

# **Cellebrite and Other Digital Investigative Techniques**





# Edgar Fritz

- Bachelor's degree in Applied Mathematics
- FBI for 20 years
  - Surveillance Specialist
  - Analyst for violent crime squad
  - Field Photographer
    - Member of FAVP
    - Member of ERT
- Master's in Digital Media Forensics
- Digital Forensic Examiner for 3 years



# So, what IS Digital Forensics?

"Digital Forensics is a branch of Forensic Science that focuses on identifying, acquiring, imaging, processing, analyzing, preserving, and reporting on data stored electronically"

# Why acquire a phone?

- Beyond call detail records
- Associated applications
  - Communications
  - Images/Videos
  - Location related
  - Databases
- Certain data may reside ONLY on devices
  - Text messages
  - Detailed system data or health-related data
  - Device event
  - Screen orientation





# Cell Phones....Aren't they all the same?



# How do you “image” a phone?

- Special hardware and software required
- Technical skills and certification
- Not like imaging a computer, where we remove the hard drive
- Different level of extractions

# What is to preserve a phone?

- So, before you say:
  - “We’ve imaged everything”
  - “We downloaded the phone, so we’ve got it”
  - “Give me everything”
- ***Understand the type of extraction (or extractions) you have, and the limitations***

# Phone memory

- Solid state or “flash” memory chips
- No spinning HD inside phones
- Important to understand concepts:
  - “Wear leveling”
  - “Garbage collection”
- Phone data is 1) fragmented, but 2) efficient
  - Large deleted files typically disposed of quickly
  - Smaller deleted files and fragments, however, may be recoverable
  - Data stored in databases

# Phone memory

- Can't fully image phone without **writing** to flash memory
  - Using phone's own operating system
  - Using "boot loader" added to system by extraction device
    - Deleted upon completion

What kind of  
extractions  
exist?

**Manual**

**Logical**

**File System**

**Advanced Logical**

**Full File System**

**Physical**

**Chip-Off**

**Hex Dumping/JTAG**

**Micro-Read**



# Manual

---

Basic extraction

---

Copying files from the device to a computer

---

Only access to user data

---

Process changes metadata

---

Cannot recover deleted data

# Manual

- **Manual** is the most basic
- Can be as simple as taking pictures of the phone screen
- Doesn't include any deleted files or unused/unallocated memory space

# Logical

---

Communicating with device operating system using API (Application Programming Interface)

---

Call logs/Text messages

---

Application data

---

Selective process

---

Cannot recover deleted data

---

# Logical Extraction

- **Logical extraction** is an extraction of the then-active files and file system/databases
- Doesn't include many deleted files or unused/unallocated memory space
  - **Unless** small/stored in SQLite databases
  - SMS messages, contacts, notes files, call records

# File System

---

Similar to Logical but doesn't require API

---

Direct access to internal memory

---

Database and System files

---

Web browsing/app usage

---

Can recover deleted data

---

# File System

- **File System** is an extraction used to target specific types of data, such as documents, email messages, or photos, rather than the entire contents of the device's storage
- Doesn't include many deleted files or unused/unallocated memory space



# Advanced Logical

---

Combines both the Logical and File System extractions

---

Call logs/Text messages

---

Application Data

---

Not a selective process on iPhone

---

Cannot recover deleted data

---

# Advanced Logical

- **Advanced Logical** is an extraction of the then-active files and file system/databases
- Process gathers all data on iPhones
- Can be selective on Androids

## Full File System

---

Complete copy of file system

---

Requires additional Hardware

---

Database and System files

---

Third party applications

---

Can recover deleted data

---

# Full File System

- **Full File System** is an extraction that goes beyond the user data
- Can include some deleted files
- Third Party applications
- Email

# Physical

---

Recover hidden or deleted information

---

Bit-for-bit replica of flash memory

---

Can bypass system locks and passcodes

---

Does not leave a trace of being used

---

Can recover deleted data

---

# Physical Extractions

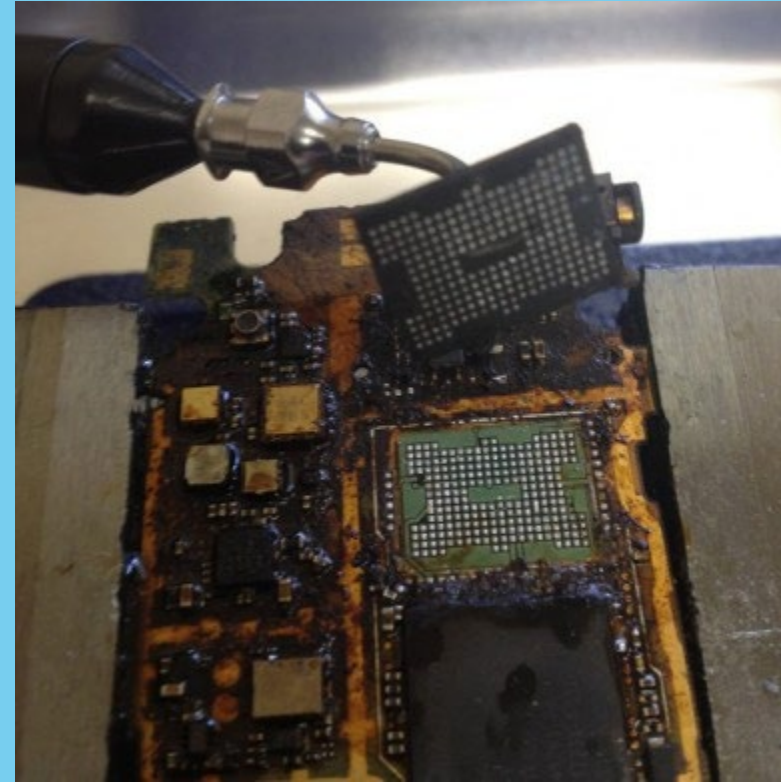
- **Physical extraction** is a capture of ALL 1's and 0's on hard disk or phone – the “binary” file
  - *Can* recover deleted data
  - Potentially other items not retrievable by logical extraction scripts



# What if Phone is Damaged/Won't Power On?

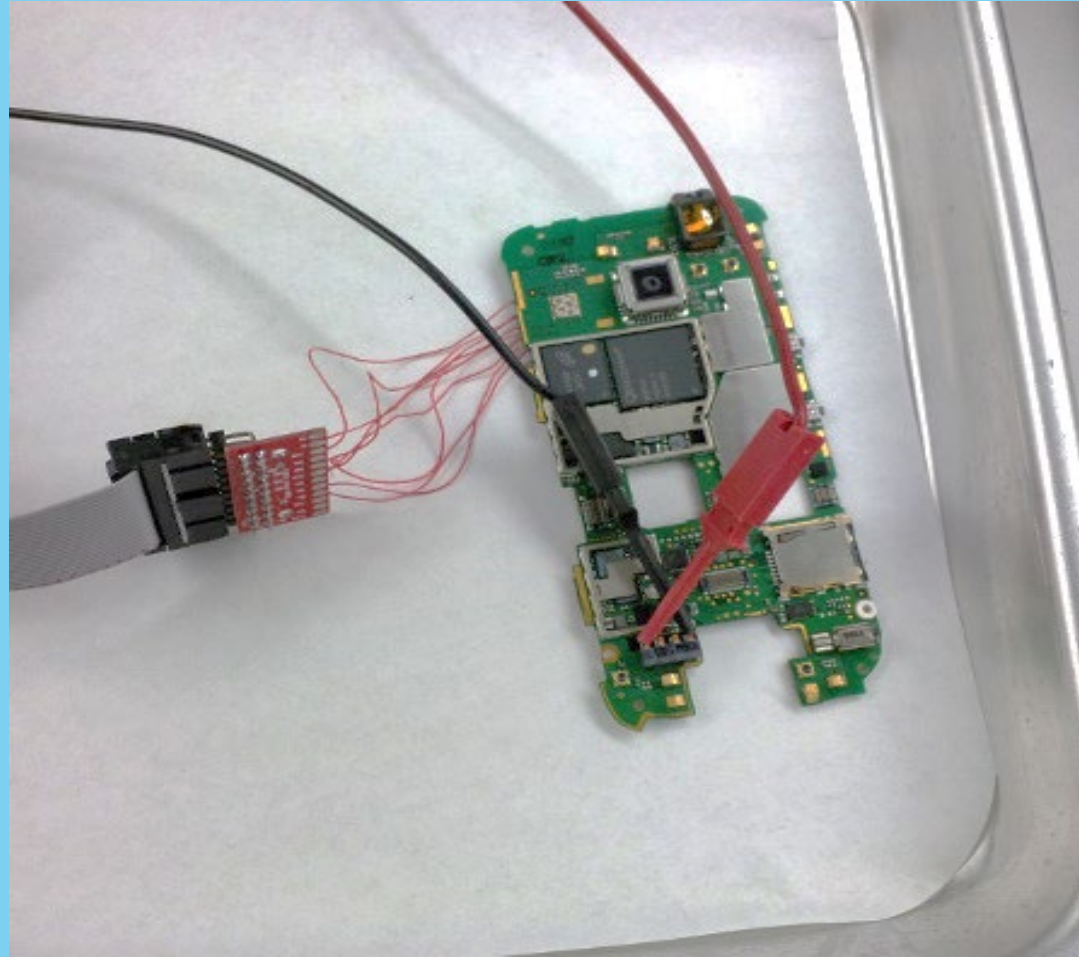
- Extract Binary File from Flash Chip
- Via the circuit board, a "JTAG" extraction
- "Chip-off" – physically remove chip from circuit board and read binary file
- Which can then be ingested into forensic software such as Cellebrite for processing
- Doesn't work on devices with default encryption

# CHIP-OFF



- Technique where the flash memory chip is physically removed from the device's circuit board to extract data

# JTAG



- Technique involves connecting to the phone's Test Access Ports (TAPs) (JTAG port) and using specialized software to transfer raw data from the memory chips.

# MICRO-READ



- Technique involves physically examining the memory chip using an electron microscope to read the data stored on it.

# Why not Physical every time?

- iPhone (4s and above) full-disk encryption
  - **Apple's chips encrypt unallocated space on a phone**
  - So when you delete a file/text, the area occupied by that file is encrypted and rendered unreadable
- Cannot access data without passcode or decryption key
- Same on Samsung Galaxy S6, Note 5 and newer
- Jailbreak iPhone is not common
- Rooted Android is not common

