CSCI: 6638-01: Small Scale Digital Forensics

**Week # 3 Assignment: Exploring the Android File System**

TC

Contents

[Executive Summary 3](#_Toc146809504)

[Evidence 3](#_Toc146809505)

[Paper Purpose 3](#_Toc146809506)

[Tools 4](#_Toc146809507)

[Laboratory Procedures 4](#_Toc146809508)

[Calendar Account Location and Information 6](#_Toc146809509)

[Calendar Time-zone Location and Information 6](#_Toc146809510)

[Downloads Location and Information 7](#_Toc146809511)

[Photo Location and Information 8](#_Toc146809512)

[MMS/SMS Location and Information 8](#_Toc146809513)

[Contacts Location and Information 11](#_Toc146809514)

[Associated Accounts Location and Information 12](#_Toc146809515)

[Contact Information and Location 13](#_Toc146809516)

[Wi-Fi XML Information and Location 14](#_Toc146809517)

[Autopsy MMS/SMS Information 15](#_Toc146809518)

[Autopsy Installed Applications Information 15](#_Toc146809519)

[Autopsy Network Website Information 16](#_Toc146809520)

[Findings 16](#_Toc146809521)

[Conclusions and Recommendations 18](#_Toc146809522)

[Problem Solving/ Troubleshooting 18](#_Toc146809523)

[Citations 18](#_Toc146809524)

# Executive Summary

Tasked with discovering the filesystem of a google pixel 3 android device there have been provided tasks to determine where each possible data point could be on the storage device. This involves utilizing the command line interface to manually navigate through all the filesystems of the Pixel 3 android device. The investigator will 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.

# Evidence

Breakdown of all information found via task assignment.

* Calendar and associated account information, Account associated [thisisdifir@gmail.com](mailto:thisisdifir@gmail.com)
* Installed Applications found totaling over 1,115 most notable were tor browser for the dark web, magik used for rooting android devices, and multiple messenger accounts.
* MMS/SMS information was found with 87 messages located within the files of the device most messages detail ways to communicate in secret along with “I wonder where it stores the message data” as another message of interest.
* Photos on device were not found as the original photo folder was removed however on another user folder multiple screenshots were found.
* Device information could not be located as the system/build.prop file could not be located or any associated files with device information.
* Wi-Fi passwords could not be found however there was a Wi-Fi configuration setup xml file containing information pertaining to device default name and device manufacturer.
* Network connections to other items on the network could not be found however internet network connections could be found along with website history and cache revealing websites visited and information for accounts associated with those websites.
* Time zone was found to be America/ New York
* Synced accounts found on the account of note were 858233690(org.telegram.messenger), Unkown App: Signal (org.thoughtcrime.securesms), user: thisisdfir (com.silentcircle.account), Social: TextNow(com.enflick.android.TextNow.account), Number For Messenger: (+1)9195794674 (com.viper.voip)Voice over IP video call messengers.
* Contact information was found first with only phone numbers stored and no contact id, soon after one name was revealed as John Hickman.

# Paper Purpose

Paper in this lab was used to keep track of tasks at hand to provide checks to ensure not repeating same tasks for locating desired files.

# 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

# 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 lab files were then downloaded to host machine, following these settings in VirtualBox were set to allowed filesharing between one folder for host and virtual machine.
* After this was set in place the zipped file from the android download was then imported into the virtual machine to then be processed through the window command line interface and using the graphical file system interface as well
* To ensure easier time navigating files the file marked “Non-Cellebrite Extraction” was extracted to the desktop as its own file and the pixel 3 folder was then extracted to this same location.
* To navigate to the file folder on desktop the following cmd commands were used.

Cd desktop

Cd Non-Cellebrite Extraction

Cd Pixel 3

* After successful navigation to the main folder the following commands were entered to navigate to each of the points of interest marked in requirements.
* Attempted use of “cd /data/com.android.providers.calendar/databases/calendar.db”
* Going to be utilizing graphical interface for navigating file structure until the need arises for use of command line interface, database file was found within /Users/User/Desktop/Non-Cellebrite Extraction/Pixel 3/data/data/com.android.providers.calendar/databases/
* Once location of database file for calendar was located DB Browser was then opened to read through the file to obtain the requested outcome of information associated with the accounts
* Once inside of DB Browser click open database and navigate to the folder mentioned above once the calendar.db file is selected proceed to click open database.
* Following this the procedure was to navigate to the most notable files within the system that could pertain to important information the following paths were used along with the database associated.
* “Non-Cellebrite Extraction/Pixel 3/data/data/” after the last backslash is where these file paths begin.
* Breakdown of files visited and how to obtain information requested
* Information regarding the accounts associated with the calendar would be.
* A screenshot of a computer

