CSCI: 6638-01: Small Scale Digital Forensics

**Week # 6 Lab 3: Exploring the IOS File System**

TC

Contents

[Executive Summary 3](#_Toc148009436)

[Evidence 3](#_Toc148009437)

[Paper Purpose 4](#_Toc148009438)

[Tools 4](#_Toc148009439)

[Laboratory Procedures 4](#_Toc148009440)

[Build Info 4](#_Toc148009441)

[SMS/MMS Messages 6](#_Toc148009442)

[Accounts Associated with Device 7](#_Toc148009443)

[Calendar Information 8](#_Toc148009444)

[Wi-Fi Information 8](#_Toc148009445)

[Time Zone information 12](#_Toc148009446)

[Photos Found on Device 12](#_Toc148009447)

[Application Downloads on Device 13](#_Toc148009448)

[Contacts On Device 13](#_Toc148009449)

[Findings 14](#_Toc148009450)

[Conclusions and Recommendations 15](#_Toc148009451)

[Problem Solving/ Troubleshooting 16](#_Toc148009452)

# Executive Summary

Assigned with doing a filesystem analysis on the IOS platform investigators were tasked with locating the following items. 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 via manual search through notepad and SQLite DB Browser.

* Device Class: iPhone
* Device Color: #c8caca
* Device Name: This Is’s iPhone
* Firmware Version: pongoOS-1.2.0-63f6449e
* Hardware Model: N69AP
* Hardware Platform: s8003
* IMEI: 355800076093966
* MLB Serial Number: FJ665040595GP3VD
* Password Protected: false
* Time Interval Since 1970: 1587057180.910440
* Time Zone: America/New\_York
* Time Zone Offset From UTC: -14400.000000
* Trusted Host Attached: true
* Unique Chip ID: 7886149313958842
* Unique Device ID: c623fbd7e91b041e07a68f8523f53a35973e475d
* Device Enclosure Color: #e5bdb5
* Pretty Name: iPhone SE (GSM)
* Backup Encrypted: True
* Requirements were to find locations of file and their respective paths found reference findings and laboratory procedure for detailed description file paths listed below:
* NOTE: All file paths begin with 13-4-1.tar/volumes/
  + 13-4-1.tar/volumes/private/var/mobile/Library/SMS/sms.db
  + 13-4-1.tar/volumes/private/var/mobile/Library/Suggestions/entities.db
  + private/var/private/root/Librairy/Caches/com.apple.wifid/ThreeBars.sqlite
  + /private/var/private/root/library/ApplicationSupport/WiFiNetworkStoreModel.sqlite
  + /private/var/preferences/SystemConfiguration/NetworkInterfaces.plist
  + /private/var/preferences/com.apple.secuirty.cloudkeychain.proxy3.keysToRegister.plist
  + /private/var/root/system/SystemConfiguration/NetworkInterfaces.plist
  + 13-4-1.tar/volumes/private/var/mobile/Library/Calendar/calendar.sqlitedb
  + 13-4-1.tar/volumes/private/var/mobile/Library/Accounts/Accounts3.sqlite
  + Volumes/Josh/NoTar-13-4-1/private/installd/Library/Logs/MobileInstallation/mobile\_installation.log
  + private/var/mobile/Library/AddressBook/AddressBook.sqlitedb
  + NoTar-13-4-1/private/var/db/timed/Library/Preferences/com.apple.preferences.datetime.plist
  + /Volumes/Josh/NoTar-13-4-1/private/mobile/Media/DCIM/100APPLE

# 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)
* Notepad ++

# 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 located in isolated environment begin to work towards navigate to gather the required information as stated in the task.
* Start first by navigating to the location in which you extracted the data from the zip file in which case you can navigate to the folder NoTar-13-4-1 and from there you will begin the processes within the path 13-4-1.tar/volumes/private/var/db/systemstats/current\_build

## Build Info

* A screenshot of a computer

  Description automatically generated
* Navigate to the directory title “Volumes” found via the following path13-4-1.tar/volumes/private/var this will be where most of the investigation takes place.
* Following navigate to find the device information within the file with the following path.

path13-4-1.tar/volumes/private/var/installd/Library/MobileInstalltion/LastBuildinfo.plist (With a plist viewer you can read through the files and retrieve the above information)