# What can be recovered?

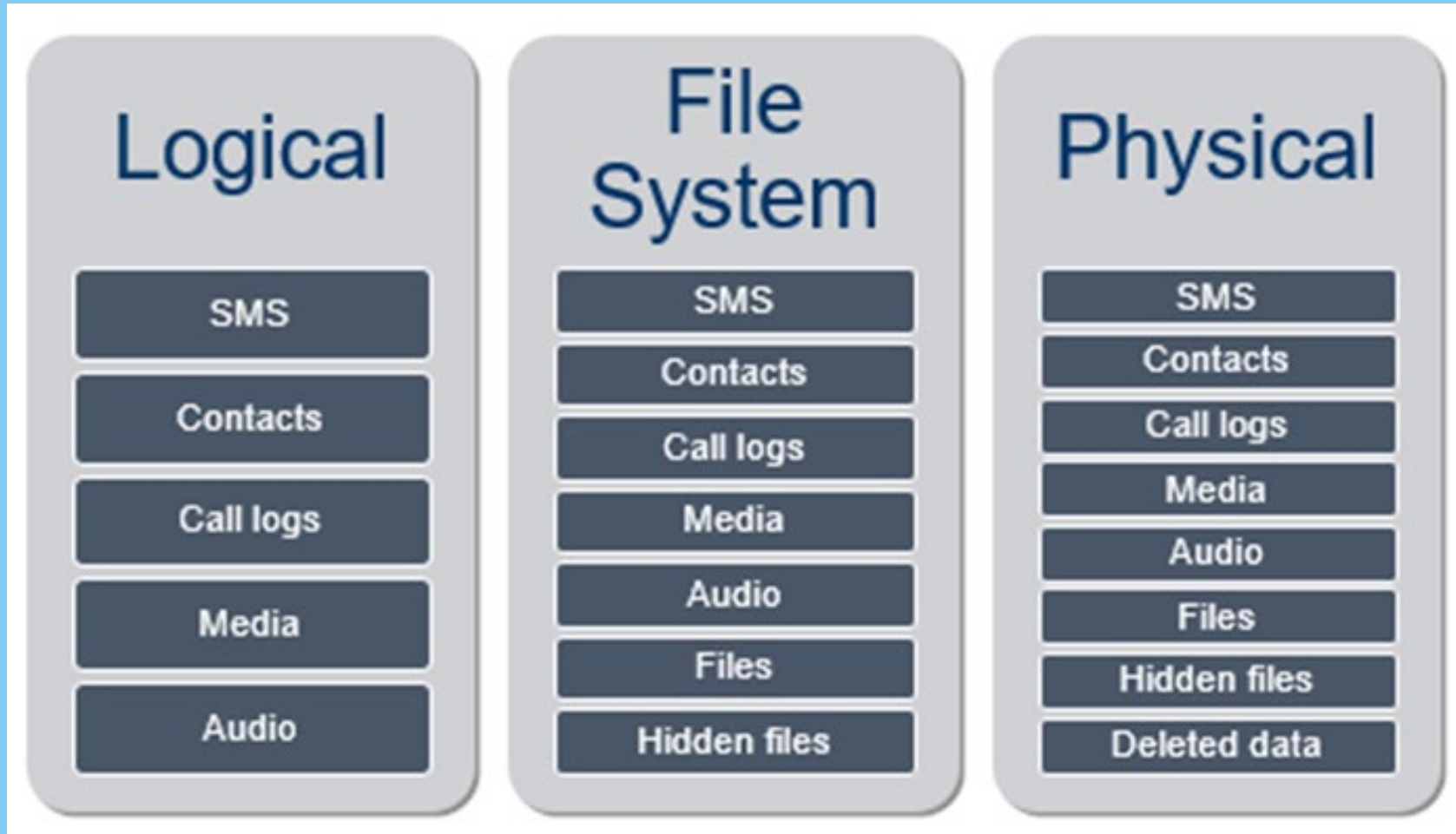
- Call logs (incoming, outgoing, missed)
- Pictures (including location)
- Texts/iMessages/"Chats"
- E-mail
- Browsing History
- GPS/cell site data
- Certain app data
- Malware scans/analysis
- Databases



# Cellebrite Support Matrix

Search		Device Vendor		Marketing Name		Model			
<input type="text" value="Search"/>		<input type="text" value="Search or choose an option"/>		<input type="text" value="Search or choose an option"/>		<input type="text" value="Search or choose an option"/>		<button>Expand</button>	
Device Vendor	Marketing Name	Device Model	Chipset	Device OS Version	Latest Security Patch Level	Extraction Method	Last Reported Date	Pre Ver	
Samsung	Galaxy S23 Ultra	SM-S9180	KALAMA	N/A		Full file system	2025-04-14	7.6i	
Samsung	Galaxy S9	SM-G960U1	SDM845	10	2022-03-01	Full file system	2025-04-14	7.6i	
Samsung	Galaxy A12	SM-A125U	MT6765V/CA	12	2023-07-01	Full file system	2025-04-14	7.6i	
Samsung	Galaxy A13	SM-A135M	EXYNOS850	14.0		Full file system	2025-04-14	10.0	
Apple	N/A	N104AP	N/A	16.1.2		iOS_Full_Filesystem	2025-04-14	7.6i	
Samsung	Galaxy S20+ 5G	SM-G986U	SM8250	13		Full file system	2025-04-14	7.7i	
Samsung	Galaxy S24	SM-S921B	ERD9945	N/A		Full file system	2025-04-14	7.7i	
Samsung	N/A	SM-S135DL	MT6765V/CB	N/A		Full file system	2025-04-14	7.7	
Apple	N/A	D53gAP	N/A	17.4.1		iOS_Full_Filesystem	2025-04-14	7.7	
Apple	N/A	D73AP	N/A	17.6.1 (21G93)		iOS_Full_Filesystem	2025-04-14	10.0	

# What do we get with each type of extractions?

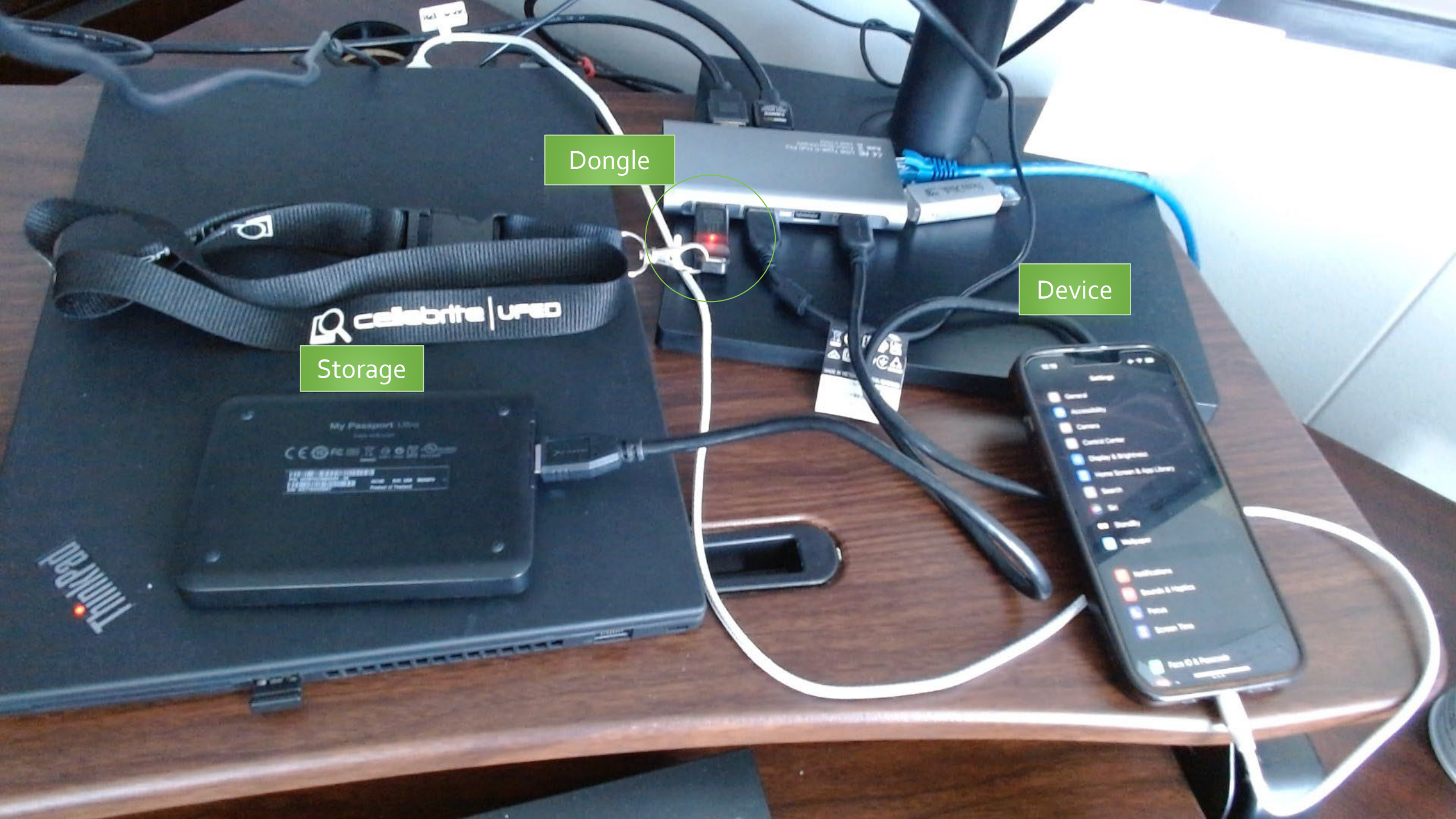




Dongle

Storage

Device





SAMSUNG GSM SM-S916U GALAXY S23+  
USB cable 170 or Original Cable



Advanced Logical



File system



Physical (Rooted)



Camera



Screenshot



Chat Capture





# Advanced Logical extraction on Samsung

SELECT CONTENT TYPE



SAMSUNG GSM SM-S916U GALAXY S23+  
USB cable 170 or Original Cable



Extract from



Device



SIM



Memory Card



Choose data types to extract



Skip extraction popups



All



Call Logs



Locations



Advertising ID



Contacts



SMS



MMS



Calendar



Pictures



Audio/Music



Videos



Ringtones



Documents



Archives



Email



IM



Browsing Data



User Dictionary



Files



APPLE A2482 IPHONE 13  
USB cable 210 or Original Cable



Logical (Partial)



Advanced Logical



Camera



Screenshot



# Advanced Logical extraction on iPhone

SELECT MODE



APPLE A2482 IPHONE 13  
USB cable 210 or Original Cable



File System



APPLE A2482 IPHONE 13

USB cable 210 or Original Cable



Extraction to Local Drive

G:\iOSExtractionExample







## APPLE A2482 IPHONE 13

USB cable 210 or Original Cable

---

Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.

### A2482 iPhone 13:

Before starting the extraction, you must set the screen timeout to Never.

Note:

For iOS 18.2 and above: Disable Stolen Device Protection from the device settings or remove the passcode/FaceID completely.

Settings → FaceID&Passcode → Stolen Device Protection → Turn off.

If the device is already jailbroken\*\*, a more thorough extraction can be performed.

\*\*The Cydia third-party app and the Apple File Conduit "2" addon must be pre-installed.

Don't touch any button on the device during the extraction.

Devices running Mobile Device Management (MDM) may experience unexpected behavior. It is recommend not to perform extractions for these devices.

MDM is specified under device settings.

Before connecting, disable Auto-Lock on the device:

for iOS 2.x - 9.3.5:

Settings → General → Auto-Lock → select "Never" and return to Home screen.

for iOS 10.0 and higher:

Settings → Display and Brightness → Auto-Lock → select "Never" and return to Home screen.

To allow device connection:

Battery should be fully charged

1. Power on the device and wait until it's fully booted.
2. Insert SIM card if required by the phone to boot.
3. Connect the device to the Inseyets UFED.
4. Press Continue.



APPLE A2482 IPHONE 13  
USB cable 210 or Original Cable

Please wait, this can take some time...



Please Wait...

Connecting



APPLE A2482 IPHONE 13  
USB cable 210 or Original Cable

Please wait, this can take some time...

### Backup Encryption

To extract user credentials from an iOS device, backup encryption should be enabled (encryption is automatically disabled at the end of a successful extraction).

Enable backup encryption? (Inseyets UFED will temporary set the password to "1234".)

NO

YES



APPLE A2482 IPHONE 13

USB cable 210 or Original Cable

Please wait, this can take some time...



### iTunes Password

This device has iTunes backup encryption. The password is required for collecting data. If you know the password, click OK.



APPLE A2482 IPHONE 13

USB cable 210 or Original Cable

Please wait, this can take some time...



