CSCI: 6638-01: Small Scale Digital Forensics

**Week # 5 Lab 3: Exploring the IOS File System**

TC

Contents

[Executive Summary 3](#_Toc147341518)

[Evidence 3](#_Toc147341519)

[Paper Purpose 3](#_Toc147341520)

[Tools 3](#_Toc147341521)

[Laboratory Procedures 3](#_Toc147341522)

[Device Information (ALEAPP) 4](#_Toc147341523)

[Physical Address, Phone Number, Name (ALEAPP) 5](#_Toc147341524)

[Accounts on Device (ALEAPP) 6](#_Toc147341525)

[Bluetooth Connections (ALEAPP) 8](#_Toc147341526)

[Calls Made (ALEAPP) 9](#_Toc147341527)

[Web URLS Visited and Search History (ALEAPP) 10](#_Toc147341528)

[Device Build Information (ALEAPP) 11](#_Toc147341529)

[Event List (ALEAPP) 12](#_Toc147341530)

[Google Map Search History (ALEAPP) 13](#_Toc147341531)

[Keystroke Log (ALEAPP) 14](#_Toc147341532)

[Installed Apps (ALEAPP) 15](#_Toc147341533)

[Messaging Applications Contacts and Messages Sent (ALEAPP) 18](#_Toc147341534)

[Permissions on Device (ALEAPP) 23](#_Toc147341535)

[Recent Activity (ALEAPP) 24](#_Toc147341536)

[Operating System Version (ALEAPP) 26](#_Toc147341537)

[Messaging (Andriller) 27](#_Toc147341538)

[Call Logs (Andriller) 28](#_Toc147341539)

[WhatsApp Messages (Andriller) 29](#_Toc147341540)

[Chrome Search History(Andriller) 30](#_Toc147341541)

[Findings 31](#_Toc147341542)

[Conclusions and Recommendations 32](#_Toc147341543)

[Problem Solving/ Troubleshooting 32](#_Toc147341544)

# Executive Summary

Assigned with doing a filesystem analysis on the IOS platform investigators were tasked with located the following items. Proceed to find accounts associated with the calendar, information regarding the instillation of applications and types of applications on the device, information about MMS/SMS and if any devices are located on the device, device information(photos), Wi-Fi information, time zone of device, the accounts associated with the pixel device, and the contacts stored on the device. The main objective is familiarization to the IOS filesystem platform.

# Evidence

Breakdown of all information found in Andriller and ALEAPP graphical tools.

* Manufacturer: Google
* Model: Pixel 3
* SIM Number: 6513381146 – 310260974867669
* SIM Display Name: Google-Fi
* Addresses for Joshua K Hickman: 120 Braxberry Way/ 152 Sweet Vista Lane
* Phone Number: 919-538-2339/ 910-269-7333

# Paper Purpose

No paper was utilized in this lab.

# Tools

* Virtual Box: Virtual Windows 11 OS, 12GB RAM s, Version: WinDev2309Eval
* Host Computer: Windows 10 OS, 16GB RAM, Version: 22H2
* Windows CMD
* Windows Filesystem
* DB Browser (SQLite)
* Autopsy Version 4.21.0
* Andriller 3.6.3
* ALEAPP 3.1.8

# Laboratory Procedures

* Beginning the lab, the investigator booted up the windows virtual machine to ensure the most security when working on the documentation containing it within an isolated environment.
* Once an isolated environment was setup the proper procedures were taken to install the applications
* First navigate to the respective GitHub portfolio of the two creators of ALEAPP and Andriller. Download the respective zip files and extract them to a folder on your desktop for easy reference when navigating the cmd.
* Assuming that python and its pathing and environment variables are properly setup\* Proceed to launch the cmd and enter cd desktop to navigate to desktop from there type cd ALEAPP-main (cd andriller-master) to navigate to ALEAPP-main folder , once inside the folder type the folloiwnng command for windows machine “pip install -r requirements.txt” this should install required packages to run software(Utilize this command for both the requirements text on andriller and ALEAPP)(to navigate to andriller-main) once inside folder type py aleappGUI.py (py andriller-gui.py) to launch into either app following this select the google pixel 3 data from previous report and navigate to zip folder titled Pixel 3 select this as your data and begin the ALEAPP extraction.
* NOTE: You can also select whichever folder desired, Desktop was selected for this lab
* Once the zip is loaded and output destination is specified run the ALEAPP software to retrieve the first piece of data. (Pictured below)

## Device Information (ALEAPP)

* A screenshot of a computer

  Description automatically generated
* *Device information*
* On the side of the ALEAPP web dashboard displaying results there is a section titled Chromium (Chrome) to find the associated physical address for the user [thisisdfir@gmail.com](mailto:thisisdfir@gmail.com) and Joshua K Hickman.

## Physical Address, Phone Number, Name (ALEAPP)

* A screenshot of a computer

  Description automatically generated
* Once retrieval of the Owner, Name, phone number, email address, physical address has been located the rest of the files to look through are easily laid out in the side navigation menu. Which highlights some important details and places to look such as internet history, accounts associated with the phone, calls & text, Bluetooth device connections, recent Wi-Fi activity such as last connection.
* Once finished with the web data there is important information located within the accounts\_ce tab and accounts\_ce\_0 is to be selected reveal the information below.