* After locating the device information navigate towards the SMS and MMS folder found via the path below this will result in the following information
* /private/var/installd/Library/MobileInstalltion/LastBuildinfo.plist (Operating System)
* Following this located within the files itself of the image there is an image info segment that describes in detail the specifications and version of this phone (Image found below).
* A screenshot of a computer

  Description automatically generated

## SMS/MMS Messages

* A screenshot of a computer

  Description automatically generated
* 13-4-1.tar/volumes/private/var/mobile/Library/SMS (Table: chat)
* Pictured here is the information regarding the SMS logs specifically the sms.db file and once loaded into DB viewer select the browse data table and select the chat dropdown.
* Once SMS located select the browse data tab again and select the messages table to view (Pictured below)
* A screenshot of a computer

  Description automatically generated
* 13-4-1.tar/volumes/private/var/mobile/Library/SMS (DB Browser Table: message)
* After proceeding to navigate towards the file path 13-4-1.tar/volumes/private/var/mobile/Library/Suggestions/entities.db within this file location select the browse data tab within the DB viewer and select the email Metadata table. (Pictured Below)
* A screenshot of a computer

  Description automatically generated
* After navigation to the above directory is complete proceed to click on the table dropdown and select identifyPerson. (Pictured Below with File Path)
* A screenshot of a computer

  Description automatically generated
* 13-4-1.tar/volumes/private/var/mobile/Library/Suggestions/entities.db (DB Browser Table: identify person)
* Proceed to navigate towards the 13-4-

## Accounts Associated with Device

* 1.tar/volumes/private/var/mobile/Library/Accounts/Accounts3.sqlite to view the accounts associated with this device (Pictured Blow)
* A screenshot of a computer

  Description automatically generated

## Calendar Information

* Navigate towards the following file path 13-4-1.tar/volumes/private/var/mobile/Library/Calendar/calendar.sqlitedb once sqlitedb file located right click to select open with the database viewer once inside the DB viewer click on browse data tab and select the calendar table to view the associated account thisisdfir@gmail.com

## Wi-Fi Information

* A screenshot of a computer

  Description automatically generated
* To find information regarding network connections and Wi-Fi information navigate to the following directory /private/var/private/root/library/Application Support/WiFiNetworkStoreModel.sqlite
* Select the browse data tab and select the ZNETWORK Table to reveal the following.
* A screenshot of a computer

  Description automatically generated
* private/var/private/root/Librairy/Caches/com.apple.wifid/ThreeBars.sqlite once file path followed and require file located and openedn within DB viewer look at the ZACCESSPOINT Table in the browse data tab for some wifi information (Pictured Below)
* A screenshot of a computer

  Description automatically generated
* Navigate to the following file location in order to right click and select open with on the .plist file /private/var/preferences/SystemConfiguration/NetworkInterfaces.plist notepad++ is the recommended free version to view and edit XML files. (Pictured Below Network Information)
* A screenshot of a computer

  Description automatically generated
* /private/var/preferences/SystemConfiguration/preferences.plist after finding the other plist file within this folder select to open with Notepad++ to view the XML file here it shows exceptions and preferences set by the user of the device. (Pictured Below)
* A close up of a text

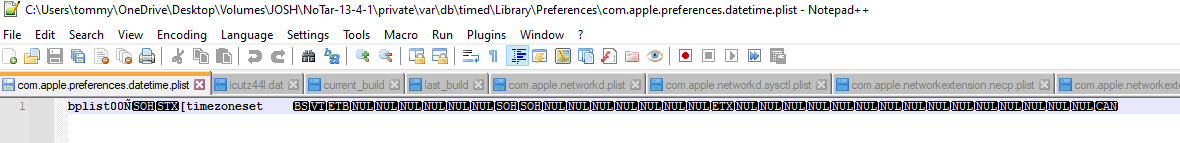
  Description automatically generated
* Finally navigate towards the following path /private/var/preferences/com.apple.secuirty.cloudkeychain.proxy3.keysToRegister.plist this file (Pictured Below) Will show all apps that have a pending password being saved for them and displays the unlocked keys within the array.
* A screenshot of a computer

  Description automatically generated
* Navigate towards the path /SystemConfiguration/NetworkInterfaces.plist to view the interfaces that have been connected to the apple device including Active connection and the type of connection in this case ethernet towards Apple Samsung Serial.
* A screenshot of a computer