/.b/6/Containers/Data/Application/9DA2A1E4-6312-4A7F-A89A-31D9FAEB9733/  
Library/WebKit/WebsiteData/Default/  
rk6sG5uQtlKUp94FLF0CkPTcP5mPihh5MlhJXFLH8Ds/  
rk6sG5uQtlKUp94FLF0CkPTcP5mPihh5MlhJXFLH8Ds/CacheStorage/Version 16/  
Records/11599AB1392DBBDE7979A08AC64519646EA556F0/31cc1592-  
c1f3-4e99-96c3-df0da07fe288/86CE5D3D96515F3C6D63BDC52730FA43E541746F-  
blob

# Full File System extraction

- Is phone Make/Model/Operating System supported?
- Device State (Hot or Cold)

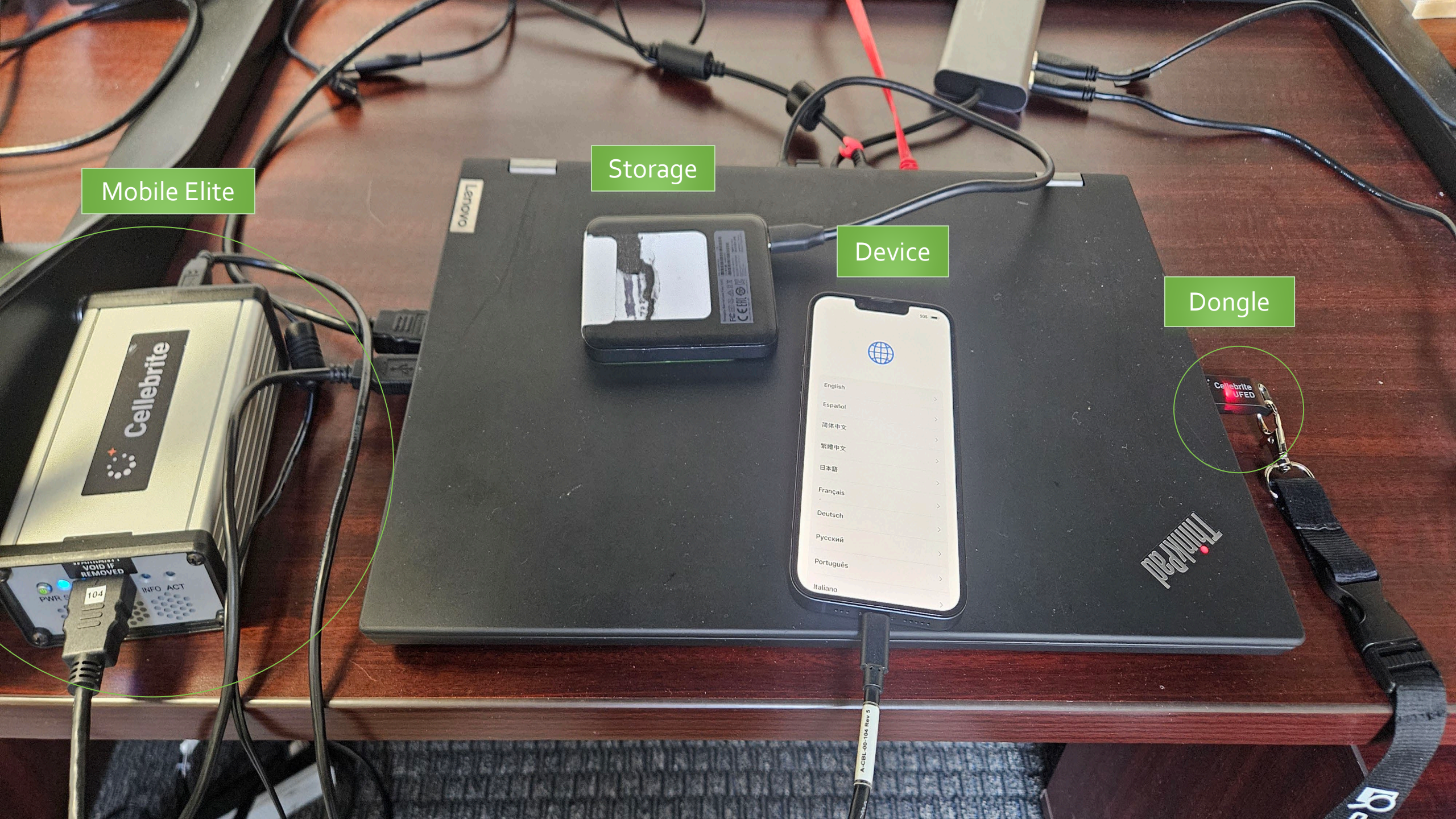


Mobile Elite

Storage

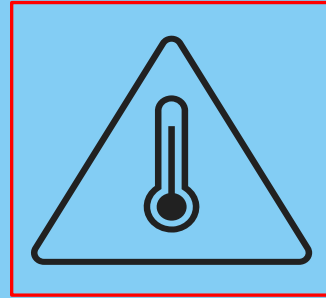
Device

Dongle





# What state are we in?



## AFU(HOT)

After First Unlock

State of the device once the passcode has been entered for the first time. Most of the data is accessible and decrypted.

Unlocked



## BFU(COLD)

Before First Unlock

State after the phone reboots and the password hasn't been entered. Most data is securely encrypted and cannot be accessed.

Locked



Welcome to Inseyets UFED

To perform advanced  
access, choose an  
operating system



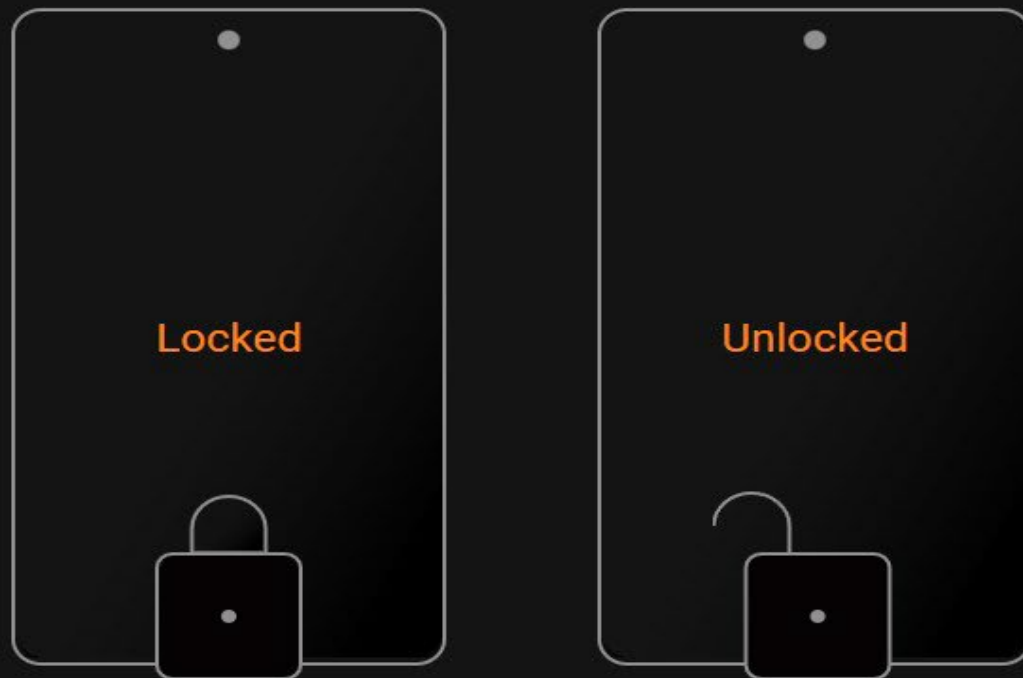
Search Supported Devices


iOS

Android

?

Select if the device is locked or unlocked



 When to Select Locked vs. Unlocked?

Android &gt; Unlocked

## Preparation steps

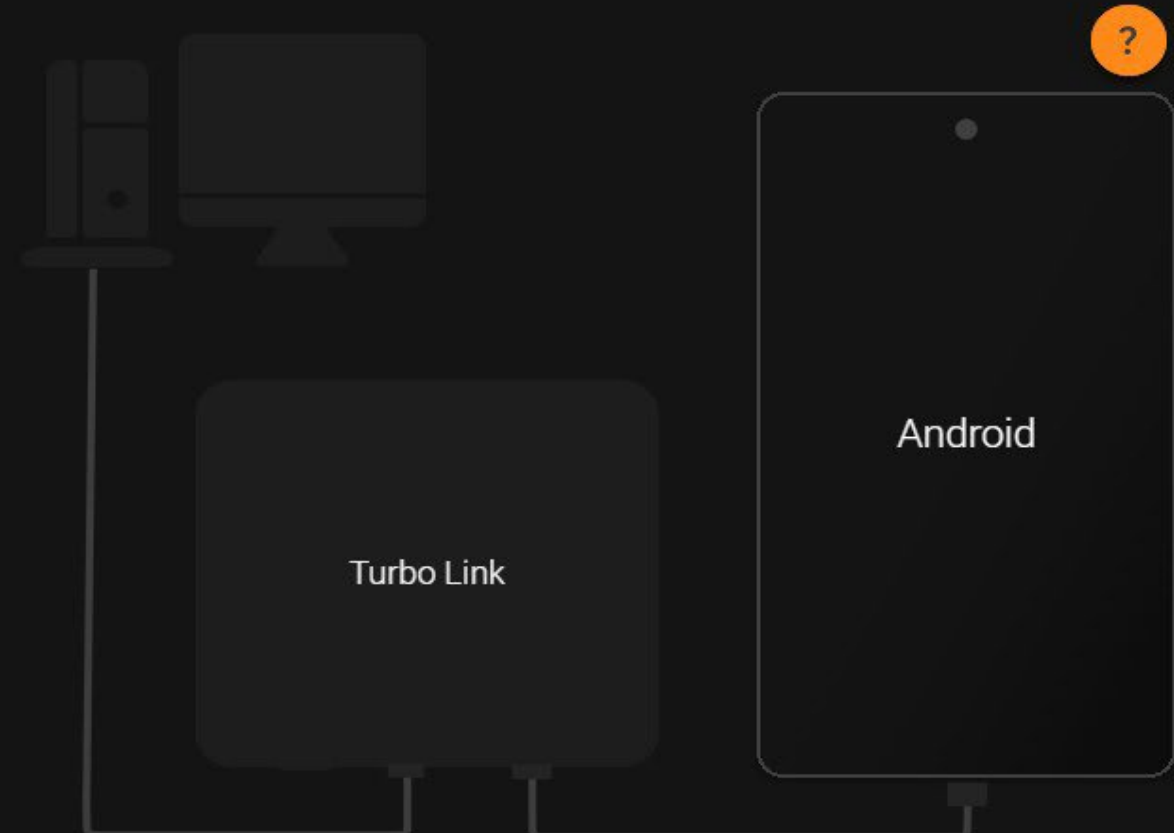
01 Connect Turbo Link to computer.



02 Initializing the Turbo Link environment.



03 Connect device to Turbo Link.



Android > **Unlocked**

# Initializing...

**Device status**

## Quick view

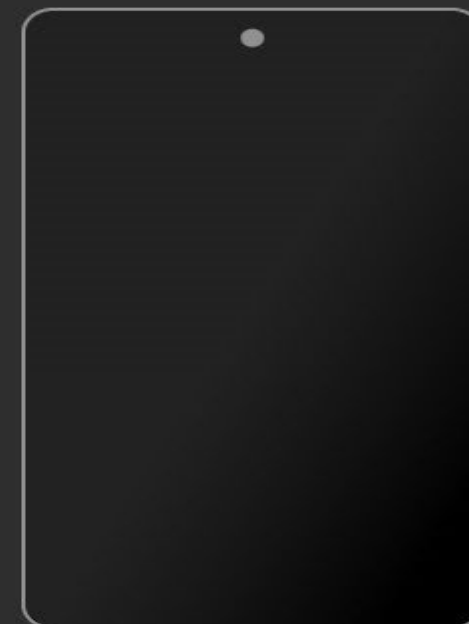
Device	Model	Chipset
<b>SAMSUNG</b>	<b>SM-S916U</b>	—
OS version	Security patch level	Encryption type
—	—	—
Live encryption state		
—		

**Extraction path**

D:\

 **Progress console**

```
5/2/2025 1:43 PM - Adapter: 2.3.0, Framework: framework_v1.5.32.tar.gz
5/2/2025 1:43 PM - Downloading resource: Android_Unlocked_v7.73.4.4.tar.gz
5/2/2025 1:43 PM - Downloading resource: Mits_Venv_v2.0.4.tar.gz
5/2/2025 1:44 PM - Device fingerprint: S916USQS6CYB3/S916UOYN6CYB3/S916USQS6CYB3/S916USQS6CYB3
5/2/2025 1:44 PM - Device IMEI: 355802956004071
5/2/2025 1:44 PM - OneUI version: 6.1.1
5/2/2025 1:44 PM - OneUI version: 6.1.1
```



Notify Me

Android > **Unlocked**

?