  Description automatically generatedFile location for the calendar database file

## Calendar Account Location and Information

* A screenshot of a computer

  Description automatically generatedAfter opening database file within DB Browser navigate to the browse data tab and select the colors table in the dropdown to find an account name “thisisdfir@gmail.com”

## A screenshot of a computer Description automatically generatedCalendar Time-zone Location and Information

* After noting down the email, proceed to the drop-down menu for table select and select calendar cache to find the time zone is set to America/New\_York
* Following navigate back to Non-Cellebrite Extraction/Pixel 3/data/data/ once in the folder proceed using this path Non-Cellebrite Extraction/Pixel 3/data/data/com.android.providers.downloads/databases/downloads.db

## Downloads Location and Information

* A screenshot of a computer

  Description automatically generated
* Once inside the database file proceed to the Browse Data tab and then click on the dropdown menu for Table select and click on downloads.
* Following this return to the file browser and navigate back to Non-Cellebrite Extraction/Pixel 3/data/data/ once in this location follow the path com.google.android.gms/shared\_prefs/databases this will reveal activity on the device along with the ICCID and the google account as well.
* A screenshot of a computer

  Description automatically generatedNavigate back to DB Browser and open a new database Non-Cellebrite Extraction/Pixel 3/data/data/ com.google.android.gms/shared\_prefs/databases/downloads.db
* Navigate to the Browse Data tab and click on the dropdown menu to view the downloads table.

## Photo Location and Information

* After this click open database again and navigate to Non-Cellebrite Extraction/Pixel 3/data/data/com.google.android.apps.photos/databases/gphotos().db

A screenshot of a computer

Description automatically generated

* Once there click on the browse data tab and click on the dropdown table menu to open shared\_media\_view to find screenshots taken.

## MMS/SMS Location and Information

* Following click open database and proceed to navigate to /Non-Cellebrite Extraction/Pixel 3/data/data/com.android.providers.telehpony/databases/mmssms.db
* A screenshot of a computer

  Description automatically generated
* Once the database has been opened look within the browse data tab and select the table, “part” to view the above information.
* A screenshot of a computer

  Description automatically generated
* Click on the table tab again, this will then view the SMS logs and messages received along with date, address, and the body of the message.
* A screenshot of a computer

  Description automatically generated
* Tab words\_content to reveal more of the messaging taking place.

## Contacts Location and Information

* A screenshot of a computer

  Description automatically generated
* To look for the contacts associated with the account look in the addr table.

## Associated Accounts Location and Information

* A screenshot of a computer

  Description automatically generated
* Navigate to the following path Non-Cellebrite Extraction/Pixel 3/data/system\_de/0/accounts\_de.db open this as the database path and then navigate to the browse data tab and click on the dropdown menu and select accounts table to view associated accounts.

## Contact Information and Location

* A screenshot of a computer

  Description automatically generatedClick on the open database button to navigate to Non-Cellebrite Extraction/Pixel 3/data/data/com.android.providers.contacts/databases/contacts2.db then navigate to the data table within the browse data tab.

Wi-Fi XML Information and Location A screenshot of a computer

Description automatically generated

* The following is the WiFi information tab this is an xml document that was located within the path Non-Cellebrite Extraction/Pixel 3/data/misc\_ce/0/wifi/WifiConfigStore.xml
* Following this for a more in-depth search autopsy was then used once autopsy is launched create a new case file and then once inside the case add files. Select Logical files and then continue, this should then prompt you to navigate to the desktop screen to select the android 10 image with documentation navigate to the Non-Cellebrite Extraction folder and click on the pixel 3.zip folder and select this one for your logic files to be analyzed and then wait until files have been processed.

## Autopsy MMS/SMS Information

* A screenshot of a computer

  Description automatically generated
* First navigate to messages within the data artifacts section on the side of the screen in autopsy to see all access to MMS/SMS message logs.

## Autopsy Installed Applications Information

* A screenshot of a computer

  Description automatically generated
* Click on the installed programs to retrieve 385 programs to be installed on the device this screenshot is just the beginning of the list of programs and software a notable install was the tor browser which suspects use of the dark web, along with multiple different messenger apps.

## Autopsy Network Website Information

* A screenshot of a computer

  Description automatically generated
* The network connections that were made online were located within the web history tab of the autopsy software pictured above are the websites frequently visited.

