

# iOS Forensics for Investigators

---

Take mobile forensics to the next level by analyzing, extracting, and reporting sensitive evidence



Gianluca Tiepolo



# Chapter 1

## Images

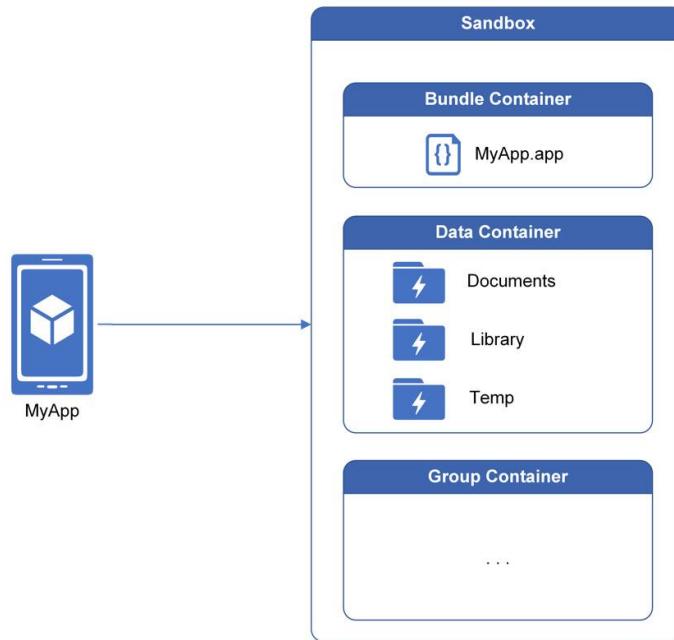


Figure 1.1 – A representation of application containers

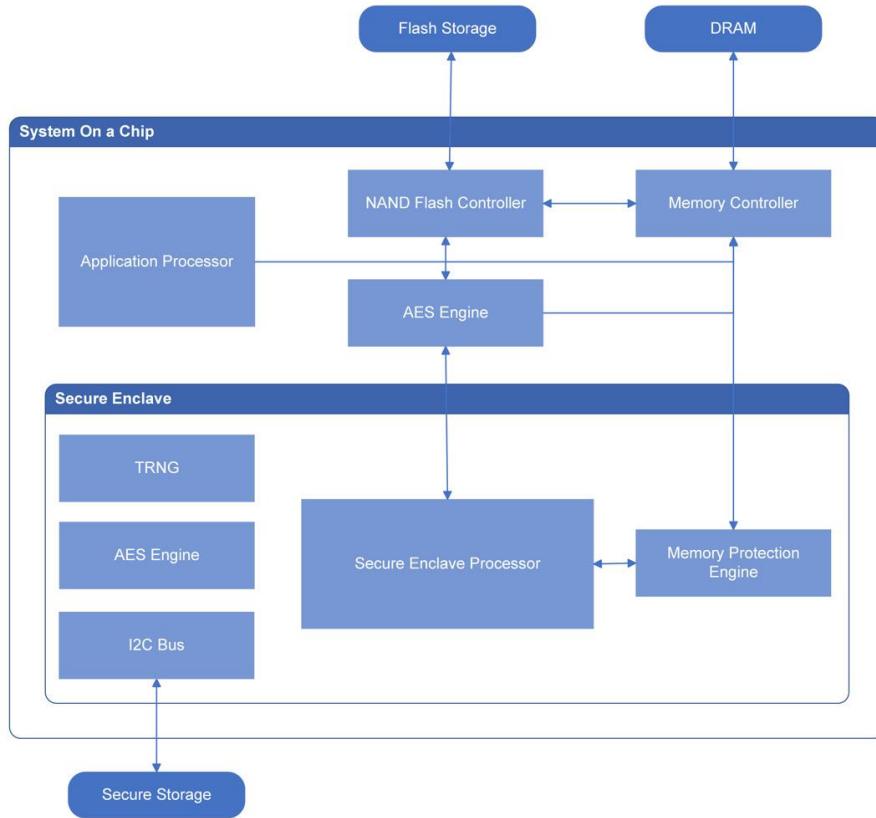


Figure 1.2 – Secure Enclave components

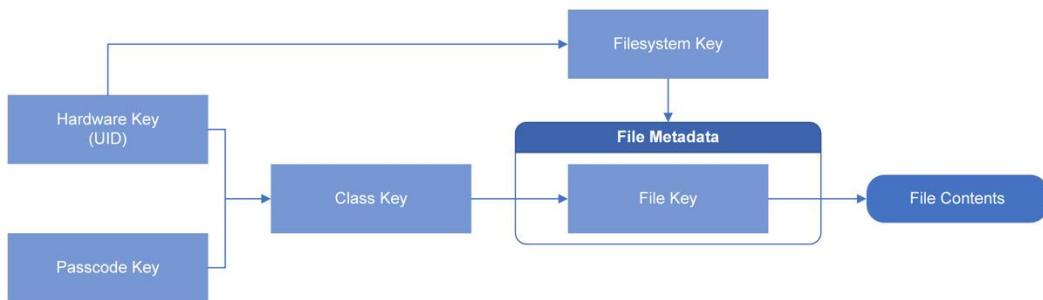


Figure 1.3 – Cryptographic keys used for iOS data protection

## Tables

	Logical	Filesystem	Physical
Calls, calendars, contacts, and messages	✓	✓	✓
User content (photos, videos, notes, and so on)	✓	✓	P
Keychain	Limited	✓	✓
Third-party app data	Limited	✓	✓
Apple Pay	-	✓	✓
Location data (radio cells, GPS fixes, and so on)	-	✓	✓
Mail	-	✓	✓
User activity logs	-	✓	✓
System logs	-	✓	✓
Deleted data (unallocated space)	-	-	✓
Deleted data (SQLite databases)	Limited	✓	✓

**Table 1.1 – Comparison of data that can be extracted with different acquisition methods**

## Code and Commands

### Code 1.1 – property list in XML format

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
    <dict>
        <key>UUID</key>
        <string>3bdd52c7-ee36-4689-8517-
c5fed2c98s5</string>
        <key>ClientID</key>
        <string>3bdd52c7-ee36-4689-8517-
c5fed2c98s5</string>
```

```
<key>ClientEnabled</key>
<false/>
</dict>
</plist>
```

# Chapter 2

## Images

### Data

 Calendar 21	 Call Log 2	 Chats 9
 Contacts 9	 Cookies 47	 Device Locations 10
 Installed Applications 373	 Instant Messages 6	 Log Entries 36
 Notes 1	 Searched Items 15	 User Accounts 12
 Web Bookmarks 10	 Web History 189	 Wireless Networks 9

### Data Files

 Archives 2	 Configurations 370 (3)	 Databases 54
 Images 51	 Text 2	 Uncategorized 300
 Videos 1		

Figure 2.1 – Data acquired through a logical acquisition

Logical		Apple_iPhone 6 (A1586)	
	Analyzed Data		Analyzed Data
>	Application (373)	>	Application (928) (2)
>	Calendar (21)	>	Calendar (21)
>	Calls (2)	>	Calls (1)
>	Contacts (9)	>	Contacts (24) (2)
>	Devices & Networks (9)	>	Devices & Networks (478) (102)
>	Location Related (10)	>	Location Related (1195) (196)
>	Media (52)	>	Manual Data Collection (3)
>	Memos (1)	>	Media (13160)
>	Messages (15)	>	Memos (1)
>	Search & Web (261)	>	Messages (25) (1)
>	System & Logs (36)	>	Physical Activities (4)
>	User Accounts & Details (12)	>	Search & Web (336)
Data files		>	System & Logs (48)
	Archives (2)	>	User Accounts & Details (281)

Figure 2.2 – Comparison of data extracted from a logical and a filesystem acquisition

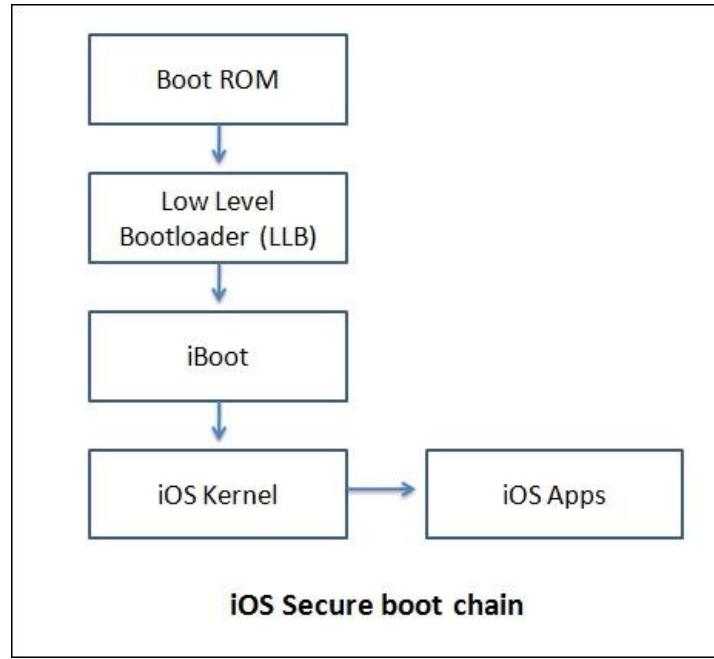


Figure 2.3 – iOS secure boot chain

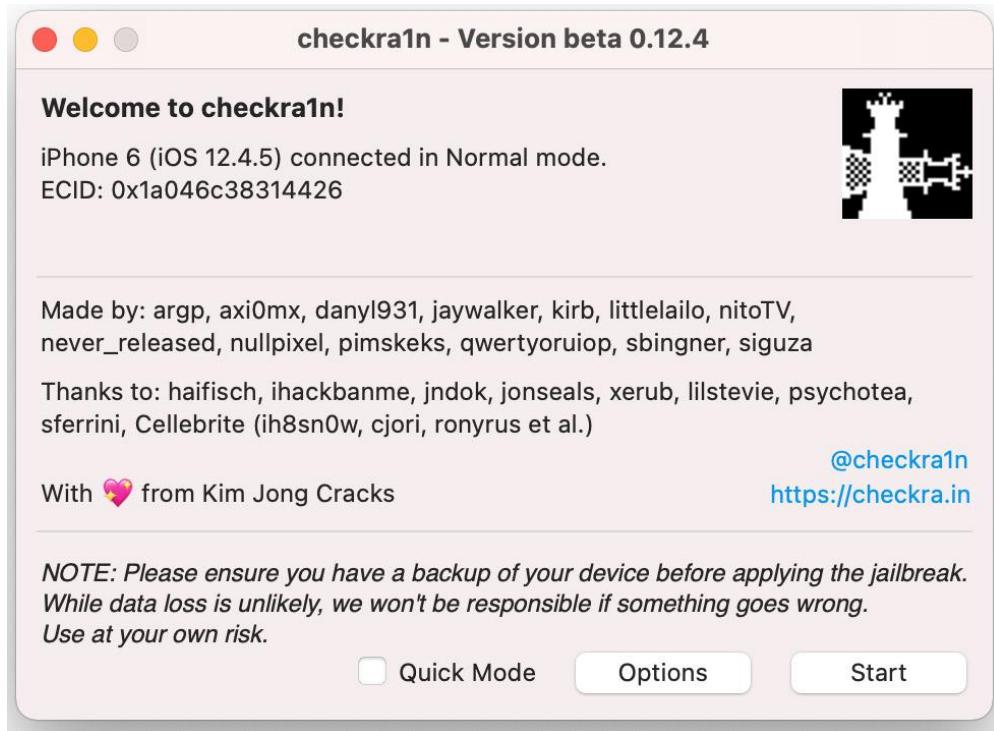


Figure 2.4 – The main check-rain screen

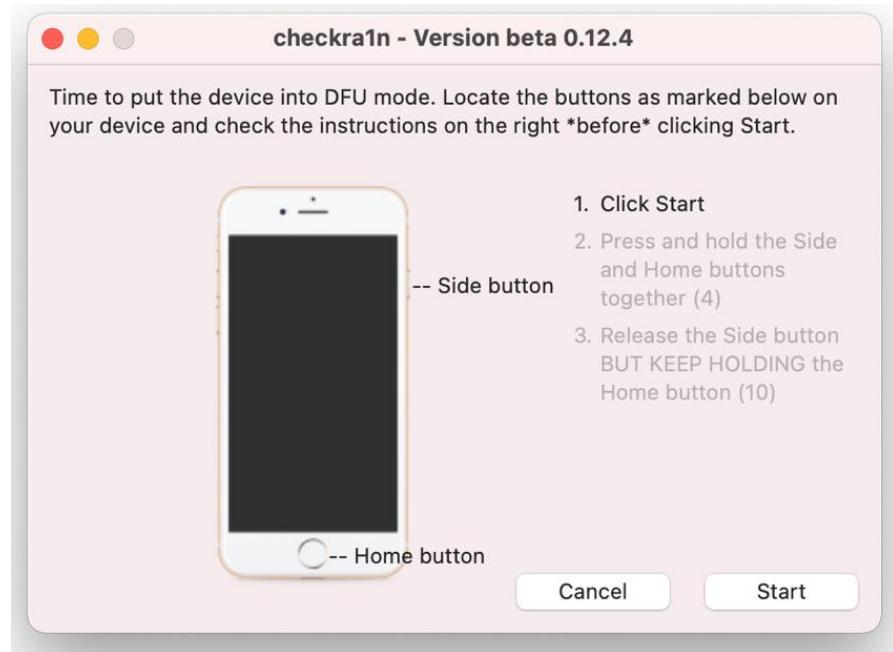


Figure 2.5 – Follow the instructions to put the device in DFU mode

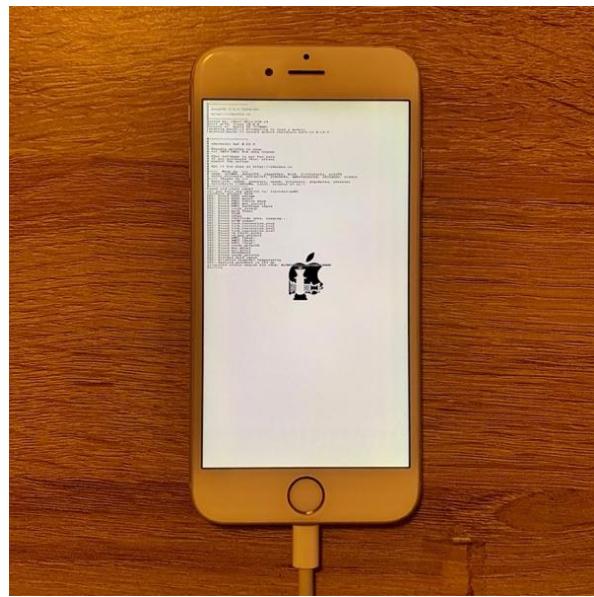
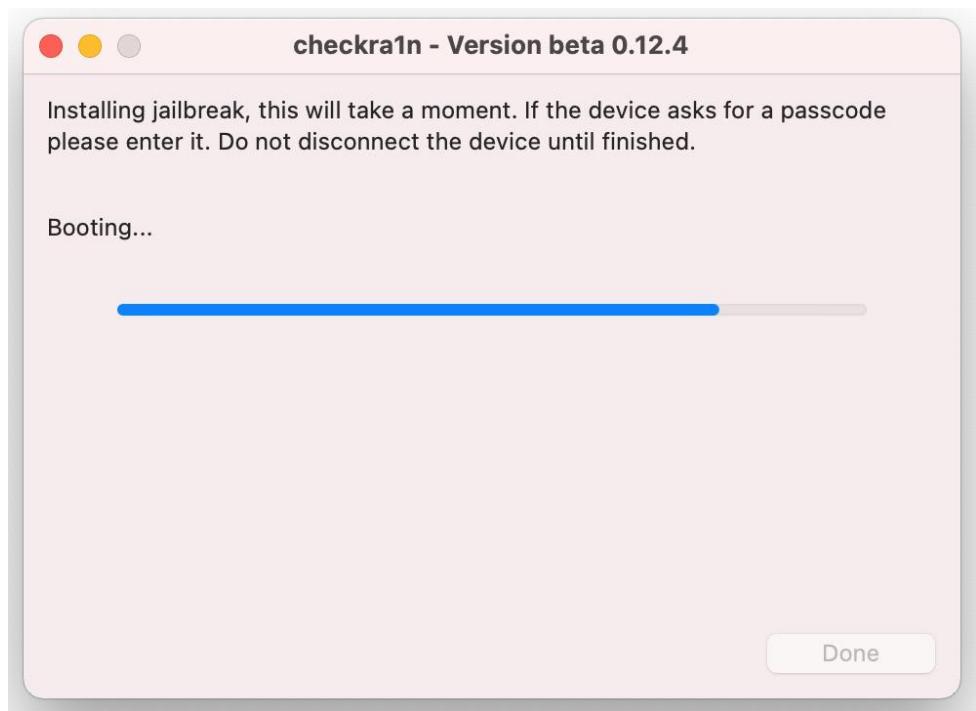
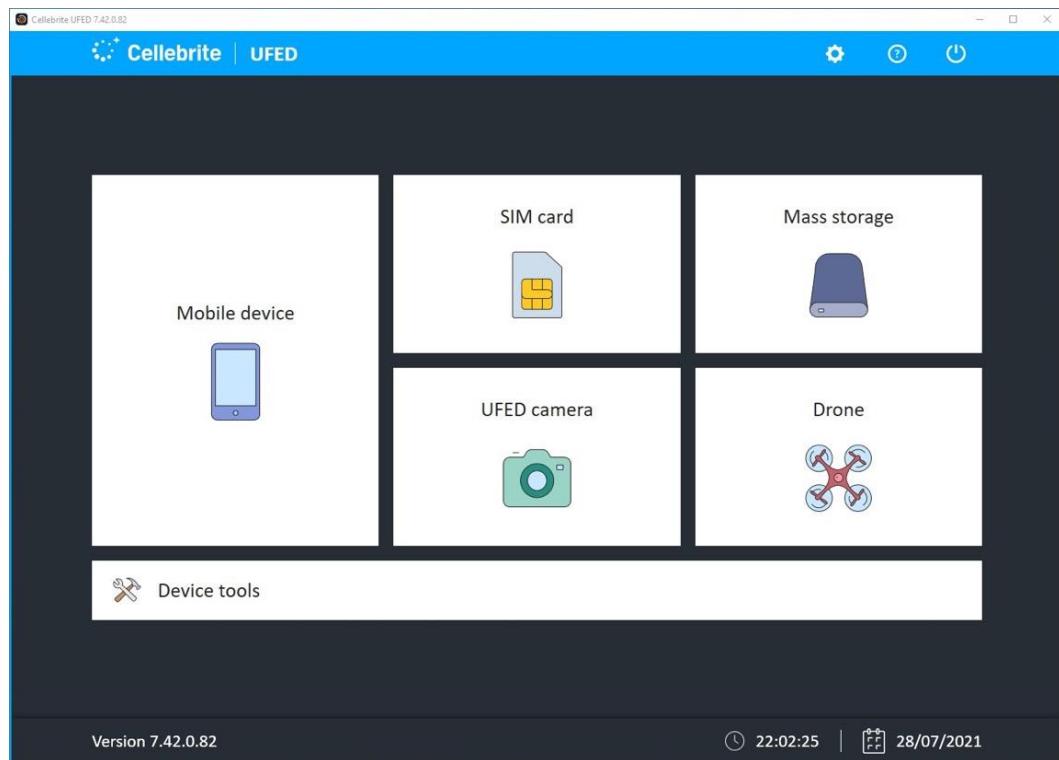


Figure 2.6 – The device booting PongoOS



**Figure 2.7 – Enter the passcode when requested**



**Figure 2.8 – The home screen of Cellebrite UFED**

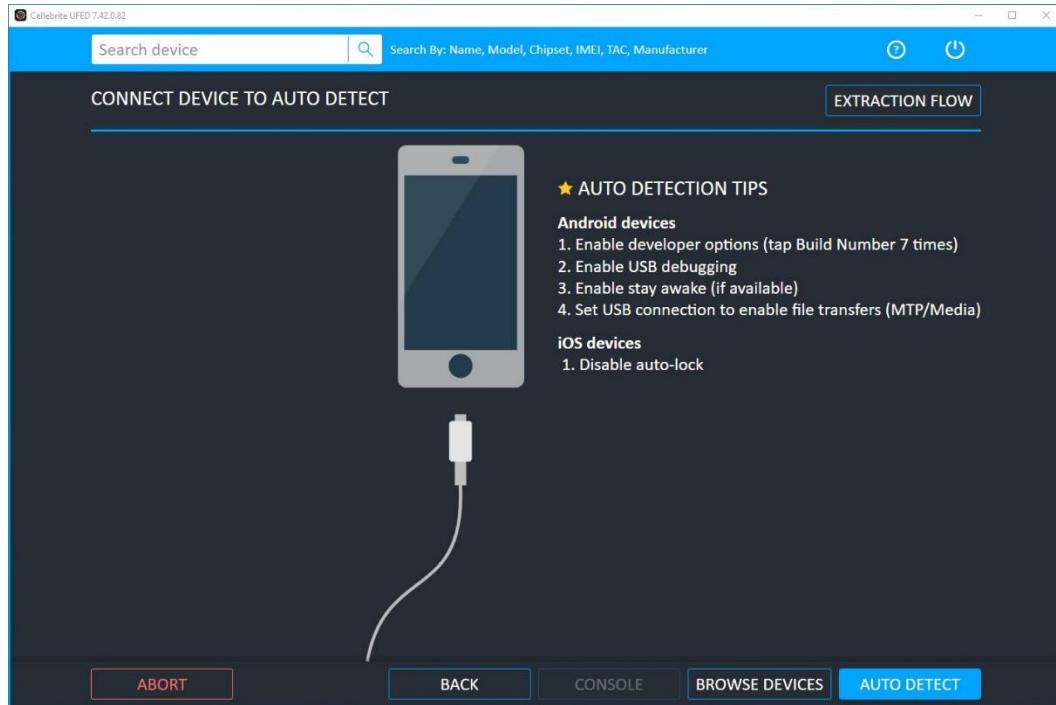


Figure 2.9 – Choose the device or let UFED auto-detect it

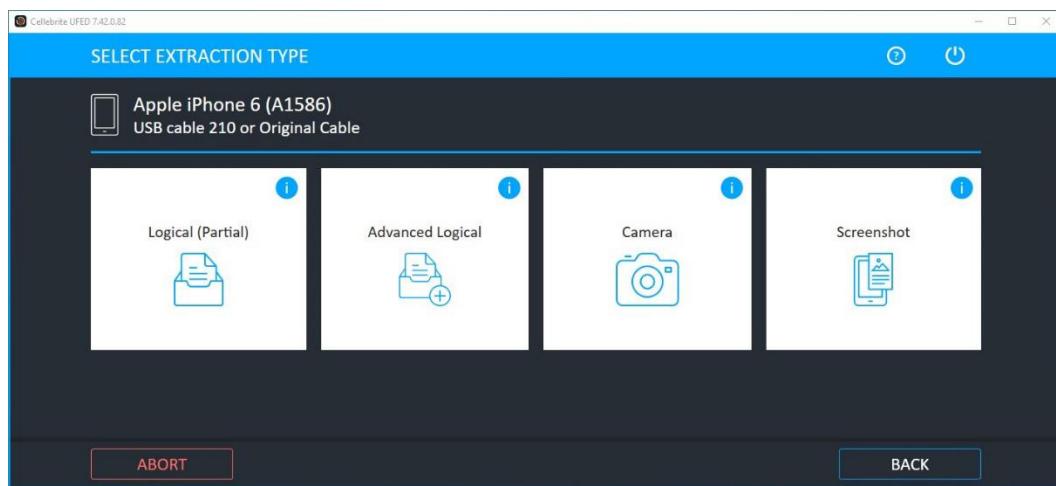


Figure 2.10 – Choose the type of acquisition

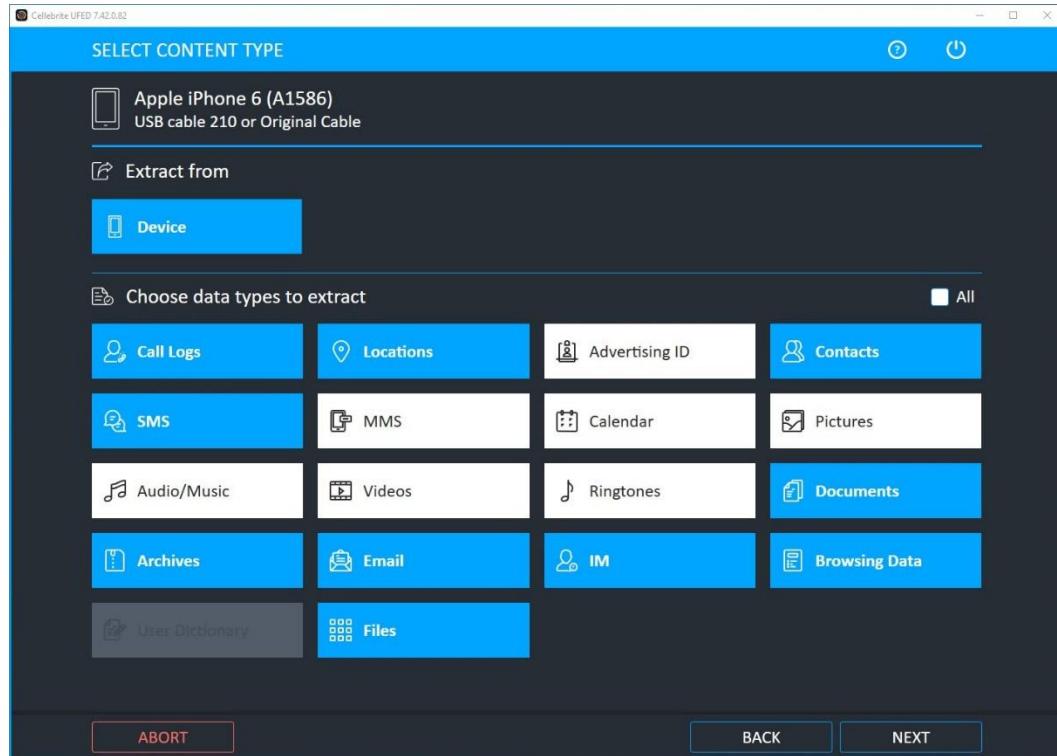


Figure 2.11 – Choose what artifacts should be extracted

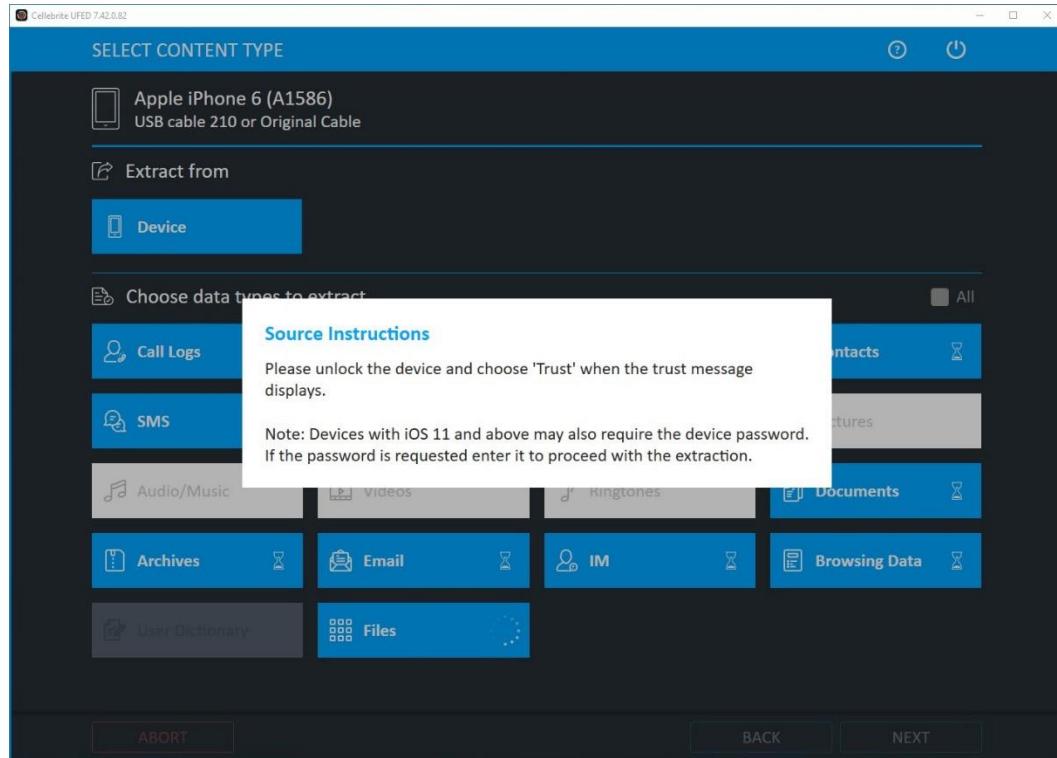


Figure 2.12 – Establish pairing between the workstation and the device

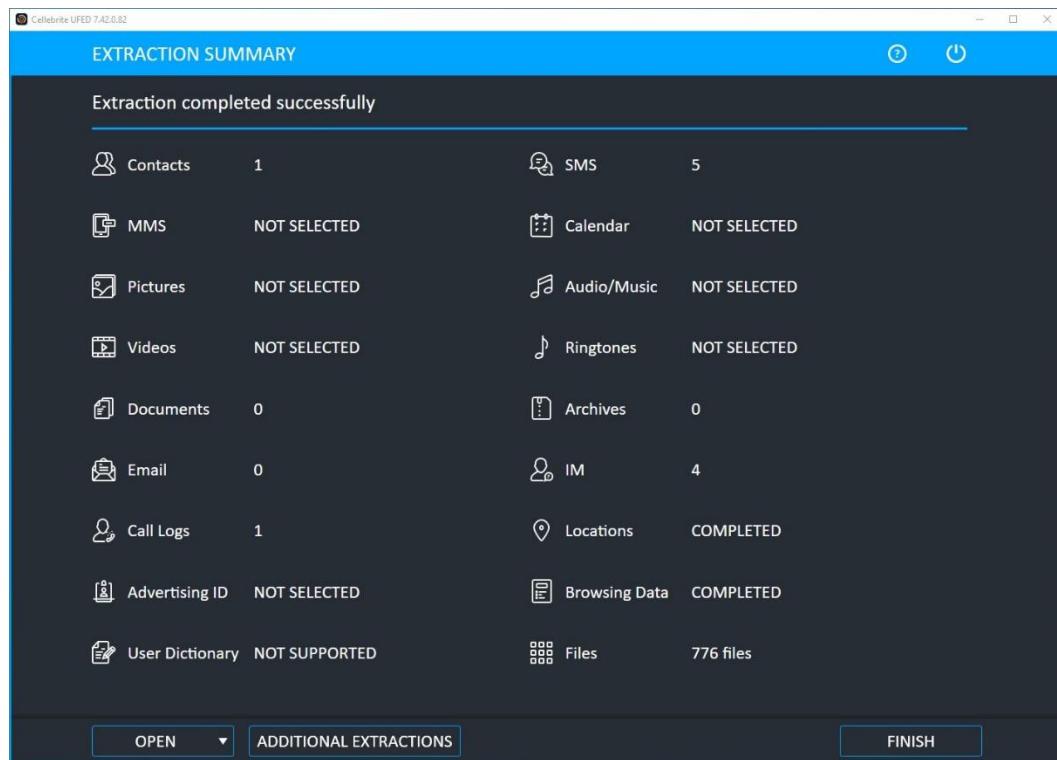


Figure 2.13 – The extraction summary displays what data was extracted

```
Toolkit.command
Elcomsoft iOS Forensic Toolkit 7.02
(c) 2011-2021 Elcomsoft Co. Ltd.

Device connected: iPhone
Hardware model: N61AP
Serial number: F78PNPSKG5MT
OS version: 12.4.5
Device ID: 7cf85b3179a6c136ae723636e6467a27888ab928

Please select an action

Logical acquisition
I DEVICE INFO      - Get basic device information
R RECOVERY INFO   - Get information on device in DFU/Recovery mode
B BACKUP          - Create iTunes-style backup of the device
M MEDIA            - Copy media files from the device
S SHARED          - Copy shared files of the installed applications
L LOGS             - Copy crash logs

Jailbroken devices acquisition
D DISABLE LOCK    - Disable screen lock (until reboot)
K KEYCHAIN         - Decrypt device keychain
F FILE SYSTEM     - Acquire device file system (as TAR archive)

Acquisition agent (limited compatibility)
1 INSTALL          - Install acquisition agent on device
2 KEYCHAIN         - Decrypt device keychain
3 FILE SYSTEM     - Acquire device file system (as TAR archive)
4 FILE SYSTEM (USER) - Acquire user files only (as TAR archive)
5 UNINSTALL        - Uninstall acquisition agent from device

Legacy devices acquisition
A LEGACY           - Legacy devices acquisition (iPhone 4/5/5C)

X EXIT

>:
```

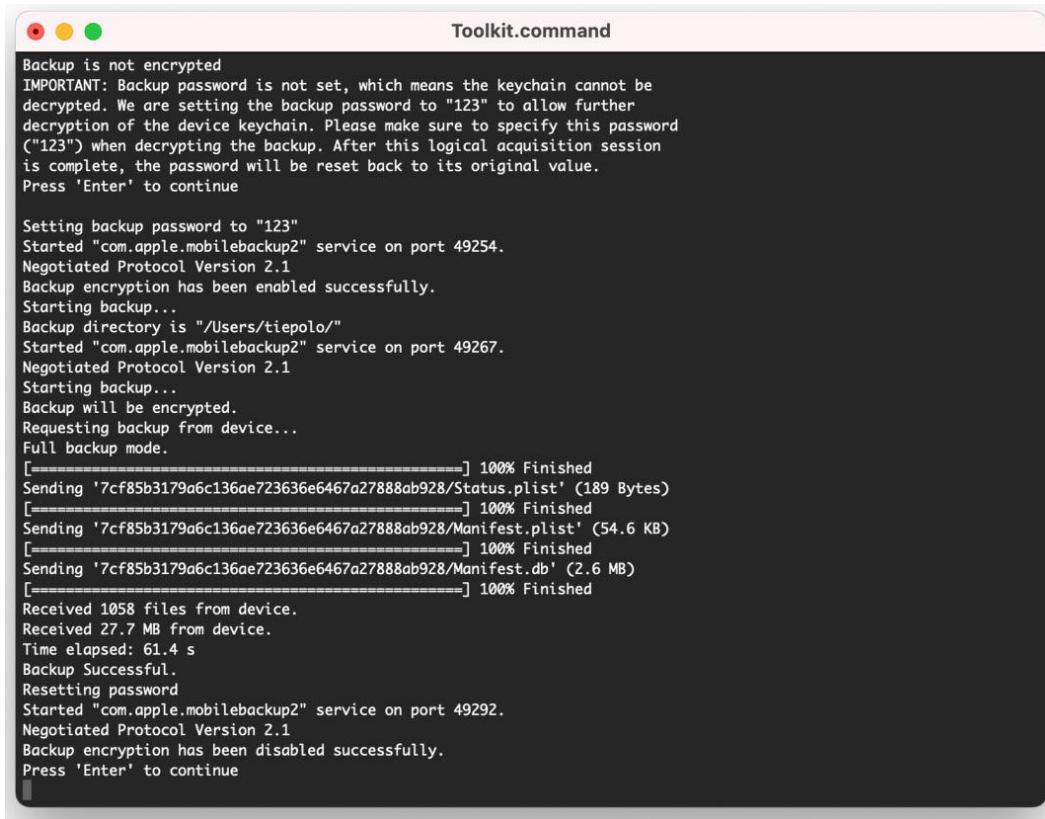
Figure 2.14 – The home screen of Elcomsoft iOS Forensic Toolkit

```
Toolkit.command
Elcomsoft iOS Forensic Toolkit 7.02
(c) 2011-2021 Elcomsoft Co. Ltd.

