859  5017 D dalvik-internals: skipping HasCollisions check for incoming dex file, version 6.0
Line 5: 11-21 22:16:05.729  4859  5017 D dalvik-internals: skipping HasCollisions check for incoming dex file, version 6.0
Line 6: 11-21 22:16:05.729  4859  5017 D dalvik-internals: skipping HasCollisions check for incoming dex file, version 6.0
Line 7: 11-21 22:16:05.729  4859  5017 D dalvik-internals: skipping HasCollisions check for incoming dex file, version 6.0
Line 8: 11-21 22:16:05.729  4859  5017 D dalvik-internals: skipping HasCollisions check for incoming dex file, version 6.0
Line 9: 11-21 22:16:05.729  4859  5017 D dalvik-internals: skipping HasCollisions check for incoming dex file, version 6.0
None
Connected!
Scrapping the facebook database...
Pulling the database...
0
0
Database has been pulled!
```

In order to analyse and show the data on the program, you first need to choose a target from the dropdown menu and choose a target. After choosing the target the program will ask you for the DB Path of the database that is related to the target. If you don't know which file is related, you can just choose a target and leave the DB Path field empty and click "Scrap", the program will tell you what database file it requires. Once you input the correct target and DB Path, the program will analyse and show you the relevant information regarding the target that was able to be pulled from the android database.



52035e69b27253b9 is Conn

Target: contacts

DB Path: D:/Script/ForensicFacebook/facebook_datal

Sendy Palma Delphi
Firmansyah Al Imanulloh
Dhiya Ar
Rifqi Ramadhan
Alfin Alrroyan
Rizaldo Frendy Kurniawan
Maulidewi Rizky
Yoggi
Agung Aji Raharjono
Novan Bravo
Prabaswara Noval
Wisal Ananta
Aura Bintang
Theala Devi
Jessica Christy
Febby
Christo Willy Kurniawan
Matheus Dharma
Kanda
RNote

```
('Ronald Alvaro', 'Y29udGFjdDoxMDAwMDY4MzQyMTAxNTQ6MTAwMDAzMTU4ODE1NjA2OjYwMzUzMDI4MzA4MzA4MA==', 'R', 0, 0)
('Mega Novalina Gasper', 'Y29udGFjdDoxMDAwMDY4MzQyMTAxNTQ6MTAwMDA0MjE0ODU3ODkzOjYwMzUzMDI4MzA4MzA4MA==', 'M', 1, 11)
('Vebby Nathasya', 'Y29udGFjdDoxMDAwMDY4MzQyMTAxNTQ6MTAwMDAxODI5ODcwMzE3OjYwMzUzMDI4MzA4MzA4MA==', 'V', 28, 2)
('Reni S Heksariadi', 'Y29udGFjdDoxMDAwMDY4MzQyMTAxNTQ6MTAwMDA2MDM5NDg4ODAzOjYwMzUzMDI4MzA4MzA4MA==', 'R', 27, 5)
('Joseph Axel', 'Y29udGFjdDoxMDAwMDY4MzQyMTAxNTQ6MTAwMDA0OTM5OTI3MTkxOjYwMzUzMDI4MzA4MzA4MA==', 'J', 28, 10)
('Daniel Bimantara', 'Y29udGFjdDoxMDAwMDY4MzQyMTAxNTQ6MTAwMDAyOTMwODQyMjg3OjYwMzUzMDI4MzA4MzA4MA==', 'D', 10, 4)
('Yulius Rada', 'Y29udGFjdDoxMDAwMDY4MzQyMTAxNTQ6MTAwMDA2MzQyMzcwMDU1OjYwMzUzMDI4MzA4MzA4MA==', 'Y', 24, 10)
('Ajar Pandukusumo', 'Y29udGFjdDoxMDAwMDY4MzQyMTAxNTQ6MTgzNzM4MzQ0Mjo2MDM1MzAyODMwODMwODA=', 'A', 4, 5)
('O Rang', 'Y29udGFjdDoxMDAwMDY4MzQyMTAxNTQ6MTAwMDAzODc0NjE5MTgxOjYwMzUzMDI4MzA4MzA4MA==', 'O', 18, 10)
('Sebastian Christiadi', 'Y29udGFjdDoxMDAwMDY4MzQyMTAxNTQ6MTAwMDAyMDk2NDU2ODcwOjYwMzUzMDI4MzA4MzA4MA==', 'S', 30, 1)
('Mithodius Nicho', 'Y29udGFjdDoxMDAwMDY4MzQyMTAxNTQ6MTAwMDAyNDMyNzQ5NTM0OjYwMzUzMDI4MzA4MzA4MA==', 'M', 16, 2)
('Monique Seruina', 'Y29udGFjdDoxMDAwMDY4MzQyMTAxNTQ6MTAwMDA2NDg4MDg1OTUwOjYwMzUzMDI4MzA4MzA4MA==', 'M', 1, 11)
('Billy Luista', 'Y29udGFjdDoxMDAwMDY4MzQyMTAxNTQ6MTAwMDA1OTI2MTUzNDM3OjYwMzUzMDI4MzA4MzA4MA==', 'B', 5, 8)
Data scrap success!
```