# Findings

* Information regarding the accounts associated with the calendar were located wihin the file path "Non-Cellebrite Extraction/Pixel 3/data/data/com.android.providers.calendar/databases/calendar.db
* Within this database if you navigate to the browse tab in DB browser you can select the table titled “colors" This shows the attached gmail account "thisisdfir@gmail.com"
* For the information pertaining to installed apps that was found within the downloads tab in autopsy after loading in the case files over 770 programs have been installed on the account and it has been found within the autsopsy scan, but the file path used for the downloads on the device are. Non-Cellebrite Extraction/Pixel 3/data/data/com.android.providers.downloads/databases/downloads.db & Non-Cellebrite Extraction/Pixel 3/data/data/com.google.android.gms/shared\_prefs/databases/downloads.db
* Along with this magisk an open-source software for rooting android devices was found within the following path Non-Cellebrite Extraction/Pixel 3/data/cache/magisk.txt
* To find the location of MMS/SMS follow file path Non-Cellebrite Extraction/Pixel 3/data/data/com.android.providers.telehpony/databases/mmssms.db once loaded into the DB browser navigate to the browse data tab and select the sms table along with the part table these two contain messenger items.
* The photos on the system were very difficult to find as most of them were presumed to be deleted but photos that were located were located on com.google.android.apps.photos/databases/gphotos().db
* To find the information regarding the network proved difficult to find but located within the following path Non-Cellebrite Extraction/Pixel 3/data/misc\_ce/0/wifi/WifiConfigStore.xml was an xml file that detailed some information about the Wi-Fi network that has been connected.
* For the timezone inforation it was found along the file path "Non-Cellebrite Extraction/Pixel 3/data/data/com.android.providers.calendar/databases/calendar.db the calnedar.db file and located within the calendarcache table this revealed the timezone to be set to America/New York
* The information of the synced accounts was found wthin the follwoing file path "Non-Cellebrite Extraction/Pixel 3/data/system\_de/0/accounts\_de.db" this directly led to multiple differnet synced accounts on the device pertaining to multiple different apps.
* Such as email: thisisdfir@gmail.com, Number Used For Messenger: 858233690(org.telegram.messenger), Unkown App: Signal (org.thoughtcrime.securesms), Android IMO: imo HD (com.imo.android.imous), Social: TikTok (com.zhiliaoapp.musically), Social: Facebook Messenger (com.facebook.messenger), Social: TDfir(com.twitter.android), Messeging: Whatsapp (com.whatsapp), user: thisisdfir (com.silentcircle.account), Social: Skype (com.skype.raider), Social: TextNow(com.enflick.android.TextNow.account), Number For Messenger: (+1)9195794674 (com.viper.voip)Voice over IP video call messengers, Authenticator: Duo (com.google.android.apps.tachyon)
* Accounts could also be found within the Non-Cellebrite Extraction/Pixel 3/data/system/dropbox to reveal txt file logs with all account activity.
* Contacts that were located on the device were found with the following path ccom.android.providers.telehpony/databases/mmssms.db and once database was loaded into the DB browser in the browse data tab the addr table was used to located contacts on the device that were message frequently.
* However, none of the contacts have names associated with them but the phone numbers are there. However, within the following file path Non-Cellebrite Extraction/Pixel 3/data/data/com.android.providers.contacts/databases/contacts2.db within this a list of contents with some names were written the names on this list were Josh Hickman and Silent Circle,

# 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. The device information path /system/build.prop was not to be located within the folders system, system\_ce, or system\_se however through some data recorded from the features of the phone were found. Utilizing multiple different methods, the file locations of calendar information with associated accounts, installed applications, MMS/SMS information, photo information, Wi-Fi network information (passwords could not be found), network connections, synced accounts, and contacts were all located and documented. Recommendations lie solely in getting a PC that can process the files for autopsy fast enough to recover more detailed information about all the above areas. This would assist greatly in finding out about a lot of the missing information specifically network connections (besides the connections made to websites and internet traffic that was found), device specifications, and Wi-Fi passwords or network documentation.

# Problem Solving/ Troubleshooting

Issues run into during the task included mainly software setup and file sharing problems as the virtual machine needed to have a shared folder for proper file sharing that was remedied with a reference search on virtual boxes website. VM seemed to not be able to run autopsy but was able to properly run DB Browser for SQLite, to run autopsy, it was then installed on host machine. Final problem involved not being having enough time on the desktop to run autopsy long enough to complete the data artifact recover however it did complete the folder and file analysis It was greater than two days’ time and since host computer is used for many other tasks, could not risk that load on host systems hardware. Most of the issues were locating the files but were remedied with trial and error and reference to SANS institute’s advanced smartphone forensics.

# Citations

SANS Institute. "DFIR Advanced Smartphone Forensics Poster." SANS Digital Forensics and Incident Response Resources, <https://www.sans.org/security-resources/posters/dfir/dfir-advanced-smartphone-forensics-30>.

Oracle Corporation. "VirtualBox Documentation." <https://www.virtualbox.org/wiki/Documentation>.