## Accounts on Device (ALEAPP)

* A screenshot of a computer

  Description automatically generated
* Further investigation on the ALEAPP extraction we can see accounts\_de which contains accounts\_de\_0 and accounts\_de\_1, within the accounts\_de\_0 is where the app accounts information has been found pictured below.
* A screenshot of a computer

  Description automatically generated
* After location of the associated accounts there are some other sections of the nav menu that may prove useful navigate towards Bluetooth connections report this may help to locate the physical location of a certain user, Bluetooth information below.

## Bluetooth Connections (ALEAPP)

* A screenshot of a computer

  Description automatically generated
* Once Bluetooth connections are located move onto the call logs to see what type of calls were being made, the number associated with the calls, location the call was going to, and lastly any information pertaining to who made the call.

## Calls Made (ALEAPP)

* A screenshot of a phone number

  Description automatically generated
* Further down will be a section for Chrome-Cookies this can lead directly to saved or cached information within the google account and other items of importance.

## Web URLS Visited and Search History (ALEAPP)

* A screenshot of a computer

  Description automatically generated
* Pictured above are several URLs that have been visited that could lead to potential account recovery information or password locations for said accounts along with figuring out what information particularly was cached within google chrome browser.
* A screenshot of a computer

  Description automatically generated
* For the above detailing the chrome download report doesn’t show much but it could be useful to see what was downloaded on the device and identifying dangerous applications.

## Device Build Information (ALEAPP)

* A screenshot of a computer

  Description automatically generated
* Important information relating to the build information of the phone but more importantly is where it is stored within the masks folder an open-source software used for rooting and customizing android devices.
* Scrolling further down the side navigation menu an events selection is shown this could lead to useful information pertaining to the type of actions and activity that was performed on the device. Which could point to other directories with useful information.

## Event List (ALEAPP)

* A screenshot of a computer

  Description automatically generated
  + *Pictured above events that occurred on Pixel 3 device.*
* Further scrolling down the side navigation bar will show Google Search History Maps report this could show what locations were searched and could potentially lead to a physical location to connect the phone to.

## Google Map Search History (ALEAPP)

* A screenshot of a search engine

  Description automatically generated
  + *Pictured above the Google Search History Report with two locations and found within the magisk software folder*
* Directly underneath the Google Search History option there is a keylogger titled trainingcache2.db which opens to show each text input for apps and for some the input type.

## Keystroke Log (ALEAPP)

* A screenshot of a computer

  Description automatically generated
  + *Pictured above listed keylogged entries for application on Pixel 3*
* Navigate towards the Installed Apps to view all installed applications on the android device, could lead to detecting any software or programs that could be used for malicious intent. Along with this you can also see underneath the other types of installed apps. (All pictured below)

## Installed Apps (ALEAPP)

* A screenshot of a computer

  Description automatically generated
  + *Pictured above the installed applications.*
* A screenshot of a computer

  Description automatically generated
* A screenshot of a computer

  Description automatically generated
* Looking at the SMS/MMS is another good data probe to gather impactful information, one other interesting item is the alternate chats associated with this device such as MeWe Chat, Skout, Snapchat, TextNow, Viber, and WhatsApp. Each can be found within the navigation menu MeWe is first followed by MMS/SMS and the rest, each section labeled as their respective application name.

## Messaging Applications Contacts and Messages Sent (ALEAPP)

* A screenshot of a computer

  Description automatically generated
  + *MeWe Chat*
* A screenshot of a report

  Description automatically generated
  + *MMS messages*
* A screenshot of a computer

  Description automatically generated
  + *SMS messages*
* A screenshot of a computer

  Description automatically generated
  + *Skout messages*
* A screenshot of a computer

  Description automatically generated
  + *Users associated with Skout Messaging*
* A screenshot of a computer

  Description automatically generated
  + *Snapchat friends associated with snapchat account*
* A screenshot of a report

  Description automatically generated
  + *Snapchat my eyes own picture vault*
* A screenshot of a report

  Description automatically generated
  + *Snapchat messages*
* A screenshot of a computer

  Description automatically generated
  + *TextNow Contact List*
* A screenshot of a computer

  Description automatically generated
  + *TextNow Messages*
* A screenshot of a computer

  Description automatically generated
  + *Viber Calls*
* A screenshot of a computer

  Description automatically generated
  + *Messages associated with Viber*
* A screenshot of a computer

  Description automatically generated
  + *WhatsApp messages*
* Note that not all messaging searching will lead to useful information but there could be potential for evidence within these message logs.
* Once finished with the messaging move towards the Permissions category on the side navigation, within this section shows the permissions and runtime permissions of the users on this device which could potentially aid in deciphering if someone’s phone had an alternate account with elevated privileges.