Device connected: iPhone
Hardware model: N61AP
Serial number: F78PNPSKG5MT
OS version: 12.4.5
Device ID: 7cf85b3179a6c136ae723636e6467a27888ab928

Write backup to directory <>>: /Users/lab/Desktop/
```

Figure 2.15 – Choose where the backup should be stored



```
Toolkit.command
Backup is not encrypted
IMPORTANT: Backup password is not set, which means the keychain cannot be decrypted. We are setting the backup password to "123" to allow further decryption of the device keychain. Please make sure to specify this password ("123") when decrypting the backup. After this logical acquisition session is complete, the password will be reset back to its original value.
Press 'Enter' to continue

Setting backup password to "123"
Started "com.apple.mobilebackup2" service on port 49254.
Negotiated Protocol Version 2.1
Backup encryption has been enabled successfully.
Starting backup...
Backup directory is "/Users/tiepolo/"
Started "com.apple.mobilebackup2" service on port 49267.
Negotiated Protocol Version 2.1
Starting backup...
Backup will be encrypted.
Requesting backup from device...
Full backup mode.
[=====] 100% Finished
Sending '7cf85b3179a6c136ae723636e6467a2788ab928/Status.plist' (189 Bytes)
[=====] 100% Finished
Sending '7cf85b3179a6c136ae723636e6467a2788ab928/Manifest.plist' (54.6 KB)
[=====] 100% Finished
Sending '7cf85b3179a6c136ae723636e6467a2788ab928/Manifest.db' (2.6 MB)
[=====] 100% Finished
Received 1058 files from device.
Received 27.7 MB from device.
Time elapsed: 61.4 s
Backup Successful.
Resetting password
Started "com.apple.mobilebackup2" service on port 49292.
Negotiated Protocol Version 2.1
Backup encryption has been disabled successfully.
Press 'Enter' to continue
```

Figure 2.16 – The toolkit will show progress and debug information on screen

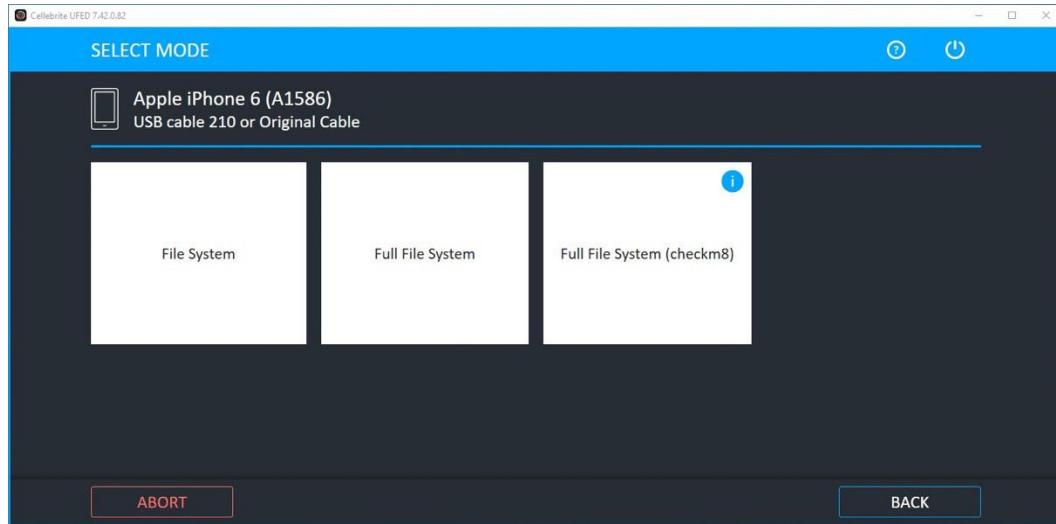


Figure 2.17 – Choose the Full File System (checkmate) option

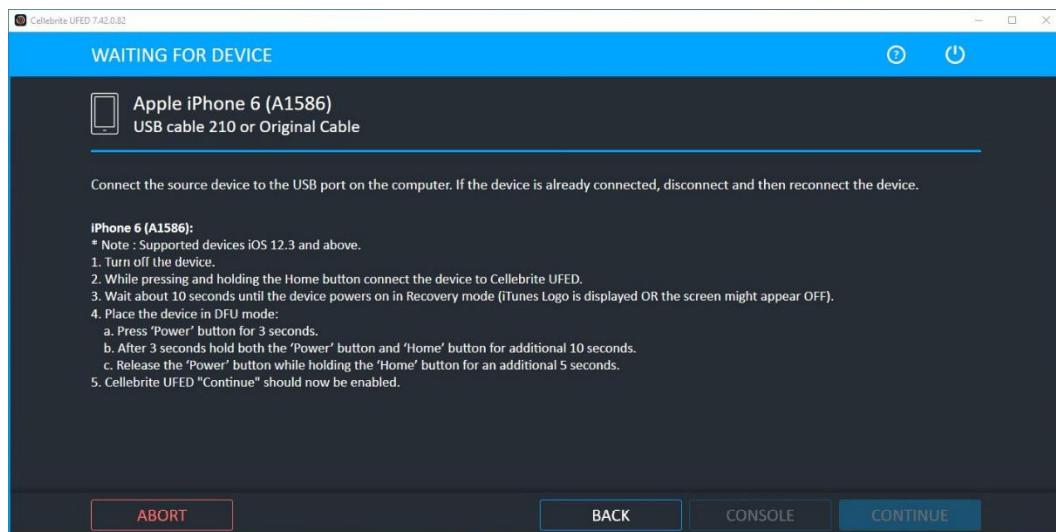


Figure 2.18 – UFED will display instructions on how to enter Recovery and DFU modes

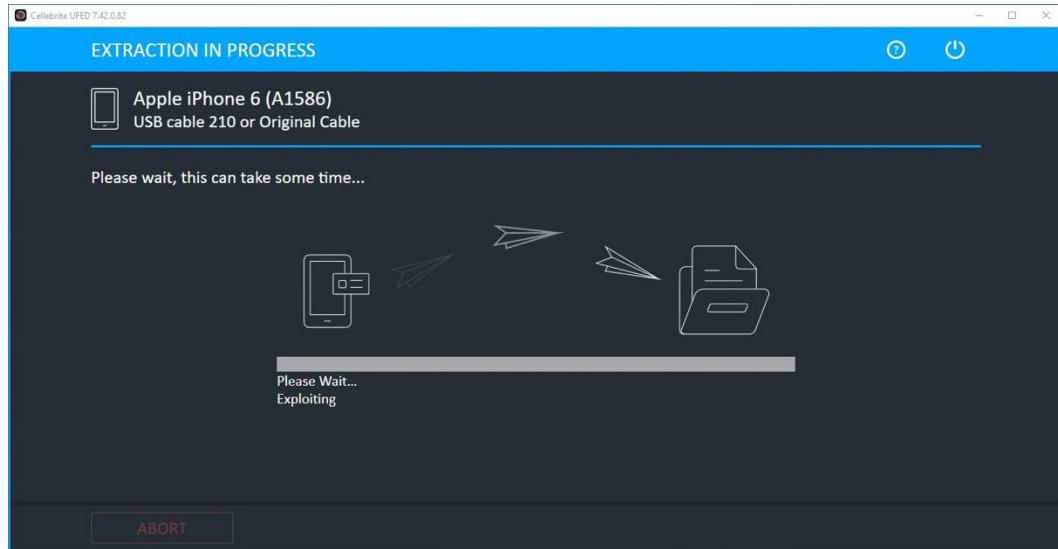


Figure 2.19 – Exploiting the device could take a few minutes

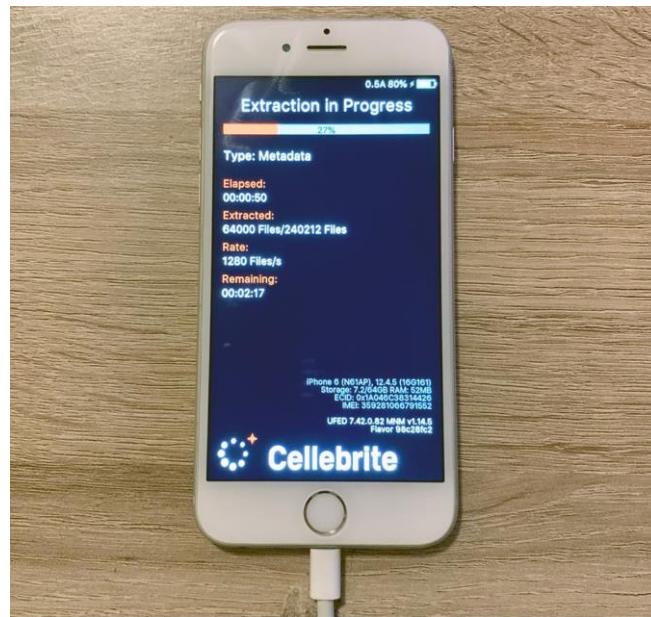


Figure 2.20 – Acquisition in process

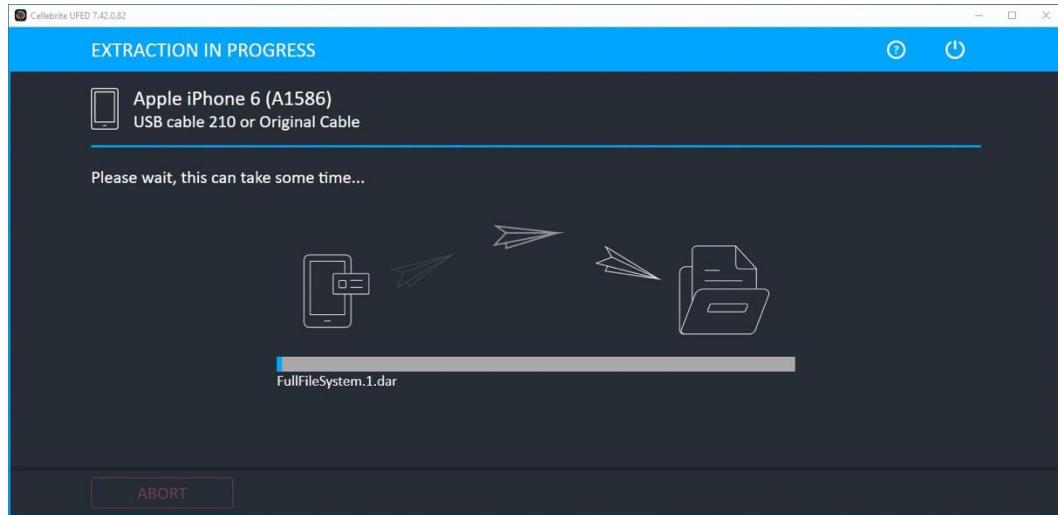


Figure 2.21 – The extraction will be archived in a DAR file

The screenshot shows the command-line interface of the Elcomsoft iOS Forensic Toolkit version 7.02. The window title is "Toolkit.command". The interface displays the following information:

Elcomsoft iOS Forensic Toolkit 7.02  
(c) 2011-2021 Elcomsoft Co. Ltd.

Device connected: iPhone  
Hardware model: N61AP  
Serial number: F78PNPSKG5MT  
OS version: 12.4.5  
Device ID: 7cf85b3179a6c136ae723636e6467a27888ab928

Please select an action

Logical acquisition

I DEVICE INFO	- Get basic device information
R RECOVERY INFO	- Get information on device in DFU/Recovery mode
B BACKUP	- Create iTunes-style backup of the device
M MEDIA	- Copy media files from the device
S SHARED	- Copy shared files of the installed applications
L LOGS	- Copy crash logs

Jailbroken devices acquisition

D DISABLE LOCK	- Disable screen lock (until reboot)
K KEYCHAIN	- Decrypt device keychain
F FILE SYSTEM	- Acquire device file system (as TAR archive)

Acquisition agent (limited compatibility)

1 INSTALL	- Install acquisition agent on device
2 KEYCHAIN	- Decrypt device keychain
3 FILE SYSTEM	- Acquire device file system (as TAR archive)
4 FILE SYSTEM (USER)	- Acquire user files only (as TAR archive)
5 UNINSTALL	- Uninstall acquisition agent from device

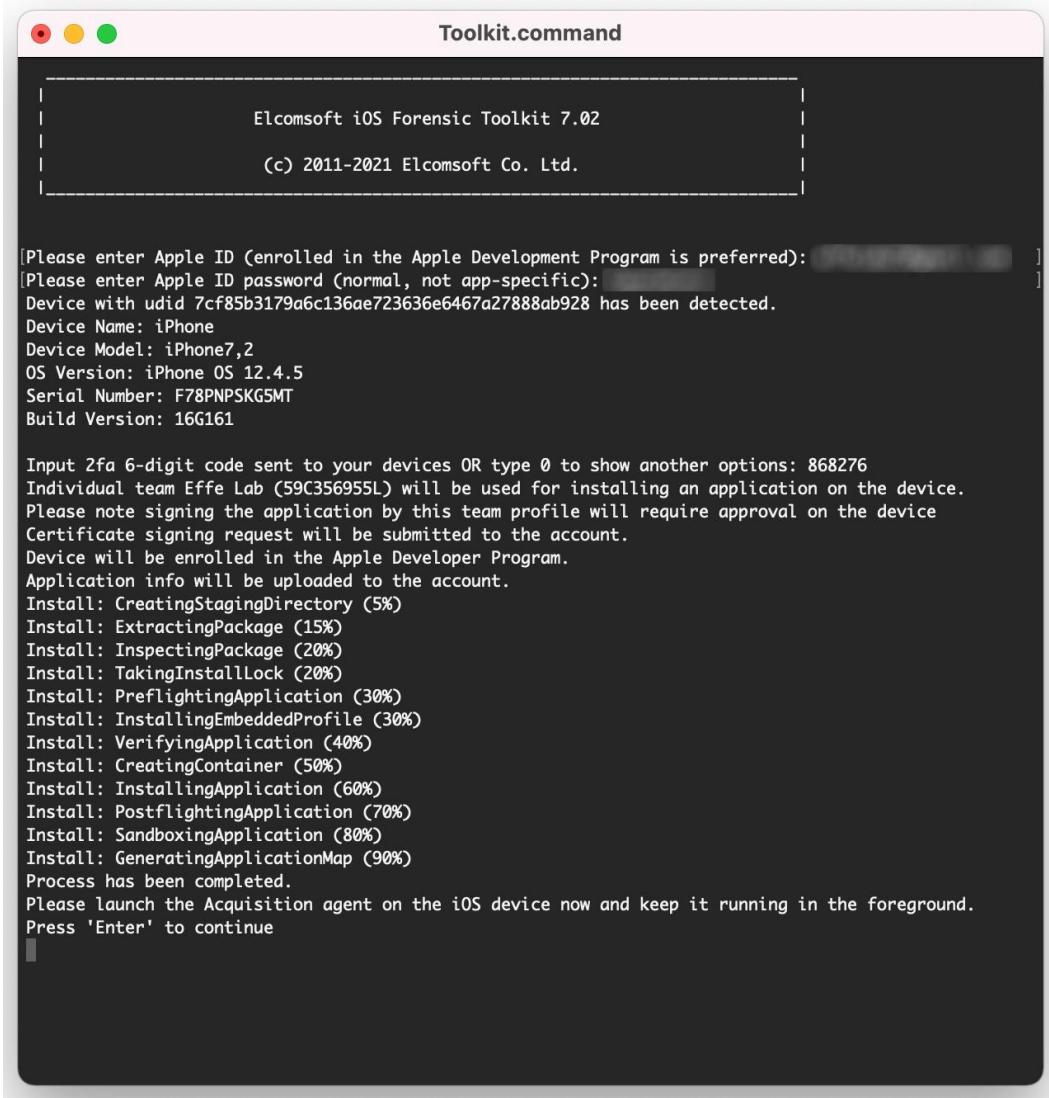
Legacy devices acquisition

A LEGACY	- Legacy devices acquisition (iPhone 4/5/5C)
----------	--

X EXIT

>: |

Figure 2.22 – Elcomsoft iOS Forensic Toolkit home screen



The screenshot shows a terminal window titled "Toolkit.command". The title bar has three colored circles (red, yellow, green) on the left. The main area displays the following text:

```
|           Elcomsoft iOS Forensic Toolkit 7.02           |
|           (c) 2011-2021 Elcomsoft Co. Ltd.           |
|
[Please enter Apple ID (enrolled in the Apple Development Program is preferred): ]]
[Please enter Apple ID password (normal, not app-specific): ]]

Device with udid 7cf85b3179a6c136ae723636e6467a27888ab928 has been detected.
Device Name: iPhone
Device Model: iPhone7,2
OS Version: iPhone OS 12.4.5
Serial Number: F78PNPSKG5MT
Build Version: 16G161

Input 2fa 6-digit code sent to your devices OR type 0 to show another options: 868276
Individual team Effe Lab (59C356955L) will be used for installing an application on the device.
Please note signing the application by this team profile will require approval on the device
Certificate signing request will be submitted to the account.
Device will be enrolled in the Apple Developer Program.
Application info will be uploaded to the account.
Install: CreatingStagingDirectory (5%)
Install: ExtractingPackage (15%)
Install: InspectingPackage (20%)
Install: TakingInstallLock (20%)
Install: PreflightingApplication (30%)
Install: InstallingEmbeddedProfile (30%)
Install: VerifyingApplication (40%)
Install: CreatingContainer (50%)
Install: InstallingApplication (60%)
Install: PostflightingApplication (70%)
Install: SandboxingApplication (80%)
Install: GeneratingApplicationMap (90%)
Process has been completed.
Please launch the Acquisition agent on the iOS device now and keep it running in the foreground.
Press 'Enter' to continue
```

Figure 2.23 – Installing the agent onto the device

```
Elcomsoft iOS Forensic Toolkit 7.02
(c) 2011-2021 Elcomsoft Co. Ltd.

[Write archive to directory <>>: /Users/tiepolo/
Device with udid 7cf85b3179a6c136ae723636e6467a27888ab928 has been detected.
Device Name: iPhone
Device Model: iPhone7,2
OS Version: iPhone OS 12.4.5
Serial Number: F78PNPSKG5MT
Build Version: 16G161

Please keep application in foreground while the image is being created.
Progress: 85%
File system imaging has been completed. Now you can close the acquisition agent on the device.
File has been saved to: /Users/tiepolo//7cf85b3179a6c136ae723636e6467a27888ab928_20210802T162918.tar
File hash (SHA-1): fa267dda0eb6bfffff1c192ba7e4125cec71

Total time elapsed: 226
Press 'Enter' to continue
```

**Figure 2.24 – Acquiring the full filesystem using the agent**

## Tables

	<b>checkra1n</b>	<b>unc0ver</b>
iPhone 6/6 Plus/6s/ 6s Plus	iOS 8–12.5 ✓	iOS 11–12.5 ✓
iPhone SE	iOS 9–14.8 ✓	iOS 11–14.3 ✓
iPhone 7/7 Plus	iOS 10–14.8 ✓	iOS 11–14.3 ✓
iPhone 8/8 Plus	iOS 11–14.8 ✓	iOS 11–14.3 ✓
iPhone X	iOS 11–14.8 ✓	iOS 11–14.3 ✓
iPhone XR	✗	iOS 12–14.3 ✓
iPhone XS/XS Max	✗	iOS 12–14.3 ✓
iPhone 11/11 Pro/11 Pro Max	✗	iOS 13–14.3 ✓
iPhone 12/12 Pro/12 Pro Max	✗	iOS 14–14.3 ✓
iPhone 13	✗	✗

**Table 2.1 – iPhone model compatibility with checkra1n and unc0ver**

## Code and Commands

Command 2.1:

```
brew install libimobiledevice
```

Command 2.2:

```
sudo apt-get install usbmuxd libimobiledevice6  
libimobiledevice-utils
```

Command 2.3

```
ideviceinfo
```

Command 2.4

```
ideviceinfo | grep ModelNumber
```

Command 2.5:

