



Cell Phone Forensics Capability

Achieve Positive Client Experience

Protect Client Interests

AALPI 2023



AZ Lic. 1784260

Introduction

- Lonnie Dworkin
 - CompuFor Forensics and Forensics4U
 - Scottsdale AZ
 - Digital Forensic Examiner
 - Prog. Mgmt. Professional & Electrical Engineer
 - 30+ years of experience in communications, systems, computers, and software



Desired Learning Objectives

1. CDRs vs Cell Phone Extractions
2. Identify Evidence Opportunities
3. Safely Collect Evidence
4. Cell Phone Extraction Types
5. Manage Client Expectations
6. Search a Cell Phone Extraction
7. Generate a Filtered Cell Phone Report

Desired Learning Objectives

1. **CDRs vs Cell Phone Extractions**
2. Identify Evidence Opportunities
3. Safely Collect Evidence
4. Cell Phone Extraction Types
5. Manage Client Expectations
6. Search a Cell Phone Extraction
7. Generate a Filtered Cell Phone Report

CDRs vs Cell Phone Extractions

Call Detail Records (CDR)	Cell Phone Extraction
Obtained from: Sprint, Verizon, T-Mobile AT&T etc.	Obtained from cell phone or backup
Doesn't require cell phone	Requires cell phone
Location of 1 st and last cell tower connections	Approximate location of cell phone (Towers, Wifi, EXIF
SMS events, but not content	SMS, MMS message content
Report contains: <ul style="list-style-type: none"> 1. Tower location plots w/azimuth, and approximate ranging to towers. 2. Voice and SMS history 	Report contains: <ul style="list-style-type: none"> 1. Geo-location data (photos, other) 2. Voice and Various Messaging App Content 3. Installed applications 4. 3rd Party app content 5. Internet history 6. Log files 7. Other

Desired Learning Objectives

1. CDRs vs Cell Phone Extractions
- 2. Identify Evidence Opportunities**
3. Safely Collect Evidence
4. Cell Phone Extraction Types
5. Manage Client Expectations
6. Search a Cell Phone Extraction
7. Generate a Filtered Cell Phone Report

Identify Evidence Opportunities

- No cell phone, no problem
- Check for backups on computers (i.e. iTunes, Android 3rd party apps)
- iCloud backups
- Google account backups
- Forgotten older devices
- Devices from the other participants

Desired Learning Objectives

1. CDRs vs Cell Phone Extractions
2. Identify Evidence Opportunities
- 3. Safely Collect Evidence**
4. Cell Phone Extraction Types
5. Manage Client Expectations
6. Search a Cell Phone Extraction
7. Generate a Filtered Cell Phone Report

Safely Collect evidence

- If powered on, place in "Airplane" mode (AP)
- If powered off, can leave powered off
- If powered on but don't currently have passcode to turn off, use Faraday bag.



Cell / Tablet Evidence Preservation

- Place device in “Airplane” mode, if powered on.
 - Safeguard against remote wipe
 - Safe guard against remote sync and delete
- If powered off, leave off.
 - Powered-off, may not be sufficient !!
- Recommended practice,
 - Use RF shield for storage and transport.
- Minimize interacting with device
 - Don’t risk deleting
 - Don’t create additional evidence (i.e. accidental photos)

Maintain Event Log

- Document device:
 - Serial #
 - Make and Model
 - Storage capacity
 - Date/time, received / released
 - Date & Time placed into AP mode
 - How it was secured
 - Passcode, swipe code
 - General physical condition of device
- Watch out for bloated Li batteries



Desired Learning Objectives

1. CDRs vs Cell Phone Extractions
2. Identify Evidence Opportunities
3. Safely Collect Evidence
- 4. Cell Phone Extraction Types**
5. Manage Client Expectations
6. Search a Cell Phone Extraction
7. Generate a Filtered Cell Phone Report

Extraction Types

- Not all methods are supported on all devices
- Logical
- File System
- Physical
- Alt-Physical Methods: Rooting and jail-breaking
 - Runs the risk of “bricking” cell phone.
 - Not recommended.