## Initial Access...

Device status

Quick view

Device	Model	Chipset
<b>SAMSUNG</b>	<b>SM-S916U</b>	—
OS version	Security patch level	Encryption type
—	—	—
Live encryption state		
—		

### Extraction path

D:\



### Progress console



5/2/2025 1:43 PM - Downloading resource: Mits\_Venv\_v2.0.4.tar.gz  
5/2/2025 1:44 PM - Device fingerprint: S916USQS6CYB3/S916UOYN6CYB3/S916USQS6CYB3/S916USQS6CYB3  
5/2/2025 1:44 PM - Device IMEI: 355802956004071  
5/2/2025 1:44 PM - OneUI version: 6.1.1  
5/2/2025 1:44 PM - OneUI version: 6.1.1  
5/2/2025 1:44 PM - Checking if Cellebrite Agent is present...  
5/2/2025 1:44 PM - Attempt to connect to Cellebrite Agent. Waiting up to 4 minutes  
5/2/2025 1:46 PM - Downloading resource: Petroleum\_v7.73.4.4.tar.gz **36%**



Notify Me



# Executing Consent Method...

Device status

Quick view

Device	Model	Chipset
samsung	SM-S916U	SM8550
OS version	Security patch level	Encryption type
14	2025-03-01	File-based Encryption (...)
Live encryption state		
—		

Extraction path

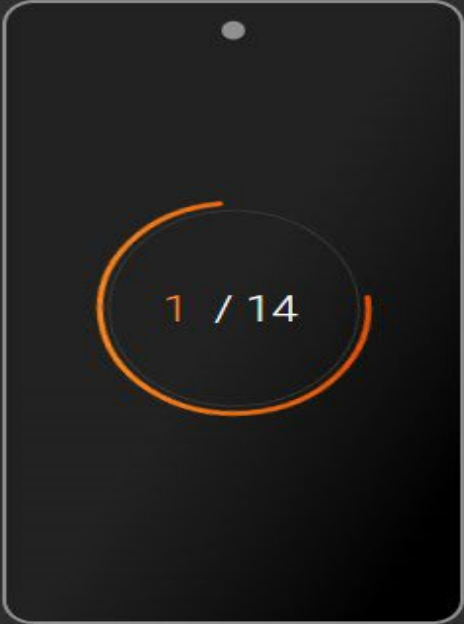
D:\



Progress console



5/2/2025 1:47 PM - Establishing connection with the device  
5/2/2025 1:47 PM - OneUI version: 6.1.1  
5/2/2025 1:47 PM - Uploading and checking device compliance  
5/2/2025 1:47 PM - Establishing connection with the device  
5/2/2025 1:47 PM - Uploading and checking device compliance  
5/2/2025 1:47 PM - Establishing connection with the device  
5/2/2025 1:47 PM - Uploading and checking device compliance  
5/2/2025 1:47 PM - Executing Cellebrite capability...



Notify Me



Android > Unlocked

Select an action

Device status

Quick view

Device	Model	Chipset
samsung	SM-S916U	SM8550
OS version	Security patch level	Encryption type
14	2025-03-01	File-based Encryption (...)
Live encryption state		
Hot (decrypted)		

Extraction path

D:\

Progress console

5/2/2025 1:51 PM - OneUI version: 6.1.1  
5/2/2025 1:51 PM - OneUI version: 6.1.1  
5/2/2025 1:52 PM - Device bluetooth name: EDGAR's S23+  
5/2/2025 1:52 PM - Found 1 IMEIs/MEIDs: 355802956004071  
5/2/2025 1:52 PM - Users configured on the device: UID 0: edgar Fritz, Decrypted. UID 150: Secure Folder, Decrypted.  
5/2/2025 1:52 PM - Secure Folder (UID 150) data detected and fully decrypted on the device and can be extracted.



Access completed successfully

Notify Me

Finish

Extraction Methods



STEP 1

**Operation Method**

STEP 2

**Extraction Method**

STEP 3

**Path & Summary**

## 1. Select Operation Method

Please select your preferred operation method.

**Streamline**

Provides a quick and simple process of extracting data in Inseyets UFED and automatically syncing the case information to Inseyets PA for decoding and reporting, streamlining their work.

**Autonomy****Not Available**

Provides a quick and simple process of extracting data in UFED and automatically syncing the case information to Autonomy for decoding and reporting, streamlining their work.

**Manual**

Select extraction type and then manually proceed with processing the extraction file.

**Support**

Cancel

**Continue**



Ins<sup>o</sup>t

Android &gt; U

Select a

Device

Device

lg

Security pa

2022-02-01

Extraction pa

D:\UFED 2025

Prog

2/21

2/21

2/21

2/21



STEP 1

Operation Method

Manual



STEP 2

Extraction Method



STEP 3

Path &amp; Summary

&lt; Back



## 2. Select Extraction Method

Extractions available based on the connected device.

**Full file system**

Completed

Extracts all data from active file system, including /system/ location, but excludes unallocated space.

**Applications**

You can selectively extract specific installed applications on the device.

**Physical**

Completed

Entire memory range of the device, includes full file system, user data, and unallocated space. (FDE ONLY).

**Triage scan**

Identify device status as clear or suspect using predefined profiles, decoding, and reporting features.

**User data**

Support

Cancel

Continue

Application (273)
Calendar (380)
Calls (198)
Contacts (1756) (2)
Devices & Networks (1113)
Location Related (84774)
Media (25455)
Memos (2)
Messages (1409)
Physical Activities (41431)
Search & Web (3322)
Social Media (1)
System & Logs (22880) (1)
User Accounts & Details (1034)

## Cellebrite Phone Extraction

Apple iPhone 13  
iOS 17.3.1

← Advanced Logical  
(iTunes backup)

Full File System  
Add-on tool  
(Mobile Elite)




Application (1276) (44)
Calendar (606)
Calls (379) (97)
Contacts (2648) (15)
Device Info (43)
Finance & Purchase (151)
Location Related (43)
Media (177881)
Memos (2)
Messages (33987) (12)
Networks & Connections (9368) (362)
Physical Activities (42375)
Search & Web (21773) (125)
Social Media (20)
System & Logs (23198) (1)
User Accounts & Details (2650)

Q

Search

Analyzed Data

>



Application (378)

>



Calendar (165)

>




Calls (464)

>




Contacts (2792)

>




Device Info (48)

>




Location Related (30)

>




Media (16264)

>




Memos (22)

>




Messages (2001)

>



Networks & Connections (1650)

>




Search & Web (1648)

>




Social Media (34)

>




System & Logs (7786)

>



User Accounts & Details (434)


Data files



All Files (41494)




Archives (36)




Configurations (4411)




Databases (691)



Documents (39)



Shortcuts (263)



Text (190)

# Cellebrite Phone Extraction

Apple iPhone 16 Pro  
iOS 18.2.1



Advanced Logical  
(iTunes backup)



Full File System  
Add-on tool  
(Mobile Elite)

Q Search

Analyzed Data

>

Application (8989) (46)

>

Calendar (166) (1)

>

Calls (1970) (2)

>

Contacts (3597) (5)

>

Device Info (42)

>

Finance & Purchase (6)

>

Location Related (47)

>

Media (114777)

>

Memos (22)

>

Messages (3286)

>

Networks & Connections (29536) (196)

>

Physical Activities (42755)

>

Search & Web (4245) (7)

>

Social Media (28)

>

System & Logs (10310) (1)

>

User Accounts & Details (1055)

Data files

All Files (445818)

Applications (6311)

Archives (1756)

Configurations (123853)

Databases (1446)

Data	VeraKey	Advanced Logical
Activity Sensor Data	23756 (0)	23757 (0)
Aggregated Application Usage	14 (0)	
Applications Usage Log	29 (0)	
Autofill	4 (4)	4 (4)
Calendar	652 (269)	408 (25)
Call Log	471 (105)	237 (0)
Cell Towers	14 (14)	
Chats	956 (1)	923 (0)
Contacts	1250 (1)	1203 (1)
Cookies	602 (0)	416 (0)
Device Connectivity	1727 (616)	1111 (0)
Device Events	33 (0)	1 (0)
Device Locations	3604 (1599)	1690 (0)
Devices	21 (0)	
Emails	5105 (2)	267 (0)
Installed Applications	221 (0)	205 (0)
Instant Messages	8638 (0)	230 (0)
Log Entries	9658 (1)	9622 (1)
Notes	88 (5)	83 (0)
Passwords	1136 (0)	528 (0)
Recordings	1 (1)	1 (1)
Searched Items	15058 (1948)	90 (0)
User Accounts	20 (0)	16 (0)
Web Bookmarks	39 (0)	39 (0)
Web History	67370 (9574)	204 (0)
Wireless Networks	119 (0)	119 (0)
Applications	3477 (0)	
Archives	2910 (0)	219 (0)
Audio	24057 (0)	591 (0)
Configurations	204088 (0)	3607 (0)
Databases	1784 (0)	305 (0)
Documents	4099 (0)	14 (0)
Exchange	4764 (0)	
Images	88545 (1)	19206 (0)
Shortcuts	1 (0)	
Text	19016 (0)	124 (0)
Uncategorized	295623 (30)	3150 (0)
Videos	4313 (0)	808 (0)
User Dictionary		18 (0)























Figure 1: Data Point Comparison FFS vs AL

# VeraKey FFS vs Advanced Logical











Calendar	652 (269)	408 (25)
Call Log	471 (105)	237 (0)
Cell Towers	14 (14)	
Chats	956 (1)	923 (0)
Contacts	1250 (1)	1203 (1)
Cookies	602 (0)	416 (0)
Device Connectivity	1727 (616)	1111 (0)
Device Events	33 (0)	1 (0)
Device Locations	3604 (1599)	1690 (0)
Devices	21 (0)	
Emails	5105 (2)	267 (0)
Installed Applications	221 (0)	205 (0)
Instant Messages	8638 (0)	230 (0)
Log Entries	9658 (1)	9622 (1)
Notes	88 (5)	83 (0)
Passwords	1136 (0)	528 (0)
Recordings	1 (1)	1 (1)
Searched Items	15058 (1948)	90 (0)
User Accounts	20 (0)	16 (0)
Web Bookmarks	39 (0)	39 (0)
Web History	67370 (9574)	204 (0)
Wireless Networks	119 (0)	119 (0)

# Magnet FFS vs Advanced Logical




















## COMMUNICATION 175

 Apple Contacts - iOS	10
 Discord Messages	17
 Facebook Messenger Messages	1
 Facebook Messenger Users Contacted	15
 GroupMe Accounts	1
 iOS Call Logs	1
 iOS iMessage/SMS/MMS	11
 iOS Messages Preferences	1
 iOS TextNow Chat	49
 iOS TextNow Contacts	12
 iOS TextNow Groups	5
 iOS TextNow Profile	1
 IP Addresses - Audio/Video Calls	6
 Signal Local User	1
 Signal Messages - iOS	2
 Signal Stories	5
 Signal Users	5
 Snapchat Chat Messages	19
 Snapchat Contacts	4
 Snapchat Memories	1
 TextPlus Messages	1
 Viber Messages	7



## COMMUNICATION 87




















 Apple Contacts - iOS	4
 GroupMe Accounts	1
 iOS Call Logs	1
 iOS iMessage/SMS/MMS	6
 iOS Messages Preferences	1
 iOS TextNow Chat	49
 iOS TextNow Contacts	12
 iOS TextNow Groups	5
 iOS TextNow Profile	1
 Viber Messages	7




## OPERATING SYSTEM 33,447

 .DS_Store Records	139
 Apple Accounts	15
 File System Information	2
 iOS Home Screen Items	4
 Network Interfaces - iOS, macOS	3
 Network Usage - Application Data	364
 Owner Information	1
 PowerLog App Usage	740
 PowerLog Application State	9,470
 PowerLog Battery Level	21,426
 PowerLog Battery Shutdown	1
 PowerLog Camera State	199
 PowerLog Device Lock State	212
 PowerLog In Call Service	398
 PowerLog Lightning Cable Status	248
 PowerLog Screen Autolock	14
 PowerLog Timezone Information	204
 Private MAC Addresses - iOS	6
 User Notification Events	1