```
iDeviceinfo | grep ProductVersion
```

Command 2.6:

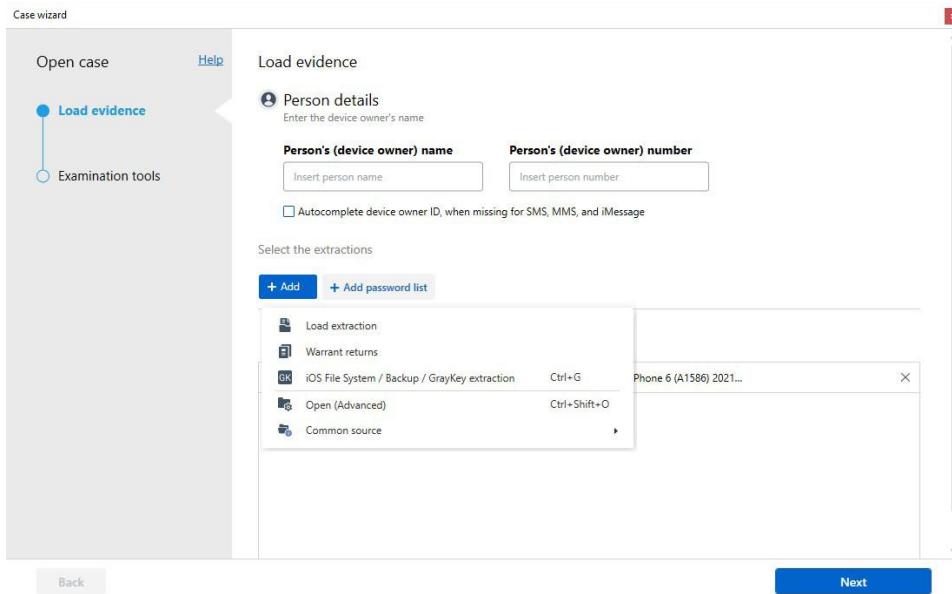
```
iDeviceinfo | grep SerialNumber
```

Command 2.7:

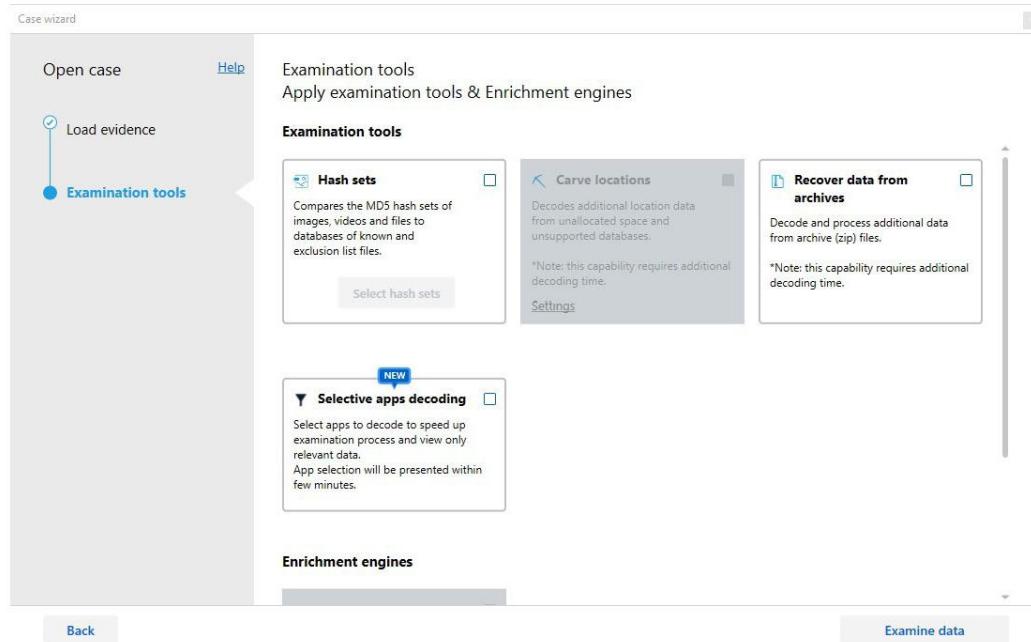
```
iDeviceinfo | grep PhoneNumber
```

# Chapter 3

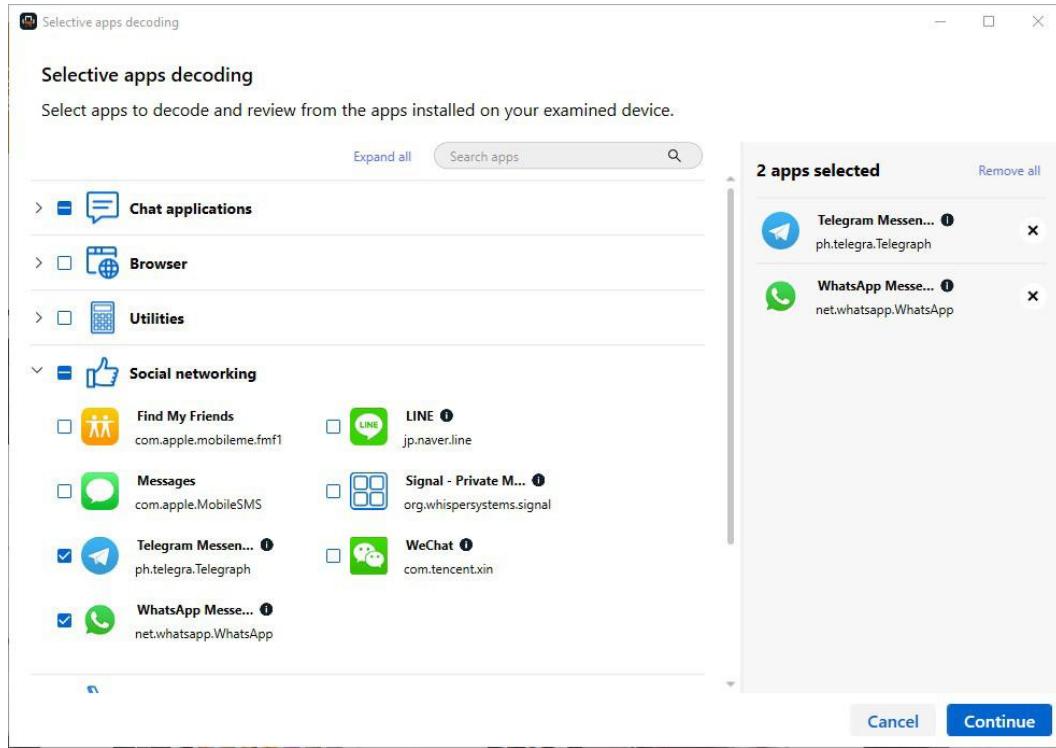
## Images



**Figure 3.1 – Open the case wizard and add the folder or file that contains your data**



**Figure 3.2 – The case wizard also allows you to enable specific examination tools**



**Figure 3.3 – Choose which applications should be decoded**

## Extraction Summary

Extractions: 1



File System - Selective apps decoding  
Apple iPhone 6 (A1586)  
File System  
  
Extraction start date/time  
28/07/2021 22:19:13(UTC+2)  
Extraction end date/time  
28/07/2021 22:47:49(UTC+2)  
C:\Users\LAB\Documents\My UFED Extra...

### Device Info

[Generate preliminary device report](#)

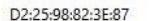
Advertising Id (IDFA) #1	AE8AOE64-8B2E-4E2D-9439-CB233DD9428E	<a href="#">com.apple.lsidentifiers.plist : 0xC4E</a>
AirDrop ID	A4E655FDBCE7	<a href="#">com.apple.sharingd.plist : 0x199F</a>
Apple ID	 [redacted]@apple.com	<a href="#">Accounts3.sqlite-wal : 0x1EFD1C</a>
Detected Phone Model	iPhone 6	<a href="#">External Enrichment</a>
iCloud account present	True	<a href="#">Accounts3.sqlite-wal : 0x1EF0C1</a>
Model number	N61AP	<a href="#">preferences.plist : 0xAAE</a>
Owner Name	iPhone	<a href="#">data_ark.plist : 0x23D</a>
Serial	F78PNPSKG5MT	<a href="#">AccountToken.txt : 0x449</a>
Time Zone	(UTC+01:00) Rome (Europe)	<a href="#">com.apple.AppStore.plist : 0x264</a>
Unique ID	7cf85b3179a6c136ae723636e6467a27888ab928	<a href="#">AccountToken.txt : 0x4BC</a>
ICCID	 [redacted]	<a href="#">com.apple.commcenter.plist : 0x202</a>
IMEI	 [redacted]	<a href="#">AccountToken.txt : 0x2D</a>
Last user ICCID	 [redacted]	<a href="#">CellularUsage.db : 0x6FD8</a>
Last used MSISDN	 +39311889077	<a href="#">CellularUsage.db : 0x6FEB</a>
MSISDN	 [redacted]	<a href="#">com.apple.commcenter.plist : 0x3FA</a>
<b>Network Interfaces</b>		
MAC address	D2:25:98:82:3E:78	<a href="#">NetworkInterfaces.plist : 0x26A</a>
MAC address	D2:25:98:82:3E:87	<a href="#">NetworkInterfaces.plist : 0x35D</a>
Wi-Fi MAC address	D0:25:98:82:3E:76	<a href="#">NetworkInterfaces.plist : 0x173</a>
<b>Phone Settings</b>		
Find my iPhone enabled	True	<a href="#">com.apple.icloud.findmydevice.FMIPAccounts.plist : 0x0</a>
Locale language	it_IT	<a href="#">data_ark.plist : 0x21</a>
Location Services Enabled	True	<a href="#">com.apple.locationd.plist : 0x7F</a>
Message Retention Duration	Forever	
<b>Tethering</b>		
Last Activation Time	28/07/2021 09:38:46(UTC+0)	

Figure 3.4 – Extraction Summary

Device Info		 Generate preliminary device report	
Advertising Id (IDFA) #1	AE8A0E64-8B2E-4E2D-9439-CB233DD9428E	<a href="#">com.apple.lsdd identifiers.plist : 0xC4E</a>	
AirDrop ID	A4E655FDBCE7	<a href="#">com.apple.sharingd.plist : 0x199F</a>	
Apple ID		<a href="#">Accounts3.sqlite-wal : 0x1EFD1C</a>	
Detected Phone Model	iPhone 6	External Enrichment	
iCloud account present	True	<a href="#">Accounts3.sqlite-wal : 0x1EF0C1</a>	
Model number	N61AP	<a href="#">preferences.plist : 0xAAE</a>	
Owner Name	iPhone	<a href="#">data_ark.plist : 0x23D</a>	
Serial		<a href="#">AccountToken.txt : 0x449</a>	
Time Zone	(UTC+01:00) Rome (Europe)	<a href="#">com.apple.AppStore.plist : 0x264</a>	
Unique ID	7cf85b3179a6c136ae723636e6467a27888ab928	<a href="#">AccountToken.txt : 0x4BC</a>	
ICCID	893950000005372957	<a href="#">com.apple.commcenter.plist : 0x202</a>	
IMEI	359281066791552	<a href="#">AccountToken.txt : 0x2D</a>	
Last user ICCID	893950000005372957	<a href="#">CellularUsage.db : 0x6FD8</a>	
Last used MSISDN		<a href="#">com.apple.commcenter.plist : 0x3FA</a>	
MSISDN		<a href="#">NetworkInterfaces.plist : 0x26A</a>	
<b>Network Interfaces</b>		<a href="#">NetworkInterfaces.plist : 0x35D</a>	
MAC address	D2:25:98:82:3E:78	<a href="#">NetworkInterfaces.plist : 0x173</a>	
MAC address	D2:25:98:82:3E:87		
Wi-Fi MAC address	D0:25:98:82:3E:76		
<b>Phone Settings</b>			
Find my iPhone enabled	True	<a href="#">com.apple.icloud.findmydevice.FMIPAccounts.plist : 0x0</a>	
Locale language	it_IT	<a href="#">data_ark.plist : 0x221</a>	
Location Services Enabled	True	<a href="#">com.apple.locationd.plist : 0x7F</a>	
Message Retention Duration	Forever		
<b>Tethering</b>			
Last Activation Time	28/07/2021 09:38:46(UTC+0)		

**Figure 3.5 – The Device Info section gives the investigator some key data on the device**

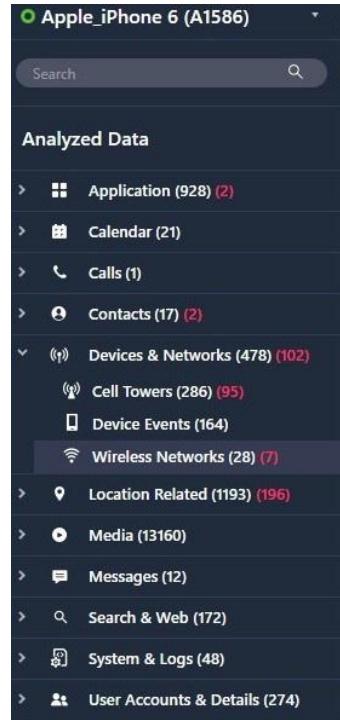


Figure 3.6 – The project tree displays all decoded data grouped into categories

A screenshot of the Physical Analyzer interface. At the top are buttons for "Add extraction", "Add external file", "Project settings", and "Generate report". Below is a section titled "Insights from Installed Apps" with a red border. It lists app categories with their counts: Chat applications (3 apps), Social networking (6 apps), Browser (1 apps), Lifestyle (5 apps), Hide files or pictures (1 apps), Entertainment (3 apps), Utilities (20 apps), and News &amp; Books (2 apps). A blue "View all" button is at the bottom right of this section. A small "..." icon is in the bottom right corner of the entire interface.

Figure 3.7 – Physical Analyzer extraction summary

### Select apps for more data

Browse the apps on the device sorted by category and select the apps for which you require additional data.

Note: Internal application services are not displayed in this view

Select apps for more data				
Refine by: ▾ Expand all Search apps				
> <input type="checkbox"/>  Chat applications		0 of 3 apps decoded by Cellebrite		
> <input type="checkbox"/>  Browser	 Apps no longer in store: 1	0 of 1 apps decoded by Cellebrite		
> <input type="checkbox"/>  Hide files or pictures		0 of 1 apps decoded by Cellebrite		
> <input type="checkbox"/>  Utilities	 Apps no longer in store: 6	2 of 20 apps decoded by Cellebrite		
> <input type="checkbox"/>  Social networking	 Apps no longer in store: 1	0 of 6 apps decoded by Cellebrite		
> <input checked="" type="checkbox"/>  Lifestyle	 Apps no longer in store: 2	0 of 5 apps decoded by Cellebrite		
<input type="checkbox"/>  com.apple.camera	 com.apple.Home	 com.apple.mobile...	 Snapchat 	com.toyopagroup.picaboo
<input checked="" type="checkbox"/> Uber  com.ubercab.UberClient				
> <input type="checkbox"/>  Entertainment		0 of 3 apps decoded by Cellebrite		
> <input type="checkbox"/>  News & Books		0 of 2 apps decoded by Cellebrite		
> <input type="checkbox"/>  Finance		0 of 2 apps decoded by Cellebrite		
> <input type="checkbox"/>  Music		0 of 1 apps decoded by Cellebrite		
> <input type="checkbox"/>  Health & Fitness	 Apps no longer in store: 1	0 of 1 apps decoded by Cellebrite		

Figure 3.8 – A list of applications installed on the device

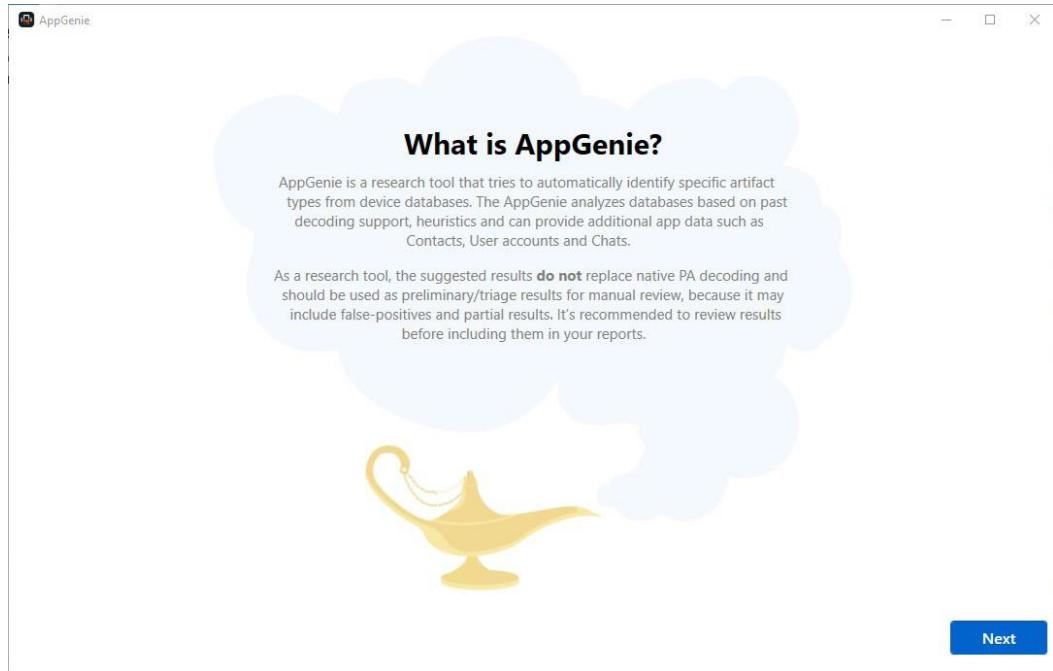


Figure 3.9 – A reminder that validation is required

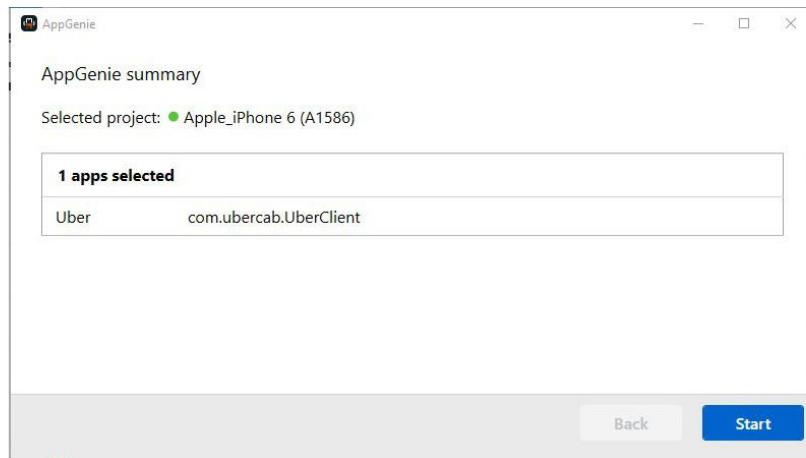


Figure 3.10 – A summary of applications that should be parsed by the AppGenie

## CASE DETAILS

**CASE INFORMATION**

Case number

Case type

**LOCATION FOR CASE FILES**

Folder name

File path  [BROWSE](#)

Available space: 840.47 GB

**LOCATION FOR ACQUIRED EVIDENCE**

Folder name

File path  [BROWSE](#)

Available space: 840.47 GB

**SCAN INFORMATION**

**SCAN 1**

Scanned by

Description

**REPORT OPTIONS**

Cover logo  [BROWSE](#)

Image resized to 150x150 pixels

Figure 3.11 – Fill in the case details

MOBILE

SELECT EVIDENCE SOURCE



ANDROID



IOS



WINDOWS PHONE



KINDLE FIRE



MEDIA DEVICE (MTP)



SIM CARD

Figure 3.12 – Select the evidence source

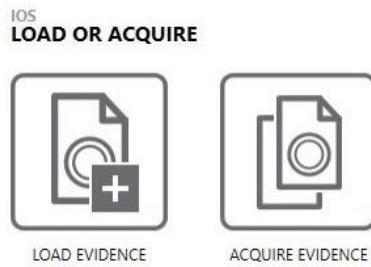


Figure 3.13 – Choose the file or folder that contains the extraction

The image shows a software interface titled "EVIDENCE SOURCES". At the top, there is a section titled "SELECT EVIDENCE SOURCE" with four icons: "COMPUTER" (monitor), "MOBILE" (smartphone), "CLOUD" (cloud), and "REMOTE COMPUTER" (monitor with a network connection icon). Below this is a section titled "EVIDENCE SOURCES ADDED TO CASE" which contains a table with one row. The table has columns for "Type", "Image - location name", "Evidence number", "Search type", and "Status". The "Type" column shows "Image". The "Image - location name" column is empty. The "Evidence number" column is empty. The "Search type" column is empty. The "Status" column is empty. At the bottom of the screen are two buttons: "BACK" and "GO TO PROCESSING DETAILS".

Type	Image - location name	Evidence number	Search type	Status
Image				

Figure 3.14 – The EVIDENCE SOURCES screen displays all data sources for the case

## PROCESSING DETAILS

### ADD KEYWORDS TO SEARCH

Provide the keywords and regular expressions that you want to include in your search. If a keyword gets a hit during the search, it's added to a Keywords filter in AXIOM Examine.

[ADD KEYWORDS TO SEARCH](#)

### CATEGORIZE CHATS WITH MAGNET.AI

Enable chat categories so that AXIOM Examine automatically categorizes chat conversations, based on the categories you select, and tags them in the Artifacts explorer.

[CATEGORIZE CHATS WITH MAGNET.AI](#)

### SEARCH ARCHIVES AND MOBILE BACKUPS

Container files such as archives and mobile backups can be found within other evidence sources. Configure options on this page to search any containers found during your search.

[SEARCH ARCHIVES AND MOBILE BACKUPS](#)

### CALCULATE HASH VALUES

Import hashes for non-relevant files so they don't appear in your case.

[CALCULATE HASH VALUES](#)

### CATEGORIZE PICTURES AND VIDEOS

You can enable picture categories so that AXIOM Examine automatically categorizes and tags them in the Artifacts explorer.

[CATEGORIZE PICTURES AND VIDEOS](#)

### FIND MORE ARTIFACTS

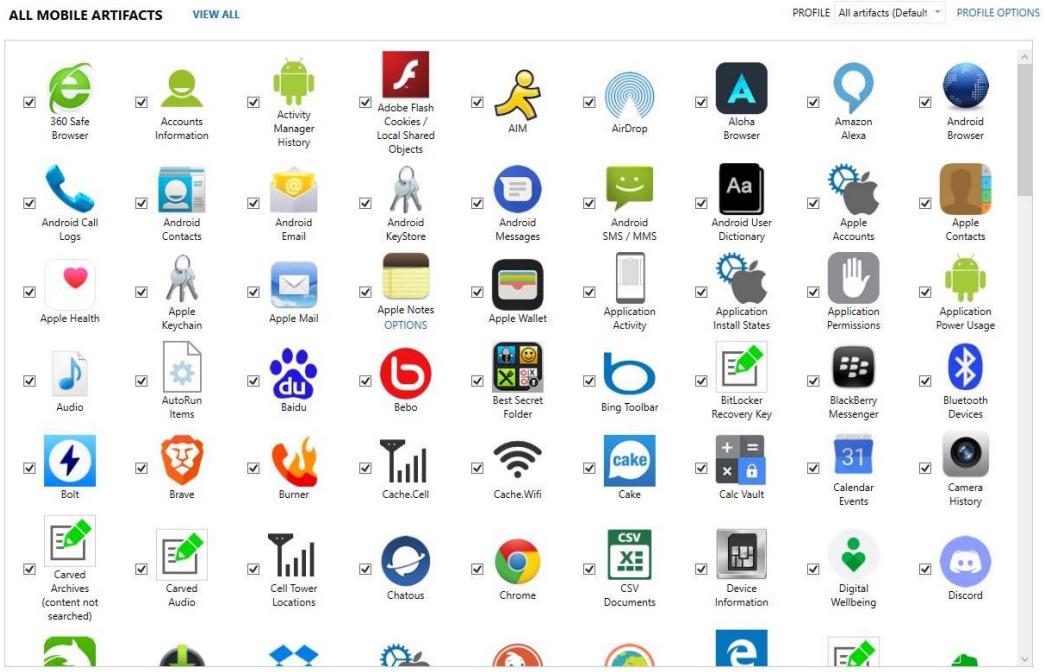
Enable the Dynamic App Finder and configure the Custom File Types list to search for artifacts that aren't currently supported by Magnet AXIOM.

[FIND MORE ARTIFACTS](#)

[BACK](#)

[GO TO ARTIFACT DETAILS](#)

Figure 3.15 – Enable additional parsing tools and utilities



**Figure 3.16 – Choose which artifacts should be decoded**

File Tools Process Help

Case dashboard

### CASE OVERVIEW

#### CASE SUMMARY NOTES

Record your case summary notes here. These notes will appear in the case report when the setting is enabled.

Examiner name: Effesecurity Lab

Case summary:

#### CASE PROCESSING DETAILS

##### CASE NUMBER

SCAN 1

Scanned by: Effesecurity Lab  
Scan date: 11/08/2021 00:10:49

Scan description:

#### CASE INFORMATION

The Case Information.txt file contains information about how the case was processed. For example, the file includes the settings that were applied to the search, search type, number of artifacts discovered, and more.

[OPEN CASE INFORMATION FILE](#)

The AXIOMExamine.log file contains information about any errors encountered, jobs that were run, and general debugging information.

[OPEN LOG FILE](#)

### EVIDENCE OVERVIEW

#### FullFileSystem.1.dar (545)

VIEW EVIDENCE FOR THIS SOURCE ONLY

Evidence number: FullFileSystem.1.dar

Description:

Location: FullFileSystem.1.dar

Platform: Mobile

No picture added

CHANGE PICTURE

Figure 3.17 – The Case dashboard screen

**EVIDENCE (26)**

Column view ▾

Potential Activity	Artifact	Artif...	Source
At Facebook home page	WebKit Browser Web History (Carved)	108	FullFileSystem.1.dar\Applications\MobileSafari.app\BuiltInBookmarkItems.plist
At Facebook home page	Safari History	149	FullFileSystem.1.dar\Applications\MobileSafari.app\BuiltInBookmarkItems.plist
At Facebook home page	Safari History	149	FullFileSystem.1.dar\private\var\db\uuidtext\9E\12E6B290D344DA2002AECB9...
Unknown	Potential Browser Activity	11617	FullFileSystem.1.dar\private\var\db\uuidtext\9E\12E6B290D344DA2002AECB9...
Looking at Facebook legal information	Potential Browser Activity	11623	FullFileSystem.1.dar\private\var\db\uuidtext\9E\12E6B290D344DA2002AECB9...
Looking at Facebook legal information	Potential Browser Activity	11621	FullFileSystem.1.dar\private\var\db\uuidtext\9E\12E6B290D344DA2002AECB9...
Looking at Facebook legal information	Potential Browser Activity	11631	FullFileSystem.1.dar\private\var\db\uuidtext\49\0116807F93F48AD657DE2768...
At Facebook home page	KnowledgeC Application Web Usage	14397	FullFileSystem.1.dar\private\var\mobile\Library\CoreDuet\Knowledge\knowledg...
At Facebook login page	KnowledgeC Application Web Usage	14397	FullFileSystem.1.dar\private\var\mobile\Library\CoreDuet\Knowledge\knowledg...
At Facebook home page	KnowledgeC Application Web Usage	14404	FullFileSystem.1.dar\private\var\mobile\Library\CoreDuet\Knowledge\knowledg...
At Facebook login page	KnowledgeC Application Web Usage	14404	FullFileSystem.1.dar\private\var\mobile\Library\CoreDuet\Knowledge\knowledg...
At Facebook home page	KnowledgeC Application Web Usage	14407	FullFileSystem.1.dar\private\var\mobile\Library\CoreDuet\Knowledge\knowledg...
At Facebook login page	KnowledgeC Application Web Usage	14407	FullFileSystem.1.dar\private\var\mobile\Library\CoreDuet\Knowledge\knowledg...
At Facebook home page	KnowledgeC Application Web Usage	14410	FullFileSystem.1.dar\private\var\mobile\Library\CoreDuet\Knowledge\knowledg...
Unknown	KnowledgeC Application Web Usage	14410	FullFileSystem.1.dar\private\var\mobile\Library\CoreDuet\Knowledge\knowledg...
Unknown	KnowledgeC Safari History	15102	FullFileSystem.1.dar\private\var\mobile\Library\CoreDuet\Knowledge\knowledg...
At Facebook login page	KnowledgeC Safari History	15119	FullFileSystem.1.dar\private\var\mobile\Library\CoreDuet\Knowledge\knowledg...
At Facebook login page	KnowledgeC Safari History	15161	FullFileSystem.1.dar\private\var\mobile\Library\CoreDuet\Knowledge\knowledg...
Unknown	Safari History	22789	FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\45D7E9EB...
At Facebook login page	Safari History	22789	FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\45D7E9EB...
At Facebook login page	Safari History	22791	FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\45D7E9EB...
Unknown	Safari History	22950	FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\45D7E9EB...
At Facebook login page	Safari History	22952	FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\45D7E9EB...
Unknown	Potential Browser Activity	23110	FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\45D7E9EB...
Unknown	Safari History	23191	FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\45D7E9EB...
At Facebook login page	Safari History	23193	FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\45D7E9EB...

**Figure 3.18 – The Artifacts explorer**

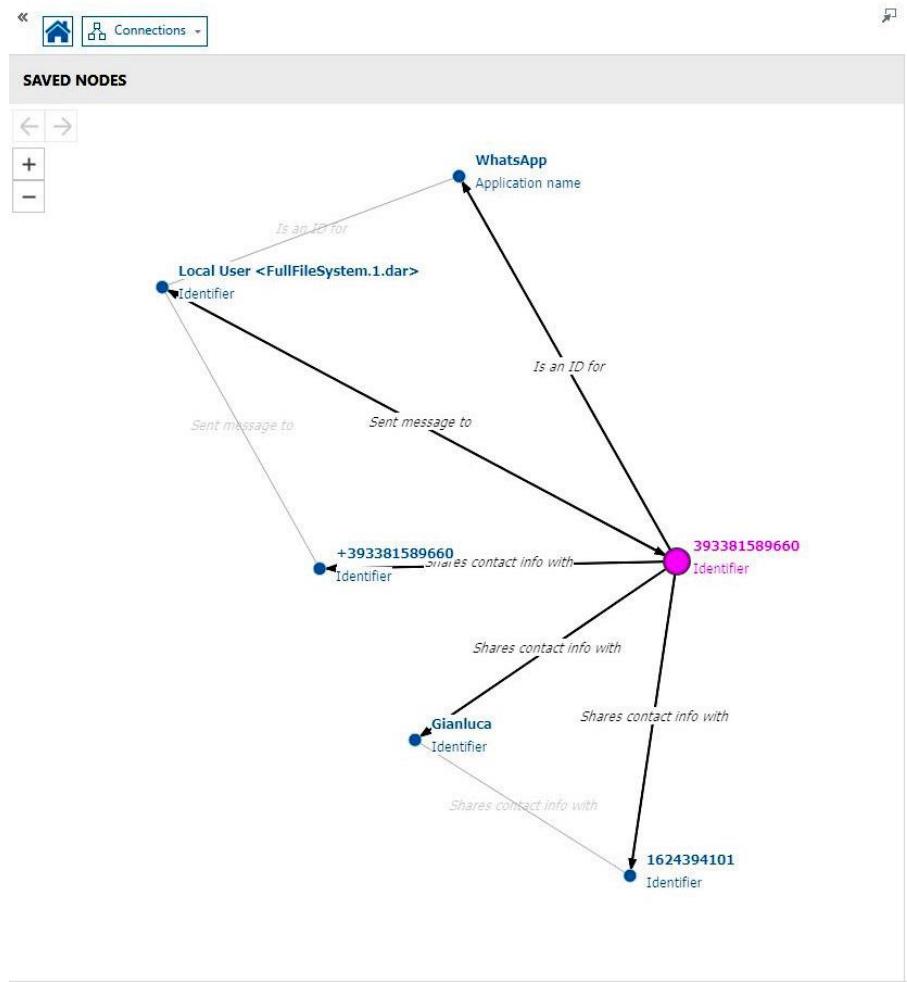


Figure 3.19 – The Connections explorer

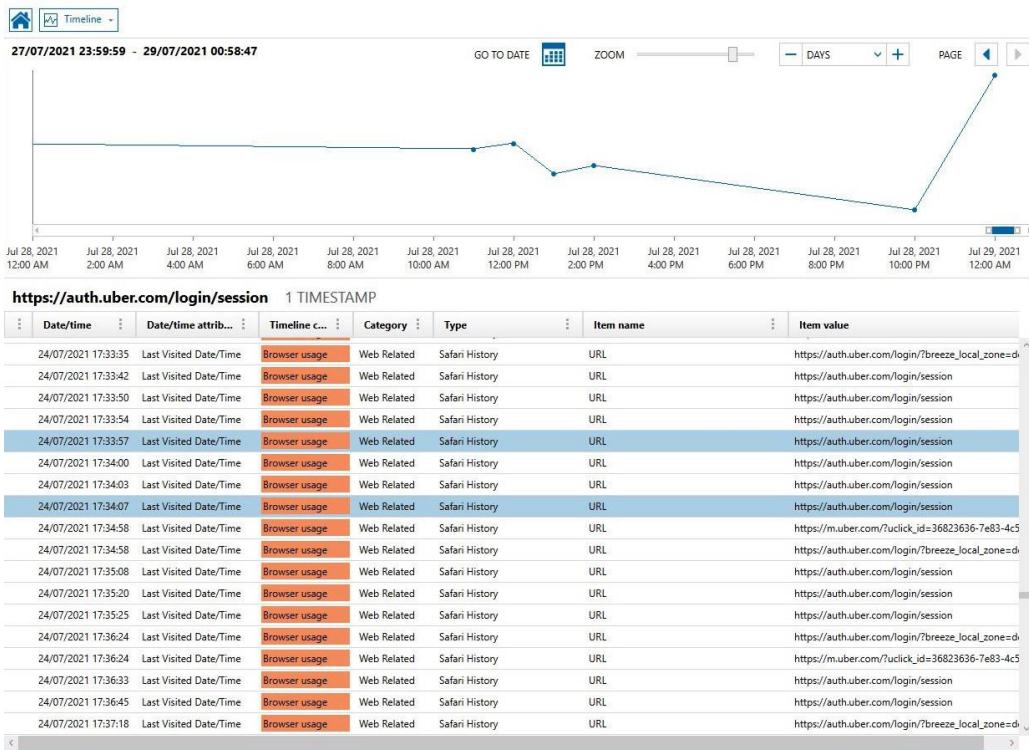


Figure 3.20 – The Timeline explorer

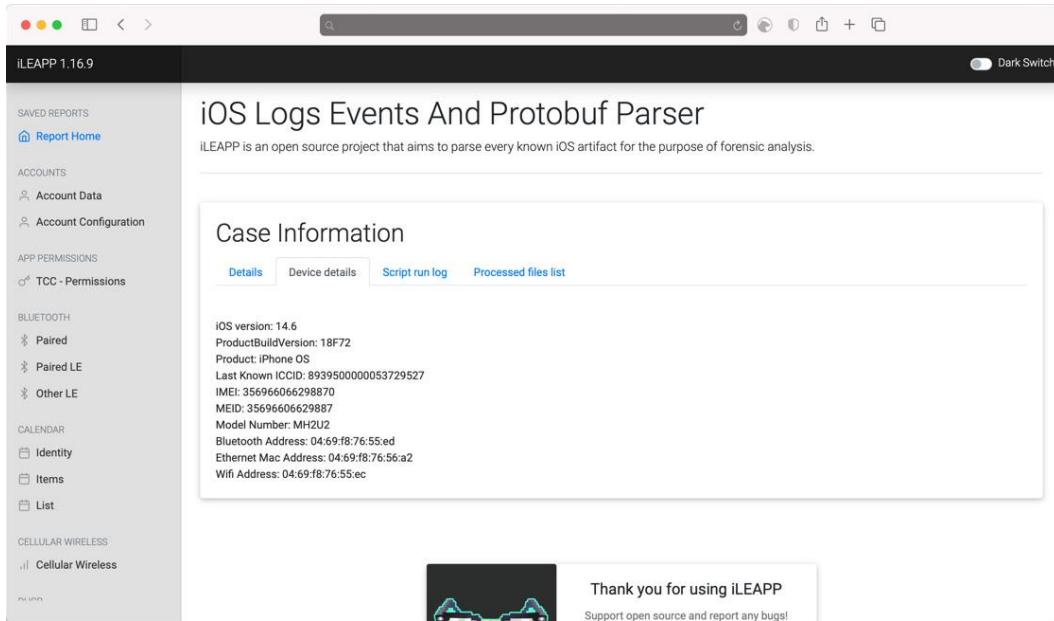


Figure 3.21 – The report generated by iLEAPP

## Code and Commands

Command 3.1

```
git clone https://github.com/abrignoni/iLEAPP.git
```

Command 3.2:

```
cd iLEAPP  
pip install -r requirements.txt
```

Command 3.3:

```
python3 ileapp.py -t zip -i ../iphone_dump.zip -o output
```

## Links

- You can download APOLLO from the project's GitHub repository:  
<https://github.com/mac4n6/APOLLO>

- iLEAPP can be downloaded from <https://github.com/abrigon/iLEAPP>.
- You can download this iOS Triage from GitHub:  
[https://github.com/RealityNet/ios\\_triage](https://github.com/RealityNet/ios_triage).
- You can download the Sysdiagnose scripts from  
[https://github.com/cheeky4n6monkey/iOS\\_sysdiagnose\\_forensic\\_scripts](https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts).

# Chapter 4

## Images

	ROWID	text
1	25	By the way... you should change that password ;-)
2	24	Thanks!
3	22	Hey, I forgot the password to the EC2 instance, what is it?
4	21	That would be great 
5	20	We can watch the late show ..I think it starts at 9.45

Execution finished without errors.  
Result: 5 rows returned in 18ms  
At line 1:  
SELECT ROWID, text FROM message ORDER BY ROWID DESC LIMIT 5;

Figure 4.1 – The result of a query displayed in DB Browser for SQLite

```
00000000  53 51 4c 69 74 65 20 66  6f 72 6d 61 74 20 33 00 |SQLite format 3.|  
00000010  10 00 02 02 00 40 20 20  00 00 00 13 00 00 00 43 |.....@ .....C|  
00000020  00 00 00 00 00 00 00 00  00 00 00 50 00 00 00 04 |.....P....|  
00000030  00 00 00 00 00 00 00 00  00 00 00 01 00 00 00 00 |.....|  
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 |.....|  
00000050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 13 |.....|  
00000060  00 2e 24 80                                     |..$.|  
00000064
```

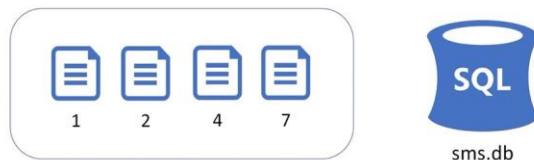
Figure 4.2 – The output from the hexdump command

Offset	Size	Description
0	16	The header string: "SQLite format 3\000"
16	2	The database page size in bytes.
18	1	File format write version. 1 for legacy; 2 for <a href="#">WAL</a> .
19	1	File format read version. 1 for legacy; 2 for <a href="#">WAL</a> .
20	1	Bytes of unused "reserved" space at the end of each page. Usually 0.
21	1	Maximum embedded payload fraction. Must be 64.
22	1	Minimum embedded payload fraction. Must be 32.
23	1	Leaf payload fraction. Must be 32.
24	4	File change counter.
28	4	Size of the database file in pages. The "in-header database size".
32	4	Page number of the first freelist trunk page.
36	4	Total number of freelist pages.
40	4	The schema cookie.
44	4	The schema format number. Supported schema formats are 1, 2, 3, and 4.
48	4	Default page cache size.
52	4	The page number of the largest root b-tree page when in auto-vacuum or zero otherwise.
56	4	The database text encoding. A value of 1 means UTF-8. A value of 2 means UTF-16le. A value of 3 means UTF-16be.
60	4	The "user version" as read and set by the <a href="#">user_version pragma</a> .
64	4	True (non-zero) for incremental-vacuum mode. False (zero) otherwise.
68	4	The "Application ID" set by <a href="#">PRAGMA application_id</a> .
72	20	Reserved for expansion. Must be zero.
92	4	The <a href="#">version-valid-for number</a> .
96	4	<a href="#">SQLITE_VERSION_NUMBER</a>

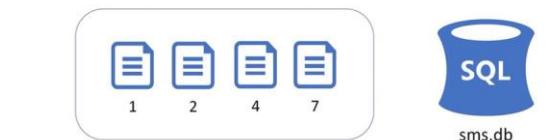
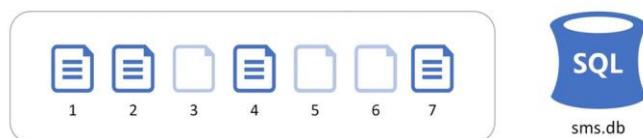
Figure 4.3 – The SQLite database header reference

Offset	Size	Description
0	1	The one-byte flag at offset 0 indicating the b-tree page type. <ul style="list-style-type: none"> <li>A value of 2 (0x02) means the page is an interior index b-tree page.</li> <li>A value of 5 (0x05) means the page is an interior table b-tree page.</li> <li>A value of 10 (0xa) means the page is a leaf index b-tree page.</li> <li>A value of 13 (0xd) means the page is a leaf table b-tree page.</li> </ul>
1	2	The two-byte integer at offset 1 gives the start of the first freeblock on the page, or is zero if there are no freeblocks.
3	2	The two-byte integer at offset 3 gives the number of cells on the page.
5	2	The two-byte integer at offset 5 designates the start of the cell content area. A zero value for this integer is interpreted as 65536.
7	1	The one-byte integer at offset 7 gives the number of fragmented free bytes within the cell content area.
8	4	The four-byte page number at offset 8 is the right-most pointer. This value appears in the header of interior b-tree pages only and is omitted from all other pages.

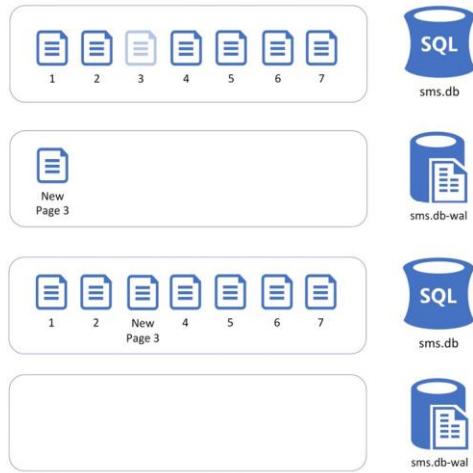
Figure 4.4 – The SQLite page header reference



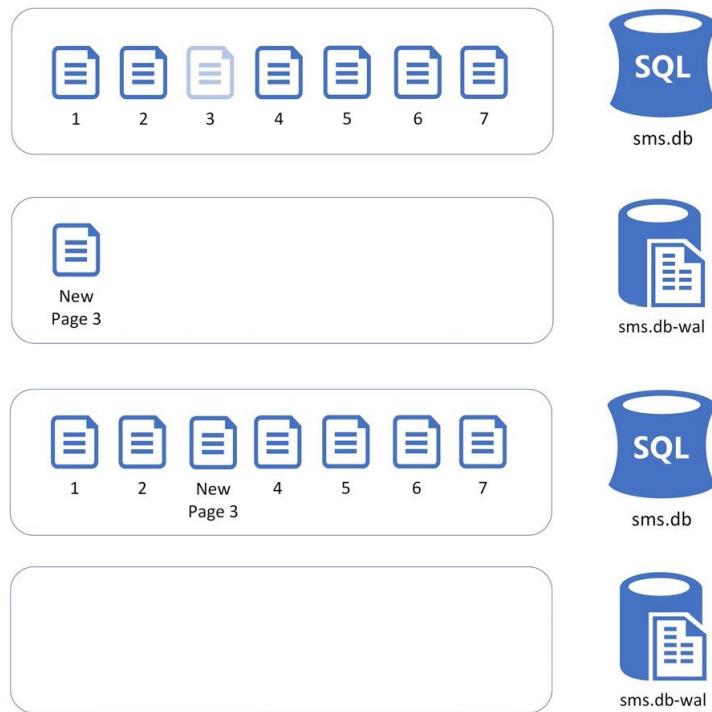
**Figure 4.5 – Pages in a fragmented SQLite database**



**Figure 4.6 – Pages in an SQLite database after the vacuuming process**



**Figure 4.7 – New records added to the database are appended to the WAL file**



**Figure 4.8 – A checkpoint transfers data from the WAL file back into the main database**

Offset	Size	Description
0	4	Magic number. 0x377f0682 or 0x377f0683
4	4	File format version. Currently 3007000.
8	4	Database page size. Example: 1024
12	4	Checkpoint sequence number
16	4	Salt-1: random integer incremented with each checkpoint
20	4	Salt-2: a different random number for each checkpoint
24	4	Checksum-1: First part of a checksum on the first 24 bytes of header
28	4	Checksum-2: Second part of the checksum on the first 24 bytes of header

Figure 4.9 – The WAL file header

Offset	Size	Description
0	4	Page number
4	4	The size of the database file in pages after the commit
8	4	Salt-1 copied from the WAL header
12	4	Salt-2 copied from the WAL header
16	4	Checksum-1: Cumulative checksum up through and including this page
20	4	Checksum-2: Second half of the cumulative checksum.

Figure 4.10 – The WAL frame header

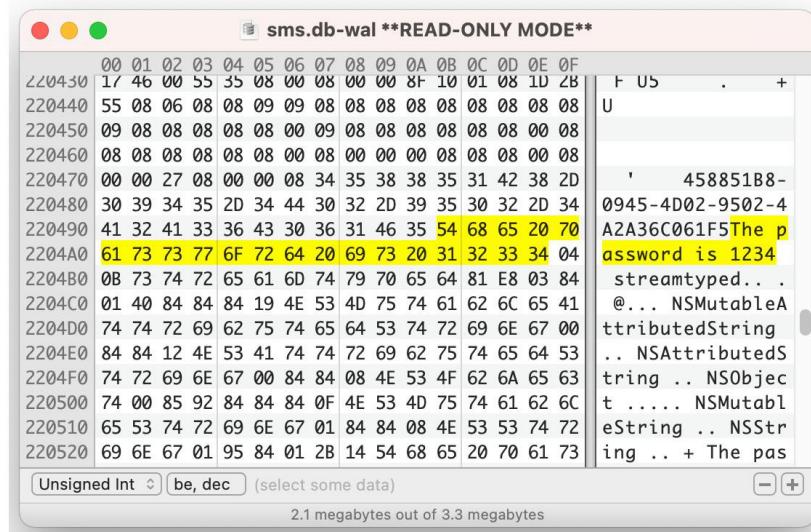


Figure 4.11 – Using a hex viewer to display the contents of an SQLite file

1    **SELECT \* FROM Fruits;**

ROWID	Fruit
1	Peach
2	Orange
3	Banana

Figure 4.12 – The table contains three rows of data

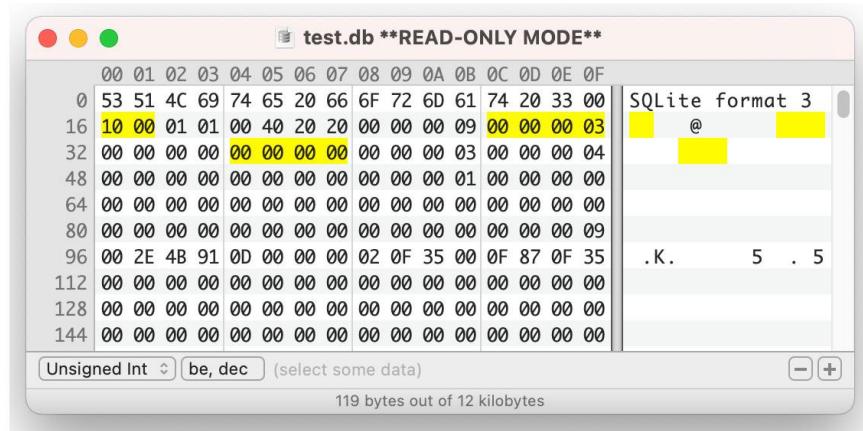


Figure 4.13 – The SQLite database header

Page	Offset (Dec)	Offset (HEX)
1	0	0x0000
2	4096	0x1000
3	8192	0x2000

Figure 4.14 – The decimal offset for each page

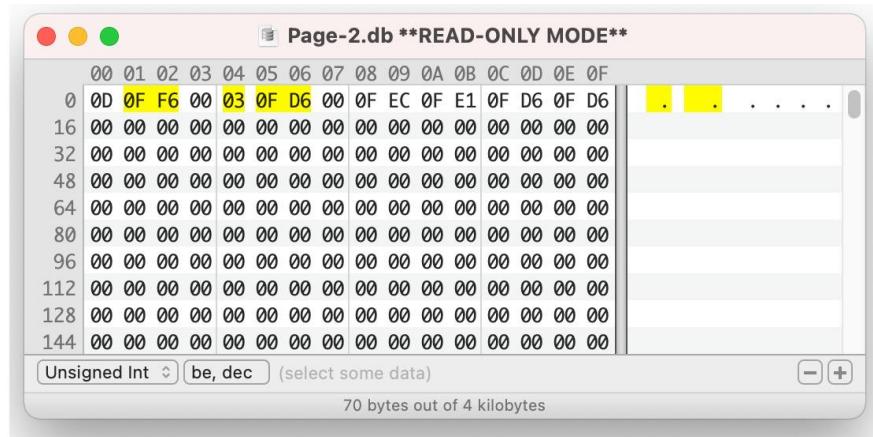


Figure 4.15 – The page header

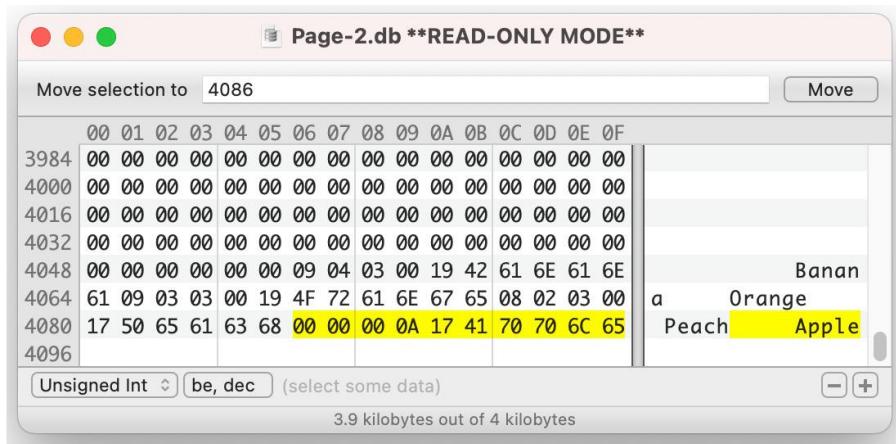


Figure 4.16 – The free block shows previously deleted data

FQLite Carving Tool

File Info

data bases

- sms.db
  - \_SqliteDatabaseProperties
  - \_UNASSIGNED
  - chat
    - chat\_idx\_chat\_identifier
    - chat\_idx\_chat\_identifier\_service\_name
    - chat\_idx\_is\_archived
    - chat\_message\_join
    - chat\_message\_join\_idx\_chat\_id
    - chat\_message\_join\_idx\_message\_date
    - chat\_message\_join\_idx\_message\_id\_oi
    - message\_idx\_associated\_message
    - message\_idx\_cache\_has\_attachments
    - message\_idx\_date
    - message\_idx\_expire\_state
    - message\_idx\_failed
    - message\_idx\_handle
    - message\_idx\_handle\_id
    - message\_idx\_isRead\_isFromMe\_itemT
    - message\_idx\_is\_read
    - message\_idx\_is\_sent\_is\_from\_me\_err

INFO: Couldn't locate any free pages to recover.  
Lines after free page recovery: 0  
Start with scan...  
Duration of scanning all pages in ms : 187  
End of Scan...  
Number of records recovered: 326

Ready

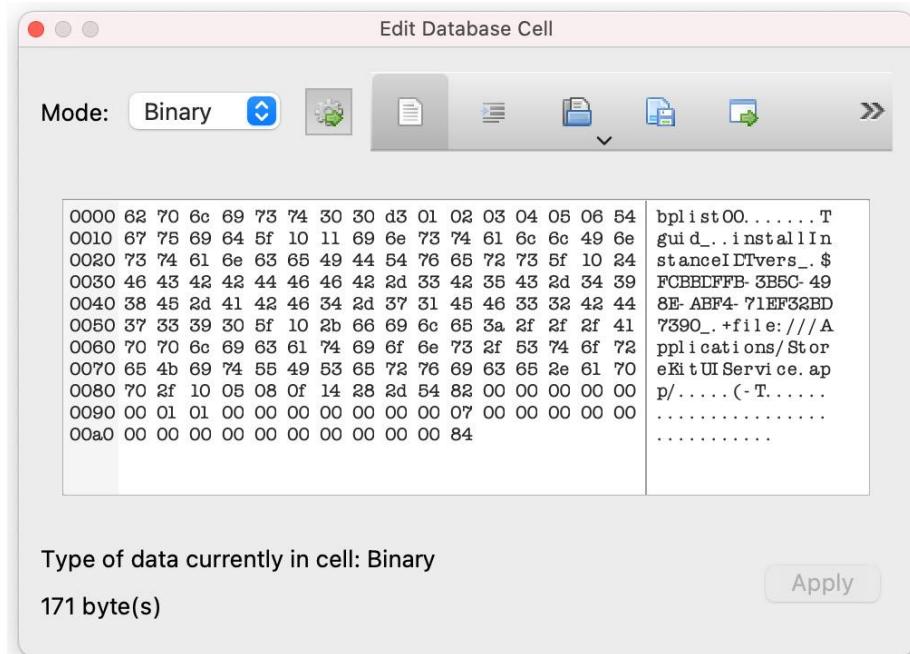
...	Offset	com...	d...	wal...	salt1	salt2	... guid	text
1	180E68	true	65	430	1442624...	860043617	22	8C4A270... Hey, I forgot the password to the EC2 instance, what is it?
10	1D71FA	true	65	468	1442624...	860043617	22	8C4A270... Hey, I forgot the password to the EC2 instance, what is it?
11	1D740F	true	65	468	1442624...	860043617	21	04E6930... Chat would be great.
12	1D759F	true	65	468	1442624...	860043617	21	465A798... We can watch the late show ...I think it starts at 9.45
13	1E6362	true	65	483	1442624...	860043617	22	8C4A270... Hey, I forgot the password to the EC2 instance, what is it?
14	1E6577	true	65	483	1442624...	860043617	21	04E6930... Chat would be great.
15	1E6761	true	65	483	1442624...	860043617	20	465A798... We can watch the late show ...I think it starts at 9.45
16	1F54C2	true	65	498	1442624...	860043617	22	8C4A270... Hey, I forgot the password to the EC2 instance, what is it?
17	1F56DF	true	65	498	1442624...	860043617	21	04E6930... Chat would be great.
18	1F58C9	true	65	498	1442624...	860043617	20	465A798... We can watch the late show ...I think it starts at 9.45
19	1F8502	true	65	501	1442624...	860043617	22	8C4A270... Hey, I forgot the password to the EC2 instance, what is it?
2	1B107E	true	65	430	1442624...	860043617	21	04E6930... Chat would be great.
20	1F8727	true	65	501	1442624...	860043617	21	04E6930... Chat would be great.
21	1F8911	true	65	501	1442624...	860043617	20	465A798... We can watch the late show ...I think it starts at 9.45
22	22042E	true	65	541	1442624...	860043617	23	4588518... The password is 1234
23	2208C2	true	65	541	1442624...	860043617	22	8C4A270... Hey, I forgot the password to the EC2 instance, what is it?
24	220AE7	true	65	541	1442624...	860043617	21	04E6930... Chat would be great.
25	220CD1	true	65	541	1442624...	860043617	20	465A798... We can watch the late show ...I think it starts at 9.45
26	225A55	true	65	546	1442624...	860043617	23	4588518... The password is 1234
27	22593A	true	65	546	1442624...	860043617	22	8C4A270... Hey, I forgot the password to the EC2 instance, what is it?
28	225B5F	true	65	546	1442624...	860043617	21	04E6930... Chat would be great.
29	225D49	true	65	546	1442624...	860043617	20	465A798... We can watch the late show ...I think it starts at 9.45
3	1B1269	true	65	430	1442624...	860043617	23	4588518... The password is 1234
30	22D561	true	65	554	1442624...	860043617	23	4588518... We can watch the late show ...I think it starts at 9.45
31	22D9FA	true	65	554	1442624...	860043617	22	8C4A270... Hey, I forgot the password to the EC2 instance, what is it?

Figure 4.17 – FQLite recovers deleted records from an SQLite database

Table: kvs

	<b>id</b>	<b>application_identifier</b>	<b>key</b>	<b>value</b>
1	44		24	3 BLOB
2	46		26	3 BLOB
3	47		27	3 BLOB
4	48		28	3 BLOB
5	49		29	3 BLOB
6	50		30	3 BLOB
7	51		31	3 BLOB
8	52		32	3 BLOB
9	53		33	3 BLOB
10	54		34	3 BLOB

Figure 4.18 – A SQLite database containing BLOBS of binary data



**Figure 4.19 – The hex viewer shows the bplist in binary format**

Path	Description
installd/Library/MobileInstallation/LastBuildInfo.plist	OS version
mobile/Library/Preferences/com.apple.springboard.plist	Order of apps
mobile/Library/Preferences/com.apple.mobilegestalt.plist	Device name
mobile/Library/Preferences/com.apple.Preferences.plist	Disk usage
mobile/Library/Preferences/com.apple.purplebuddy.plist	Language
mobile/Library/Preferences/com.apple.commcenter.shared.plist	Phone number
mobile/Library/Preferences/com.apple.corerecents.recentsd.plist	iCloud data
preferences/SystemConfiguration/com.apple.networkidentification.plist	Network data
preferences/SystemConfiguration/NetworkInterfaces.plist	WiFi data
preferences/SystemConfiguration/preferences.plist	Cellular + WiFi

**Figure 4.20 – Common iOS device artifacts**

Path	Description
mobile/Library/Mail/Recents.db	Recent SMS and email metadata
mobile/Media/Recordings/Recordings.db	Audio recordings
mobile/Media/PhotoData/Photos.sqlite	Photo categorization
mobile/Library/CallHistoryDB/CallHistory.storedata	Call log
mobile/Library/SMS/sms.db	SMS/MMS/iMessage
mobile/Library/Safari/History.db	Browsing history
mobile/Media/DCIM/*	Photos
mobile/Library/Accounts/Accounts3.sqlite	Account details

**Figure 4.21 – Common iOS user artifacts**

## Code and Commands

Code 4.1:

