

Device Forensics

Assignment 1



February 22, 2024

William Vasilev

20093711

Introduction

In this assignment I am required to obtain and analyse an Android mobile device. I am required to install 3 apps and generate some data on the mobile device. I must then make a forensic copy of the device and examine the artefacts left by my chosen apps. For the android mobile device, I will be using an emulated Pixel 3A XL with Android 14 (API 34).

The apps I’m going to install are:

Social Media Application: X(Twitter)

Communications Application: Slack

Spyware Application: CamScanner

Imaging

Imaging is the process of creating a copy or snapshot of a storage device such as a hdd, ssd or other storage devices. This copy creates replicas of all files on the device. For my case I will be using imaging on the android emulator to be able to use the data on my own main system.

I chose to use adb pull as my imaging method because it allowed me to copy specific files and directories onto my main system when I couldn’t get other imaging methods to work.

Adb aims to preserve metadata and ensure original data is not modified or corrupted.

I had an error when first attempting to image the device.

A computer screen shot of a black and white screen

Description automatically generated

Instead, I had to pull each individual directory on the device for me to extract data onto my main system.

Here I pull the system directory.

A black background with white text

Description automatically generated

And here I pull the data/data directory.



I pulled these directories because I think they store the most important information relevant to my assignment.

A screenshot of a computer

Description automatically generated

Contents of System directory.

A screenshot of a computer

Description automatically generated

Preliminary Analysis

In this section I will find some data about the android device and show the procedure of how I got the data.

First I used the “adb devices” command to see the available android emulators active on my main system.

A black background with white text

Description automatically generated

From the screenshot you can see “emulator-5554” which is the android emulator I am running.

I used “adb shell” to access the shell of the emulator and the listed all services on the device.

A computer screen shot of text

Description automatically generated

Dumpsys battery shows information on the battery of the emulator.

A screenshot of a computer

Description automatically generated

Dumpsys wifi shows information on the wifi of the device.

A screenshot of a computer program

Description automatically generated

Dumpsys usagestats shows the usage in the last 24 hours.

A screen shot of a computer screen

Description automatically generated

Android Folders

A computer screen shot of a program

Description automatically generated

I tried to find the build properties of the device but I did not have root access so I had to use whoami to check what privileges I had and then I had to use su to gain root access.

A black screen with white text

Description automatically generated

Build properties

A screen shot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screen shot of a computer

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screen shot of a computer code

Description automatically generated

Found email connected to the device.

A screenshot of a computer

Description automatically generated

A screen shot of a computer code

Description automatically generated

Found where the settings of the device are stored.

A screenshot of a computer

Description automatically generated

Found Packages installed on the device.

A screen shot of a computer screen

Description automatically generated

Device Information

A screenshot of a phone

Description automatically generated

A screenshot of a phone

Description automatically generated

A screenshot of a phone

Description automatically generated

Twitter

I chose Twitter as my social media app to investigate because Twitter is a popular social media platform where users engage in public conversations. I will try to generate some messages on Twitter by direct messages and try to interact with posts to see if I can find that data on adb.

A screenshot of a social media post

Description automatically generated

App Information

Here is some information on Twitter from the emulator.

A screenshot of a phone

Description automatically generated

A screenshot of a phone

Description automatically generated

I found where Twitter was located.





Found what Twitter version was installed.

A black screen with white text

Description automatically generated

Found permissions.

A screen shot of a computer

Description automatically generated

Files, Directories and Databases

Found files belonging to Twitter.



A computer screen shot of white text

Description automatically generated

Found databases.

A screenshot of a computer

Description automatically generated

I pulled the Twitter directory onto my main system.

A black background with white text

Description automatically generated

From this I found a cookies file where it shows me the cookies of Twitter.

A screenshot of a computer

Description automatically generated

I searched through the databases in SQlite db browser.

A screenshot of a computer

Description automatically generated

Found ID’s in the databases.

A screenshot of a computer

Description automatically generated

I tried using sqlite in cmd prompt to retrieve some data from the databases.

A screen shot of a computer

Description automatically generated

Some databases were encrypted and needed a password to access.

A screenshot of a computer

Description automatically generated

Found more ID’s in Twitter.

A screenshot of a computer

Description automatically generated

Found access tokens.

A screenshot of a computer

Description automatically generated

Found preferred Language of the App.

A close up of a text

Description automatically generated

These are the dm’s I sent on Twitter.

A screenshot of a phone

Description automatically generated

And here is the DM I found.

A screenshot of a computer

Description automatically generated

I wasn’t able to retrieve the data on the other 2 dm’s but I found that the conversations were pending in the database.

A screenshot of a computer

Description automatically generated

Found the search queries I generated on the app.

A screenshot of a computer

Description automatically generated

Found what emojis are on Twitter.