## OPERATING SYSTEM 206

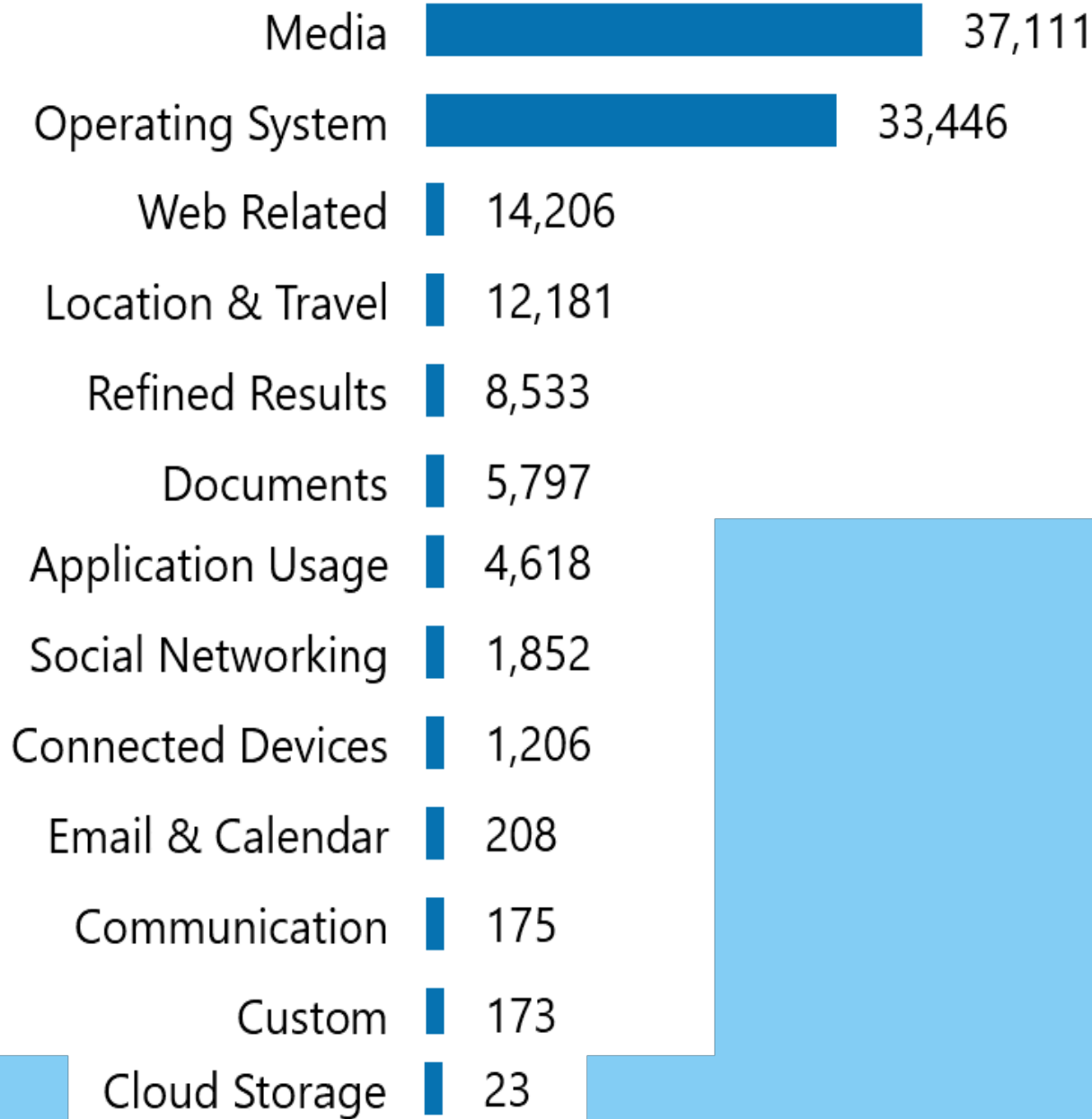
 .DS_Store Records	12
 Apple Accounts	15
 File System Information	2
 iOS Home Screen Items	4
 Network Usage - Application Data	165
 Owner Information	2
 Private MAC Addresses - iOS	6

^ APPLICATION USAGE	4,618
 Application Install States	821
 Application Permissions - MacOS, iOS	97
 Biome Application Focus	20
 Biome Application Install States	1
 Biome Application Launch	40
 Biome Device Orientation States	6
 Biome Device Plugged-in States	63
 Biome Device Screen Backlight States	64
 Biome Keybag Lock States	13
 Biome User Activity	1
 Installed Applications	232
 iOS App Cache	2,962
 iOS Device Information	1
 iOS User Word Dictionary	230
 KnowledgeC Application Usage	10
 KnowledgeC Device Lock States	13
 KnowledgeC Notification Usage	1
 KnowledgeC Screen Backlight States	40
 Wallet Payment Cards	3

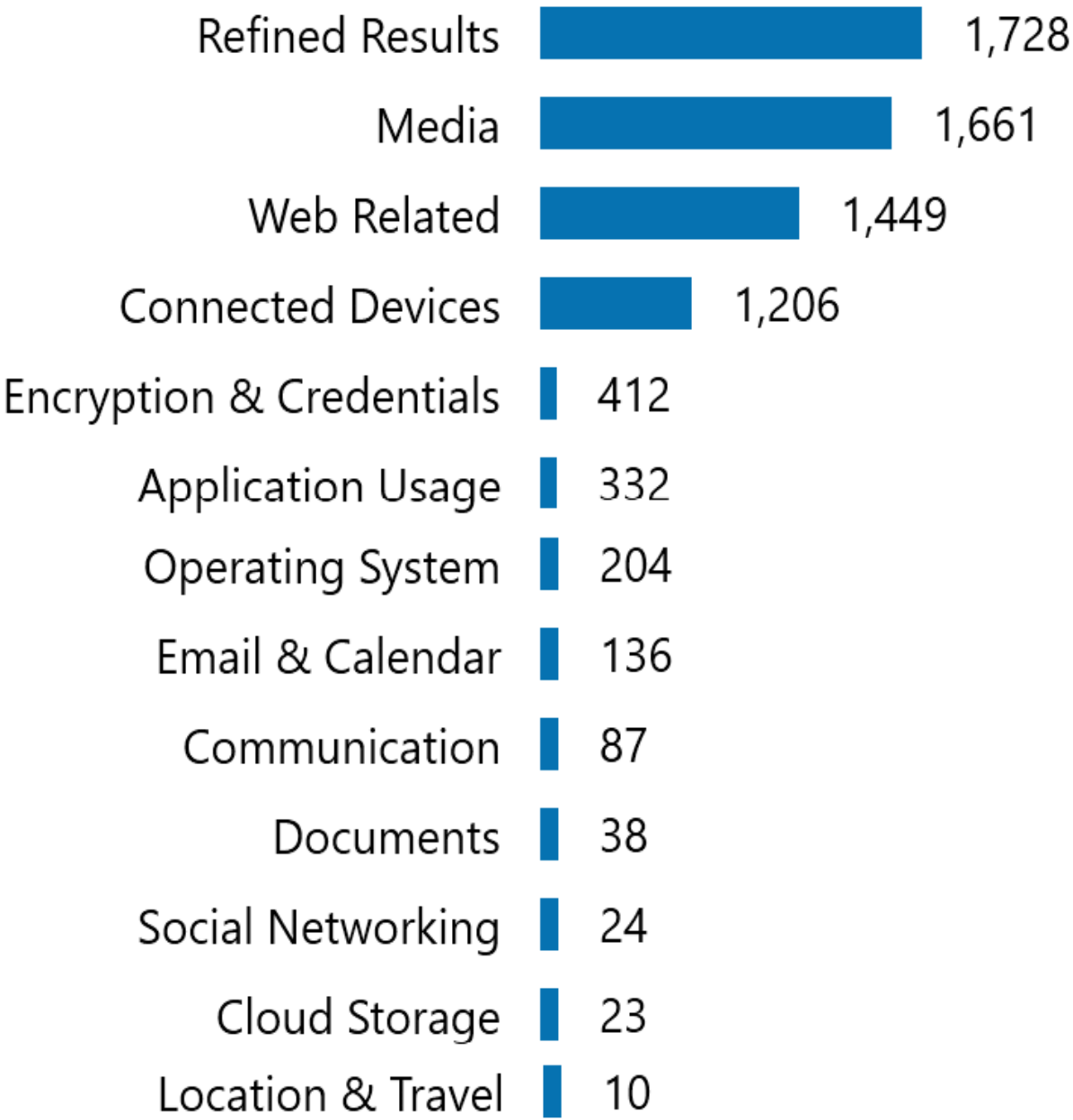
APPLICATION USAGE	333
 Application Permissions - MacOS, iOS	99
 Installed Applications	232
 iOS Device Information	2



Number of artifacts **119,529**



Number of artifacts **7,310**



# Limitations of Full File System

- Passcode
- Operating System
- Lockdown Mode
- Time to install Cellebrite Agent
- Time to extract data
- Internet Connection
- Power Source

# What does the data look like?

- Dashboard
- Timeline
- Analyze Data
- File System
- Locations
- Insights
- Cloud Data

InsightsPA

FileViewToolsCloudPlug-insReportHelp

AdvanceLearning Hub

Cases

Dashboard

Timeline

Analyzed Data

File Systems

Locations

Insights

Tags

Reports

Cloud

Extraction Summary (1)

Dashboard View

Data Details View

Date Range

Preliminary Device Report

Generate Report

Evidence Pack

1 Evidence

Extraction...  
File S...

Model na...  
Apple D...

Extraction...  
FileSyst...

Extraction...  
4/22/20...

Path  
F:\Ne...

Image Hash  
Hash data not available

Content

Device Data

Device Data Files

75,452  
Activity Sensor Data

3,236  
Aggregated Application Usage

44,728  
Applications Usage Log

32,405  
Calendar

Show All

Device info

Go

Detected Phon... iPhone 15

IMEI: 355180950120460

MAC address: FA:E5:CE:4B:22:67, FA:E5:CE:4B:22:98

Serial: M42XX5Y6K2

Time Zone: (UTC-05:00) New\_York (America)

Unique ID: 00008120-0012518C2292201E

Top 5 messaging parties

311952: My Number

45324: Elizabeth Harrison

16074: Brian Maher

8859: Scott Smith

8403: Wes Cook

10 most visited locations

Go

35.8353,-78.6889  
1641 visits

35.8271,-78.6353  
1490 visits

35.8477,-78.6504  
1000 visits

35.8175,-78.6546  
364 visits

35.8875,-78.5447  
324 visits

35.8463,-78.6504  
292 visits

35.8147,-78.6738  
264 visits

35.8862,-78.5447  
191 visits

35.8175,-78.6559  
180 visits

35.8504,-78.6916  
149 visits

Map

Satellite

Last 10 calls

Go

TYPE	IDENTIFIER	TIME
Incoming	+1 (985) 202-998...	4/18/2025 1:18:3...
Incoming	+1 (803) 227-228...	4/18/2025 1:00:0...
Incoming	+1 (803) 227-228...	4/18/2025 1:00:0...
Outgoing	Melissa Dickinso...	4/18/2025 11:09:...
Outgoing	Melissa Dickinso...	4/18/2025 11:09:...
Outgoing	April Gladkin +19...	4/18/2025 10:31:...
Outgoing	April Gladkin +19...	4/18/2025 10:31:...

Last 10 sent or received media

Go

Top 5 messaging apps

Go

Native Messages 321,...

WhatsApp 2,754

Microsoft Teams 631

Facebook 586

Facebook Messenger ...

Last 10 searches

Go

SEARCHED	APP	TIME
181 Harbor Drive,...	Gmail	4/18/2025 12:05:...
2269 Chestnut St...	Gmail	4/18/2025 11:21:...
6230 Pesta Ct	Gmail	4/18/2025 11:11:...
4300 U.S. Ro ute 1	Gmail	4/18/2025 6:46:0...
car wash raleigh ...	KnowledgeC	4/17/2025 7:36:3...
car wash raleigh ...	Safari	4/17/2025 7:33:2...
car wash raleigh ...	Safari	4/17/2025 7:32:5...