```
SELECT ROWID, text FROM message
ORDER BY ROWID DESC
LIMIT 5;
```

Command 4.1:

```
sqlite3 filename.db
```

Command 4.2:

```
sqlite> .tables
attachment          message
```

chat	message_attachment_join
chat_handle_join	message_processing_task
chat_message_join	sync_deleted_attachments
deleted_messages	sync_deleted_chats

**Command 4.3:**

```
sqlite> .schema handle
CREATE TABLE handle (ROWID INTEGER PRIMARY KEY
AUTOINCREMENT UNIQUE, id TEXT NOT NULL, country TEXT,
service TEXT NOT NULL);
```

**Command 4.4:**

```
SELECT * FROM handle;
```

**Command 4.5:**

```
hexdump -n 100 -C sms.db
```

**Command 4.6:**

```
CREATE TABLE "Fruits" (
    "ROWID"      INTEGER,
    "Fruit"       TEXT,
    PRIMARY KEY("ROWID" AUTOINCREMENT)
);

INSERT INTO "Fruits" VALUES (1,'Apple');
INSERT INTO "Fruits" VALUES (2,'Peach');
INSERT INTO "Fruits" VALUES (3,'Orange');
INSERT INTO "Fruits" VALUES (4,'Banana');
DELETE FROM Fruits WHERE ROWID == 1;
```

**Code 4.2:**

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">
<dict>

    <key>DCSAssetPreferenceKeyDownloadedDictionaries</key>
    <array>

        <string>Apple Dictionary.dictionary</string>
        <string>Italian.dictionary</string>
        <string>Italian - English.dictionary</string>
    </array>
</dict>
</plist>
```

Command 4.7:

```
plutil -convert xml1 filename.plist
```

Command 4.8:

```
protoc --decode_raw < [protobuf_blob_file]
```

## Links

- To download FQLite, visit <https://www.staff.hs-mittweida.de/~pawlaszc/fqlite/> or head over to the GitHub repository that is located at <https://github.com/pawlaszczyk/fqlite>.
- The `protoc` tool is part of the protocol buffers package and can be downloaded from the GitHub repository located at <http://github.com/protocolbuffers/protobuf>.

# Chapter 5

## Images

Device Events (567)						
	#	Start time	End time	Event type	Value type	Value
	100	31-Jan-19 12:19:16(UTC+0)	31-Jan-19 12:19:16(UTC+0)	Device Plugin Status	Plugged in	Plugged in
	101	31-Jan-19 12:39:28(UTC+0)	31-Jan-19 12:41:24(UTC+0)	Display On/Off	Display on	Display on
	102	31-Jan-19 12:39:28(UTC+0)	31-Jan-19 12:43:32(UTC+0)	Device Plugin Status	Plugged in	Plugged in
	103	31-Jan-19 12:43:32(UTC+0)	31-Jan-19 12:43:40(UTC+0)	Display On/Off	Display on	Display on
	104	31-Jan-19 12:43:32(UTC+0)	31-Jan-19 13:57:20(UTC+0)	Device Plugin Status	Plugged in	Plugged in
	105	31-Jan-19 12:55:32(UTC+0)	31-Jan-19 12:57:44(UTC+0)	Display On/Off	Display on	Display on
	106	31-Jan-19 12:55:32(UTC+0)	31-Jan-19 12:55:44(UTC+0)	Device Lock Status	Unlocked	Unlocked
	107	31-Jan-19 13:46:32(UTC+0)	31-Jan-19 13:46:44(UTC+0)	Display On/Off	Display on	Display on
	108	31-Jan-19 13:57:20(UTC+0)	31-Jan-19 13:57:32(UTC+0)	Display On/Off	Display on	Display on
	109	31-Jan-19 13:57:32(UTC+0)	31-Jan-19 13:57:36(UTC+0)	Display On/Off	Display on	Display on
	110	03-Feb-19 06:31:48(UTC+0)	03-Feb-19 09:27:20(UTC+0)	Device Lock Status	Unlocked	Unlocked
	111	03-Feb-19 06:38:52(UTC+0)	03-Feb-19 06:42:52(UTC+0)	Audio Output Route	Speaker	Speaker
	112	03-Feb-19 06:43:00(UTC+0)	03-Feb-19 06:43:28(UTC+0)	Display On/Off	Display on	Display on
	113	03-Feb-19 06:43:08(UTC+0)	03-Feb-19 06:43:11(UTC+0)	Audio Output Route	Speaker	Speaker
	114	03-Feb-19 06:43:12(UTC+0)	03-Feb-19 06:43:14(UTC+0)	Audio Output Route	Speaker	Speaker
	115	03-Feb-19 06:43:16(UTC+0)	03-Feb-19 06:43:24(UTC+0)	Audio Output Route	Speaker	Speaker
	116	03-Feb-19 06:43:28(UTC+0)	03-Feb-19 06:51:12(UTC+0)	Display On/Off	Display on	Display on
	117	03-Feb-19 06:50:36(UTC+0)	03-Feb-19 07:34:12(UTC+0)	Audio Output Route	Speaker	Speaker
	118	03-Feb-19 06:55:56(UTC+0)	03-Feb-19 06:56:08(UTC+0)	Display On/Off	Display on	Display on
	119	03-Feb-19 07:00:00(UTC+0)	03-Feb-19 07:00:00(UTC+0)	Display On/Off	Display on	Display on
	120	03-Feb-19 07:29:08(UTC+0)	03-Feb-19 08:29:52(UTC+0)	Display On/Off	Display on	Display on
	121	03-Feb-19 07:34:32(UTC+0)	03-Feb-19 07:39:48(UTC+0)	Audio Output Route	Speaker	Speaker
	122	03-Feb-19 07:40:00(UTC+0)	03-Feb-19 07:40:01(UTC+0)	Audio Output Route	Speaker	Speaker

Figure 5.1 – Device events in Cellebrite Physical Analyzer

## Convert epoch to human-readable date and vice versa

1633614474 Timestamp to Human date [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:

**GMT:** Thursday 7 October 2021 13:47:54

**Your time zone:** giovedì 7 ottobre 2021 15:47:54 **GMT+02:00 DST**

**Relative:** A few seconds ago

Figure 5.2 – Converting a Unix timestamp to a string

SELECT * FROM Events;			
	id	uuid	timestamp
1	1	dbcba62a-7766-453a-b3b0-3a14ald6d417	1633360229
2	2	25e66b36-f1ce-4fe3-9a30-3379bf724b00	1633360299
3	3	2844c9a3-df4a-4ac0-ab51-d68a47fld0f3...	1633360406

Figure 5.3 – The Events table in a SQLite database

SELECT id, uuid, datetime(timestamp, 'unixepoch') AS date FROM Events;			
	id	uuid	date
1	1	dbcba62a-7766-453a-b3b0-3a14ald6d417	2021-10-04 15:10:29
2	2	25e66b36-f1ce-4fe3-9a30-3379bf724b00	2021-10-04 15:11:39
3	3	2844c9a3-df4a-4ac0-ab51-d68a47fld0f3...	2021-10-04 15:13:26

Figure 5.4 – Converting a timestamp to a string

Name	Type
Tables (16)	
> ZADDITIONCHANGESET	
> ZCONTEXTUALCHANGEREGISTRATION	
> ZCONTEXTUALKEYPATH	
> ZCUSTOMMETADATA	
> ZDELETIONCHANGESSET	
> ZHISTOGRAM	
> ZHISTOGRAMVALUE	
> ZKEYVALUE	
> ZOBJECT	
> ZSOURCE	
> ZSTRUCTUREDMETADATA	
> ZSYNCPEER	
> Z_4EVENT	
> Z_METADATA	
> Z_MODELCACHE	
> Z_PRIMARYKEY	
> Indices (25)	
Views (0)	
Triggers (0)	

Figure 5.5 – The schema of the KnowledgeC database

## Result

Conversion of date and time: **Monday, 2021-05-24 00:00:00 UTC**

Date and Time:	<b>Monday, 2021-05-24 00:00:00 UTC</b>
UNIX Epoch Time:	<b>1621814400</b>
UNIX Epoch Time (Hex):	<b>60AAEC80</b>
CF Absolute Time:	<b>643507200</b>

Figure 5.6 – Converting date and time to a MAC timestamp using  
<https://www.gaijin.at/en/tools/time-converter>



ID	Z_DKNOWPLAYINGMETADATAKEY__TITLE
1	51732 Netflix - Quo Vadis?

Figure 5.10 – The metadata associated with the /media/nowPlaying event

	DATE / TIME	GMT OFFSET	IS LOCKED
1	2021-05-23 14:49:13	2	LOCKED
2	2021-05-23 15:41:55	2	UNLOCKED
3	2021-05-23 15:58:59	2	LOCKED
4	2021-05-23 16:05:33	2	UNLOCKED
5	2021-05-23 16:52:36	2	LOCKED
6	2021-05-23 22:11:48	2	UNLOCKED
7	2021-05-23 22:50:47	2	LOCKED
8	2021-05-23 22:54:20	2	UNLOCKED
9	2021-05-23 23:23:24	2	LOCKED
10	2021-05-23 23:33:14	2	UNLOCKED
11	2021-05-24 00:08:13	2	LOCKED
12	2021-05-24 00:10:48	2	UNLOCKED

Figure 5.11 – The query shows the device lock status

Key	Activity	Output	Database	
			Filter	Filter
106553	Device/App Assertions	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106554	WiFi Connection	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106555	WiFi Connection	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106556	WiFi Connection	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106557	Process ID	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106558	Process ID	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106559	Battery Level UI	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106560	Battery Level	{...}	tmp_apollo/private/var/mobile/Library/CoreDuet/...	modul
106561	Battery Level	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106562	Battery Level	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106563	WiFi Connection	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106564	WiFi Connection	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106565	Routined Location	{...}	tmp_apollo/private/var/mobile/Library/Caches/...	modul
106566	App Usage by Hour	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106567	App Usage by Hour	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106568	App Usage by Hour	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106569	App Usage by Hour	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106570	App Usage by Hour	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106571	App Usage by Hour	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106572	App Usage by Hour	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106573	App Usage by Hour	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106574	App Usage by Hour	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul
106575	App Usage by Hour	{...}	tmp_apollo/private/var/containers/Shared/SystemGroup/...	modul

106553 - 106575 of 209564    Go to: 1

Figure 5.12 – The Apollo database displayed in DB Browser

```

1  {
2      "ADJUSTED_TIMESTAMP": "2021-06-19 07:57:09",
3      "LEVEL": 31.0,
4      "RAW LEVEL": 31.226496962684408,
5      "IS CHARGING": 0,
6      "FULLY CHARGED": 0,
7      "ORIGINAL_TIMESTAMP": "2021-04-26 06:36:55",
8      "OFFSET_TIMESTAMP": "2021-04-28 15:48:55",
9      "TIME_OFFSET": 4674074.367777824,
10     "PLBATTERYAGENT_EVENTBACKWARD_BATTERY TABLE ID":
11      480012
12  }

```

Figure 5.13 – The JSON object stored in Apollo's Output column

## Code and Command

Command 5.1

```
SELECT id, uuid, datetime(timestamp, 'unixepoch') AS date  
FROM Events;
```

**Command 5.2:**

```
SELECT id, uuid, datetime(timestamp, 'unixepoch',  
'localtime') AS date FROM Events;
```

**Command 5.3:**

```
SELECT id, uuid, datetime(timestamp + 978307200,  
'unixepoch', 'localtime') AS date FROM Events;
```

**Command 5.4:**

```
SELECT DISTINCT Z_object.ZSTREAMNAME FROM Z_object ORDER BY  
ZSTREAMNAME;
```

**Command 5.5**

```
SELECT  
  
datetime(Z_object.ZSTARTDATE+978307200, 'UNIXEPOCH',  
'LOCALTIME') as "START",  
  
datetime(Z_object.ZENDDATE+978307200, 'UNIXEPOCH',  
'LOCALTIME') as "END",  
  
Z_object.ZSECONDSFROMGMT/3600 AS "GMT OFFSET",  
  
(Z_object.ZENDDATE-Z_object.ZSTARTDATE) as "USAGE IN  
SECONDS",  
  
Z_object.ZSTREAMNAME,  
  
Z_object.ZVALUESTRING  
  
FROM Z_object  
  
WHERE ZSTREAMNAME IS "/app/inFocus"  
  
AND Z_object.ZSTARTDATE > 643507200  
  
AND Z_object.ZSTARTDATE < 643680000  
  
ORDER BY "START";
```

**Command 5.6**

```
SELECT

datetime(Z object.ZSTARTDATE+978307200,'UNIXEPOCH',
'LOCALTIME') as "START",

datetime(Z object.ZENDDATE+978307200,'UNIXEPOCH',
'LOCALTIME') as "END",

Z object.ZSECONDSFROMGMT/3600 AS "GMT OFFSET",

(Z object.ZENDDATE-Z object.ZSTARTDATE) as "USAGE IN
SECONDS",

Z object.ZSTREAMNAME,

Z object.ZVALUESTRING

FROM Z object

WHERE ZSTREAMNAME IS "/app/inFocus"

ORDER BY "USAGE IN SECONDS" DESC;
```

#### Command 5.7

```
SELECT

datetime(Z object.ZSTARTDATE+978307200,'UNIXEPOCH',
'LOCALTIME') as "START",

datetime(Z object.ZENDDATE+978307200,'UNIXEPOCH',
'LOCALTIME') as "END",

Z object.ZSECONDSFROMGMT/3600 AS "GMT OFFSET",

(Z object.ZENDDATE-Z object.ZSTARTDATE) as "USAGE IN
SECONDS",

Z object.ZSTREAMNAME,

Z object.ZSTRUCTUREDMETADATA,

Z object.ZVALUESTRING

FROM Z object

WHERE Z object.ZSTARTDATE > 644266800
```

```
AND Z_object.ZSTARTDATE < 644277599  
ORDER BY "START";
```

**Command 5.8:**

```
SELECT  
Z_PK AS "ID",  
Z_DKNOWPLAYINGMETADATATEKEY__TITLE  
FROM ZSTRUCTUREDMETADATA  
WHERE "ID" = "51732";
```

**Command 5.9:**

```
SELECT  
datetime(Z_object.ZSTARTDATE+978307200,'UNIXEPOCH',  
'LOCALTIME') as "DATE / TIME",  
Z_object.ZSECONDSFROMGMT/3600 AS "GMT OFFSET",  
CASE Z_object.ZVALUEINTEGER  
    WHEN '0' THEN 'UNLOCKED'  
    WHEN '1' THEN 'LOCKED'  
END "IS LOCKED"  
FROM Z_object  
WHERE Z_object.ZSTREAMNAME LIKE "/device/isLocked"  
ORDER BY "DATE / TIME";
```

**Command 5.10:**

```
SELECT  
datetime(Z_object.ZSTARTDATE+978307200,'UNIXEPOCH',  
'LOCALTIME') as "DATE / TIME",  
Z_object.ZSECONDSFROMGMT/3600 AS "GMT OFFSET"  
FROM Z_object
```

```
WHERE Z_object.ZSTREAMNAME LIKE "/display/isBacklit"  
AND Z_object.ZVALUEINTEGER = '1'  
ORDER BY "DATE / TIME";
```

Command 5.11:

```
python apollo.py -output sql modules/ fs-extraction/
```

## Links

- Apollo's Github repository: <https://github.com/mac4n6/APOLLO>

# Chapter 6

## Images

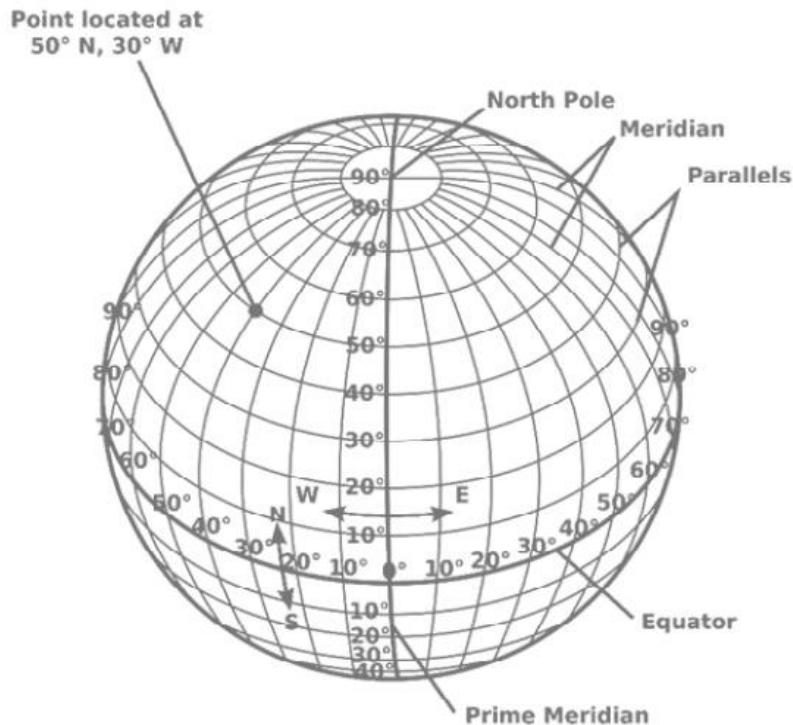


Figure 6.1 – Geographic locations are expressed using latitude and longitude

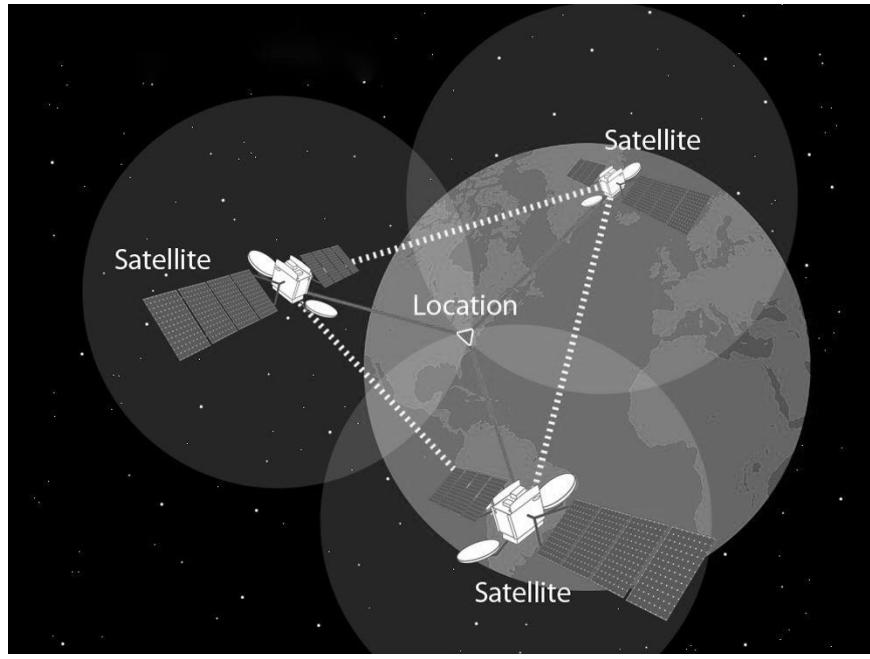
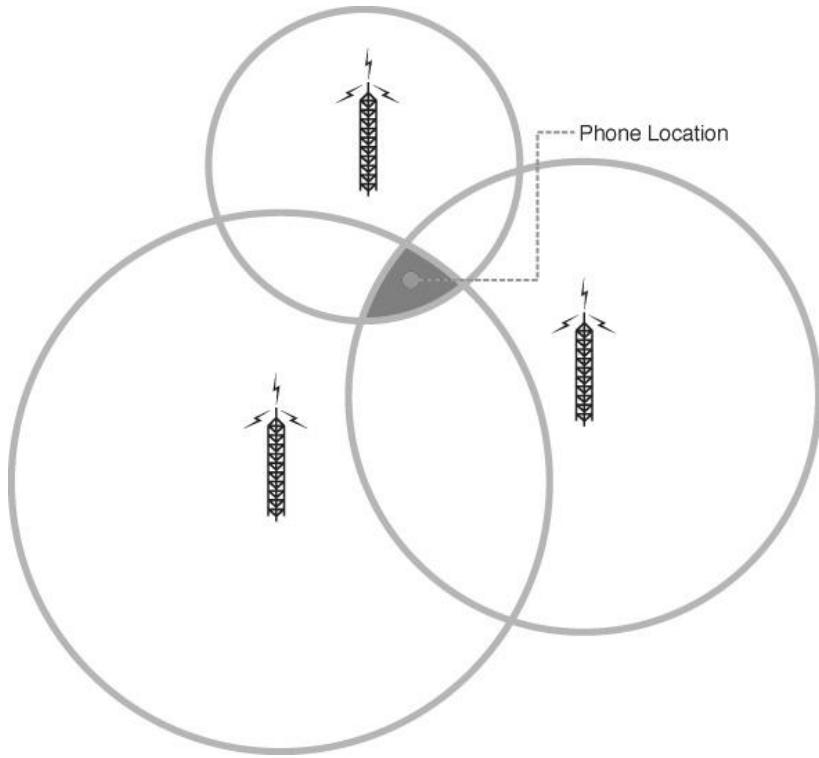


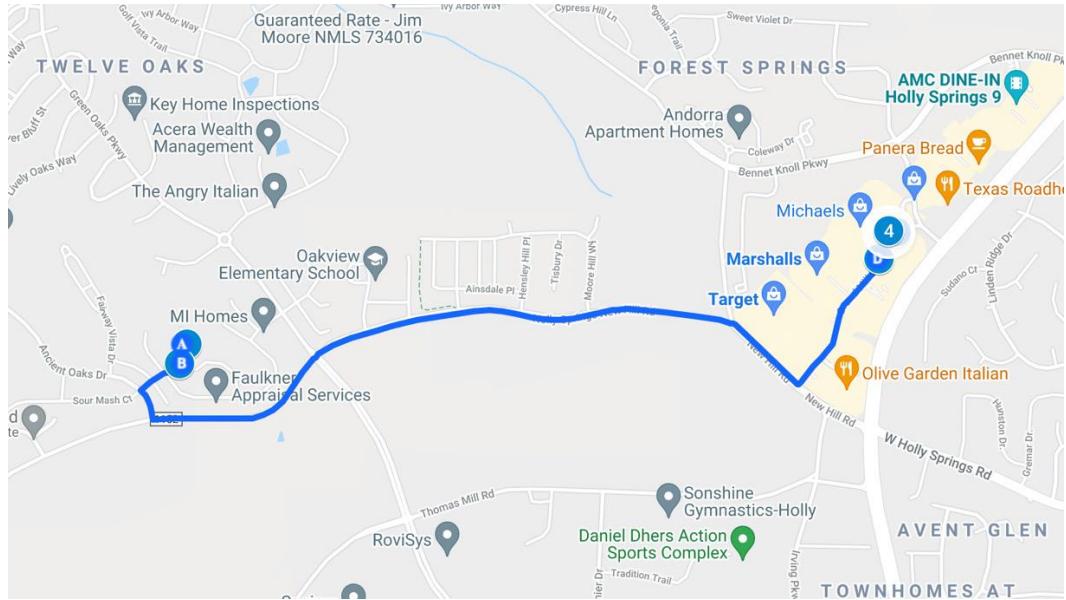
Figure 6.2 – GPS satellite triangulation calculates the receiver's location



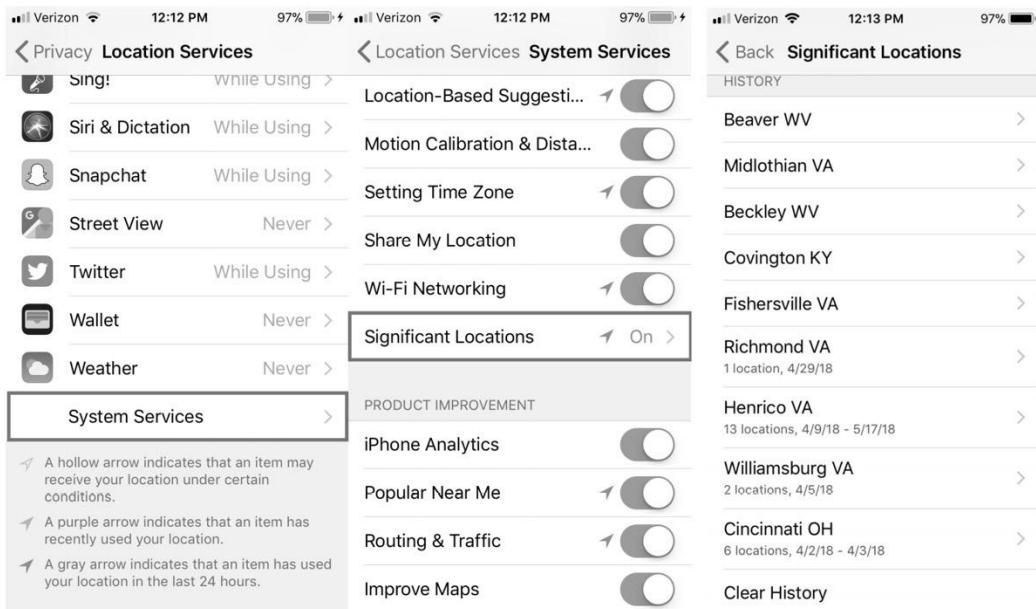
**Figure 6.3 – Cell tower trilateration process**