  Description automatically generated

## Time Zone information

* Once finished with the Wi-Fi and the Network Information navigate towards the following folder, NoTar-13-4-1/private/var/db/timed/Library/Preferences/com.apple.preferences.datetime.plist This displays a lot of NUL and SOH (Start of Header) But it finally shows the time zone set to America/New York.
* A close up of a text

  Description automatically generated
* 

## Photos Found on Device

* Once done navigate to /Volumes/Josh/NoTar-13-4-1/private/mobile/Media/DCIM/100APPLE to find all the pictures on the device (Pictured Below)
* A screenshot of a computer

  Description automatically generated

## Application Downloads on Device

* After photos have been visited proceed to navigate towards the file path Volumes/Josh/NoTar-13-4-1/private/installd/Library/Logs/MobileInstallation/mobile\_installation.log to find the applications installed on the device
* Also, a list of downloads can be found through the path /private/var/mobile/Media/Downloads (Pictured Below)
* A screenshot of a computer

  Description automatically generated

## Contacts On Device

* Once device installation has been found follow the path private/var/mobile/Library/AddressBook/AddressBook.sqlitedb once DB is opened in SQlite browser go to the browse data tab and select ClientCursor table (Pictured Below)
* A screenshot of a computer

  Description automatically generated
* Also switching the table to ABPerson will reveal Josh Hickman and another name as This Is DFIRA screenshot of a computer

  Description automatically generated
* Switching the table once more to ABMultiValue will reveal phone numbers and emails stored (Pictured Below)A screenshot of a computer

  Description automatically generated

# Findings

File Paths for Requested Search

* Location of the SMS/MMS logs were found via the following file path:
  + 13-4-1.tar/volumes/private/var/mobile/Library/SMS/sms.db &
  + 13-4-1.tar/volumes/private/var/mobile/Library/Suggestions/entities.db
* Location of the Wi-Fi and the Network information as found via opening the plist files that were generated by apple as backup files but can be used in notepad++ to view the xml code written. This location of the following information was found, Network Information in general, Wi-Fi information connections that are saved within the device and connections that are allowed through this device with connectivity permissions,
  + private/var/private/root/Librairy/Caches/com.apple.wifid/ThreeBars.sqlite & /private/var/private/root/library/Application Support/WiFiNetworkStoreModel.sqlite
  + /private/var/preferences/SystemConfiguration/NetworkInterfaces.plist & /private/var/preferences/com.apple.secuirty.cloudkeychain.proxy3.keysToRegister.plist & /SystemConfiguration/NetworkInterfaces.plist
* Following this the device information was also locked behind a plist file and notepad was used to extract the IOS version and the build version of the device, along with that mobile specifications were listed, and location was found via the following path.
  + 13-4-1.tar/volumes/private/var/db/systemstats/current\_build
  + 13-4-1.tar/volumes/private/var/installd/Library/MobileInstalltion/LastBuildinfo.plist
* Locating the associated accounts with the calendar and the calendar app were once again found via a list file and a database file this was determined to have the email thisisdfir@gmail.com associated with the calendar on the account. Along with this listing of different calendars, saved information and events are also found via the path.
  + 13-4-1.tar/volumes/private/var/mobile/Library/Calendar/calendar.sqlitedb
* Associated accounts with the device can be found relating to the installed applications on the device. It was found that there were multiple accounts found via the path below.
  + 13-4-1.tar/volumes/private/var/mobile/Library/Accounts/Accounts3.sqlite
* Using the file path for installed applications
  + Volumes/Josh/NoTar-13-4-1/private/installd/Library/Logs/MobileInstallation/mobile\_installation.log
* Contacts on the account were located via the following file path –
  + private/var/mobile/Library/AddressBook/AddressBook.sqlitedb
* Time Zone was located via the following path.
  + NoTar-13-4-1/private/var/db/timed/Library/Preferences/com.apple.preferences.datetime.plist,
  + Also, notepad information from the imaging software
* Photos on the device were found via the following path.
  + /Volumes/Josh/NoTar-13-4-1/private/mobile/Media/DCIM/100APPLE

# Conclusions and Recommendations

To conclude, each of the required tasks were accomplished by being able to locate and find the correct file paths within the IOS 13.4.1 device system. 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.

# Problem Solving/ Troubleshooting

No issues with the set-up and successful processing of the data, information was difficult to view as the plist files had most of the required information fo the investigation. However, utilizing the notepad++ feature of XML markup code to view the plist files and retrieve information proved successful.