Crypto artifacts

Go

11: Wallet address

1: Mnemonic phrase

Top 10 Bluetooth connections

Go

TYPE	IDENTIFIER	CONNECT...	TIME
Headset	wgh airpod...	Connected	4/17/2025 ...
Headset	webster Po...	Connected	4/18/2025 ...
Unknown	0E650D71-...	Connected	4/22/2025 ...
Unknown	9E75C002-...	Connected	4/22/2025 ...
Unknown	3F9AB6D0-...	Connected	4/18/2025 ...
Unknown	Anker A7722	Connected	4/16/2025 ...
Unknown	C966FE19-...	Connected	4/22/2025 ...

Top crypto risk severity wallets

Go

Wallets at Severe Risk

0

Wallets at High Risk

0

Wallets at Medium-High ...

0

Wallets at Medium Risk

0

Windows Taskbar

Search

Icons

System Tray



rch...

Search...

Table contains more than 1 Million items, please use filters to narrow down results

										Type	↑ Timestamp	Part
1/18/1604 (2)												
		<input checked="" type="checkbox"/>	1							Calendar	1/19/1604 12:00:00 AM [StartDate]	
		<input checked="" type="checkbox"/>	2							Calendar	1/19/1604 12:00:00 AM [StartDate]	
1/19/1604 (2)												
		<input checked="" type="checkbox"/>	3							Calendar	1/19/1604 11:59:59 PM [EndDate]	
		<input checked="" type="checkbox"/>	4							Calendar	1/19/1604 11:59:59 PM [EndDate]	
3/27/1604 (1)												
		<input checked="" type="checkbox"/>	5							Calendar	3/28/1604 12:00:00 AM [StartDate]	
3/28/1604 (1)												
		<input checked="" type="checkbox"/>	6							Calendar	3/28/1604 11:59:59 PM [EndDate]	
4/6/1604 (1)												
		<input checked="" type="checkbox"/>	7							Calendar	4/7/1604 12:00:00 AM [StartDate]	
4/7/1604 (2)												
		<input checked="" type="checkbox"/>	8							Calendar	4/7/1604 11:59:59 PM [EndDate]	
		<input checked="" type="checkbox"/>	9							Calendar	4/8/1604 12:00:00 AM [StartDate]	
4/8/1604 (1)												

Total: 1721519   Deduplication: 281671   Items: 1439848/1439848   Selected: 1439848

Cellebrite Insecrets Physical Analyzer | Version 10.5.0.1022

Ins<sup>ts</sup>.PA File View Tools Cloud Plug-ins Report

Cases

Dashboard

Timeline

Analyzed Data

File Systems

Locations

Insights

Tags

Reports

Cloud

MGC - Webster Harrison iPhone

Search...

### Analyzed Data

- > Application (48695) (58)
- > Calendar (32405) (13)
- > Calls (3517) (11)
- > Contacts (17485) (1290)
- > Device Info (46)
- > Finance & Purchase (352) (2)
- > Location Related (58)
- > Media (378119)
- > Memos (81) (71)
- > Messages (17673) (335)
- > Networks & Connections (69768) (2457)
- > Physical Activities (75452)
- > Search & Web (43085) (1893)
- > Social Media (404)
- > System & Logs (45905) (77)
- > User Accounts & Details (8068) (1)

### Data files

- All Files (1000497)
- Applications (10068)
- Archives (3886)
- Configurations (258563)
- Databases (6498)



Cellebrite Inseets Physical Analyzer | Version 10.5.0.1022

Ins<sup>ts</sup> PA File View Tools Cloud Plug-ins Report

Cases

Dashboard

Timeline

Analyzed Data

**File Systems**

Locations

Insights

Tags

Reports

Cloud

File Systems

- File Systems
  - DropBox user: 3171985584 (54 files, 0 KB)
    - EXTRACTION\_FFS.zip (1 file, 31,599 KB)
  - EXTRACTION\_FFS.zip (1326230 files, 199,275,198 KB)
    - root (1326230 files, 199,275,198 KB)
      - .b (0 files, 0 KB)
        - .nofollow (0 files, 0 KB)
        - .resolve (0 files, 0 KB)
      - Applications (4176 files, 326,553 KB)
        - bin (2 files, 139 KB)
        - cores (0 files, 0 KB)
      - dev (66 files, 0 KB)
        - Developer (0 files, 0 KB)
      - Library (2302 files, 230,531 KB)
      - private (1127573 files, 188,444,066 KB)
        - etc (21 files, 688 KB)
          - system\_data (0 files, 0 KB)
        - var (1127551 files, 188,443,377 KB)
          - .fseventsd (6 files, 153 KB)
          - audit (0 files, 0 KB)
          - buddy (0 files, 0 KB)
        - containers (537448 files, 42,375,474 KB)
          - datamigrator (0 files, 0 KB)
        - db (2436 files, 258,854 KB)
          - dextcores (0 files, 0 KB)
          - dirs\_cleaner (0 files, 0 KB)
          - empty (0 files, 0 KB)

Cellebrite Insecrets Physical Analyzer | Version 10.5.0.1022

Ins<sup>ts</sup> PA File View Tools Cloud Plug-ins Report

Cases

Dashboard

Timeline

Analyzed Data

File Systems

**Locations**

Insights

Tags

Reports

Cloud

⌕ MGC - Webster Harrison iPhone

Locations

- Visited (12140) (2841)
- Point of Interest (4532) (18)
  - Mentioned (364)
  - Navigation (1395)
  - Searched Places (1439) (18)
  - Shared (48)
  - Significant Location (208)
  - Unknown (1069)
  - User Specified (9)
- Media (27195)
  - Media (16451)
  - Media Probably Captured (10744)
- Other (311049) (196)
  - Carved (304171)
  - Cell Tower (424) (17)
  - Harvested Cell Tower (94) (74)
  - Harvested WIFI (6360) (105)



Cellebrite Inseynets Physical Analyzer | Version 10.5.0.1022

InsightsPAFileViewToolsCloudPlug-insReport

Cases

Dashboard

Timeline

Analyzed Data

File Systems

Locations

Insights

Tags

Reports

Cloud

<<

● ▲ MGC - Webster Harrison iPhone

⌵ ⋮

Insights

⋮

▼ ₿ Cryptocurrency (12)

📁 Crypto wallets (11)

🔑 Crypto artifacts (1)

▼ ≡ Watch Lists

≡ Keywords

🔍 Malware scanner

?



Cases



Dashboard



Timeline

Analyzed  
Data

File Systems



Locations



Insights



Tags



Reports



Cloud



Help

MGC - Webster Harrisc

Extraction Summary (1)

Timeline (1721519)

Locations (354916)

Cloud (20)

20 data sources found

**Amazon Alexa**

Contacts, Messages, UserProfile, UserActivities

Gain access to suspects' Amazon Alexa data, including audio.

**Amazon Shopping**

UserProfile, UserActivities, Messages

Obtain purchase records and user activity

**Facebook**

Messages, Contacts, Images, Videos

Account name: 53503245

Enrich mobile data and acquire posts, comments, likes, direct messages, and events.

**Facebook Messenger**

Messages, Contacts

Account name: 53503245

Gain access to suspects' activities from the Facebook messenger data source.

**Gmail**

Messages

Account name: webharrison@gmail.com

Enrich mobile data and gain access to historical email information (beyond date range).

**Google Calendar**

UserActivities

Account name: webharrison@gmail.com

Enrich mobile data and acquire calendar information from Google Calendar

**Google Chrome Sync**

UserProfile, UserActivities

Account name: webharrison@gmail.com

Enrich mobile data and obtain visited pages, bookmarks, saved passwords, and auto complete data.

**Google Contacts**

Contacts

Account name: webharrison@gmail.com

Acquire contact information.

**Google Drive**

Images, Videos, Files

Account name: webharrison@gmail.com

Enrich mobile data and acquire stored files.

**Google Hangouts**

Messages, Contacts, Call

Account name: webharrison@gmail.com

Gain access to suspects' activities from Google Hangouts.

**Google Home**

UserActivities

Account name: webharrison@gmail.com

Gain access to suspects' Google Home activities, including audio.

**Google Keep**

UserActivities

Account name: webharrison@gmail.com

Enrich mobile data and acquire tasks information from Google Keep.



Cases



Dashboard



Timeline

Analyzed  
Data

File Systems



Locations



Insights



Tags



Reports



Cloud



MGC - Webster Harrisc

Extraction Summary (1) x

Timeline (1721519) x

Locations (354916) x

Cloud (20) x

**Google Location History**  
LocationsAccount name: webharrison@gmail.com  
Acquire minute-by-minute location information.**Google My Activity**  
UserProfile, UserActivitiesAccount name: webharrison@gmail.com  
Acquire searches, click results, visited pages, and voice commands.**Google Photos**  
Images, VideosAccount name: webharrison@gmail.com  
Enrich mobile data and acquire photos and videos from Google Photos.**Google Play**  
UserProfile

Account name: webharrison@gmail.com

**Google Tasks**  
UserActivitiesAccount name: webharrison@gmail.com  
Enrich mobile data and acquire tasks information from Google Tasks.**Instagram**  
Messages, Contacts

Enrich mobile data and acquire grams and comments.

**Lyft**  
UserActivities, UserProfileAccount name: 1112566919890064950  
Gain access to trip activity and rider and driver identifiers.**Uber**  
UserActivities, UserProfileAccount name: 142dd5d1-bed9-436f-9c11-1aee9231a5cd  
Gain access to trip activity and rider and driver identifiers

4 applications found without access

Unfortunately we couldn't find cloud access keys on the mobile device. Try to get the username and password from the user and use UFED Cloud

**Coinbase**  
UserProfile, UserActivities**Dropbox**  
Images, Videos, Files**Google Home**  
UserActivities**LinkedIn**  
Messages, Contacts, UserProfile

# Reporting

- Format type
- E-Discovery
- What to include

# Report Formats

Format

**Case Information**

Examiner name:

Location:

Case number:

Case name:

Evidence number:









Department:

Organization:

Investigator:

Crime type:

Notes:

- ☐  UFDR (For Cellebrite Reader, Pathfinder or Guardian)
- ☐  PDF Report
- ☐  HTML Report
- ☐  Excel Workbook (xlsx)
- ☐  Word report
- ☐  XML Report
- ☐  Relativity Short Message Format
- ☐  e-Discovery Load File

Close

General

Legalview

Load File

Metadata Fields

Report Dataset

**Bart Evans - Su...**

Security

Formatting

Table Sorting

**Report Dataset - Bart Evans - Summit Funding****Time range filter**☐ Only events between these dates**From:**

M/d/yyyy h:mm:ss tt

**To:**

M/d/yyyy h:mm:ss tt

Apply

☐ Include items without a timestamp**Data types**☒ Select/Deselect All

Enter text to filter ...



- ☒ Activity Sensor Data (147/147)
- ☒ Applications Usage Log (32/32)
- ☒ Autofill (2389/2389)
- ☒ Calendar (3696/3696)
- ☒ Call Log (1491/1491)
- ☒ Chats (9712/9712) (104435 messages)
- ☒ Contacts (29586/29586)
- ☒ Cookies (5623/5623)
- ☒ Credit Cards (23/23)
- ☒ Device Connectivity (6076/6076)
- ☒ Device Info (45/45)
- ☒ Emails (1268/1268)

- ☒ Journeys (16/16)
- ☒ Locations (17519/17519)
- ☒ Locations View (41663/41663)
- ☒ Log Entries (62157/62157)
- ☒ Network Connections (60/60)
- ☒ Notes (98/98)
- ☒ Passwords (777/777)
- ☒ Searched Items (55/55)
- ☒ Timeline (240956/240956)
- ☒ Transfers (566/566)
- ☒ User Accounts (722/722)
- ☒ Voicemails (2548/2548)

**File types**☒ Select/Deselect All

Enter text to filter ...