	TIMESTAMP	LATITUDE	LONGITUDE	ALTITUDE	SPEED (M/S)	SPEED (MPH)	SPEED (KMPH)	HORIZO
1	2020-04-12 08:28:48	35.6578612348278	-78.8705126020217	102.232818603516	-1.0	-2.23694	-3.6	
2	2020-04-12 08:28:49	35.6578694814717	-78.8705127743498	102.232818603516	-1.0	-2.23694	-3.6	
3	2020-04-12 08:28:51	35.6553155556039	-78.8704595665105	102.232818603516	-1.0	-2.23694	-3.6	19
4	2020-04-12 08:28:51	35.6513724593481	-78.8703774158301	102.232818603516	-1.0	-2.23694	-3.6	19
5	2020-04-12 08:28:51	35.653168602849	-78.8704148367899	102.232818603516	-1.0	-2.23694	-3.6	19
6	2020-04-12 08:32:23	35.6558862343305	-78.8704714569495	102.232818603516	-1.0	-2.23694	-3.6	
7	2020-04-12 08:32:24	35.6568810173752	-78.8704921817063	102.232818603516	-1.0	-2.23694	-3.6	
8	2020-04-12 08:32:22	35.6457080733981	-78.8702594108219	102.232818603516	-1.0	-2.23694	-3.6	
9	2020-04-12 08:33:54	35.6574534521418	-78.8705041068972	102.232818603516	-1.0	-2.23694	-3.6	
10	2020-04-12 08:35:33	35.6528454092581	-78.8704081031046	102.232818603516	-1.0	-2.23694	-3.6	19
11	2020-04-12 08:35:30	35.6575081235283	-78.8705052462567	102.232818603516	-1.0	-2.23694	-3.6	
12	2020-04-12 08:35:30	35.6571394683115	-78.8704975656647	102.232818603516	-1.0	-2.23694	-3.6	

**Figure 6.4 – The query results show the device's location**



**Figure 6.5 – The query results are mapped out to determine the user's journey**



**Figure 6.6– Significant Locations can be viewed directly on the device**

	ENTRY	EXIT	DURATION (MINUTES)	LATITUDE	LONGITUDE	LOCATION UNCERTAINTY	DATA POINTS
1	2020-04-15 16:32:51	2020-04-16 23:06:51	1834.0	35.6593609837169	-78.8730660027371	32.8602404963937	7365
2	2020-04-17 19:35:14	2020-04-19 18:50:29	2835.25	35.6593609837169	-78.8730660027371	19.6819985540774	11438
3	2020-04-15 16:10:47	2020-04-15 16:20:19	9.5366063396136	35.6638133919877	-78.8479745012675	216.865382961763	39
4	2020-04-12 14:30:27	2020-04-15 16:03:04	4412.61572608352	35.6593609837169	-78.8730660027371	31.9387684448737	17726
5	2020-04-12 08:41:27	2020-04-12 13:55:27	314.0	35.6593609837169	-78.8730660027371	21.0690629834767	1257
6	2020-04-12 14:02:27	2020-04-12 14:19:27	17.0	35.6715623958704	-78.8770194584023	21.8376117000028	69

**Figure 6.7 – The query results show details about significant location visits**

	DATE	MAC ADDRESS	CHANNEL	RSSI	
1	2020-04-12 12:46:19	f8:bb:bf:1e:fa:ea	161	-57	
2	2020-04-12 12:46:19	f8:bb:bf:1e:fa:e4	161	-57	
3	2020-04-12 12:46:20	80:da:13:72:52:64	149	-90	
4	2020-04-12 12:46:20	f8:bb:bf:1e:fa:eb	48	-51	
5	2020-04-12 12:46:20	58:ef:68:25:35:34	48	-90	
6	2020-04-12 12:46:20	d8:d7:75:b6:28:9	48	-89	
7	2020-04-12 12:46:20	80:da:13:72:52:6a	149	-89	
8	2020-04-12 12:46:20	f8:bb:bf:8d:b9:c2	48	-78	
9	2020-04-12 12:46:20	f8:bb:bf:90:a8:f2	48	-70	
10	2020-04-12 12:46:20	b8:66:85:53:d3:7	44	-85	
11	2020-04-12 12:46:20	7c:db:98:c2:30:34	40	-89	
12	2020-04-12 12:46:20	f8:bb:bf:1e:fa:e8	48	-50	

**Figure 6.8 – The results show details about wireless devices that were scanned by the device**



	Map	Category	Type	Source	Account	Source file information	Extraction
			Visited	Native Locations		<a href="#">Local.sqlite-wal : 0x1BEC8</a>	Legacy
			Visited	Native Locations		<a href="#">Local.sqlite-wal : 0x1BE44</a>	Legacy
			Visited	Native Locations		<a href="#">Local.sqlite-wal : 0x1BD3F</a>	Legacy
			Visited	Native Locations		<a href="#">Local.sqlite-wal : 0x1BCC0</a>	Legacy
			Visited	Native Locations		<a href="#">Local.sqlite-wal : 0x1BC3F</a>	Legacy
			Visited	Native Locations		<a href="#">Local.sqlite-wal : 0x1BBB7</a>	Legacy
			Visited	Native Locations		<a href="#">Local.sqlite-wal : 0x1BB35</a>	Legacy
			Visited	Native Locations		<a href="#">Local.sqlite-wal : 0x1BAB3</a>	Legacy
			Visited	Native Locations		<a href="#">Local.sqlite-wal : 0x1BA34</a>	Legacy
			Visited	Native Locations		<a href="#">Local.sqlite-wal : 0x1B9AB</a>	Legacy
			Visited	Native Locations		<a href="#">Local.sqlite-wal : 0x1B92C</a>	Legacy
			Visited	Native Locations		<a href="#">Local.sqlite-wal : 0x1B8A4</a>	Legacy
			Visited	Native Locations		<a href="#">Local.sqlite-wal : 0x1B822</a>	Legacy

Figure 6.11 – Physical Analyzer specifies the source file for the artifact

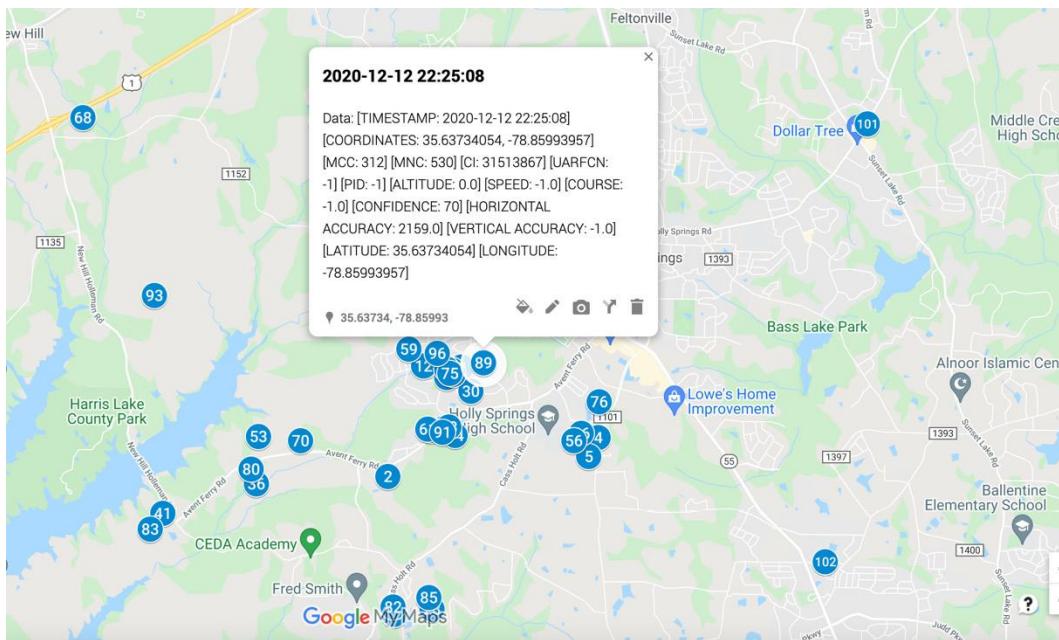


Figure 6.12 – Google Maps displaying location data exported by Apollo

## Code and Command

Command 6.1:

```
SELECT  
    DATETIME(ZTIMESTAMP + 978307200, 'UNIXEPOCH') AS  
    "TIMESTAMP",  
    ZLATITUDE AS "LATITUDE",  
    ZLONGITUDE AS "LONGITUDE",  
    ZALTITUDE AS "ALTITUDE",  
    ZSPEED AS "SPEED (M/S)",  
    ZSPEED*2.23694 AS "SPEED (MPH)",  
    ZSPEED*3.6 AS "SPEED (KMPH)",  
    ZHORIZONTALACCURACY AS "HORIZONTAL ACCURACY",  
    ZVERTICALACCURACY AS "VERTICAL ACCURACY"  
FROM  
    ZRTCLLOCATIONMO;
```

Command 6.2:

```
SELECT  
    DATETIME(ZRTLEARNEDLOCATIONOFINTERESTVISITMO.ZENTRY  
DATE + 978307200, 'UNIXEPOCH') AS "ENTRY",  
    DATETIME(ZRTLEARNEDLOCATIONOFINTERESTVISITMO.ZEXITD  
ATE + 978307200, 'UNIXEPOCH') AS "EXIT",  
    (ZRTLEARNEDLOCATIONOFINTERESTVISITMO.ZEXITDATE-  
ZRTLEARNEDLOCATIONOFINTERESTVISITMO.ZENTRYDATE)/60.00 AS  
    "DURATION (MINUTES)",  
    ZRTLEARNEDLOCATIONOFINTERESTMO.ZLOCATIONLATITUDE AS  
    "LATITUDE",
```

```

ZRTLEARNEDLOCATIONOFINTERESTMO.ZLOCATIONLONGITUDE
AS "LONGITUDE",
ZRTLEARNEDLOCATIONOFINTERESTVISITMO.ZLOCATIONUNCERTAINTY AS "LOCATION UNCERTAINTY",
ZRTLEARNEDLOCATIONOFINTERESTVISITMO.ZDATAPUNCTCOUNT
AS "DATA POINTS"
FROM
ZRTLEARNEDLOCATIONOFINTERESTVISITMO
LEFT JOIN
ZRTLEARNEDLOCATIONOFINTERESTMO
ON ZRTLEARNEDLOCATIONOFINTERESTMO.Z_PK =
ZRTLEARNEDLOCATIONOFINTERESTVISITMO.ZLOCATIONOFINTEREST;

```

**Command 6.3:**

```

SELECT
DATETIME(ZRTWIFIACCESSPOINTMO.ZDATE + 978307200,
'UNIXEPOCH') AS "DATE",
ZRTWIFIACCESSPOINTMO.ZMAC AS "MAC ADDRESS",
ZRTWIFIACCESSPOINTMO.ZCHANNEL AS "CHANNEL",
ZRTWIFIACCESSPOINTMO.ZRSSI AS "RSSI"
FROM ZRTWIFIACCESSPOINTMO
ORDER BY "DATE" ASC;

```

**Command 6.4:**

```

SELECT
DATETIME(TIMESTAMP + 978307200, 'UNIXEPOCH') AS
"TIMESTAMP",
MCC AS "MCC",
MNC AS "MNC",

```

```
        CI AS "CI",
        HORIZONTALACCURACY AS "HORIZONTAL ACCURACY",
        LATITUDE AS "LATITUDE",
        LONGITUDE AS "LONGITUDE"
FROM LTECELLLOCATION;
```

**Command 6.5:**

```
python3 apollo.py extract -o sql -p apple -v 14 -k modules/
fs-extraction/
```

**Command 6.6:**

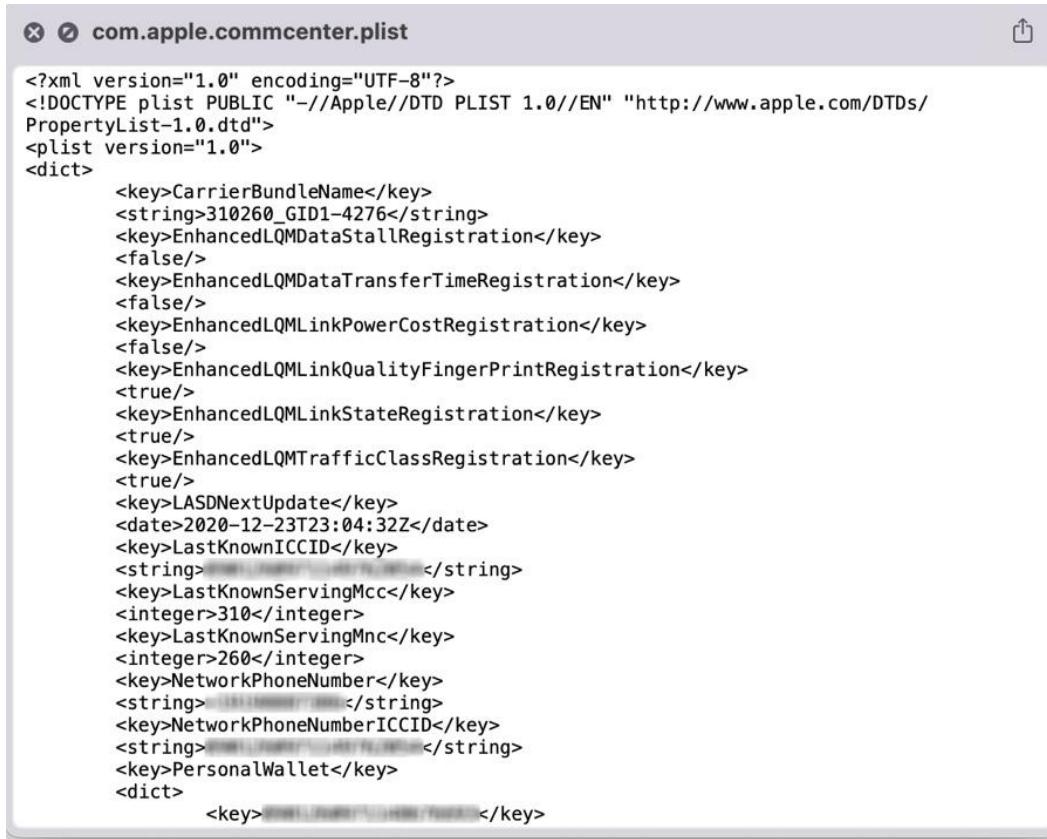
```
SELECT
        DATETIME(TIMESTAMP + 978307200, 'UNIXEPOCH') AS
"TIMESTAMP",
        MAC AS "MAC",
        CHANNEL AS "CHANNEL",
        SCORE AS "SCORE",
        REACH AS "REACH",
        HORIZONTALACCURACY AS "HORIZONTAL ACCURACY",
        LATITUDE AS "LATITUDE",
        LONGITUDE AS "LONGITUDE"
FROM WIFILOCATION;
```

## Links

- Apollo's Github repository: <https://github.com/mac4n6/APOLLO>

# Chapter 7

## Images



The screenshot shows a file viewer window with the title bar "com.apple.commcenter.plist". The content area displays the XML structure of a PLIST file. The XML code includes various keys such as CarrierBundleName, EnhancedLQMDataStallRegistration, EnhancedLQMDataTransferTimeRegistration, EnhancedLQMLinkPowerCostRegistration, EnhancedLQMLinkQualityFingerPrintRegistration, EnhancedLQMLinkStateRegistration, EnhancedLQMTrafficClassRegistration, LASDNextUpdate, LastKnownICCID, LastKnownServingMcc, LastKnownServingMnc, NetworkPhoneNumber, NetworkPhoneNumberICCID, and PersonalWallet. Some key values are redacted with black squares.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>CarrierBundleName</key>
    <string>310260_GID1-4276</string>
    <key>EnhancedLQMDataStallRegistration</key>
    <false/>
    <key>EnhancedLQMDataTransferTimeRegistration</key>
    <false/>
    <key>EnhancedLQMLinkPowerCostRegistration</key>
    <false/>
    <key>EnhancedLQMLinkQualityFingerPrintRegistration</key>
    <true/>
    <key>EnhancedLQMLinkStateRegistration</key>
    <true/>
    <key>EnhancedLQMTrafficClassRegistration</key>
    <true/>
    <key>LASDNextUpdate</key>
    <date>2020-12-23T23:04:32Z</date>
    <key>LastKnownICCID</key>
    <string>[REDACTED]</string>
    <key>LastKnownServingMcc</key>
    <integer>310</integer>
    <key>LastKnownServingMnc</key>
    <integer>260</integer>
    <key>NetworkPhoneNumber</key>
    <string>[REDACTED]</string>
    <key>NetworkPhoneNumberICCID</key>
    <string>[REDACTED]</string>
    <key>PersonalWallet</key>
    <dict>
        <key>[REDACTED]</key>
```

Figure 7.1 – The com.apple.commcenter PLIST

	TIMESTAMP	SERVICE	OPERATOR	STATUS	
3	2020-05-08 15:25:25	None	NULL	NotRegistered	
4	2020-08-24 16:55:03	None	NULL	NotRegistered	
5	2020-12-12 22:19:12	None	NULL	NotRegistered	
6	2020-12-12 22:21:15	None	NULL	NotRegistered	
7	2020-12-12 22:30:00	None	NULL	Searching	
8	2020-12-12 22:30:11	None	NULL	Emergency Only	
9	2020-12-12 22:30:49	None	NULL	Denied	
10	2020-12-12 22:30:49	None	NULL	Emergency Only	
11	2020-12-12 22:33:38	None	Google Fi	RegisteredHome	
12	2020-12-12 22:33:38	4G	Google Fi	RegisteredHome	
13	2020-12-12 22:33:43	None	Google Fi	RegisteredHome	
14	2020-12-12 22:33:43	4G	Google Fi	RegisteredHome	

Figure 7.2 – Records of cellular registration

	First Name	Last Name	Contacts	
1	Josh	Hickman	(919) 579-0479,(919) 391-2507,joshua.hickman1@me.com	
2	This Is	DFIR	NULL	

Figure 7.3 – Records extracted from the address book

	Date/Time	Phone Number	Location	Call in Seconds	Call Direction	Call Status	Service Provider
26	2020-04-10 16:19:47	+14082560700	San Jose,CA	0.0	Incoming	Call missed	com.apple.Telephony
27	2020-04-10 16:32:21	+14082560700	San Jose,CA	0.0	Incoming	Call missed	com.apple.Telephony
28	2020-04-10 16:40:42	+14082560700	San Jose,CA	0.0	Incoming	Call missed	com.apple.Telephony
29	2020-04-12 03:13:23	+17042751134	Fairview,NC	0.0	Outgoing	NULL	com.apple.Telephony
30	2020-04-12 03:14:46	+17042751134	Fairview,NC	12.2448190450668	Incoming	Call answered	com.apple.Telephony
31	2020-04-12 16:04:06	9192853680	Fuquay-Varina,NC	64.6294050216675	Outgoing	NULL	com.apple.Telephony
32	2020-04-12 17:26:43	joshua.hickman1@me.com	<<RecentsNumberLocati...	98.0257830619812	Outgoing	NULL	com.apple.FaceTime
33	2020-04-13 20:41:27	+14082560700	San Jose,CA	0.0	Incoming	Call missed	com.apple.Telephony
34	2020-04-13 23:57:05	+14082560700	San Jose,CA	0.0	Incoming	Call missed	com.apple.Telephony
35	2020-04-14 14:43:26	+14082560700	San Jose,CA	0.0	Incoming	Call missed	com.apple.Telephony
36	2020-04-14 17:25:18	+14082560700	San Jose,CA	0.0	Incoming	Call missed	com.apple.Telephony
37	2020-04-14 17:56:12	+14082560700	San Jose,CA	0.0	Incoming	Call missed	com.apple.Telephony

**Figure 7.4 – Data extracted from the call log**

A screenshot of the Xcode interface showing the contents of the 'com.apple.wifi.plist' file. The window title is 'com.apple.wifi.plist'. In the top right corner, there is a button labeled 'Open withTextEdit'. The main area displays the XML structure of the plist file. The file contains information about known Wi-Fi networks, including SSID, SaveDataMode, ScaledRSSI, ShareableStatus, Strength, VHT\_CAPS\_IE, and various WiFiManager and WiFiNetworkAttribute keys. It also includes sections for WiFiAutoInstantHotspotJoining and WiFiInstantHotspotJoining, along with details like WiFiManagerKnownNetworksEventType, WiFiNetworkAttributeIsKnown, WiFiNetworkAttributeIsMoving, WiFiNetworkAttributeIsPotentiallyMoving, WiFiNetworkAttributeLowPopularity, WiFiNetworkAttributePopularityScore, WiFiNetworkAttributeProminentDisplay, WiFiNetworkAttributeSource, WiFiNetworkIsAutoJoined, WiFiNetworkPasswordModificationDate, and WiFiNetworkEnabled status.

```
<key>SSID</key>
<data>
Q2Nvb2tpZXNEY2FzdGx1UjUgR3Vlc3Q=
</data>
<key>SSID_STR</key>
<string>CcookiesDcastleR5 Guest</string>
<key>SaveDataMode</key>
<integer>2</integer>
<key>ScaledRSSI</key>
<real>0.82863259315490723</real>
<key>ScaledRate</key>
<real>1</real>
<key>ShareableStatus</key>
<integer>1</integer>
<key>Strength</key>
<real>0.82863259315490723</real>
<key>VHT_CAPS_IE</key>
<dict>
    <key>VHT_CAPS</key>
    <integer>864041394</integer>
    <key>VHT_SUPPORTED_MCS_SET</key>
    <data>
        +v8AAPr/AAA=
    </data>
</dict>
<key>WiFiAutoInstantHotspotJoining</key>
<false/>
<key>WiFiInstantHotspotJoining</key>
<false/>
<key>WiFiManagerKnownNetworksEventType</key>
<integer>1</integer>
<key>WiFiNetworkAttributeIsKnown</key>
<true/>
<key>WiFiNetworkAttributeIsMoving</key>
<false/>
<key>WiFiNetworkAttributeIsPotentiallyMoving</key>
<true/>
<key>WiFiNetworkAttributeLowPopularity</key>
<true/>
<key>WiFiNetworkAttributePopularityScore</key>
<integer>0</integer>
<key>WiFiNetworkAttributeProminentDisplay</key>
<true/>
<key>WiFiNetworkAttributeSource</key>
<integer>2</integer>
<key>WiFiNetworkIsAutoJoined</key>
<true/>
<key>WiFiNetworkPasswordModificationDate</key>
<date>2020-03-22T19:00:00Z</date>
<key>addedAt</key>
<date>2020-03-22T19:00:00Z</date>
<key>enabled</key>
<true/>
```

Figure 7.5 – The com.apple.wifi.plist showing details of known networks

	PROCESS TIMESTAMP	PROCESS NAME	BUNDLE ID	WWAN IN	WWAN OUT
85	2020-03-22 15:14:45	com.apple.WebKit/imgurmobile	imgurmobile	3102060.0	275109.0
86	2020-03-22 15:16:40	mediaserverd/imgurmobile	imgurmobile	114007059.0	3366467.0
87	2020-03-22 15:10:24	nsurlsessiond/imgurmobile	imgurmobile	926878.0	45097.0
88	2020-03-22 18:02:57	nsurlsessiond/co.babypenguin.imo	co.babypenguin.imo	8978.0	6276.0
89	2020-03-22 18:59:22	mDNSResponder/com.burbn.instagram	com.burbn.instagram	5521.0	3440.0
90	2020-03-22 19:12:02	Instagram/com.burbn.instagram	com.burbn.instagram	15820543.0	662197.0
91	2020-03-22 18:48:48	InstagramNotific/com.burbn.instagram	com.burbn.instagram	28270.0	20203.0
92	2020-03-25 02:00:51	Threads/com.burbn.threads	com.burbn.threads	6336.0	23244.0
93	2020-03-27 19:02:30	appstored/com.kik.chat	com.kik.chat	14819.0	5875.0
94	2020-03-30 16:08:45	mDNSResponder/com.belkin.plugin	com.belkin.plugin	1452.0	1645.0
95	2020-03-30 16:07:06	WeMo_Universal/com.belkin.plugin	com.belkin.plugin	14913.0	8634.0
96	2020-04-04 16:16:50	mDNSResponder/com.facebook.talk	com.facebook.talk	367.0	485.0

Figure 7.6 – The query results showing the processes running on the device and their data usage

	Start	End	Status	Address	Device
1	2020-03-27 19:32:42	2020-03-27 19:32:52	Connected	7C:04:D0:89:89:A0	Josh's AirPods
2	2020-03-27 19:32:52	2020-03-27 19:33:03	Disconnected	7C:04:D0:89:89:A0	Josh's AirPods
3	2020-03-27 19:33:03	2020-03-27 19:33:05	Connected	7C:04:D0:89:89:A0	Josh's AirPods
4	2020-03-27 19:33:05	2020-03-27 19:54:15	Disconnected	7C:04:D0:89:89:A0	Josh's AirPods
5	2020-03-27 19:54:16	2020-03-27 20:22:18	Connected	7C:04:D0:89:89:A0	Josh's AirPods
6	2020-03-27 20:22:18	2020-03-27 21:44:02	Disconnected	7C:04:D0:89:89:A0	Josh's AirPods
7	2020-03-27 21:44:04	2020-03-27 21:44:05	Connected	7C:04:D0:89:89:A0	Josh's AirPods
8	2020-03-27 21:44:05	2020-03-27 21:44:18	Disconnected	7C:04:D0:89:89:A0	Josh's AirPods
9	2020-03-27 21:44:20	2020-03-27 21:44:42	Connected	7C:04:D0:89:89:A0	Josh's AirPods
10	2020-03-27 21:44:42	2020-03-27 21:44:48	Disconnected	7C:04:D0:89:89:A0	Josh's AirPods
11	2020-03-27 21:44:49	2020-03-27 21:44:55	Connected	7C:04:D0:89:89:A0	Josh's AirPods

Figure 7.7 – The query displaying Bluetooth connection events

```

1   SELECT
2       DATETIME(HISTORY_VISITS.VISIT_TIME+978307200,'UNIXEPOCH') AS "VISIT TIME",
3           HISTORY_ITEMS.URL AS "URL",
4           HISTORY_ITEMS.VISIT_COUNT AS "VISIT COUNT",
5           HISTORY_VISITS.TITLE AS "TITLE",
6           CASE HISTORY_VISITS.ORIGIN
7               WHEN 1 THEN "ICLOUD SYNCED DEVICE"
8               WHEN 0 THEN "VISITED FROM THIS DEVICE"
9               ELSE HISTORY_VISITS.ORIGIN
10          END 'ICLOUD SYNC'
11     FROM HISTORY_ITEMS
12    LEFT OUTER JOIN HISTORY_VISITS ON HISTORY_ITEMS.ID == HISTORY_VISITS.HISTORY_ITEM;

```

	VISIT TIME	URL	VISIT COUNT	TITLE
1	2020-03-28 01:00:17	https://www.google.com/search?...	3	when does mlb start 2020 - Google Search
2	2020-03-28 00:58:37	https://www.google.com/search?...	3	when does mlb start 2020 - Google Search
3	2020-03-28 00:58:36	https://www.google.com/search?...	3	when does mlb start 2020 - Google Search
4	2020-03-28 00:59:32	https://www.google.com/amp/s/www.mlb.com/amp/news/...	3	MLB 2020 season delayed
5	2020-03-28 00:59:31	https://www.google.com/amp/s/www.mlb.com/amp/news/...	3	MLB 2020 season delayed
6	2020-03-28 00:59:03	https://www.google.com/amp/s/www.mlb.com/amp/news/...	3	MLB 2020 season delayed
7	2020-03-28 01:02:05	https://www.google.com/search?...	1	when does mlb start 2020 - Google Search
8	2020-03-28 01:02:44	https://www.google.com/search?...	2	Is the NHL going to resume? - Google Search
9	2020-03-28 01:02:44	https://www.google.com/search?...	2	Is the NHL going to resume? - Google Search
10	2020-03-28 01:03:53	https://www.nhl.com/news/commissioner-gary-bettman-...	2	NHL expects to resume season after pause for coronavirus

Figure 7.8 – Analyzing the browsing history of History.db

	DATE	TITLE	URL	GMT OFFSET
1	2020-03-28 00:58:40	when does mlb start 2020 - Google Search	https://www.google.com/search?...	-4
2	2020-03-28 01:02:50	Is the NHL going to resume? - Google Search	https://www.google.com/search?...	-4
3	2020-03-28 01:04:05	NHL expects to resume season after pause for ...	https://www.nhl.com/news/commissioner-gary-bettman-...	-4
4	2020-03-28 01:05:45	Is the NHL going to resume? - Google Search	https://www.google.com/search?...	-4
5	2020-03-28 01:06:35	Apple	https://www.apple.com/	-4
6	2020-03-28 01:07:45	iPad Pro - Apple	https://www.apple.com/ipad-pro/	-4
7	2020-03-28 01:37:10	iPad Pro - Apple	https://www.apple.com/ipad-pro/	-4
8	2020-03-28 01:38:55	Cult of Mac   Tech and culture through an Apple lens	https://www.cultofmac.com/	-4
9	2020-03-28 01:43:45	Apple	https://www.apple.com/	-4
10	2020-03-28 01:43:55	DFIR Review	https://dfir.pubpub.org/	-4

Figure 7.9 – Analyzing the browsing history of KnowledgeC.db

## Code and Commands

Commands 7.1:

```
SELECT
    DATETIME (TIMESTAMP , 'UNIXEPOCH') AS TIMESTAMP,
```

```

        DATAIND AS "SERVICE",
        OPERATOR AS "OPERATOR",
        STATUS AS "STATUS"
FROM PLBBAGENT_EVENTFORWARD_TELEPHONYREGISTRATION;

```

**Commands 7.2:**

```

SELECT p.First           AS "First Name",
       p.Last            AS "Last Name",
       GROUP_CONCAT(c.value) AS "Contacts"
FROM   ABPerson AS p
       LEFT JOIN ABMultiValue AS c
              ON c.record_id = p.rowid
GROUP BY p.rowid,
         p.first;

```

**Commands 7.3:**

```

SELECT
DATETIME(ZDATE + 978307200, 'unixepoch', 'localtime') AS
"Date/Time",
ZADDRESS AS "Phone Number",
ZLOCATION AS "Location",
ZDURATION AS "Call in Seconds",
CASE
WHEN ZORIGINATED = 0 THEN "Incoming"
      WHEN ZORIGINATED = 1 THEN "Outgoing"
END AS "Call Direction",
CASE

```

```

        WHEN ZANSWERED = 0 AND ZORIGINATED = 0 THEN "Call
missed"

        WHEN ZANSWERED = 1 AND ZORIGINATED = 0 THEN "Call
answered"

END AS "Call Status",
ZSERVICE_PROVIDER AS "Service Provider"
FROM ZCALLRECORD;

```

**Command 7.4:**

```

SELECT

        DATETIME(ZPROCESS.ZTIMESTAMP+ 978307200,
'UNIXEPOCH') AS "PROCESS TIMESTAMP",

        ZPROCESS.ZPROCNAME AS "PROCESS NAME",
        ZPROCESS.ZBUNDLENAME AS "BUNDLE ID",
        ZLIVEUSAGE.ZWWANIN AS "WWAN IN",
        ZLIVEUSAGE.ZWWANOUT AS "WWAN OUT"

FROM ZLIVEUSAGE

LEFT JOIN ZPROCESS ON ZLIVEUSAGE.ZHASPROCESS =
ZPROCESS.Z_PK;

```

**Command 7.5:**

```

SELECT

DATETIME(ZOBJECT.ZSTARTDATE + 978307200, 'unixepoch',
'localtime') AS "Start",

DATETIME(ZOBJECT.ZENDDATE + 978307200, 'unixepoch',
'localtime') AS "End",

CASE

        WHEN ZOBJECT.ZVALUEINTEGER = 0 THEN "Disconnected"
        WHEN ZOBJECT.ZVALUEINTEGER = 1 THEN "Connected"

```

```

END AS "Status",
ZSTRUCTUREDMETADATA.Z_DKBLUETOOTHMETADATATEKEY__ADDRESS AS
"Address",
ZSTRUCTUREDMETADATA.Z_DKBLUETOOTHMETADATATEKEY__NAME AS
"Device"
FROM ZSTRUCTUREDMETADATA
LEFT JOIN ZOBJECT ON ZSTRUCTUREDMETADATA.Z_PK =
ZOBJECT.ZSTRUCTUREDMETADATA
WHERE ZOBJECT.ZSTREAMNAME = "/bluetooth/isConnected"
ORDER BY "Start" ASC;

```

**Command 7.6:**

```

SELECT
    DATETIME(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH') AS
"DATE",
    ZSTRUCTUREDMETADATA.Z_DKSAFARIHISTORYMETADATATEKEY__TIT
LE AS "TITLE",
    ZOBJECT.ZVALUESTRING AS "URL",
    ZOBJECT.ZSECONDSFROMGMT/3600 AS "GMT OFFSET"
FROM ZOBJECT
    LEFT JOIN
        ZSTRUCTUREDMETADATA
        ON ZOBJECT.ZSTRUCTUREDMETADATA =
ZSTRUCTUREDMETADATA.Z_PK
    LEFT JOIN
        ZSOURCE
        ON ZOBJECT.ZSOURCE = ZSOURCE.Z_PK
WHERE

```

```
ZSTREAMNAME IS "/safari/history"  
ORDER BY DATE ASC;
```

## Links

- Safari cookies file format specification:  
<https://github.com/libyal/dtformats/blob/main/documentation/Safari%20Cookies.asciidoc>
- Safari-Binary-Cookie-Parser Python script by Mari DeGrazia:  
<https://github.com/mdegrazia/Safari-Binary-Cookie-Parser>

# Chapter 8

## Images

	ROWID	url
	Filter	Filter
1	1	imap://4FD35256-CE13-47FE-9840-EBEB5B9FD9C1/INBOX
2	2	imap://4FD35256-CE13-47FE-9840-EBEB5B9FD9C1/%5BGmail%5D/%5CImportant
3	3	imap://4FD35256-CE13-47FE-9840-EBEB5B9FD9C1/%5BGmail%5D/%5CAllMail
4	4	imap://4FD35256-CE13-47FE-9840-EBEB5B9FD9C1/%5BGmail%5D/%5CSpam
5	5	imap://4FD35256-CE13-47FE-9840-EBEB5B9FD9C1/%5BGmail%5D/%5CSent
6	6	local://LocalAccountId/x-apple-transient-drafts
7	7	local://LocalAccountId/Outbox
8	8	imap://4FD35256-CE13-47FE-9840-EBEB5B9FD9C1/%5BGmail%5D/%5CTrash
9	9	imap://4FD35256-CE13-47FE-9840-EBEB5B9FD9C1/%5BGmail%5D/%5CStarred
10	10	imap://4FD35256-CE13-47FE-9840-EBEB5B9FD9C1/%5BGmail%5D/%5CDrafts

Figure 8.1 – The mailboxes table displayed in DB Browser