A screenshot of a computer

Description automatically generated

Found account id of the Twitter account I created.

A screenshot of a computer

Description automatically generated

Slack

I chose Slack as my communications app to investigate because Slack is widely used in professional environments for team communication and collaboration. I joined a slack workspace and created messages in general chats and direct messages some users on the workplace. I also shared some files from Twitter onto Slack to see if I can find that information.

App Information

Here is the workspace I joined.

A screenshot of a phone

Description automatically generated

App information from the android emulator.

A screenshot of a phone

Description automatically generated

A screenshot of a phone

Description automatically generated

Found the Version of Slack that was installed.

A black background with white text

Description automatically generated

Found where Slack was located.

A black screen with white text

Description automatically generated

Found Permissions.

A screen shot of a computer program

Description automatically generated

Files, Directories and Databases

Found Files belonging to Slack.

A black screen with white text

Description automatically generated

Pulled the Slack files so I can investigate them on my main system.

A black background with white text

Description automatically generated

A white background with numbers

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Found device ID that was using Slack.

A close up of a phone number

Description automatically generated

I changed the debug.log file into txt format so I can see what was inside.



I pulled the txt file so I can view it.

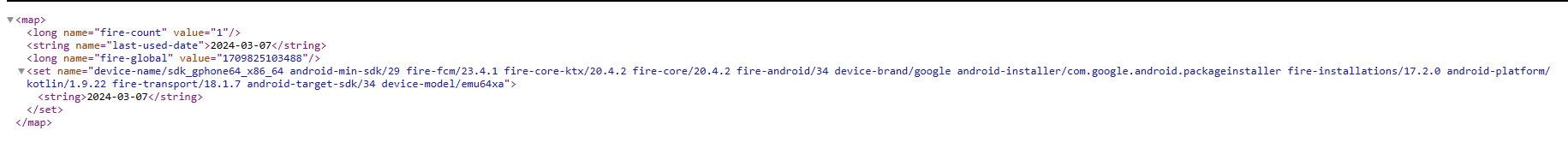


The file contained information about what was being done when the app was running.

A screenshot of a computer

Description automatically generated

Found dates on when Slack was last used.



Found email connected to the Slack account I created.

A computer code with black text

Description automatically generated with medium confidence

Found device ID of device using Slack.

A close up of text

Description automatically generated

Found last opened channel.

A close up of text

Description automatically generated

Found more information about the email connected to Slack.

A screenshot of a computer

Description automatically generated

CamScanner

I chose CamScanner as my spyware app because CamScanner is a hugely popular Android app that takes high quality photographs of documents, and it has been found to contain malware on the android version.

App Information

Some info on CamScanner from the emulator.

A screenshot of a phone

Description automatically generated

A screenshot of a phone

Description automatically generated

Found where CamScanner was located.

A black screen with white text

Description automatically generated

Found the version of the installed app.

A black screen with white text

Description automatically generated

Found permissions of the app.

A screen shot of a computer program

Description automatically generated

Files, Directories and Databases.

Found where files and directories are located.



Pulled files onto my main system.

A black background with white text

Description automatically generated

Found userdata file. Shows user id and other id’s.

A screen shot of a computer

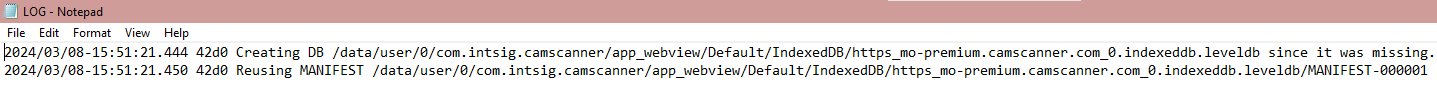
Description automatically generated

Found Logfile shows what activity the app does.

A screenshot of a computer

Description automatically generated

Log file checks to see if I had the premium version of camscanner installed.



Found a database that stores bank card information.

A screenshot of a computer

Description automatically generated

Found the 2 documents I created while using the app.

A screenshot of a computer

Description automatically generated

Found what size pdfs the app can scan.

A screenshot of a computer

Description automatically generated

It shows 3 accounts but I only made 1 account and shows 2 images and 2 documents because I only created 2.

A screenshot of a computer

Description automatically generated

Found Anonymous files that I was not able to open.

A screenshot of a computer

Description automatically generated

Conclusion

If I was to do this assignment differently I would spend more time generating more data on the apps and try to find more data using adb. Out of the 3 dm’s I created on Twitter I was only able to find one of them. I was able to find all the search queries I made on Twitter. On slack I was not able to find any of the messages I had created and links that I shared. On CamScanner I was able to find the 2 pdfs that I scanned but there were more options when I was looking at the databases. I found databases that would store data on teams, team members and messages. I should have spent more time on the app to find these features and implement them in my assignment so I could find more data about them in the database.