- ☒ Archives (90/90)
- ☒ Audio (2653/2653)
- ☒ Configurations (11055/11055)
- ☒ Databases (1130/1130)
- ☒ Documents (1484/1484)

- ☒ Images (96562/96562)
- ☒ Shortcuts (416/416)
- ☒ Text (873/873)
- ☐ Uncategorized (153681/153681)
- ☒ Videos (8690/8690)

**Preferences**

- ☒ Include tagged items table (573/574)
- ☐ Only tagged items table (574/574)
- ☐ Exclude tagged items from report (573/574)

Select tags 1/1

- ☒ Include External files (0/0)
- ☐ Calculate SHA-2 (256 bit) hash
- ☒ Calculate MD5 (128 bit) hash
- ☐ Include translations
- ☐ Include known files
- ☐ Include Malware scanner results
- ☐ Include all notes

- ☐ Include Hash set results
- ☐ Redact all attachments
- ☐ Include merged items (analyzed data)
- ☐ Include merged items (data files)
- ☐ Include source info indication
- ☒ Include enrichments
- ☐ Hide extraction source indication
- ☒ Include account package
- ☒ Include Activity sensor data samples

# Cloud Storage



What data is stored in the cloud?  
AKA what can be collected?



# Public vs. Private Cloud Data

## Private

- Verification needed
- Two-factor authentication
- Google Takeout, Data Downloads



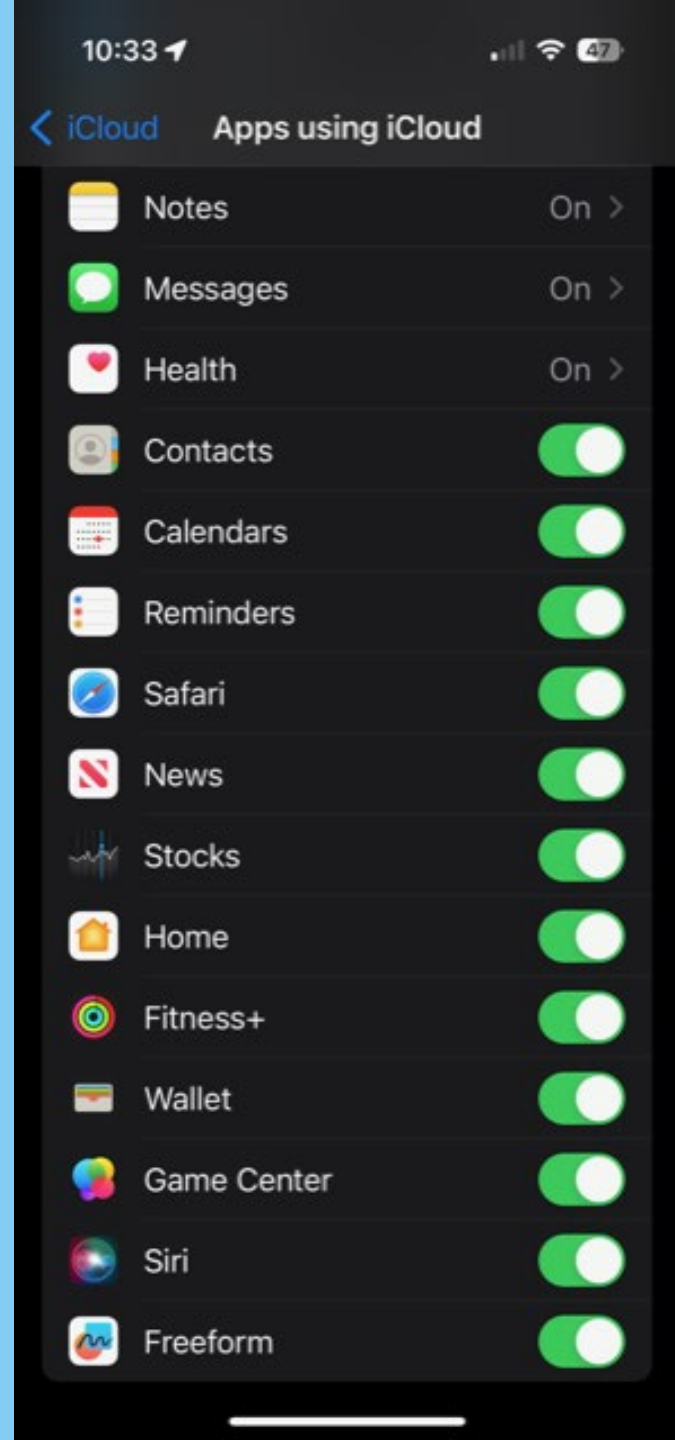
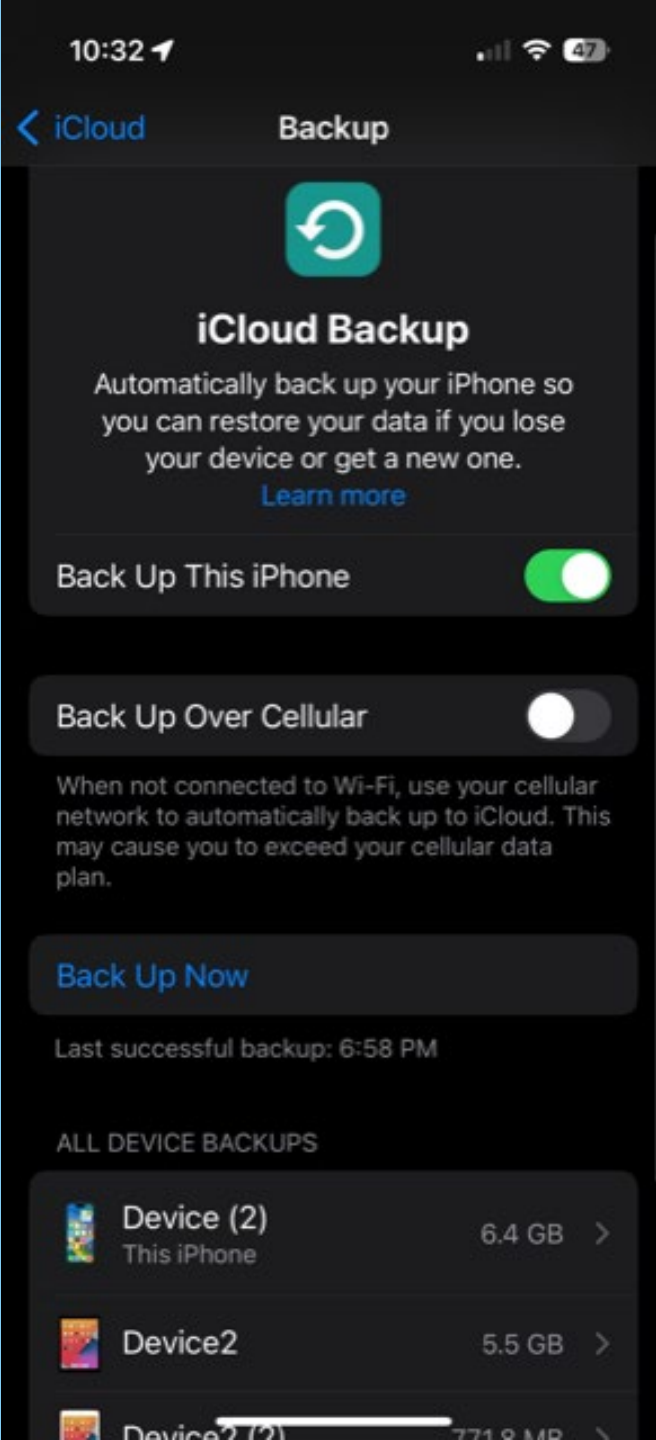
## Public

- YouTube
- Social Media
- Websites



# Cloud-based USER Data

- Backups of phone data
  - Automatic setting in iCloud
  - Whole device backups
  - Data buckets
    - Photos
    - Videos
    - Apple Notes, etc
- ***Most of the above is NOT stored encrypted by providers/would be available to law enforcement with a search warrant***



# Cloud-based USER Data

- “Content”
  - Documents, pictures, phone backups, texts, and so forth
- Most users can access this data themselves
  - Or can request the data from providers
  - Many cloud/social media allow “download your own data” option, e.g., Facebook, Google Takeout

# Cloud-based administrative data

- Who logged in, from where – what did they do? When did they do it?
- “outside the envelope” information, not as private as user content – lowered protection under Stored Communications Act
- Can come from any cloud source
  - Social media
  - Streaming services
  - IoT
  - Router/network data

# Cloud Data Acquisition Cellebrite

Private cloud data

Private Cloud Data  
Case Identifier: asdf



Search...

Supported Data Sources

























- X Social Network
- WhatsApp Web Instant Messaging
- WhatsApp Local Back... Backup Service
- WhatsApp Backup (Go... Backup Service
- WhatsApp (iCloud bac... Instant Messaging
- Vkontakte Social Network
- Viber Backup (Google ... Instant Messaging
- Viber (iCloud backup) Instant Messaging

























Account Package\manual list

























Clear All Select Tokens Import Account Package



Drag source for manual entry or  
[Import Account Package](#)

Supported Data Sources		
 X	Social Network	 
 WhatsApp Web	Instant Messaging	 
 WhatsApp Local Back...	Backup Service	 
 WhatsApp Backup (Go...	Backup Service	 
 WhatsApp (iCloud bac...	Instant Messaging	 
 VKontakte	Social Network	 
 Viber Backup (Google ...	Instant Messaging	 
 Viber (iCloud backup)	Instant Messaging	 

Supported Data Sources		
 Truth Social	Social Network	 
 TikTok	Social Network	 
 Telegram Web	Instant Messaging	 
 Telegram	Instant Messaging	 
 Snapchat	Social Network	 
 Slack	Instant Messaging	 
 Skype	Instant Messaging	 
 Samsung Cloud	Backup Service	 

Supported Data Sources		
 Ring	Security	 
 OnlyFans	Social Network	 
 OneDrive	File Host Service	 
 OkCupid	Online Dating	 
 Office365 Outlook	Email Service	 
 Office365	File Host Service	 
 Messenger	Instant Messaging	 
 MegaNz	File Host Service	 