```

1  SELECT
2    DATETIME(messages.date_sent, 'UNIXEPOCH', 'localtime') AS "DATE / TIME",
3    messages.sender AS SENDER,
4    messages.subject AS SUBJECT,
5    messages.summary AS SUMMARY,
6    messages.read AS READ,
7    mailboxes.url AS MAILBOX,
8    messages.external_id AS "EML FILENAME"
9  FROM messages
10 LEFT JOIN mailboxes ON messages.mailbox = mailboxes.ROWID
11 ORDER BY "DATE / TIME" ASC;

```

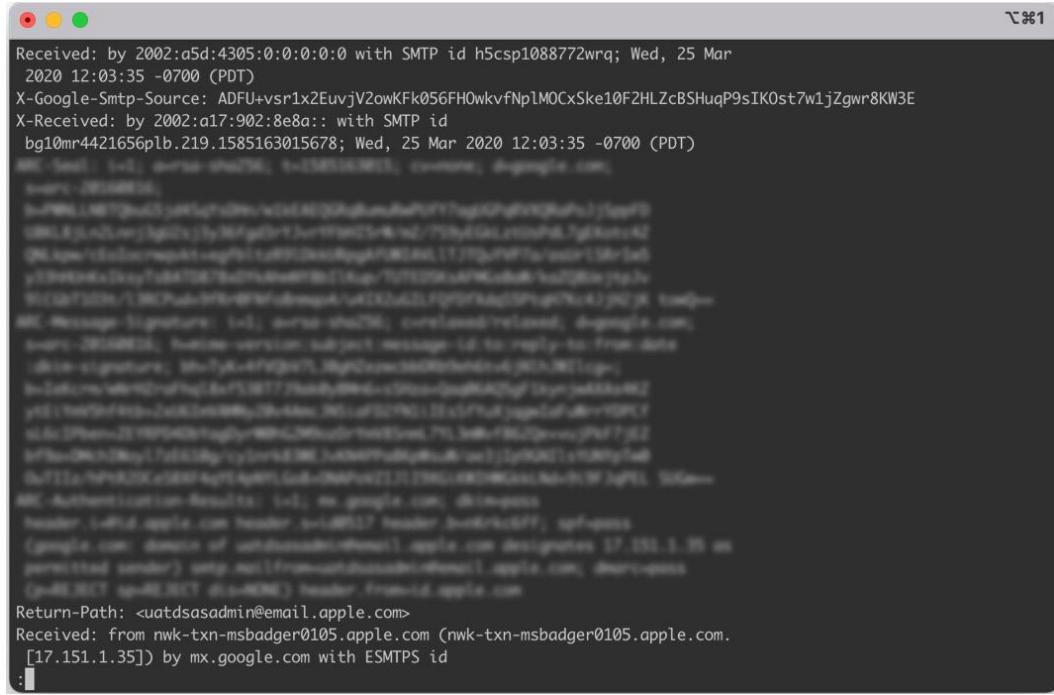
	DATE / TIME	SENDER	SUBJECT	SUMMARY	READ	MAILBOX	EML FILENAME
1	2020-01-29 16:41:06	1	1	31	1	imap://4FD35256-CE13-47FE-9840-...	93A38D70-0A55-4112-8230-CCBC4E9B0...
2	2020-01-29 16:41:06	1	1	31	1	imap://4FD35256-CE13-47FE-9840-...	40993EE2-B665-4BEE-BFC9-6B84A283...
3	2020-01-29 19:27:44	3	2	40	1	imap://4FD35256-CE13-47FE-9840-...	F2E7E782-EF41-443D-8760-7C8E2D95F...
4	2020-01-29 19:27:44	3	2	40	1	imap://4FD35256-CE13-47FE-9840-...	1CB174AC-AAEA-4B17-932D-33B31BAB1...
5	2020-01-29 19:27:44	3	2	40	1	imap://4FD35256-CE13-47FE-9840-...	BC683228-E85D-4D1F-919D-5EB953259...
6	2020-01-29 19:28:41	4	3	42	1	imap://4FD35256-CE13-47FE-9840-...	732B2990-1D4D-42A1-934A-9F63DD3D...
7	2020-01-29 19:28:41	4	3	42	1	imap://4FD35256-CE13-47FE-9840-...	18E248F4-4D3C-4510-861D-B1C1246B1...
8	2020-01-29 19:30:07	6	4	41	1	imap://4FD35256-CE13-47FE-9840-...	147EABC4-5849-459B-9254-C0A1AA114...
9	2020-01-29 19:30:07	6	4	41	1	imap://4FD35256-CE13-47FE-9840-...	E70AF34F-EE89-4E6B-97FE-63B8DA29E...
10	2020-01-31 15:00:00	8	5	6	1	imap://4FD35256-CE13-47FE-9840-...	9995C21F-D61A-46C5-8B39-F8D3E68E0...

Figure 8.2 – The SQL query extracts email metadata from the messages table

Table: **addresses**

ROWID	address		comment
=1	Filter	Filter	
1	1	no-reply@accounts.google.com	Google

Figure 8.3 – The addresses table filtered by ROWID



```

Received: by 2002:a5d:4305:0:0:0:0:0 with SMTP id h5csp1088772wrq; Wed, 25 Mar  

2020 12:03:35 -0700 (PDT)  

X-Google-Smtp-Source: ADFU+vsr1x2EuvjV2owKfk056FH0kvfNplMOCxSke10F2HLzcBSHuqP9sIK0st7w1jZgwr8KW3E  

X-Received: by 2002:a17:902:8e8a:: with SMTP id  

bg10mr4421656pb.219.1585163015678; Wed, 25 Mar 2020 12:03:35 -0700 (PDT)  

ARC-Security-Label: 1=TLS; 2=SHA256; 3=TLS; 4=SHA256; 5=TLS; 6=SHA256;  

X-Google-Mime-Version: 1.0  

X-Google-Smtp-Received: 2020 Mar 25 12:03:35 +0000 (Wed, 25 Mar 2020 12:03:35 +0000)  

X-Google-Smtp-Received: 2020 Mar 25 12:03:35 +0000 (Wed, 25 Mar 2020 12:03:35 +0000)  

X-Google-Smtp-Received: 2020 Mar 25 12:03:35 +0000 (Wed, 25 Mar 2020 12:03:35 +0000)  

X-Google-Smtp-Received: 2020 Mar 25 12:03:35 +0000 (Wed, 25 Mar 2020 12:03:35 +0000)  

X-Google-Smtp-Received: 2020 Mar 25 12:03:35 +0000 (Wed, 25 Mar 2020 12:03:35 +0000)  

ARC-Message-Signature: 1=tls; 2=sha256; 3=tls; 4=sha256; 5=tls; 6=sha256;  

X-Google-Smtp-Header-Version: 1.0  

Subject: message-test@shazam.com  

From: message-test@shazam.com  

Message-ID: <1708083844.361472.1585163015678@msbadger0105.apple.com>  

Date: Wed, 25 Mar 2020 12:03:35 +0000  

Message-ID: <1708083844.361472.1585163015678@msbadger0105.apple.com>  

X-Apple-Header-Original-Recipient: to=; me.google.com; dmarcapp  

Header: In-Path: apple.com header: arc=0317 header: double-helix=1, opt-in=0  

(google.com: domain of uatdsasadmin@uatdsasadmin01.apple.com designates 57.252.3.35 as  
permitted sender); smtppool1.fireswitch.usatdsasadmin01.apple.com; dmarcapp  

(=apple.NET; apollo36CT.alv.uatdsasadmin01.apple.com) header: From=uid.apple.com  

Return-Path: <uatdsasadmin@email.apple.com>  

Received: from nwk-txn-msbadger0105.apple.com (nwk-txn-msbadger0105.apple.com  

[17.151.1.35]) by mx.google.com with ESMTPS id  


```

**Figure 8.4 – An EML file viewed through the terminal showing the email's content**

	Message Date	text	service	account	account_login
1	2020-03-22 02:10:59	G-773293 is your Google verification code...	SMS	p:+19195794674	P:+19195794674
2	2020-03-22 16:16:16	imo code: 258465...	SMS	p:+19195794674	P:+19195794674
3	2020-03-22 20:21:40	Please enter 737950 into LINE within the next 30 mins....	SMS	p:+19195794674	P:+19195794674
4	2020-03-23 02:06:38	Please enter this code in the app to reset your MeWe ...	SMS	p:+19195794674	P:+19195794674
5	2020-03-23 02:38:03	Your Signal verification code: 903-394...	SMS	p:+19195794674	P:+19195794674
6	2020-03-23 18:41:36	🔔 Thisls,you have 2 new notifications on Facebook: ...	SMS	p:+19195794674	P:+19198887386
7	2020-03-24 02:21:34	Telegram code: 95037...	SMS	p:+19195794674	P:+19195794674
8	2020-03-24 02:27:40	[TikTok] 8494 is your verification code,valid for 5 minutes.	SMS	p:+19195794674	P:+19195794674
9	2020-03-24 02:52:23	Your WhatsApp code: 203-591...	SMS	p:+19195794674	P:+19195794674
10	2020-03-25 01:47:38	Your Skout verification code is 3079....	SMS	p:+19195794674	P:+19195794674

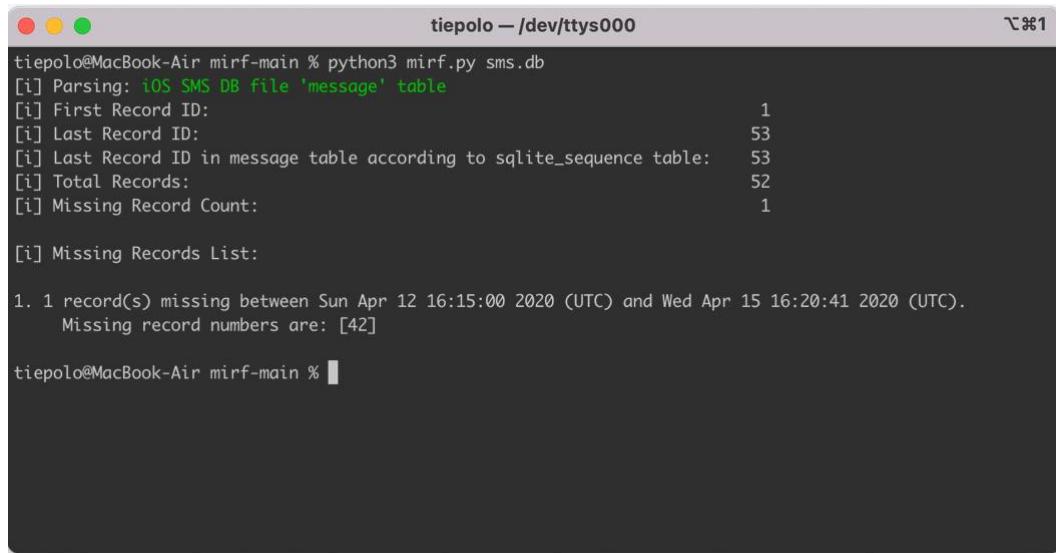
  

	account	account_login	chat_identifier	Date Read	Message Direction	Last Read
1	p:+19195794674	P:+19195794674	22000	2020-03-22 02:11:03	Incoming	2020-04-07 03:05:23
2	p:+19195794674	P:+19195794674	+18634205597	2020-03-22 16:16:19	Incoming	2020-03-22 16:16:19
3	p:+19195794674	P:+19195794674	+13176444906	2020-03-22 20:21:53	Incoming	2020-03-22 20:21:53
4	p:+19195794674	P:+19195794674	85760	2020-03-23 02:06:44	Incoming	2020-03-23 02:06:44
5	p:+19195794674	P:+19195794674	+17026604496	2020-03-23 02:38:05	Incoming	2020-03-23 02:38:05
6	p:+19195794674	P:+19198887386	32665	2020-03-24 02:00:59	Incoming	2020-04-16 00:14:06
7	p:+19195794674	P:+19195794674	+12074242620	2020-03-24 02:21:36	Incoming	2020-03-24 02:21:36
8	p:+19195794674	P:+19195794674	+13233208923	2020-03-24 02:27:42	Incoming	2020-03-24 02:27:42
9	p:+19195794674	P:+19195794674	47543	2020-03-24 02:52:25	Incoming	2020-03-24 02:52:25
10	p:+19195794674	P:+19195794674	+12349008110	2020-03-25 01:47:41	Incoming	2020-03-25 01:47:41

**Figure 8.5 – Extracting message data from sms.db**

Z_PK	DATE	ZTEXT
1	2020-03-26 19:42:57	NULL
2	2020-03-26 19:42:57	What's up?!
3	2020-03-26 19:43:48	Not much.Just waiting to hop on a conference call.You?
4	2020-03-26 19:44:44	A little busy.Finished one report this morning and going to...
5	2020-03-26 19:47:12	Not yet but the effects of this will be felt later I'm sure.
6	2020-03-27 01:35:26	NULL
7	2020-03-27 01:36:36	Lol!!
8	2020-03-27 01:37:02	My turn.
9	2020-03-27 01:38:00	NULL
10	2020-04-11 20:23:43	NULL
11		

**Figure 8.6 – The Z\_PK column stores a unique identifier for each message**

A screenshot of a terminal window titled "tiepolo — /dev/ttys000". The window shows the command "python3 mirf.py sms.db" being run. The output indicates that it is parsing an iOS SMS DB file named 'message' table. It provides statistics: First Record ID: 1, Last Record ID: 53, Last Record ID in message table according to sqlite\_sequence table: 53, Total Records: 52, and Missing Record Count: 1. It also lists the missing records: 1 record(s) missing between Sun Apr 12 16:15:00 2020 (UTC) and Wed Apr 15 16:20:41 2020 (UTC), with record numbers [42].

```
tiepolo@MacBook-Air mirf-main % python3 mirf.py sms.db
[i] Parsing: iOS SMS DB file 'message' table
[i] First Record ID: 1
[i] Last Record ID: 53
[i] Last Record ID in message table according to sqlite_sequence table: 53
[i] Total Records: 52
[i] Missing Record Count: 1

[i] Missing Records List:
1. 1 record(s) missing between Sun Apr 12 16:15:00 2020 (UTC) and Wed Apr 15 16:20:41 2020 (UTC).
Missing record numbers are: [42]

tiepolo@MacBook-Air mirf-main %
```

Figure 8.7 – Running Mirf to detect deleted messages

## Code and Commands

Command 8.1:

```
SELECT
DATETIME(messages.date_sent, 'UNIXEPOCH', 'localtime') AS
"DATE / TIME",
messages.sender AS SENDER,
messages.subject AS SUBJECT,
messages.summary AS SUMMARY,
messages.read AS READ,
mailboxes.url AS MAILBOX,
messages.external_id AS "EML FILENAME"
FROM messages
LEFT JOIN mailboxes ON messages.mailbox = mailboxes.ROWID
```

```
ORDER BY "DATE / TIME" ASC;
```

Command 8.2:

```
SELECT  
  
CASE when LENGTH(chat_message_join.message_date)=18 THEN  
      datetime(chat_message_join.message_date/1000000000 +  
978307200,'unixepoch','localtime')  
      when LENGTH(chat_message_join.message_date)=9 THEN  
      datetime(chat_message_join.message_date +  
978307200,'unixepoch','localtime')  
      else 'NA'  
  
END as "Message Date",  
  
message.text,  
  
message.service,  
  
message.account,  
  
chat.account_login,  
  
chat.chat_identifier,  
  
CASE when LENGTH(message.date_read)=18 THEN  
      datetime(message.date_read/1000000000 +  
978307200,'unixepoch','localtime')  
      when LENGTH(message.date_read)=9 THEN  
      datetime(message.date_read+978307200,'unixepoch','localtime')  
      else 'NA'  
  
END as "Date Read",  
  
CASE when message.is_read=1  
      THEN 'Incoming'  
      when message.is_read=0
```

```

        THEN 'Outgoing'
END AS "Message Direction",
CASE when LENGTH(chat.last_read_message_timestamp)=18 THEN
      datetime(chat.last_read_message_timestamp/1000000000+9
78307200,'unixepoch','localtime')
      when LENGTH(chat.last_read_message_timestamp)=9 THEN
      datetime(chat.last_read_message_timestamp +
978307200,'unixepoch','localtime')
      else 'NA'
END as "Last Read"
FROM message
left join chat_message_join on
chat_message_join.message_id=message.ROWID
left join chat on chat.ROWID=chat_message_join.chat_id
left join attachment on
attachment.ROWID=chat_message_join.chat_id
order by "Message Date" ASC;

```

**Command 8.3:**

```
pip install -r requirements.txt
```

# Chapter 9

## Images

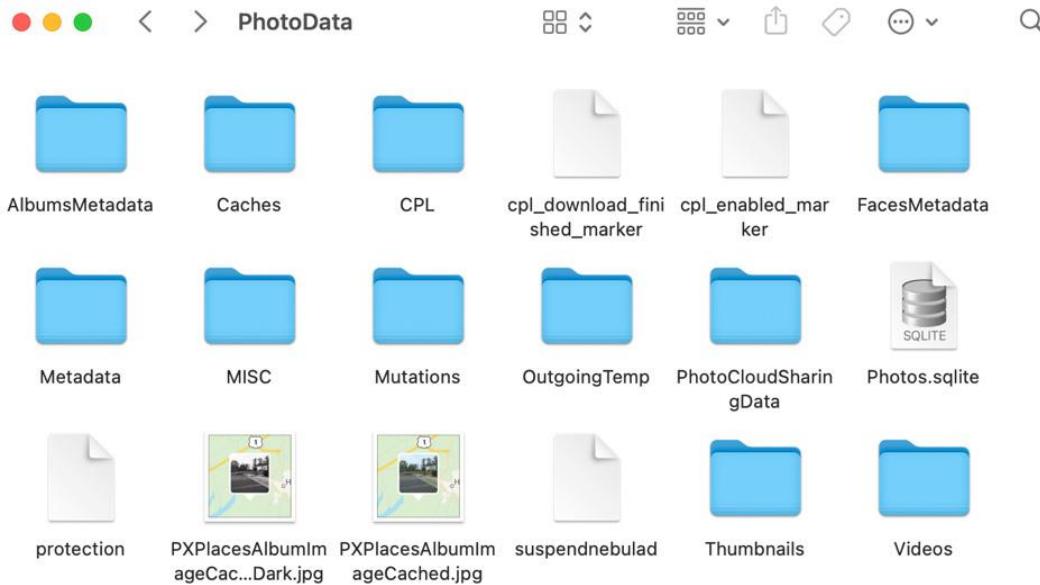


Figure 9.1 – The PhotoData folder contains media metadata

	Z_PK	Created date	Modified date	Deleted date	File name	Directory	Width	Height	Hidden
1	1	2020-03-22 13:05:24	2020-04-06 15:02:38	NULL	IMG_0001.JPG	DCIM/100APPLE	1125	1137	0
2	2	2020-03-22 13:05:39	2020-04-06 15:02:38	NULL	IMG_0002.JPG	DCIM/100APPLE	3550	3150	0
3	3	2020-03-22 13:10:50	2020-04-13 19:32:52	NULL	IMG_0003.JPG	DCIM/100APPLE	1668	860	0
4	4	2020-03-22 13:25:02	2020-04-06 15:02:38	NULL	IMG_0004.JPG	DCIM/100APPLE	1117	886	0
5	5	2020-03-22 13:25:02	2020-04-06 15:02:38	NULL	IMG_0005.JPG	DCIM/100APPLE	1522	1775	0
6	6	2020-03-22 13:25:02	2020-04-06 15:02:38	NULL	IMG_0006.JPG	DCIM/100APPLE	1170	1175	0
7	7	2020-03-22 13:25:02	2020-04-19 18:25:57	NULL	IMG_0007.JPG	DCIM/100APPLE	1178	781	0
8	8	2020-03-22 13:25:02	2020-04-13 19:32:52	NULL	IMG_0008.JPG	DCIM/100APPLE	1125	1156	0
9	9	2020-03-22 13:31:03	2020-04-06 15:02:38	NULL	IMG_0009.JPG	DCIM/100APPLE	828	637	0
10	10	2020-03-22 13:40:14	2020-04-19 18:25:58	NULL	IMG_0010.JPG	DCIM/100APPLE	620	553	0

Figure 9.2 – The results of the query from the Photos.sqlite database

Figure 9.3 – The results of the query from the Photos.sqlite database

#	AlbumTitle	CreatorBundleID	EditorBundleID	Directory	UniformResourceIdentifier
22	720D5959.jpg	Imgur	NULL	DCIM/100APPLE	public.jpeg
23	720D5959.jpg	Imgur	NULL	DCIM/100APPLE	public.jpeg
24	NULL	NULL	com.apple.ScreenshotServicesService	DCIM/100APPLE	public.jpeg
25	iA30D6460.jpg	NULL	NULL	DCIM/100APPLE	public.jpeg
26	0460310D.jpg	NULL	NULL	DCIM/100APPLE	public.jpeg
27	I-13D1A552AFDF.jpg	NULL	NULL	DCIM/100APPLE	public.jpeg
28	NULL	com.reddit.Reddit	NULL	DCIM/100APPLE	public.jpeg
29	NULL	org.whispersystems.signal	NULL	DCIM/100APPLE	public.png
30	NULL	NULL	NULL	DCIM/100APPLE	public.jpeg
31	NULL	NULL	com.apple.ScreenshotServicesService	DCIM/100APPLE	public.jpeg

Figure 9.4 – CreatorBundleID and EditorBundleID indicate where the asset originates from

	Timestamp	View Count	Play Count	Share Count	Last Shared Date	File Modification Date	Has Adjustments	Adjustments Time
31		2	0	0	NULL	2020-04-06 15:02:38	Yes	2020-03-25 01:53:
32		1	0	0	NULL	2020-04-06 15:02:38	No	NULL
33		2	0	0	NULL	2020-04-19 18:25:57	No	NULL
34		1	0	0	NULL	2020-04-06 15:02:38	No	NULL
35		1	0	1	2020-04-05 19:13:52	2020-04-19 18:25:57	No	NULL
36		1	0	1	2020-04-05 19:13:52	2020-04-19 18:25:57	No	NULL
37		1	0	1	2020-03-27 01:17:03	2020-04-19 18:25:58	No	NULL
38		1	0	1	2020-03-27 01:17:03	2020-04-19 18:25:58	No	NULL
39		1	0	1	2020-03-27 01:17:03	2020-04-19 18:25:58	No	NULL
40		0	0	0	NULL	2020-03-27 00:38:01	No	NULL

**Figure 9.5 – The ShareCount column indicates whether a media asset was shared with other devices**

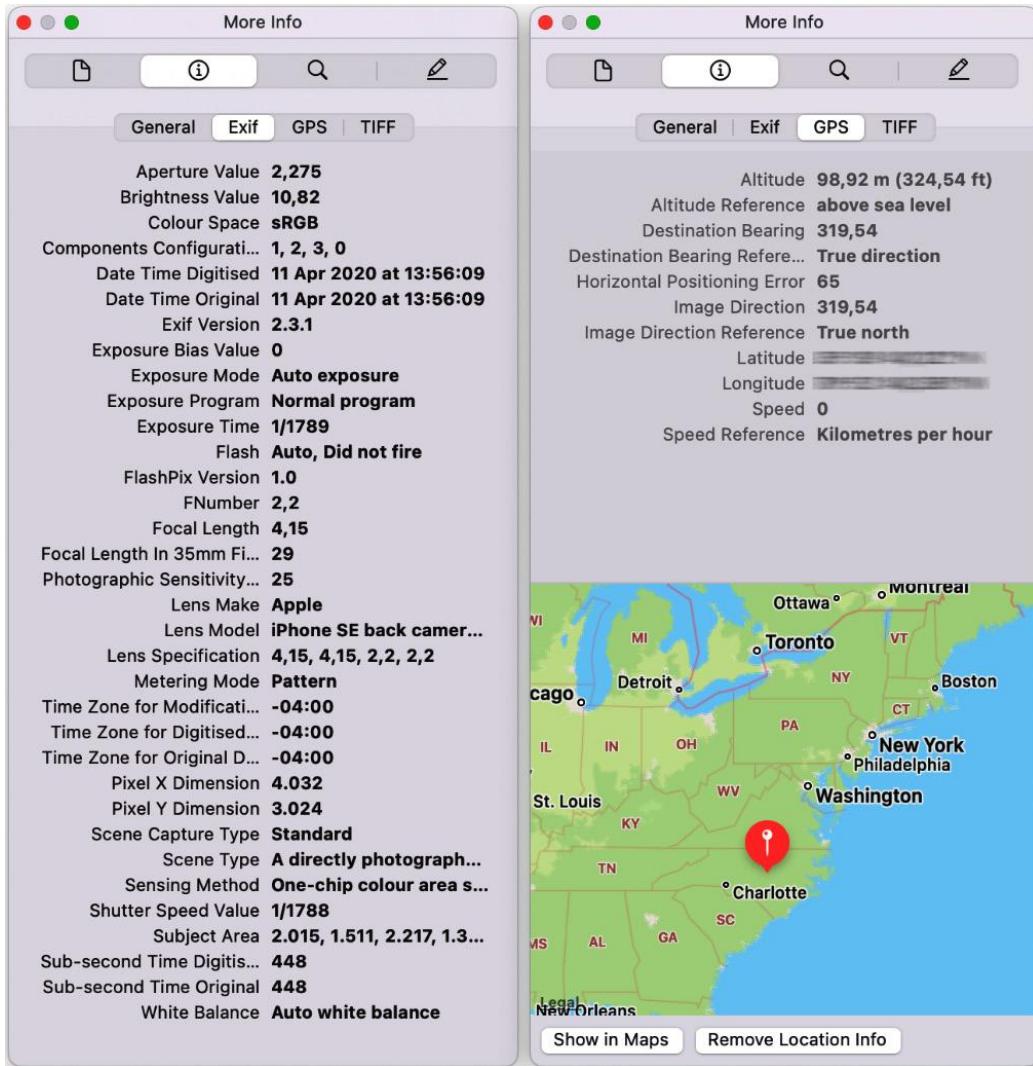


Figure 9.6 – EXIF metadata extracted from a photo that was captured on an iPhone

	ZUUID	ZSTREAMNAME	ZVALUESTRING
		/media/nowPlaying	<input type="button" value="Filter"/>
74	4698C-793C-46F2-93C0-4C3C5C6A4F2E	/media/nowPlaying	com.apple.podcasts
75	97505-A71C-494E-9CC6-59291287024C	/media/nowPlaying	com.apple.podcasts
76	9B7F4-FFFD-4E8E-931B-359E2EECC3C	/media/nowPlaying	com.apple.podcasts
77	22CEE-4834-42B3-9531-E2BDB3F3D1C4	/media/nowPlaying	com.apple.podcasts
78	5BFD9-C420-43F4-B6F2-DB1ADA37DB44	/media/nowPlaying	com.apple.podcasts
79	F2219-190C-4AAF-86C4-5CE72450F13C	/media/nowPlaying	com.apple.podcasts
80	8C843-9905-41D2-9E91-86F9EE1F0399	/media/nowPlaying	com.apple.podcasts
81	3F5AE-9168-4A64-A425-BD6E9A819D53	/media/nowPlaying	com.apple.podcasts
82	38C00-B90C-4B93-80E3-3206D399F163	/media/nowPlaying	com.apple.podcasts
83	ACB47-489B-4563-A46B-EA117D67F931	/media/nowPlaying	com.apple.podcasts
84	004A8-5501-4C06-94C9-7A7CDEAD6708	/media/nowPlaying	com.apple.podcasts
85	014E4-3F63-4A0B-9F98-1DF287575D2B	/media/nowPlaying	com.apple.podcasts
86	1E3A15-CC82-4BBD-896A-AEA0C9C93BBF	/media/nowPlaying	com.apple.podcasts

Figure 9.7 – Media events extracted from the KnowledgeC.db database

	ZVALUESTRING	NOW PLAYING ALBUM	NOW PLAYING ARTIST	NOW PLAYING GENRE
87	com.apple.Music	B.o.B Presents: The Adventures of Bobby Ray (Deluxe)	B.o.B	Hip-Hop/Rap
88	com.apple.Music	Mother's Milk	Red Hot Chili Peppers	Alternative
89	com.apple.Music	Faster Kill Pussycat (feat. Brittany Murphy)	Oakenfold	Dance
90	com.apple.Music	Mayday	Boys Noize	Breakbeat
91	com.apple.Music	Until Now	Swedish House Mafia	Dance
92	com.apple.Music	Until Now	Swedish House Mafia	Dance
93	com.apple.Music	Until Now	Swedish House Mafia	Dance
94	com.apple.Music	Until Now	Swedish House Mafia	Dance
95	com.apple.Music	Until Now	Swedish House Mafia	Dance
96	com.apple.Music	Until Now	Swedish House Mafia	Dance

Figure 9.8 – Extracting media viewing data from KnowledgeC.db

## Code and Commands

Code 9.1:

```
SELECT
    Z_PK,
    DATETIME(ZDATECREATED + 978307200, 'UNIXEPOCH') AS "Created
date",
```

```
DATETIME(ZMODIFICATIONDATE + 978307200, 'UNIXEPOCH') AS  
"Modified date",  
  
DATETIME(ZTRASHEDDATE + 978307200, 'UNIXEPOCH') AS "Deleted  
date",  
  
ZFILENAME AS "File name",  
ZDIRECTORY AS "Directory",  
ZWIDTH AS "Width",  
ZHEIGHT AS "Height",  
ZHIDDEN AS "Hidden"  
FROM ZGENERICASSET  
ORDER BY Z_PK ASC;
```

Command 9.2:

```
SELECT  
  
datetime(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH',  
'LOCALTIME') as "START",  
  
datetime(ZOBJECT.ZENDDATE+978307200,'UNIXEPOCH',  
'LOCALTIME') as "END",  
  
(ZOBJECT.ZENDDATE-ZOBJECT.ZSTARTDATE) as "USAGE IN  
SECONDS",  
  
ZOBJECT.ZVALUESTRING,  
  
ZSTRUCTUREDMETADATA.Z_DKNOWPLAYINGMETADATATEKEY__ALBUM as  
"NOW PLAYING ALBUM",  
  
ZSTRUCTUREDMETADATA.Z_DKNOWPLAYINGMETADATATEKEY__ARTIST as  
"NOW PLAYING ARTIST",  
  
ZSTRUCTUREDMETADATA.Z_DKNOWPLAYINGMETADATATEKEY__GENRE as  
"NOW PLAYING GENRE",  
  
ZSTRUCTUREDMETADATA.Z_DKNOWPLAYINGMETADATATEKEY__TITLE as  
"NOW PLAYING TITLE",
```

```
ZSTRUCTUREDMETADATA.Z_DKNOWPLAYINGMETADATATEKEY__DURATION as  
"NOW PLAYING DURATION"  
  
FROM ZOBJECT  
  
left join ZSTRUCTUREDMETADATA on  
ZOBJECT.ZSTRUCTUREDMETADATA = ZSTRUCTUREDMETADATA.Z_PK  
  
left join ZSOURCE on ZOBJECT.ZSOURCE = ZSOURCE.Z_PK  
  
WHERE ZSTREAMNAME like "/media%"  
  