## Permissions on Device (ALEAPP)

* A screenshot of a computer

  Description automatically generated
  + *Runtime Permissions\_0*
* A screenshot of a report

  Description automatically generated
  + *Runtime Permissions\_11*
* Recent activity is also a great area to look at. this can potentially lead to information to form the timeline of what happened to the device before confiscation.

## Recent Activity (ALEAPP)

* A screenshot of a computer

  Description automatically generated
  + *Recent activity screenshot showing available Wi-Fi networks*
* A screenshot of a computer

  Description automatically generated
  + *Screenshot showing Magisk open source software install*
* A screenshot of a computer

  Description automatically generated
  + *Screenshot showing snapshot of attached master card.*
* Once activity has been analyzed move towards the bottom of the side navigation bar to find Operating System (OS) Version always good to know exactly what version of the OS was operating on the phone.

## Operating System Version (ALEAPP)

* A screenshot of a computer

  Description automatically generated
* Now once ALEAPP has been utilized and output has been processed move onto the andriller tool this can be access by utilizing cd .. to go back to desktop (if you are still within the ALEAPP folder) once that is done type cd andriller-master to enter the folder, once inside type py andriller-gui.py to open the program.
* Next chose the output folder for the report generated by the tool (For ease of access recommended to create output folder on desktop) once output selected proceed to click analyze folder and select the Pixel 3 folder (not the Pixel 3.zip) after click analyze and you will be greeted to a similar landing page of Aleapp with all the sections spaced out and the associated files organized within them.
* For this part information pertaining got the device and other identifying items proved difficult to search for however the amount of call and messaging platforms that have been found along with calls and messages pertaining to each of the respective messaging platforms.

## Messaging (Andriller)

* A screenshot of a computer

  Description automatically generated
* *Information pertaining to the device and the user associated with this device found to be John Hickman*
* Further investigation within the andriller would include going through each of the messengering platforms that were found such as Facebook Messenger, Viber, and WhatsApp
* Look into the apps and see what messages were being sent as locations and other information was being transferred along with regular conversation. (Pictured Below)

## Call Logs (Andriller)

* A screenshot of a computer

  Description automatically generated
* *Image of call history of user Josh Hickman*

## WhatsApp Messages (Andriller)

* A screenshot of a computer

  Description automatically generated
* Above is the WhatsApp section with locations that were sent from the current device known to be Johnathan Hickman.
* Further investigation will lead us to investigating the rest of the applications found via andriller, such as the google chrome history (Pictured below)

## Chrome Search History(Andriller)

* A screenshot of a computer

  Description automatically generated
* *Pictured above is the search history for the user of the pixel phone found to be John Hickman.*
* Android one call logs it would be in the best interest to see what each of the call and message logs looked like for each of the different applications associated with messaging and calls (Voice over IP).

# Findings

* Items found were located quite easily with the help of the tools used ALEAPP and Andriller, findings included.
* ALEAPP
  + Device Information associated with the accounts.
  + Accounts within the device (accounts\_de\_0 & accounts\_de\_11)
  + Bluetooth connections
  + Chrome browser cache
  + Call Logs
  + Calendar Events
  + Everything associated with Chrome Browser such as autofill, cookies, downloads, keyword search, login data, history, and web visits.
  + Contacts
  + Device information such as build info
  + Downloads on the device
  + Geo Location
  + Gmail activity
  + Photos
  + Installed apps.
  + Chat applications MeWe, SMS/MMS, Skout, Snapchat, Facebook Messenger, TextNow, Viber, and WhatsApp.
  + Permissions
  + Recent Activity
  + Wi-Fi profiles as well
* Andriller
  + Chrome History
  + Chrome Passwords
  + Android One call logs
  + Facebook messenger
  + Viber Messenger, Facebook Messenger, Whatsapp
  + Wi-Fi Passwords

# Conclusions and Recommendations

To conclude the task each of the desired outcomes and file paths were located except for the location of the device information. For getting accustomed to the tools at hand with ALEAPP and andriller have been great and both of their strengths and weaknesses have shown as well. ALEAPP has a more polished look to it compared to andriller at first glance with ALEAPP separating everything into sections based on a sidebar navigation. This makes it easy to find and search for information relating to the device. It is to note that the ALEAPP took in the Pixel 3.zip file and found more information compared to the andriller. Andriller however did have a simple look to its layout but same functionality except it worked as links to take you to a new page while ALEAPP worked as if it was a dashboard reporting application. However, the presentation of the data was the same besides the graphical polish being the only difference between the two software’s. As the investigator it seems that ALEAPP is more of a complete processing of the information finding more data than andriller and presenting it more polished. While andriller seems to be a tool for analyzing induvial folders and not the entire Pixel 3 file as what it was able to find was significantly less. It seems ALEAPP and andriller are the perfect tools to be used in conjunction with eachother, for example ALEAPP can do the entire surface level searches to identify where proper file folders and locations are and you can utilize andriller to do a more precise deep dive into that specific folder. Recommend making use of both in the DFIR team and lab environments.

# Problem Solving/ Troubleshooting

No issues with the set-up and successful processing of the data, information was easy to find, and the software worked as intended.