## Supported Data Sources



Magenta Cloud  
File Host Service



LinkedIn  
Social Network



Line Backup (Google ...  
Instant Messaging



Line (iCloud backup)  
Instant Messaging



Instagram  
Social Network



IMAP  
Email Service



iCloud Photos  
File Host Service



iCloud Notes



## Supported Data Sources



iCloud Notes  
Note Taking



iCloud Messages  
Instant Messaging



iCloud Keychain  
Password Management



iCloud Find My  
Real Time Device Location



iCloud Drive  
File Host Service



iCloud Data  
User Data



iCloud Backups  
Backup Service



GooglePasswords



## Supported Data Sources



GooglePasswords  
Password Management



GoogleBooking  
Travel and E-commerce



Google Wallet  
Digital Wallet



Google Play  
Application Store



Google Photos  
File Host Service



Google MyActivity  
Usage History and Statistics
















































Google Location Histo...  
Location History



























Google Keep

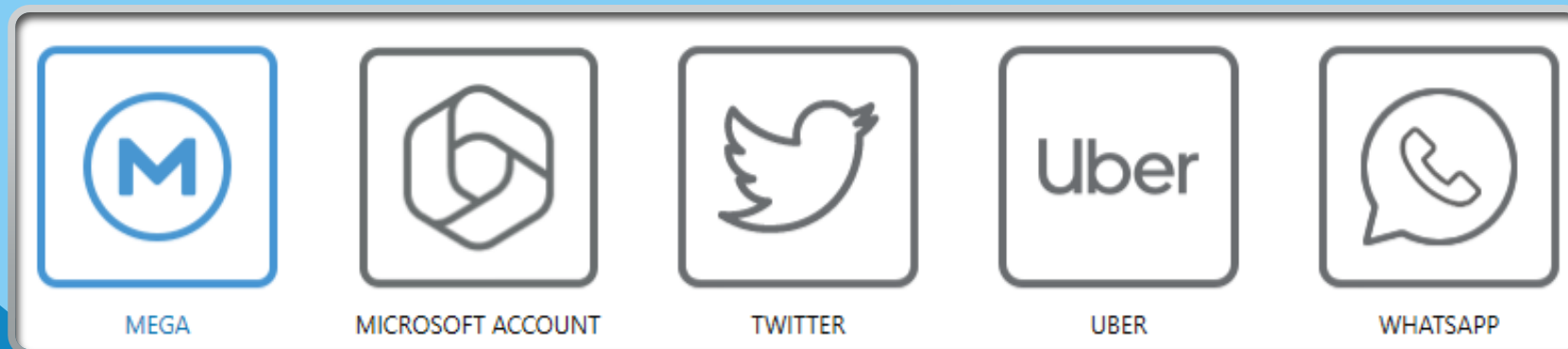
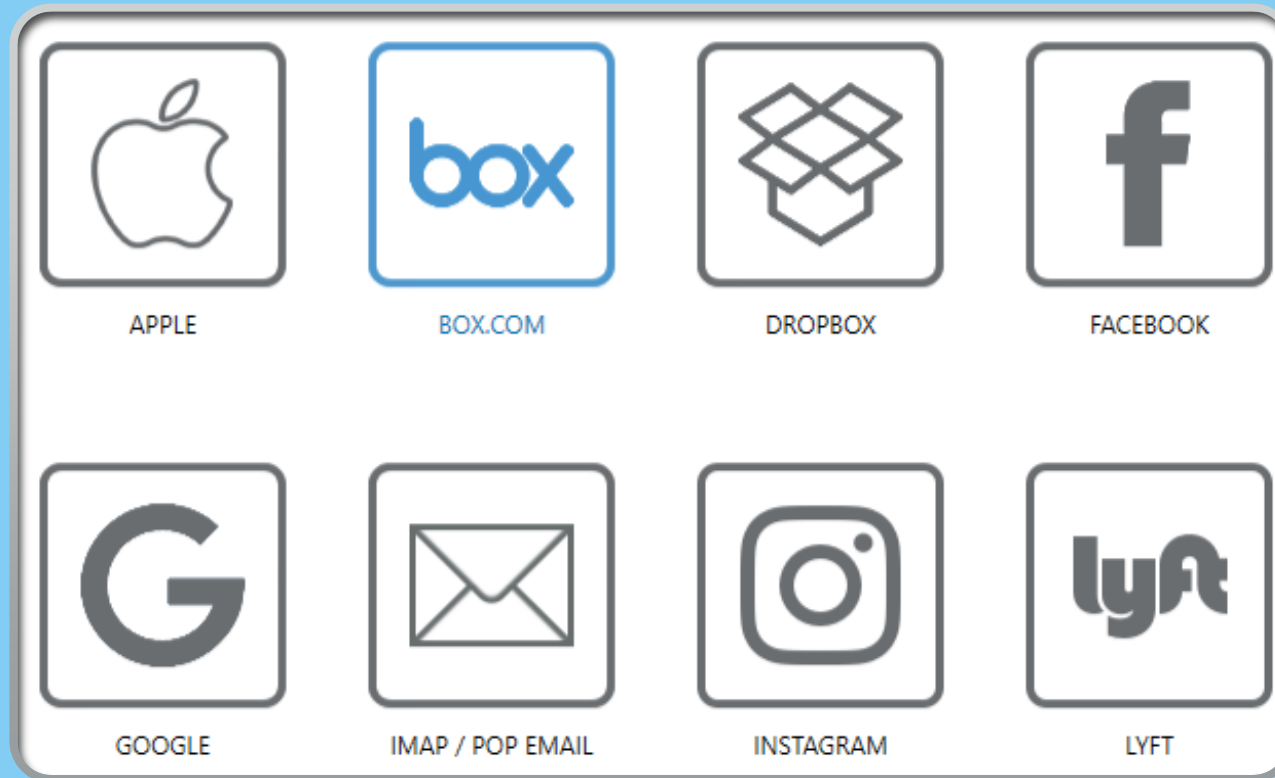


Supported Data Sources		
	Google Keep Note Taking	 
	Google Home Virtual Assistant	 
	Google Drive File Host Service	 
	Google Contacts Contact Management	 
	Google Chrome Sync Browser Data	 
	Google Calendar Calendar	 
	Google Backup Backup Service	 
	Gmail	 

Supported Data Sources		
	Gmail Email Service	 
	Fitbit Physical Activity Tracker	 
	Facebook Social Network	 
	Dropbox File Host Service	 
	DJI Go 4 Social Network	 
	Discord Instant Messaging	 
	Coinbase Cryptocurrency Wallet	 

Supported Data Sources		
	Social Network	 
	Discord Instant Messaging	 
	Coinbase Cryptocurrency Wallet	 
	Box File Host Service	 
	Booking Travel and E-commerce	 
	Bluesky Social Network	 
	Amazon Shopping Online Shopping	 
	Amazon Alexa Virtual Assistant	 

# Cloud Data Acquisition Magnet



# Common Issues

- Phone carriers DON'T keep text message content for long
- SIM cards contain little to no actual data
- Where is data backed up
  - iCloud
  - iTunes backups (local backup)
  - Type of extraction from iCloud backup
- New Operating Systems

# Passcodes

- Forensic tools/services
- Physical methods often destructive



# “MDM”

- Mobile Device Management
  - May control a single app/container on device
  - May control the entire phone
  - May allow employer to:
    - Remotely wipe the device
    - Remotely access the device
    - Monitor certain activity on the device related to an employee
  - May restrict employee's ability to copy/save data off the phone (iCloud/iTunes)
  - May also interfere with forensic process

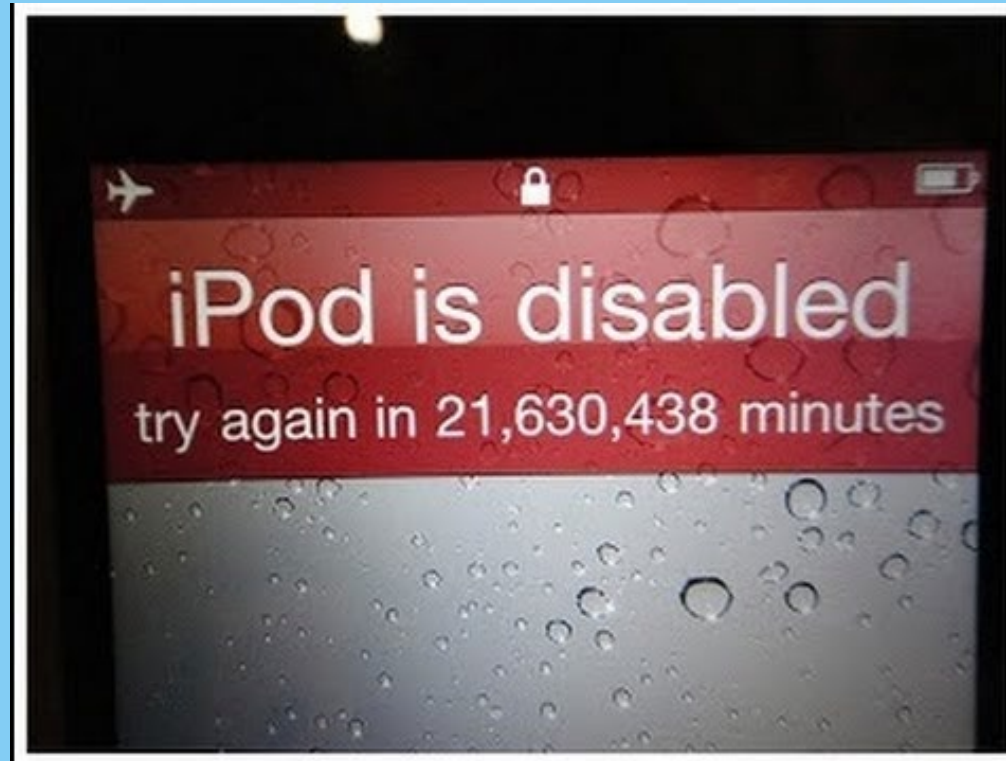
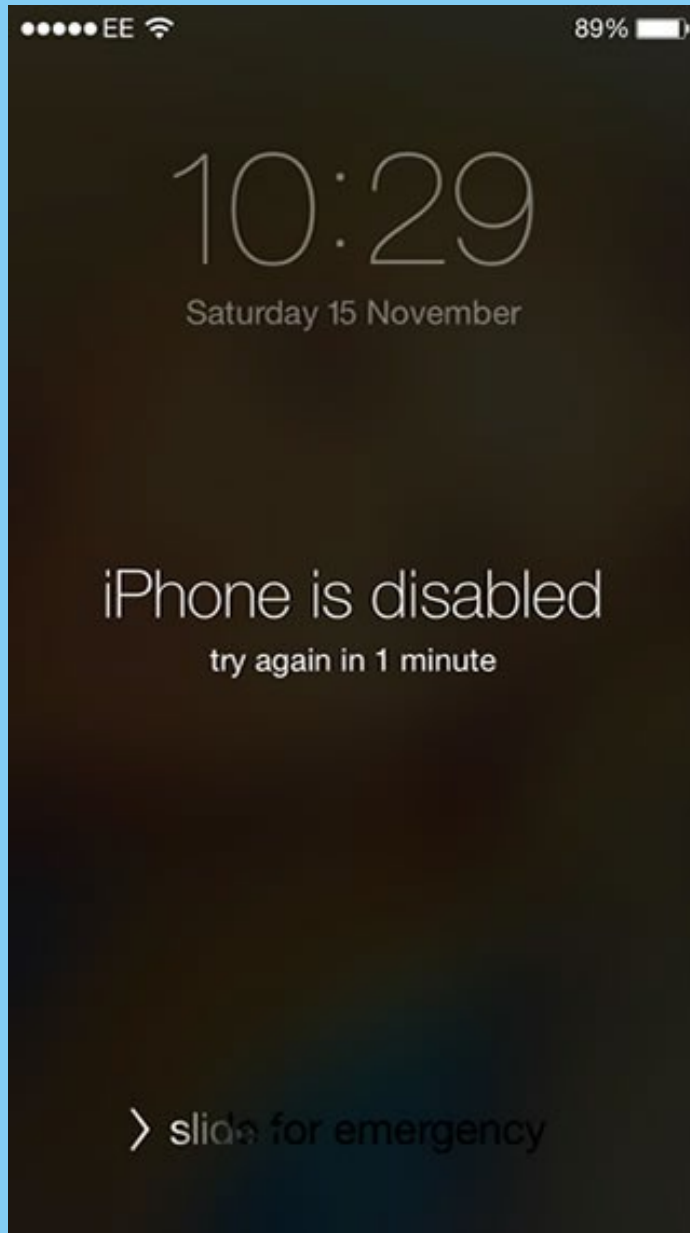


# Factory Reset

- Factory resets of newer phones DELETE the encryption key
- Render data essentially unrecoverable
- Forensic exam only to perhaps bolster spoliation claim/motion for adverse inference
- Might obtain factory reset date



# Too many failed attempts



# Digital Forensic Workflow “Loop”

- Identify Assets
- Confirm Authority to Access
  - Consent of OP, Third-Party (Employer) Ownership?, Court Order, etc.
- Collect
- Process
- Analysis
  - Review Databases
- Report
- Discuss with Attorney and Client
- Feedback/Tasking to Examiner
- *Repeat as Necessary*

# Concerns About Spoliation?

- Merely touching an electronic device may change data
  - Last accessed dates for documents, last login dates, last “written” dates
  - Auto-delete functions may need to be changed, airplane mode enabled
  - Sometimes changing things is the only way, just be able to document/articulate every step

# What happens at the end of the case?

- Examiner may continue to hold a lot of sensitive/protected data
- Consider at settlement discussions/post- trial
  - Agreement among parties as to how to dispose?
  - Retention for a certain period depending on settlement, appeal, and so forth?
- (Please) don't make the expert hunt you down for case status and disposition

The background features a dark grey area on the left filled with numerous 3D dollar signs (\$). This area is separated from the light blue area on the right by a series of diagonal lines in shades of blue and grey.

# Questions?

Edgar Fritz  
Reliance Forensics  
980-335-0710

Thank you!