ORDER BY "START";
```

## Links

- *Using Photos.sqlite to Show the Relationships Between Photos and the Application they were Created with?, DFIR Review, Koenig, S., 2021:*  
<https://dfir.pubpub.org/pub/v19rksvf>

# Chapter 10

## Images

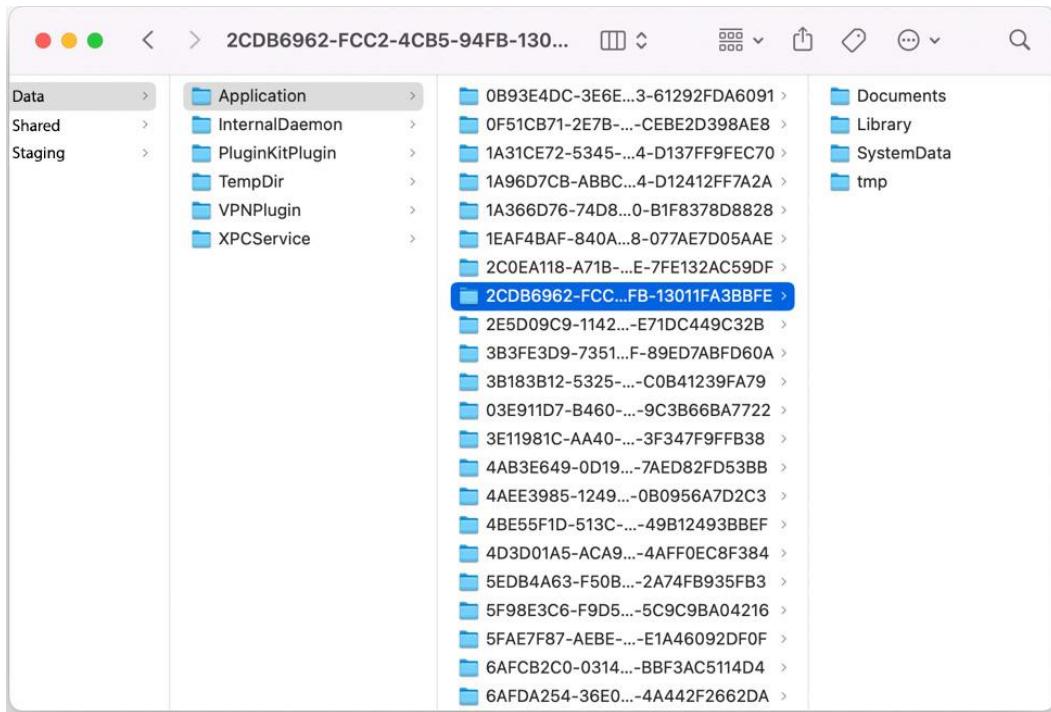


Figure 10.1 – The data container's directory structure

	<b>id</b>	<b>application_identifier</b>	
Filt...	Filter		
1	1	com.apple.MobileSMS	
2	2	com.apple.Diagnostics	
3	3	com.apple.Health	
4	4	com.apple.datadetectors.DDActionsService	
5	5	com.apple.TVRemoteUIService	
6	6	com.apple.Preferences	
7	7	com.apple.CarPlaySettings	
8	8	com.apple.Home.HomeUIService	
9	9	com.apple.Magnifier	
10	10	com.apple.BarcodeScanner	
11	11	com.apple.Passbook	
12	12	com.apple.siri	

Figure 10.2 – The application\_identifier table from applicationState.db

	<b>application_identifier</b>	<b>value</b>
1	com.apple.MobileSMS	<i>BLOB</i>
2	com.apple.Diagnostics	<i>BLOB</i>
3	com.apple.Health	<i>BLOB</i>
4	com.apple.datadetectors.DDActionsService	<i>BLOB</i>
5	com.apple.TVRemoteUIService	<i>BLOB</i>
6	com.apple.Preferences	<i>BLOB</i>
7	com.apple.CarPlaySettings	<i>BLOB</i>
8	com.apple.Home.HomeUIService	<i>BLOB</i>
9	com.apple.Magnifier	<i>BLOB</i>
10	com.apple.BarcodeScanner	<i>BLOB</i>

Figure 10.3 – The query prints bundle IDs for all the installed applications

	application_identifier	value
54	com.facebook.Messenger	BLOB
55	org.mozilla.ios.Focus	BLOB
56	imgurmobile	BLOB
57	co.babypenguin.imo	BLOB
58	com.burbn.instagram	BLOB
59	com.kik.chat	BLOB
60	jp.naver.line	BLOB
61	com.mewe	BLOB
62	com.reddit.Reddit	BLOB
63	org.whispersystems.signal	BLOB

Figure 10.4 – Each Bundle ID has an associated binary BLOB

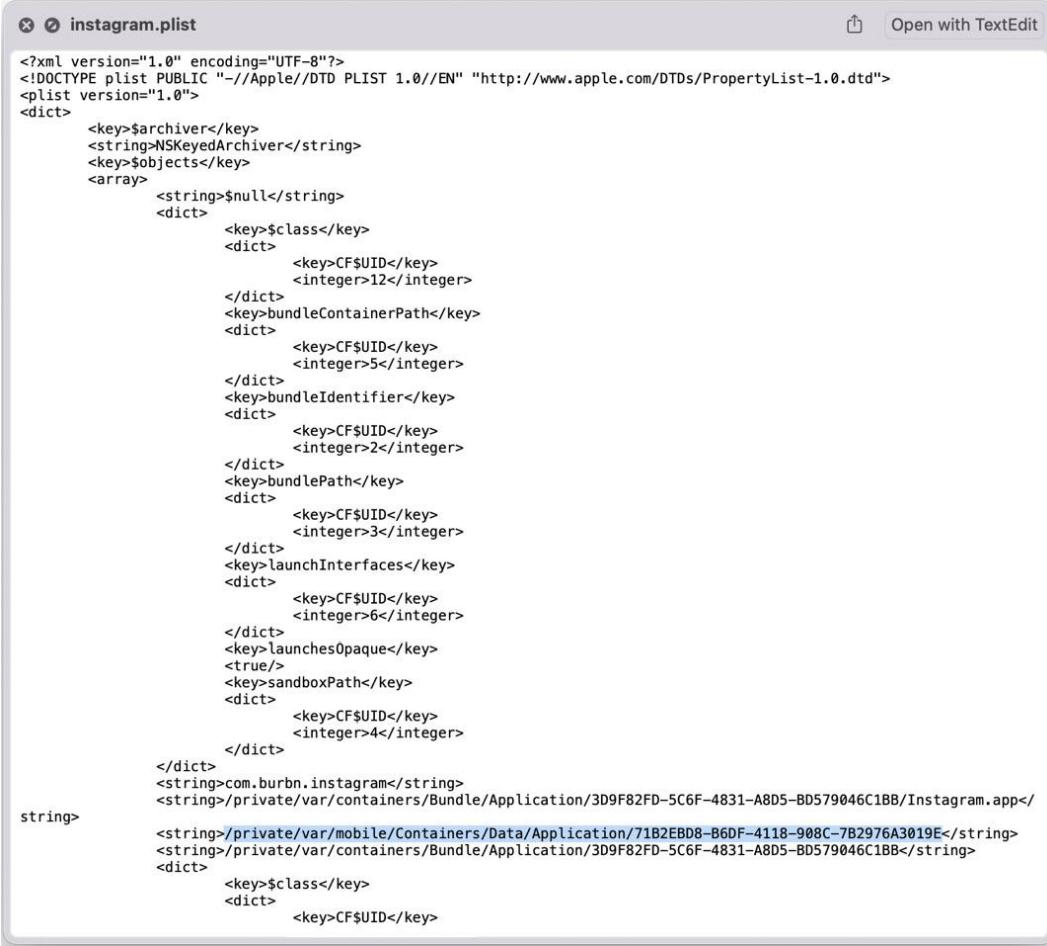
0000 62 70 6c 69 73 74 30 30 4f 11 03 f7 62 70 6c 69	bplist000...bpli st00.....X\$ver sionY\$archiver T\$topX\$obj ects.. ..._. NSKeyedArc hiver...Troot... .....\$0129=U\$n ull..... ..V\$classZbundle Path[sandboxPath _..bundleIdentif ier^launchesOpaq ue_..bundleConta inerPath_..launc hInterfaces..... .....con.b urban.instagram_. ]/private/var/co ntainers/Bundle/ Application/3D9F 82FD-5C6F-4831-A 8D5-BE579046C1BB /Instagram.app_. T/private/var/no bile/Containers/ Data/Application /71B2EBD8-B6DF-4 118-908C-7B2976A 3019E_.O/private /var/containers/ Bundle/Application/ 3D9F82FD-5C6F -4831-A8D5-BE579 046C1BB..!#ZNS. objects.".....% &() *+.-./ZurlSc hemes\defaultTtTy peTnameZidentifi er.....^IG LaunchScreen_..._ _from_UILaunchSt
--	---

Type of data currently in cell: Binary

1061 byte(s)

Apply

Figure 10.5 – The BLOB contains a binary PLIST



The screenshot shows the 'Instagram.plist' file open in Xcode's plist editor. The file is an XML-based Property List (PLIST) file. It contains several key-value pairs, primarily strings and dictionaries. One of the strings is a path to an application bundle. The file is well-formatted with indentation and line breaks.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>$archiver</key>
<string>NSKeyedArchiver</string>
<key>$objects</key>
<array>
<string>$null</string>
<dict>
<key>$class</key>
<dict>
<key>CF$UID</key>
<integer>12</integer>
</dict>
<key>bundleContainerPath</key>
<dict>
<key>CF$UID</key>
<integer>5</integer>
</dict>
<key>bundleIdentifier</key>
<dict>
<key>CF$UID</key>
<integer>2</integer>
</dict>
<key>bundlePath</key>
<dict>
<key>CF$UID</key>
<integer>3</integer>
</dict>
<key>launchInterfaces</key>
<dict>
<key>CF$UID</key>
<integer>6</integer>
</dict>
<key>launchesOpaque</key>
<true/>
<key>sandboxPath</key>
<dict>
<key>CF$UID</key>
<integer>4</integer>
</dict>
</dict>
<string>com.burbn.instagram</string>
<string>/private/var/containers/Bundle/Application/3D9F82FD-5C6F-4831-A8D5-BD579046C1BB/Instagram.app</string>
<string>/private/var/mobile/Containers/Data/Application/71B2EBD8-B6DF-4118-908C-7B2976A3019E</string>
<string>/private/var/containers/Bundle/Application/3D9F82FD-5C6F-4831-A8D5-BD579046C1BB</string>
<dict>
<key>$class</key>
<dict>
<key>CF$UID</key>
```

Figure 10.6 – The PLIST contains details related to the app's containers

```

Terminal — fsmon - sudo
FSE_RENAME      435  "analyticasd"   /System/Volumes/Data/private/var/db/analyticscd/aggregate_persist_temp -> /System/Volumes/Data/pri
FSE_CHTN        582  "cfprefsd"     /System/Volumes/Data/private/var/folders/2p/pk5jbxj6bn3lmc7_v69sc70000gn/T/TemporaryItems/com.a
FSE_CHTN        582  "cfprefsd"     /System/Volumes/Data/private/var/folders/2p/pk5jbxj6bn3lmc7_v69sc70000gn/T/TemporaryItems/com.a
FSE_CHTN        582  "cfprefsd"     /System/Volumes/Data/private/var/folders/2p/pk5jbxj6bn3lmc7_v69sc70000gn/T/TemporaryItems/com.a
FSE_CHTN        582  "cfprefsd"     /System/Volumes/Data/private/var/folders/2p/pk5jbxj6bn3lmc7_v69sc70000gn/T/TemporaryItems/com.a
FSE_CONTENT_MODIFIED 582  "cfprefsd"     /System/Volumes/Data/private/var/folders/2p/pk5jbxj6bn3lmc7_v69sc70000gn/T/TemporaryItems/com.a
FSE_CREATE_FILE  582  "cfprefsd"     /System/Volumes/Data/private/var/folders/2p/pk5jbxj6bn3lmc7_v69sc70000gn/T/TemporaryItems/com.a
FSE_CONTENT_MODIFIED 435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_persist_temp
FSE_RENAME      435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_persist_temp -> /System/Volumes/Data/pri
FSE_RENAME      435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregates/Daily/c3/0ef7ic-79e6-43df-856f-f2deb1c
FSE_XATTR_MODIFIED 435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_resume_stage
FSE_RENAME      435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_resume_stage -> /System/Volumes/Data/pri
FSE_RENAME      435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregates/Daily/0d/415f07-63ac-4eac-80d6-9cd966b4
FSE_XATTR_MODIFIED 435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_resume_stage -> /System/Volumes/Data/pri
FSE_RENAME      435  "logd_helper"   /System/Volumes/Data/private/var/db/uiddtext/AB/40FAEEB26E392B7F0EDAB6CE781B8.T0cQKUHc -> /Syste
FSE_RENAME      17035 "logd_helper"   /System/Volumes/Data/private/var/db/uiddtext/AB/40FAEEB26E392B7F0EDAB6CE781B8
FSE_CONTENT_MODIFIED 17035 "logd_helper"   /System/Volumes/Data/private/var/db/uiddtext/AB/40FAEEB26E392B7F0EDAB6CE781B8
FSE_RENAME      435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_resume_stage -> /System/Volumes/Data/pri
FSE_RENAME      435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregates/Daily/77/81e01e-f44d-4f21-aefc-4e8ac813
FSE_XATTR_MODIFIED 435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_resume_stage
FSE_RENAME      435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_resume_stage -> /System/Volumes/Data/pri
FSE_RENAME      435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregates/Daily/97/3453dc-d602-4452-9aa0-ccf7afcc
FSE_XATTR_MODIFIED 435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_resume_stage
FSE_RENAME      435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_resume_stage -> /System/Volumes/Data/pri
FSE_CONTENT_MODIFIED 435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_persist_temp
FSE_RENAME      435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_persist_temp -> /System/Volumes/Data/pri
FSE_DELETE       435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregates/Daily/97/3453dc-d602-4452-9aa0-ccf7afcc
FSE_CREATE_FILE  435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_persist_temp
FSE_CONTENT_MODIFIED 435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_persist_temp -> /System/Volumes/Data/pri
FSE_RENAME      435  "analyticasd"  /System/Volumes/Data/private/var/db/analyticscd/aggregate_persist_temp

```

Figure 10.7 – The fsmon tool prints any filesystem events

```

Flows
GET https://www.google.com/
  ↵ 200 text/html 64.52k 487ms
GET https://www.google.com/logos/doodles/2018/doodle-snow-games-day-12-6070619765473280-s.png
  ↵ 200 image/png 2.63k 184ms
GET https://www.google.com/logos/2018/snowgames_skijump/cta.png
  ↵ 200 image/png 13.4k 229ms
>> GET https://www.gstatic.com/external_hosted/createjs/createjs-2015.11.26.min.js
  ↵ 200 text/javascript 48.51k 475ms
GET https://ssl.gstatic.com/gb/images/i2_2ec824b0.png
  ↵ 200 image/png 23.64k 253ms
GET https://ssl.gstatic.com/safebrowsing/csd/client_model_v5_variation_0.pb
  ↵ 200 application/octet-stream 67.92k 356ms
GET https://ssl.gstatic.com/safebrowsing/csd/client_model_v5_ext_variation_0.pb
  ↵ 200 application/octet-stream 67.92k 412ms
GET https://www.google.com/logos/2018/snowgames_skijump/snowgames_skijump18.js
  ↵ 200 text/javascript 258.16k 900ms
POST https://www.google.com/gen_204?si=webaft&atyp=csi&ei=vCGLWr6uMsKk0gTYs6yIAw&rt=wsrt.2615,aft.1379,prt
  .1379
  ↵ 204 text/html [no content] 379ms
GET https://www.gstatic.com/og/_/js/k=og.og2.en_US.ulHn0gNl16I.0/rt=j/m=def/exm=in,fot/d=1/ed=1/rs=AA2YrT
  uVOKajN...
  ↵ 200 text/javascript 46.4k 265ms
GET https://www.google.com/xjs/_/js/k=xjs.s.en.zjivxe8fVgY.0/m=sx,sb,cdos,cr,elog,hsm,jsa,r,d,csi/am=wCL0
  eMEByP8...
  ↵ 200 text/javascript 144.26k 368ms
GET https://www.google.com/xjs/_/js/k=xjs.s.en.zjivxe8fVgY.0/m=aa,abd,async,dvl,foot,fpe,ipv6,lu,m,mu,sf,
  sonic,s...
  ↵ 200 text/javascript 30.54k 195ms
GET https://www.google.com/logos/2018/snowgames_skijump/main-sprite.png
  ↵ 200 image/png 1.26k 11ms
[*:9999]
↓ [14/36]
: replay_client [flow]

```

**Figure 10.8 – Intercepting network traffic using mitmproxy**

## Tables

### Social networking applications

In this section, we will focus on the three primary social networking applications, **Facebook**, **Instagram**, and **Twitter**. The **Reddit** app is also included in this category.

#### Facebook

The following table shows the most common artifacts for Facebook:

Artifact	Description
Library/Preferences/com.facebook.Facebook.plist	User preferences and details of logged-in users (email and Facebook ID).
Library/Caches/com.facebook.Facebook.*/*	Cached files and images, such as media, are stored while browsing through posts and pages.

**Table 10.1 – Common Facebook artifacts**

#### Instagram

The following table shows the most common artifacts for Instagram:

Artifact	Description
Library/Preferences/com.burbn.instagram.plist	User preferences and details of logged-in users (email and Instagram ID)
Library/Application Support/DirectSQLiteDatabase/*.db	SQLite database containing user data
Library/Application Support/<User_ID>/pending-requests.plist	Property List containing pending friend and message requests
Library/Caches/com.burbn.instagram.IGImageCache/*	Cached images
Library/Caches/com.burbn.instagram.IGSparseVideoCache/*	Cached videos

**Table 10.2 – Common Instagram artifacts**

## Twitter

The following table shows the most common artifacts for Twitter:

Artifact	Description
Library/Preferences/com.atebits.Tweetie2.plist	User preferences and details of logged-in users
Library/Caches/com.twitter.api.cache/Cache.db	SQLite database containing cached API requests, such as visited profiles
Library/SplashBoard/Snapshots/*	App-generated screenshots
Library/Caches/TIPIImagePipeline/*	Cached images
Library/Caches/com.atebits.Tweetie2/fsCachedData/*	Cached data

**Table 10.3 – Common Twitter artifacts**

## Reddit

The following table shows the most common artifacts for Reddit:

Artifact	Description
Library/Preferences/com.reddit.Reddit.plist	User preferences and details of logged-in users
Documents/release2/accountData/*	Binary Property Lists containing user data
Library/SplashBoard/Snapshots/*	App-generated screenshots
Library/Caches/com.reddit.Reddit/Cache.db	SQLite database containing cached API requests
Library/Caches/com.reddit.Reddit/imagedownload/*	SQLite database containing cached images

**Table 10.4 – Common Reddit artifacts**

Now, let's look at a few messaging apps.

## Messaging applications

Although messaging applications were discussed in detail in [Chapter 8, Email and Messaging Forensics](#), this section will provide a reference for some of the most commonly used instant messaging apps, such as **WhatsApp**, **Telegram**, **Facebook Messenger**, and **Signal**.

### WhatsApp

The following table shows the most common artifacts for WhatsApp:

Artifact	Description
Documents/CallHistory.sqlite	Audio and video call history
Documents/blockedcontacts.dat	Contacts blocked by user
Library/2fa.plist	Property List indicating if multi-factor authentication is enabled
Library/Caches/*	Cached media and API requests
Library/Preferences/net.whatsapp.Whatsapp.plist	User preferences
Library/SplashBoard/Snapshots/*	App-generated screenshots
Shared/AppGroup/*/ChatStorage.sqlite	SQLite database storing messages
Shared/AppGroup/*/ContactsV2.sqlite	SQLite database storing contact details
Shared/AppGroup/*/Library/Preferences/*	Property Lists storing preferences

**Table 10.5 – Common WhatsApp artifacts**

### Telegram

The following table shows the most common artifacts for Telegram:

Artifact	Description
Library/Preferences/ph.telegra.Telegraph.plist	Property List containing user preferences
Library/Caches/ph.telegra.Telegraph/fsCachedData/*	Cached media and API requests
Shared/AppGroup/telegram-data/account-<Account_ID>/postbox/db/db_sqlite	SQLite database containing chats and messages
Shared/AppGroup/telegram-data/account-<Account_ID>/postbox/media/*	Chat media files

**Table 10.6 – Common Telegram artifacts**

## Facebook Messenger

The following table shows the most common artifacts for Facebook Messenger:

Artifact	Description
Documents/com.facebook.Messenger.preferences/*	Property List containing user preferences
Library/Preferences/com.facebook.Messenger.plist	Application settings
Shared/AppGroup/shared_messenger_contacts/*.db	SQLite database containing contacts
Shared/AppGroup/shared_messenger_messages/*.db	SQLite database that stores chats and messages
Shared/AppGroup/lightspeed-imageCache/*	Cache

**Table 10.7 – Common Facebook Messenger artifacts**

## Signal

The following table shows the most common artifacts for Signal:

Artifact	Description
Library/Preferences/org.whispersystems.signal.plist	Application settings
Library/Caches/*	Cached media and API requests
Shared/AppGroup/Attachments/*	Media files
Shared/AppGroup/grdb/signal.sqlite	SQLite database containing chats and messages

**Table 10.8 – Common Signal artifacts**

Next, we'll discuss artifacts related to productivity applications.

## Productivity applications

The following tables describe artifacts concerning work and productivity applications, such as **Microsoft Teams**, **Zoom**, **Dropbox**, **Microsoft OneDrive**, and **Gmail**.

## **Microsoft Teams**

The following table shows the most common artifacts for Microsoft Teams:

Artifact	Description
Library/Preferences/com.microsoft.skype.teams.plist	User preferences and application settings
SplashBoard/Snapshots/*	App-generated screenshots
Shared/AppGroup/Library/Preferences/*	Property Lists containing user data

**Table 10.9 – Common Microsoft Teams artifacts**

## **Zoom**

The following table shows the most common artifacts for Zoom:

Artifact	Description
Library/Preferences/us.zoom.videomeetings.plist	User preferences and application settings
Documents/Data/zoommeeting.db	SQLite database containing data related to Zoom meetings and messages exchanged during a meeting
Documents/Data/zoomus.db	SQLite database that stores user data

**Table 10.10 – Common Zoom Artifacts**

## **Dropbox**

The following table shows the most common artifacts for Dropbox:

Artifact	Description
Library/Preferences/com.getdropbox.Dropbox.plist	User preferences and application settings
Documents/Users/<id>/Dropbox.sqlite	SQLite database containing user data and file information
Documents/Users/<id>/metadata.sqlite	SQLite database that stores the metadata of files stored on Dropbox

**Table 10.11 – Common Dropbox artifacts**

## **Microsoft OneDrive**

The following table shows the most common artifacts for Microsoft OneDrive:

Artifact	Description
Library/Preferences/com.microsoft.skydrive.plist	User preferences and application settings
Library/Database/moddatabase.db	SQLite database containing user data
Shared/AppGroup/OneDrive/StramCacheQT/*	Cached files

**Table 10.12 – Common OneDrive artifacts**

## **Gmail**

The following table shows the most common artifacts for Gmail:

Artifact	Description
Library/Preferences/com.google.Gmail.plist	User preferences, application settings, and logged-in user data
Library/ApplicationSupport/data/<email>/*	SQLite database containing user data
Library/Caches/*	Cached files

**Table 10.13 – Common Gmail artifacts**

Next, we'll look at a few multimedia apps.

## **Multimedia applications**

This section includes applications that allow you to view or share media files, such as **Netflix**, **YouTube**, **Spotify**, **Snapchat**, and **TikTok**.

### **Netflix**

The following table shows the most common artifacts for Netflix:

Artifact	Description
Library/Preferences/com.netflix.NFLIX.plist	User preferences and application settings
Documents/store.sqlite	SQLite database containing information on the logged-in user
Library/Caches/*	Cached video streams and API requests

**Table 10.14 – Common Netflix artifacts**

## YouTube

The following table shows the most common artifacts for YouTube:

Artifact	Description
Library/Preferences/com.google.ios.youtube.plist	User preferences and application settings
Library/Caches/*	Video and API requests caches

**Table 10.15 – Common YouTube artifacts**

## Spotify

The following table shows the most common artifacts for Spotify:

Artifact	Description
Library/Preferences/com.spotify.client.plist	User preferences and application settings
Documents/InstrumentsModel.sqlite	SQLite database that stores app events
Library/ApplicationSupport/PersistentCache/mercury.db	Playback history cached media
Library/ApplicationSupport/Users/<id>/recently_played	Recently played history in binary format
SplashBoard/Snapshots/*	App-generated screenshots

**Table 10.16 – Common Spotify artifacts**

## Snapchat

The following table shows the most common artifacts for Snapchat:

Artifact	Description
Library/Preferences/com.toyopagroup.picaboo.plist	User preferences and application settings
Documents/user.plist	Property List that stores details regarding the logged-in user
Documents/chatConversationStore.plist	Property List containing chats
Documents/stories.plist	Property List that stores story data
Library/Caches/*	Cached media and API requests

**Table 10.17 – Common Snapchat artifacts**

## TikTok

The following table shows the most common artifacts for TikTok:

Artifact	Description
Library/Preferences/com.zhiliaoapp.musically.plist	User preferences and application settings
Documents/AwemeIM.db	SQLite database that stores TikTok contacts
Documents/Aweme.db	SQLite database that contains published TikTok videos
Library/ApplicationSupport/ChatFiles/<id>/db.sqlite	SQLite database that stores chats and messages
Library/Caches/*	Cached media and API requests

**Table 10.18 – Common TikTok artifacts**

## Code and Commands

Command 10.1:

```
SELECT
application underscore identifier underscore
tab.[application underscore identifier],
kvs.[value]
```

```
FROM kvs, key underscore tab, application underscore
identifier underscore tab

WHERE key underscore tab.[id] = '1'

AND kvs.[key] = key underscore tab.[id]

AND application underscore identifier underscore tab.[id] =
kvs.[application underscore identifier]

ORDER BY application underscore identifier underscore
tab.[id];
```

**Command 10.2:**

```
brew install libimobiledevice
```

**Command 10.3:**

```
iproxy 4242 44
```

**Command 10.4:**

```
ssh root@127.0.0.1 -p 4242
```

**Command 10.5:**

```
scp -P 4242 cda root@127.0.0.1:/usr/bin/
```

**Command 10.6:**

```
ls -la /usr/bin/
```

**Command 10.7:**

```
iPhone:~ root# cda instagram
[1] Instagram (com.burbn.instagram)

Bundle:
/private/var/containers/Bundle/Application/D054F8DC-95A4-
4489-BBBD-68F3E457A575

Data:
/private/var/mobile/Containers/Data/Application/2A2FEE52-
B59D-42F1-A810-333364E12525
```

**Command 10.8:**

```
scp -P 4242 fsmon root@127.0.0.1:/usr/bin/
```

## Links

- Download and install the `libimobiledevice` library from <https://libimobiledevice.org>
- The CDA tool can be downloaded from <https://github.com/ay-kay/cda>
- 64-bit ARM Binaries for CDA <https://github.com/tiepologian/iOS-Tools>
- `Fsmon` can be downloaded from GitHub at <https://github.com/nowsecure/fsmon>. Pre-built binaries for 64-bit ARM devices can also be downloaded from <https://github.com/tiepologian/iOS-Tools>.
- To install `mitmproxy`, go to <https://mitmproxy.org> and download the installer. If your workstation has `brew` installed, you can install the proxy by running the following command from your terminal:

```
brew install mitmproxy
```
- A complete tour of all Frida's features is beyond the scope of this book; you can get started with the tool by following the tutorials at <https://frida.re/docs/home> or by reading Alexander Fadeev's blog articles; for example, <https://fadeevab.com/quick-start-with-frida-to-reverse-engineer-any-ios-application/>.
- To learn about Meduza and download the tool, visit the project's page at <https://opensourcelibs.com/lib/meduza>.

# Chapter 11

## Images

The screenshot shows a terminal window titled "Toolkit.command". The title bar also includes "Elcomsoft iOS Forensic Toolkit 7.02" and "(c) 2011-2021 Elcomsoft Co. Ltd.". The main text area displays the following information:

```
Device connected: iPhone
Hardware model: N61AP
Serial number: F78PNPSKG5MT
OS version: 12.4.5
Device ID: 7cf85b3179a6c136ae723636e6467a27888ab928

Please select an action

Logical acquisition
I DEVICE INFO      - Get basic device information
R RECOVERY INFO   - Get information on device in DFU/Recovery mode
B BACKUP           - Create iTunes-style backup of the device
M MEDIA            - Copy media files from the device
S SHARED           - Copy shared files of the installed applications
L LOGS              - Copy crash logs

Jailbroken devices acquisition
D DISABLE LOCK     - Disable screen lock (until reboot)
K KEYCHAIN          - Decrypt device keychain
F FILE SYSTEM       - Acquire device file system (as TAR archive)

Acquisition agent (limited compatibility)
1 INSTALL           - Install acquisition agent on device
2 KEYCHAIN          - Decrypt device keychain
3 FILE SYSTEM       - Acquire device file system (as TAR archive)
4 FILE SYSTEM (USER) - Acquire user files only (as TAR archive)
5 UNINSTALL         - Uninstall acquisition agent from device

Legacy devices acquisition
A LEGACY            - Legacy devices acquisition (iPhone 4/5/5C)

X EXIT

>:
```

Figure 11.1 – Elcomsoft iOS Forensic Toolkit can acquire locked devices using pairing records

```
ElcomSoft — Toolkit.command — tee < Toolkit.command — 80x21
WARNING: Please, unlock the device and specify passcode (if needed). Otherwise,
press any key to proceed in a locked state, but be aware, that not all data may
be retrieved

You pressed a key - app will try to dump all available items
Overall dumped 3031 items of class 'genp'
Overall dumped 1 items of class 'inet'
Overall dumped 29 items of class 'cert'
Overall dumped 117 items of class 'keys'
Overall dumped 6 items of class 'idnt'

Cleaning up...
[INFO] Info: New connection...
[INFO] Device connected
[INFO] USBMuxConnectByPort OK
Warning: Permanently added '[localhost]:3022' (RSA) to the list of known hosts.

Done.

Press 'Enter' to continue
```

Figure 11.2 – Elcomsoft iOS Forensic Toolkit performing a BFU acquisition

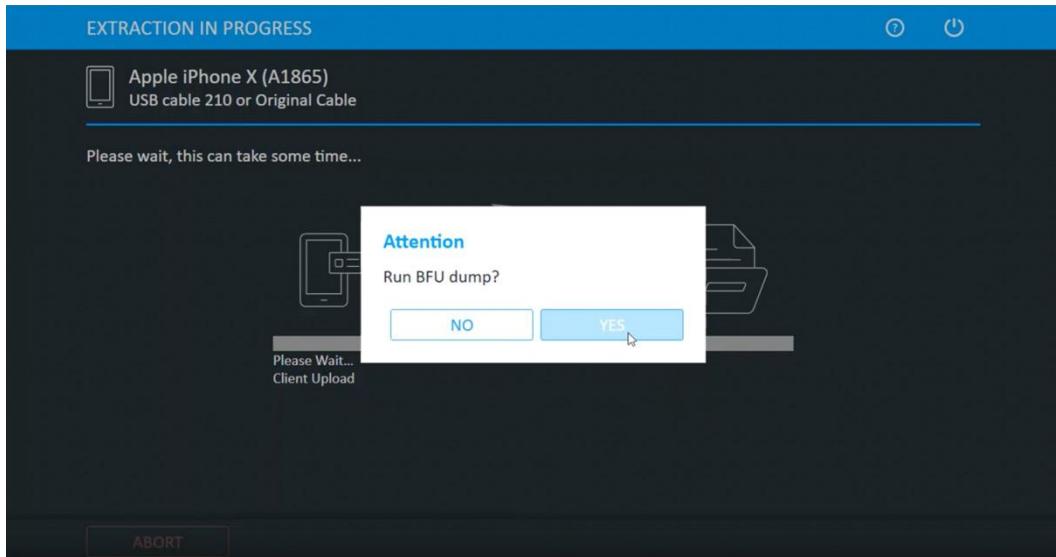
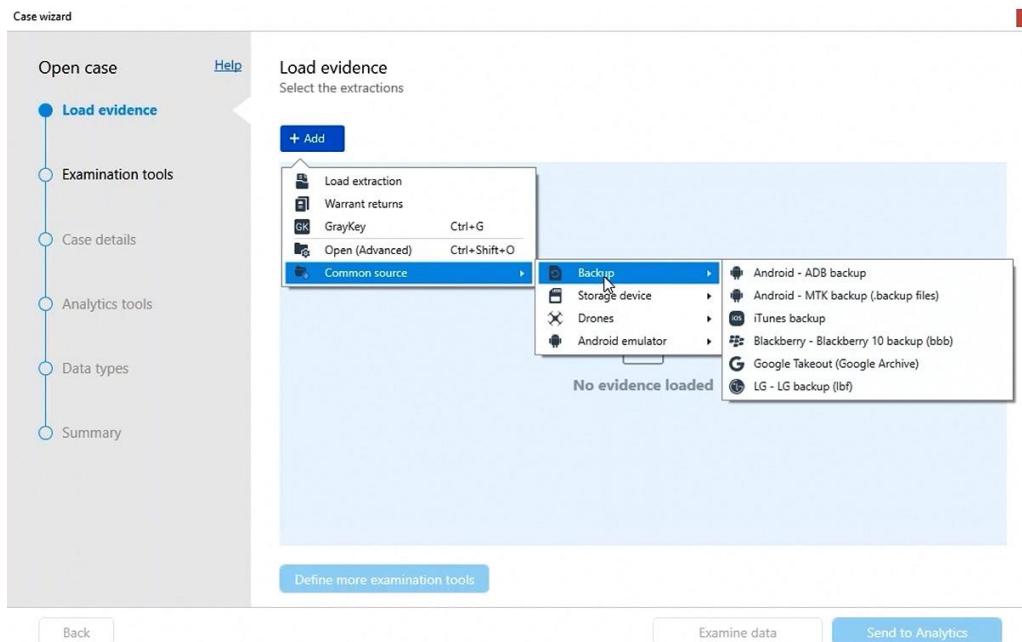


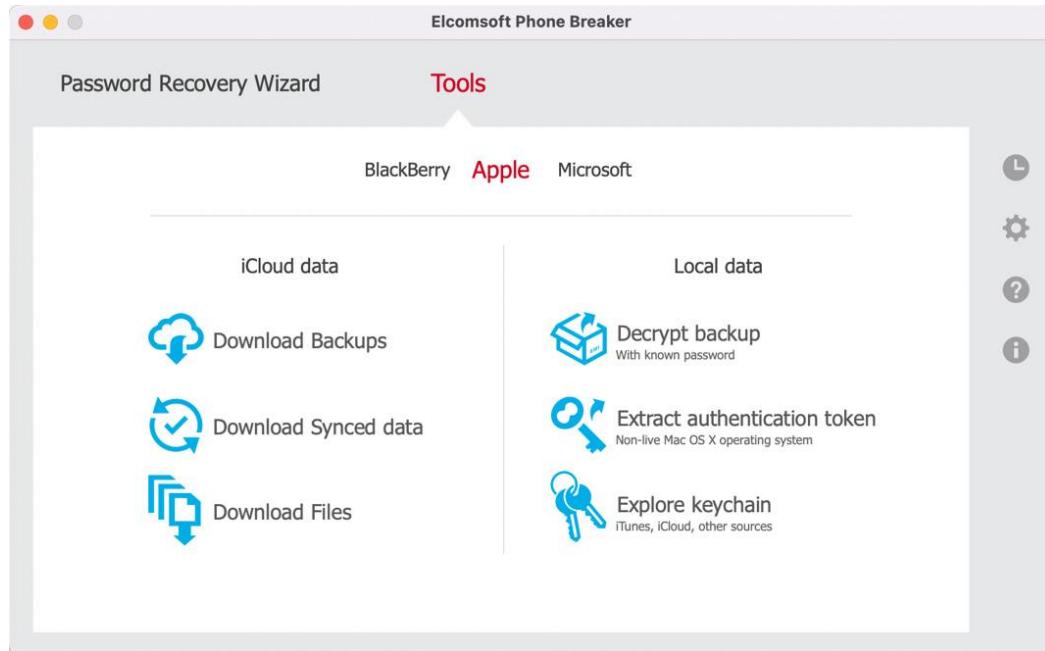
Figure 11.3 – Cellebrite UFED performing a BFU acquisition

Name	Date Modified	Size	Kind
> ea	Today at 14:59	--	Folder
> ee	Today at 14:59	--	Folder
> ef	Today at 14:59	--	Folder
> f0	Today at 14:59	--	Folder
> f1	Today at 14:59	--	Folder
> f2	Today at 14:59	--	Folder
> f3	Today at 14:59	--	Folder
> f4	Today at 14:59	--	Folder
> f5	Today at 14:59	--	Folder
> f6	Today at 14:59	--	Folder
> f7	Today at 14:59	--	Folder
> f8	Today at 14:59	--	Folder
> f9	Today at 14:59	--	Folder
> fa	Today at 14:59	--	Folder
> fb	Today at 14:59	--	Folder
> fc	Today at 14:59	--	Folder
> fd	Today at 14:59	--	Folder
> fe	Today at 14:59	--	Folder
> ff	Today at 14:59	--	Folder
Info.plist	Today at 15:00	676 KB	property list
Manifest.db	Today at 14:59	40,4 MB	Document
Manifest.plist	Today at 14:59	104 KB	property list
Status.plist	Today at 14:59	189 bytes	property list

Figure 11.4 – File structure of an iTunes backup



**Figure 11.5 – Loading an iTunes backup into Cellebrite Physical Analyzer**



**Figure 11.6 – Elcomsoft Phone Breaker home screen**

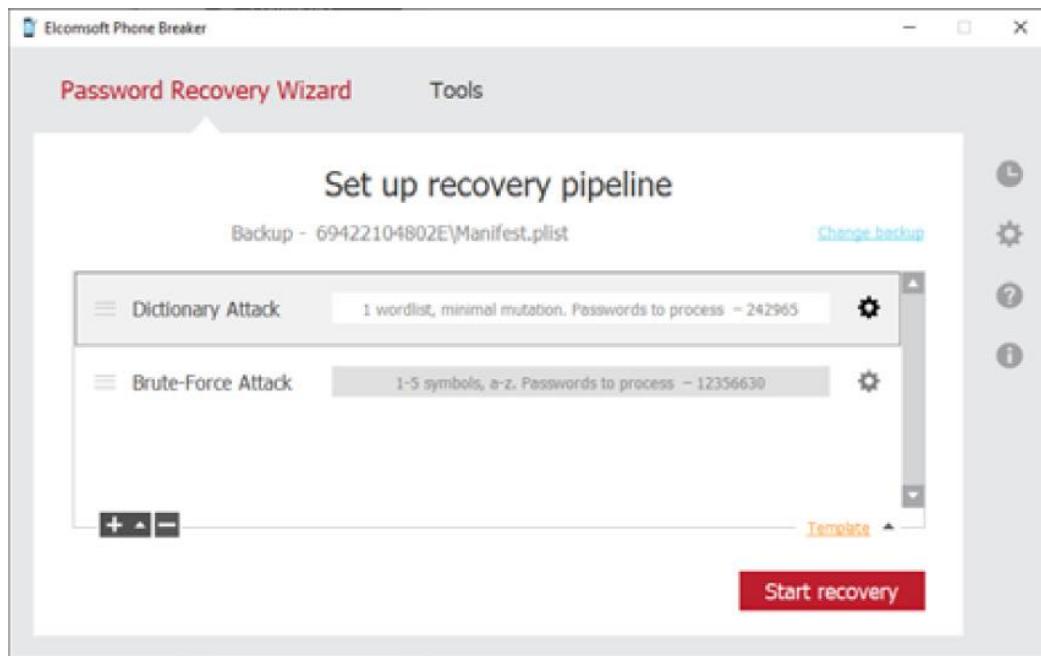
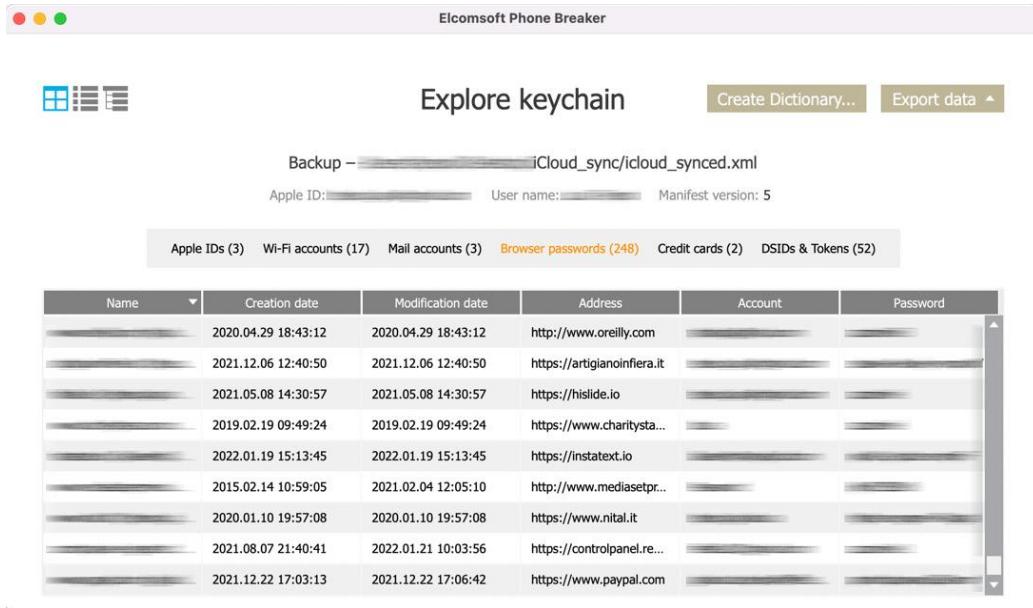


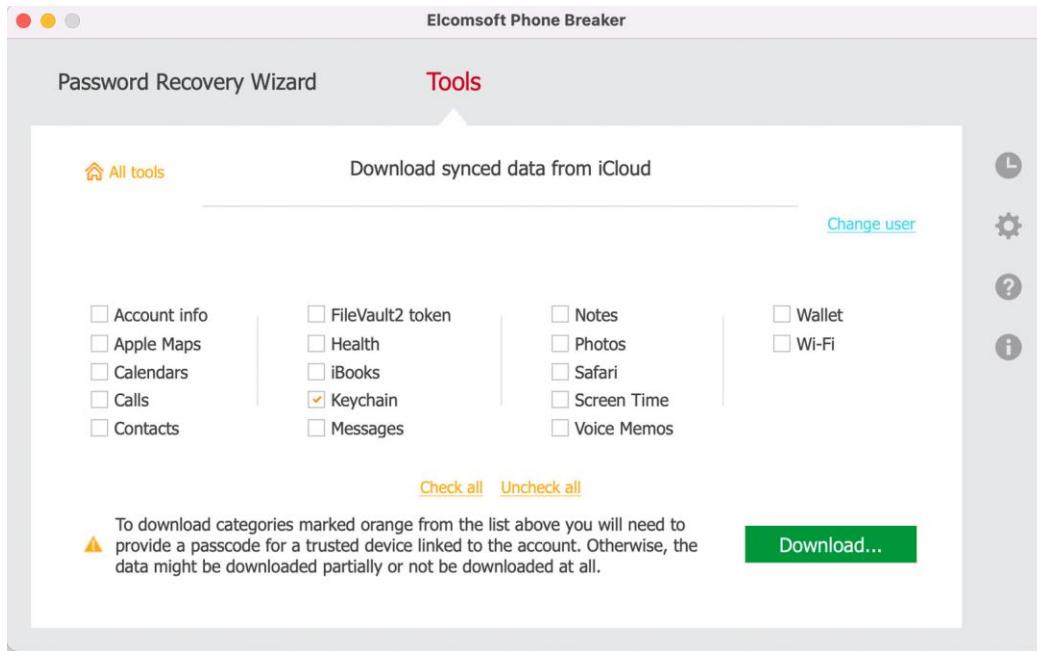
Figure 11.7 – Set up a dictionary attack or a brute-force attack



Figure 11.8 – Apps using iCloud from the device settings



**Figure 11.9 – Analyzing iCloud Keychain in Elcomsoft Phone Breaker**



**Figure 11.10 – Downloading iCloud synced data with Elcomsoft Phone Breaker**

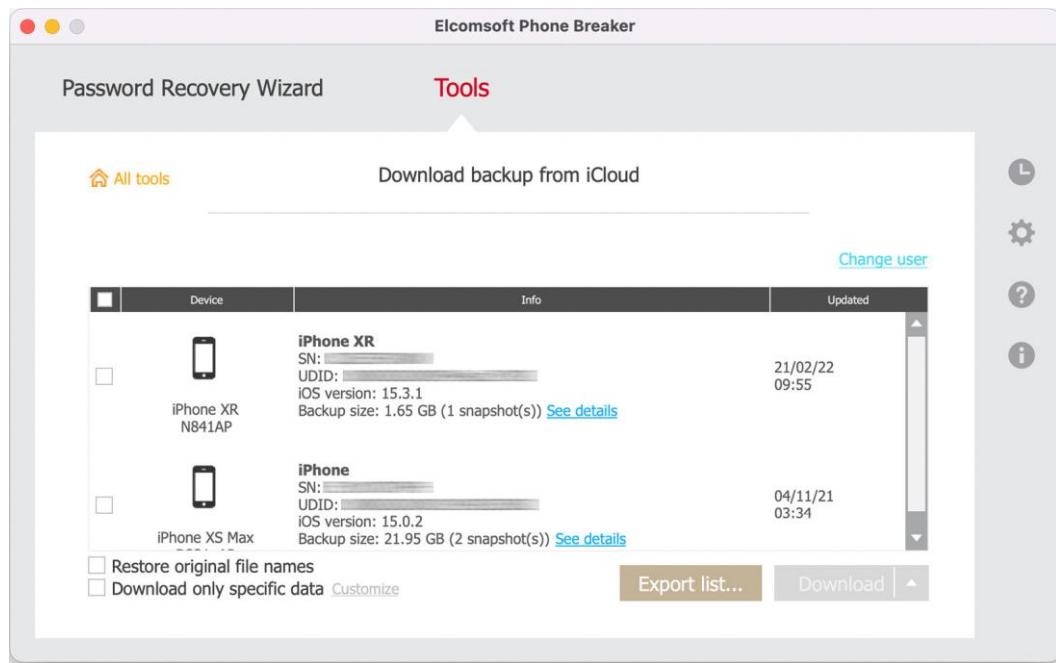


Figure 11.11 – Downloading iCloud backups using Elcomsoft Phone Breaker

## Tables

Artifacts
/private/var/mobile/Library/Preferences/*
/private/var/preferences/SystemConfiguration/*
/private/var/root/Library/Preferences/*
/private/var/mobile/Library/Accounts/Accounts3.sqlite
/private/var/mobile/Library/DataAccess/*
/private/installld/Library/Logs/MobileInstallation/*
/private/var/mobile/Library/SpringBoard/*
/private/var/mobile/Library/CallHistoryDB/CallHistoryTemp.storeddata
/private/var/mobile/Library/Preferences/com.apple.*
/private/var/mobile/Library/SMS/sms-temp.db
/private/var/mobile/Library/Preferences/com.apple.preferences.network.plist
/private/var/wireless/Library/Databases/CellularUsage.db
/private/var/root/Library/Caches/locationd/consolidated.db

**Table 11.1 – Common artifacts found in BFU acquisition**

# Chapter 12

## Images

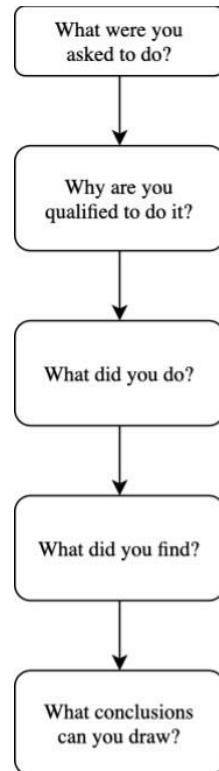


Figure 12.1 – The logical steps of a forensic report

## Extraction Summary

⊖ Extractions: 1



Legacy Apple IPHONE\_BACKUP

Extraction start date/time

Extraction end date/time

### Image Hashes

⚠ Hashes have been calculated for this extraction, but no reference data is available.

[View details](#)

## Device Info

[Generate preliminary device report](#)

...

AirDrop ID	[REDACTED]	<a href="#">com.apple.sharingd.plist : 0x418</a>
Apple ID	[REDACTED]	<a href="#">Accounts3.sqlite : 0x23F57</a>
Detected Phone Model	iPhone XR	<a href="#">External Enrichment</a>
iCloud account present	True	<a href="#">Accounts3.sqlite : 0x23155</a>
Last Cloud Backup Date		<a href="#">com.apple.mobile.ldbackup.plist : 0x...</a>
Model number	N841AP	<a href="#">preferences.plist : 0x11D9</a>
Time Zone	(UTC+01:00) Rome (Europe)	<a href="#">com.apple.AppStore.plist : 0x313</a>
ICCID	[REDACTED]	<a href="#">com.apple.commcenter.plist : 0x51C</a>
Last user ICCID	[REDACTED]	<a href="#">CellularUsage.db : 0x6FD7</a>
Last used MSISDN	[REDACTED]	<a href="#">CellularUsage.db : 0x6FEB</a>
MSISDN	[REDACTED]	<a href="#">com.apple.commcenter.plist : 0x4F0</a>
<b>iPhone XR</b>		
Backup password	[REDACTED]	<a href="#">Info.plist : 0xBB73E</a>
Detected Phone Model Identifier	iPhone11,8	<a href="#">Manifest.plist : 0x64D</a>
Is encrypted	True	

Figure 12.2 – A preliminary device report generated from Extraction Summary



Cellebrite  
www.cellebrite.com

### Preliminary Device Report - Apple iOS iTunes (Backup)

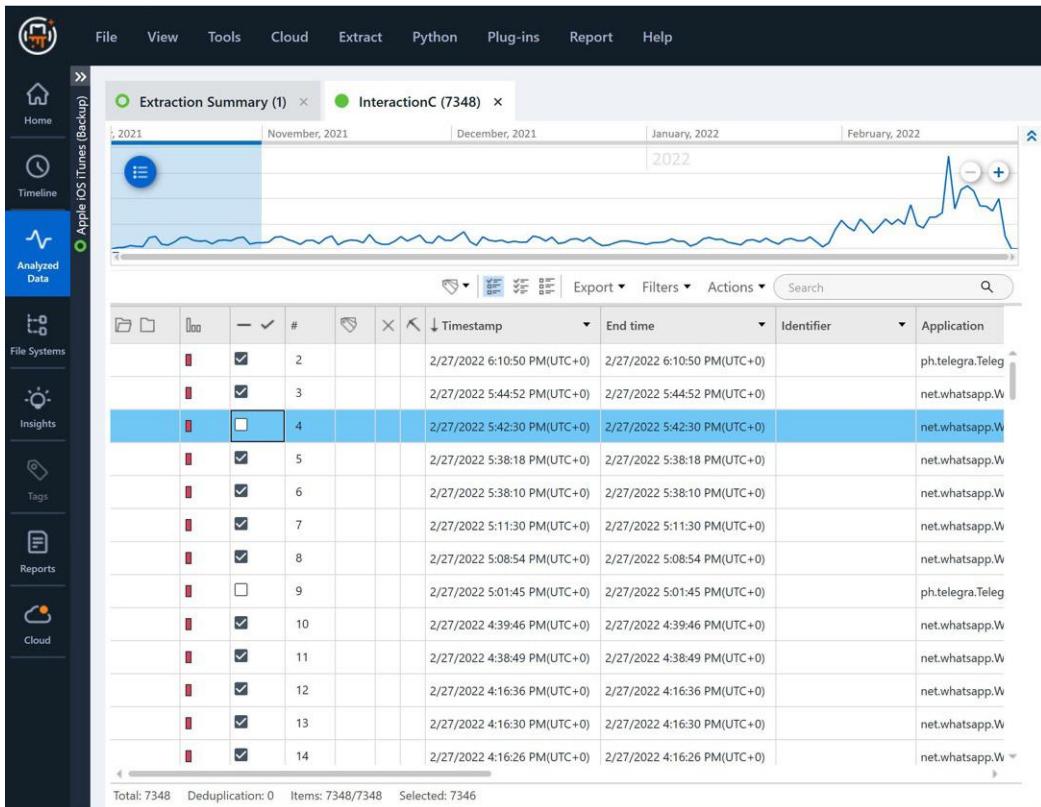
#### Device Information

Name	Value
Legacy	
iPhone XR	
MSISDN	[REDACTED]
Backup password	[REDACTED]
OS Version	15.3.1
Unique ID	00008020-000954DA3C79002E
Detected Phone Model Identifier	iPhone11,8
Serial	[REDACTED]
Is encrypted	True
Owner Name	iPhone XR
ICCID	[REDACTED]
IMEI	[REDACTED]
Phone Settings	
Message Retention Duration	Forever
Location Services Enabled	True
Find my iPhone enabled	True
Apple ID	[REDACTED]
iCloud account present	True
Model number	N841AP
Last user ICCID	[REDACTED]
Last used MSISDN	[REDACTED]
AirDrop ID	[REDACTED]
Last Cloud Backup Date	
Time Zone	(UTC+01:00) Rome (Europe)
ICCID	[REDACTED]
MSISDN	[REDACTED]
Detected Phone Model	iPhone XR
Tethering	
Last Hotspot Activity	2/27/2022 3:04:50 PM(UTC+0)

#### User Accounts (22)

#	Source	Account Name	User name	Service Type	Creation time	Entries
1			[REDACTED]	6DE9BF4F-3851-426C-9A1B-EF52BBFE9881	11/6/2021 12:06:09 PM(UTC+0)	Unknown: Account Description IMAPMail
2			[REDACTED]	85BDDDF2-0CBC-4816-A8FB-641B96C0F253	11/6/2021 12:06:13 PM(UTC+0)	Unknown: Account Description Device Locator
3			[REDACTED]	D54A7D3C-C1D3-47B2-8654-54A56472136C	11/6/2021 12:06:14 PM(UTC+0)	Unknown: Account Description Find My Friends
4			[REDACTED]	A78F32F8-204B-488B-B08A-83E1D4CBB24D	11/6/2021 12:06:16 PM(UTC+0)	Unknown: Account Description iTunes Store
5			[REDACTED]	7482D0CF-21B1-4364-A123-59B088C5F3D9	11/6/2021 12:13:33 PM(UTC+0)	Unknown: Account Description iTunes Store (Sandbox)
6			[REDACTED]	A95E99D6-4D90-4B86-95F3-9AEF0AE27DE5	11/6/2021 12:22:03 PM(UTC+0)	Unknown: Account Description Gmail
7			[REDACTED]	91916FC8-758F-493E-8120-FB4C9C22944D	11/8/2021 1:04:22 PM(UTC+0)	Unknown: Account Description Gmail
8			[REDACTED]	03C2C429-2110-4BFA-B3C4-D77117447E29		Unknown: Account Description iTunes Store
9			[REDACTED]	F64E6AC0-E358-443B-B4E4-416C8E348B3C	11/6/2021 12:05:30 PM(UTC+0)	Unknown: Account Description IDMS
10			[REDACTED]	B16C129F-9256-4A70-B52D-DEEFC72B71E1	11/6/2021 12:05:30 PM(UTC+0)	Unknown: Account Description Apple ID
11			[REDACTED]	66E62B8C-F745-4E5F-B53D-24F813A35442	11/6/2021 12:05:38 PM(UTC+0)	Unknown: Account Description Game Center
12			[REDACTED]	CB10DC6C-45F7-401E-865C-5725791F5843	11/6/2021 12:05:38 PM(UTC+0)	Unknown: Account Description Messages
13			[REDACTED]	BBD32FAF-A172-4067-A05A-F54E728DE6B6	11/6/2021 12:05:38 PM(UTC+0)	Unknown: Account Description CloudKit

**Figure 12.3 – An example of a preliminary device report**



**Figure 12.4 – An artifact will be included in the report if the checkbox is enabled**

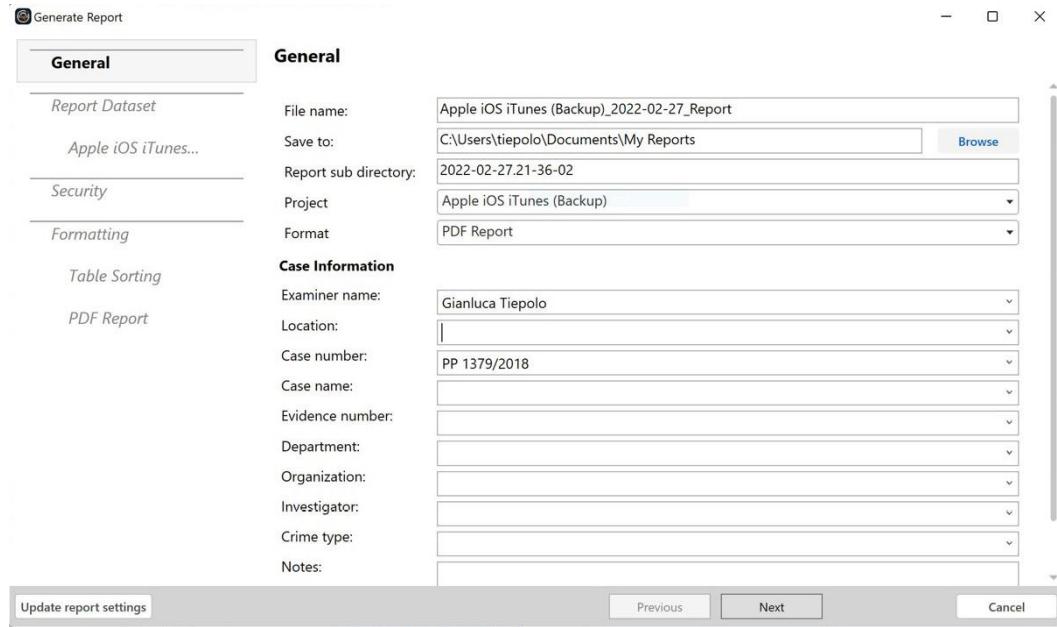


Figure 12.5 – The Generate Report window

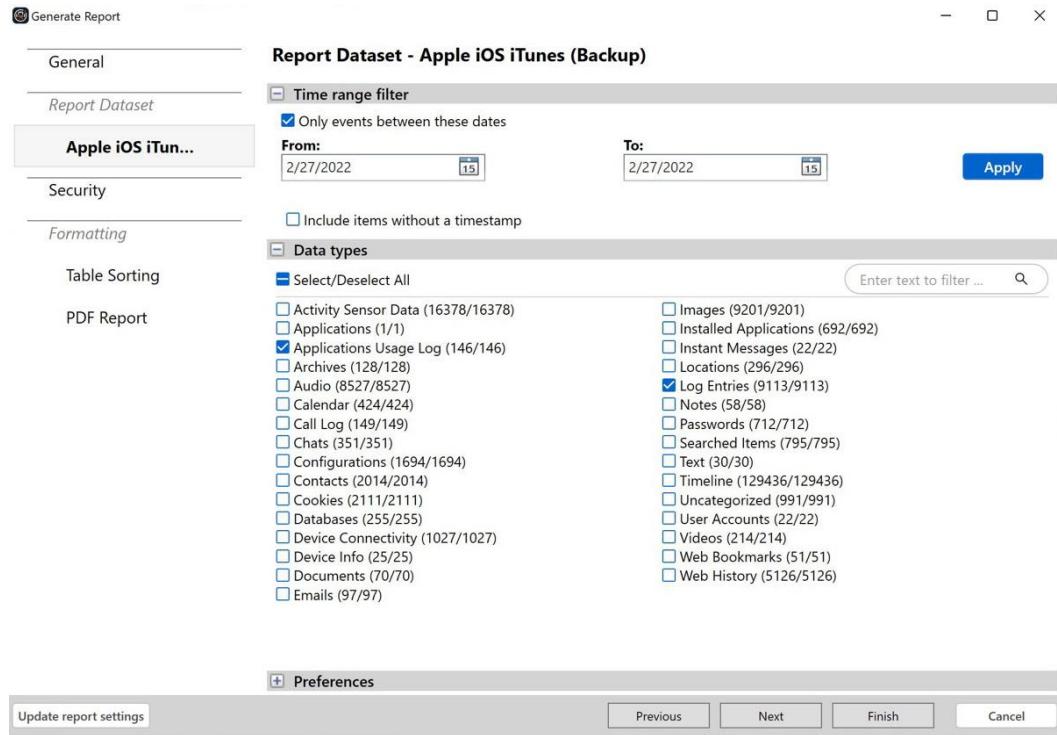


Figure 12.6 – The Report Dataset window

Generate Report

General

Report Dataset

**Apple iOS iTun...**

Security

Formatting

Table Sorting

PDF Report

Report Dataset - Apple iOS iTunes (Backup)

Time range filter

Only events between these dates

From: 2/27/2022

To: 2/27/2022

Include items without a timestamp

**[+] Data types**

**[+] Preferences**

Tags table (0/0)

Tags only (0/0)

Select tags 0/0

Calculate SHA-2 (256 bit) hash

Calculate MD5 (128 bit) hash

Include translations

Include known files

Include Malware scanner results

Include Hash set results

Redact all attachments

Redact image thumbnails

Include merged items (analyzed data)

Include merged items (data files)

Include conversation bubbles

Include source info indication

Include enrichments

Hide extraction source indication

Include account package

Include Activity sensor data samples

Update report settings Previous Next Finish Cancel

Figure 12.7 – The Preferences tab



 **Cellebrite**  
www.cellebrite.com

Extraction Report - Apple iOS iTunes (Backup)

---

**Summary**

Cellbrite Physical Analyzer version	7.53
Report creation time	2/27/2022 9:39:23 PM +01:00
Time zone settings (UTC)	Original UTC value
Examiner name	Gianluca Tiepolo
Case number	PP 1379/2018

---

**Source Extraction**

Legacy	
Selected manufacturer	Apple
Selected device name	IPHONE_BACKUP

---

**Image Hash Details (1)**

<span style="color: yellow;">⚠</span> Hashes have been calculated for this extraction, but no reference data is available.		
#	Name	Info
1	Folder	Path: 00008020-000954DA3C79002E Size (bytes): 4024701501 SHA256: B293C94E273BC3FBDD88E277017805724B6FB480D0BC0AAEF7ED7E575B2A43 26

---

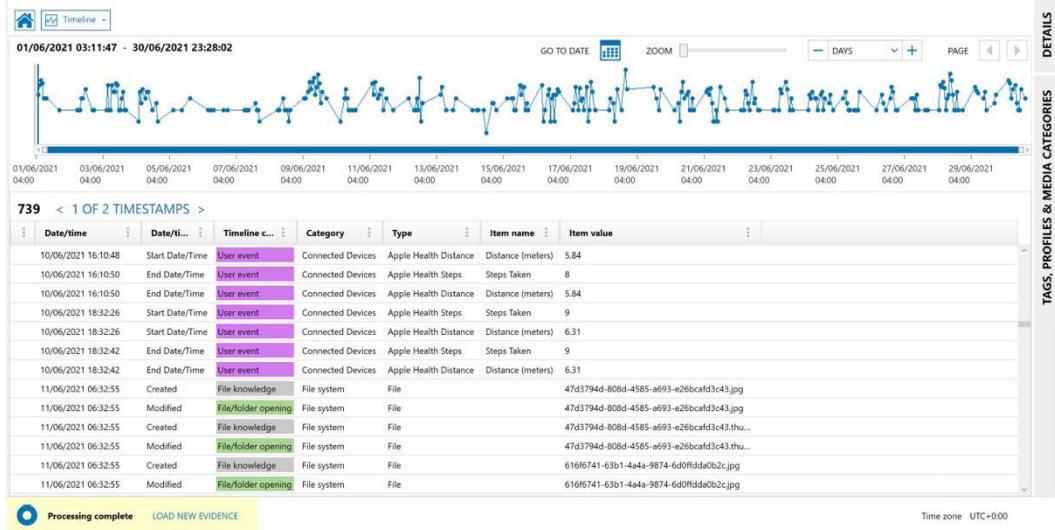
**Plugins**

#	Name	Author	Version
1	PreProject	Cellebrite	2.0
2	iPhone Backup Parser <small>Parses all iPhone Backup/Logical/FS dumps, including decryption and/or FileSystem creation when necessary</small>	Cellebrite	2.0
3	ContactsCrossReference <small>Cross references the phone numbers in a device's contacts with the numbers in SMS messages and Calls. Will fill in the Name field of calls and SMS if there's a match.</small>	Cellebrite	2.0
4	ProjectProcessorFinisher	Cellebrite	2.0
5	PostProject	Cellebrite	2.0

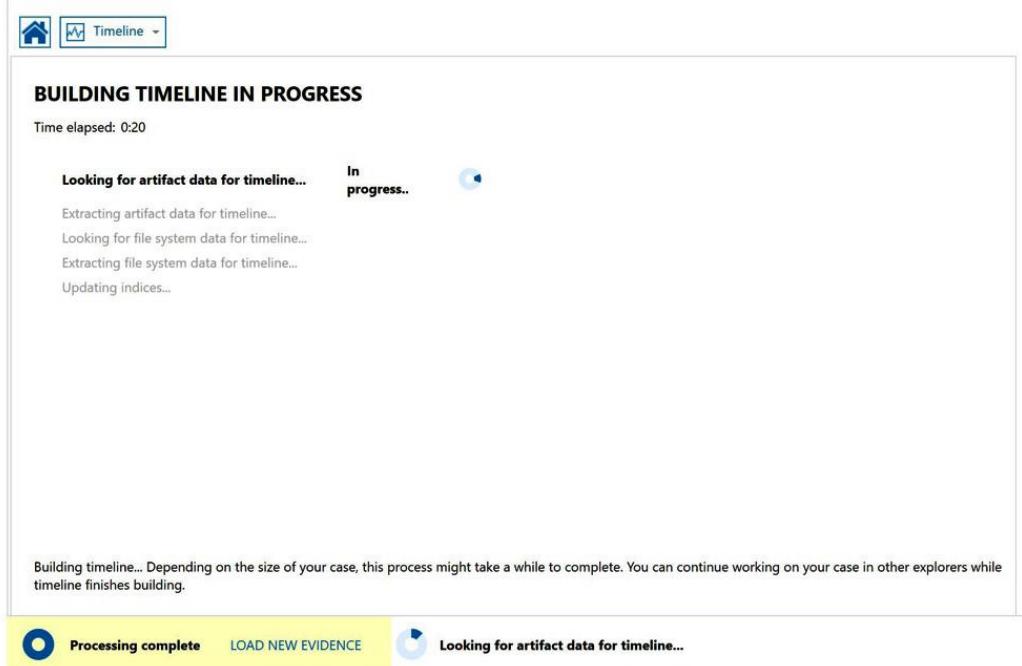
**Figure 12.8 – The Extraction Report Summary**

118		ph.telegra.Telegraph		outgoing message	2/26/2022 10:29:50 PM(UTC+0) <b>End time:</b> 2/26/2022 10:29:50 PM(UTC+0)	PID: 0 TID: 0 Effective UID: 0	Source: InteractionC	
119		ph.telegra.Telegraph		outgoing message	2/26/2022 10:29:37 PM(UTC+0) <b>End time:</b> 2/26/2022 10:29:37 PM(UTC+0)	PID: 0 TID: 0 Effective UID: 0	Source: InteractionC	
120		ph.telegra.Telegraph		incoming message	2/26/2022 10:29:34 PM(UTC+0) <b>End time:</b> 2/26/2022 10:29:34 PM(UTC+0)	PID: 0 TID: 0 Effective UID: 0	Source: InteractionC	
121		ph.telegra.Telegraph		incoming message	2/26/2022 10:29:32 PM(UTC+0) <b>End time:</b> 2/26/2022 10:29:32 PM(UTC+0)	PID: 0 TID: 0 Effective UID: 0	Source: InteractionC	
122		ph.telegra.Telegraph		incoming message	2/26/2022 10:29:29 PM(UTC+0) <b>End time:</b> 2/26/2022 10:29:29 PM(UTC+0)	PID: 0 TID: 0 Effective UID: 0	Source: InteractionC	
123		ph.telegra.Telegraph		outgoing message	2/26/2022 10:28:57 PM(UTC+0) <b>End time:</b> 2/26/2022 10:28:57 PM(UTC+0)	PID: 0 TID: 0 Effective UID: 0	Source: InteractionC	
124		ph.telegra.Telegraph		outgoing message	2/26/2022 10:28:53 PM(UTC+0) <b>End time:</b> 2/26/2022 10:28:53 PM(UTC+0)	PID: 0 TID: 0 Effective UID: 0	Source: InteractionC	
125		ph.telegra.Telegraph		outgoing message	2/26/2022 10:28:45 PM(UTC+0) <b>End time:</b> 2/26/2022 10:28:45 PM(UTC+0)	PID: 0 TID: 0 Effective UID: 0	Source: InteractionC	
126		ph.telegra.Telegraph		outgoing message	2/26/2022 10:28:39 PM(UTC+0) <b>End time:</b> 2/26/2022 10:28:39 PM(UTC+0)	PID: 0 TID: 0 Effective UID: 0	Source: InteractionC	
127		ph.telegra.Telegraph		incoming message	2/26/2022 10:28:27 PM(UTC+0) <b>End time:</b> 2/26/2022 10:28:27 PM(UTC+0)	PID: 0 TID: 0 Effective UID: 0	Source: InteractionC	
128		ph.telegra.Telegraph		incoming message	2/26/2022 10:28:23 PM(UTC+0) <b>End time:</b> 2/26/2022 10:28:23 PM(UTC+0)	PID: 0 TID: 0 Effective UID: 0	Source: InteractionC	
129		ph.telegra.Telegraph		incoming message	2/26/2022 10:28:20 PM(UTC+0) <b>End time:</b> 2/26/2022 10:28:20 PM(UTC+0)	PID: 0 TID: 0 Effective UID: 0	Source: InteractionC	
130		ph.telegra.Telegraph		outgoing message	2/26/2022 10:27:56 PM(UTC+0) <b>End time:</b> 2/26/2022 10:27:56 PM(UTC+0)	PID: 0 TID: 0 Effective UID: 0	Source: InteractionC	

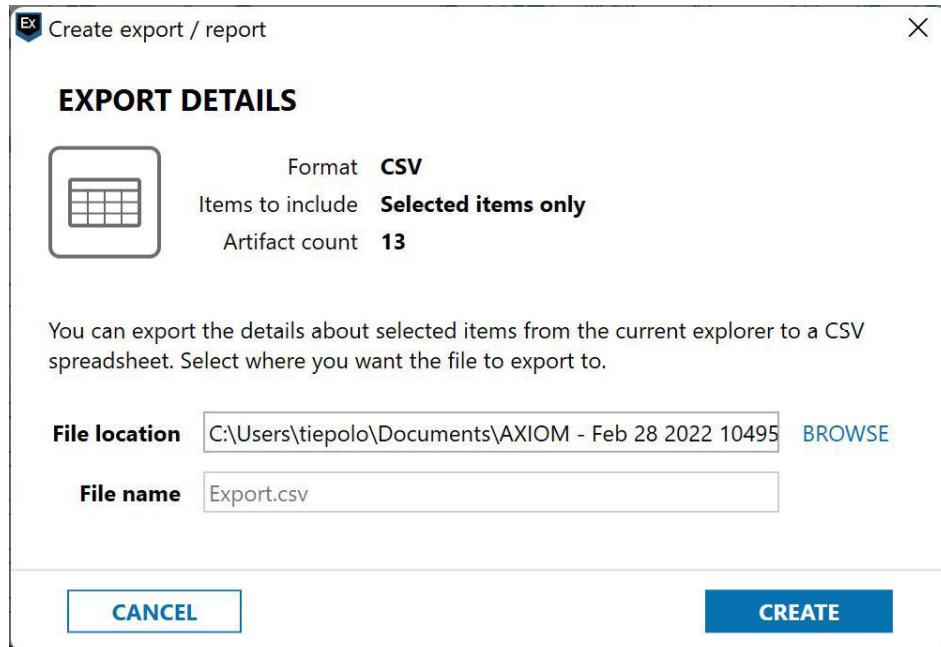
**Figure 12.9 – The Extraction Report Evidence list**



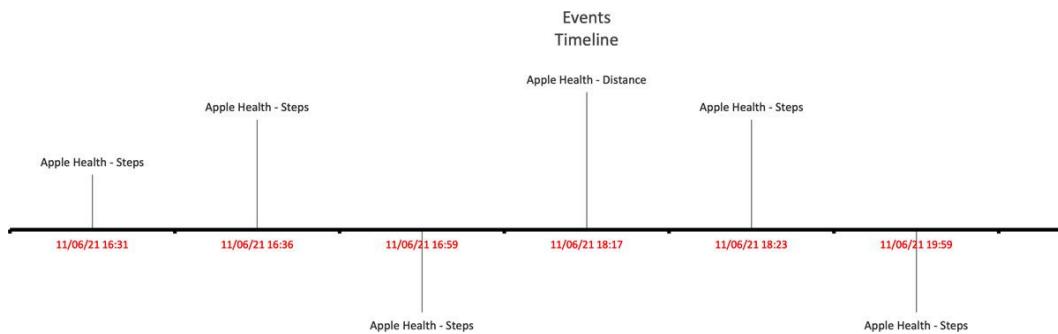
**Figure 12.10 – A timeline displayed in Magnet AXIOM**



**Figure 12.11 – Building a timeline in Magnet AXIOM**



**Figure 12.12 – Exporting the timeline to a CSV file**



**Figure 12.13 – A timeline created in Microsoft Excel**