Desired Learning Objectives

1. CDRs vs Cell Phone Extractions
2. Identify Evidence Opportunities
3. Safely Collect Evidence
4. Cell Phone Extraction Types
- 5. Manage Client Expectations**
6. Search a Cell Phone Extraction
7. Generate a Filtered Cell Phone Report

Manage Client Expectations

- CSI Effect
- ***“It Depends”***
- **Can all email be extracted?**
 - Depends on:
 - installed webkits
 - model and firmware version
 - installed security certificates
 - available extraction methods
 - ***Alt-Method: Preserve email directly via ISP (Google, Proton, Outlook)***
- **Can deleted text messages be recovered?**
 - Native apps– database sync / vacuum command
 - *Caution when using unvetted recovery applications, avoid affecting SQLite db.*
 - Recovery of messages from 3rd party apps (FB Messenger, WhatsApp, etc.)

Manage Client Expectations


- **Can passcodes be broken or avoided?**
 - Some iPhone and Android models and firmware releases have potential
 - Extraction techniques
 - Brute-force attacks
 - ***Don't get locked out !!***
- Forensic Tools Publish Compatibility
 - Supported Devices and App Decoding
 - Research device ahead of time
 - Documented extraction and decoding support is not always correct.
- Tools and capabilities are always changing.



Photo and Video Metadata

- Exchangeable Image File (EXIF) Data
 - Used with still, video, audio and other media formats
 - Standard tags
 - device information
 - Image information
 - Location information
 - Not all tags always populated
 - Requires device GPS to be operational

Photo Metadata - example

320	Name: 20180331_213536.jpg Path: Samsung GSM_SM-G965U Galaxy S9+.zip/sdcard/DCIM/Camera/20180331_213536.jpg MD5: 0e2673662fdb2fa18c11335f11cdd371 Duplicates(2)	Size (bytes): 6931148 Modified: 12/31/1969 5:00:00 PM(UTC-7) Source Extraction File System (2), Logical Meta Data: Camera Make: samsung Camera Model: SM-G965U Capture Time: 3/31/2018 9:35:36 PM Pixel resolution: 4032x1960 Resolution: 72x72 (Unit: Inch) Orientation: Horizontal (normal) Lat/Lon: 33.437754 / -112.439690		Intact
-----	---	---	---	--------

Video Metadata - example

- Doesn't require user action
- Requires active GPS

(33.437900, -112.439700, 301.809)	Description: com.apple.quicktime.location.ISO6709 Name: IMG_8069.MOV Time: 12/21/2017 12:49:02 PM(UTC+0) Elevation (meters): 301.81 Source Extraction: File System		Media Locations
-----------------------------------	--	--	-----------------

Wireless Network

- Doesn't require user action
- Doesn't require active GPS
- BSSID can indicate general location
 - Basic Service Set Identifier
- Operational GPS add accuracy

Locations (6)			Events indicated in red are for data that is not extracted from the device.			
Name	Description	Time	Latitude	Longitude	Map Address	Type
8C25FE	BSSID: 90:9D:7D:8C:25:FE SSID: 8C25FE	9/15/2017 3:39:55 PM(UTC-5)	33.4773191582	-112.17314152132	5234 W Cambridge Ave, Phoenix, AZ 85035	Wireless Network Last Auto Connection
8C25FE	BSSID: 90:9D:7D:8C:25:FE SSID: 8C25FE	9/15/2017 1:17:06 PM(UTC-5)	33.4773191582	-112.17314152132	5234 W Cambridge Ave, Phoenix, AZ 85035	Wireless Network Last Connection
Samsung Galaxy Note 4 7000	BSSID: C0:BD:D1:38:48:9A SSID: Samsung Galaxy Note 4 7000	11/28/2016 1:25:56 AM(UTC-6)	33.48401006583	-112.13472659769	3100 N 35th Ave, Phoenix, AZ 85017	Wireless Network Last Auto Connection
Samsung Galaxy Note 4 7000	BSSID: C0:BD:D1:38:48:9A SSID: Samsung Galaxy Note 4 7000	11/28/2016 1:02:24 AM(UTC-6)	33.48401006583	-112.13472659769	3100 N 35th Ave, Phoenix, AZ 85017	Wireless Network Last Connection
CenturyLink3246	BSSID: B2:B2:DC:4E:9F:18 SSID: CenturyLink3246	11/27/2016 5:12:49 PM(UTC-6)	52.35304204426	4.90863616038	Amsteldijk 723A, 1074 Amsterdam, Netherlands	Wireless Network Last Auto Connection




Desired Learning Objectives

1. CDRs vs Cell Phone Extractions
2. Identify Evidence Opportunities
3. Safely Collect Evidence
4. Cell Phone Extraction Types
5. Manage Client Expectations
- 6. Search a Cell Phone Extraction**
7. Generate a Filtered Cell Phone Report

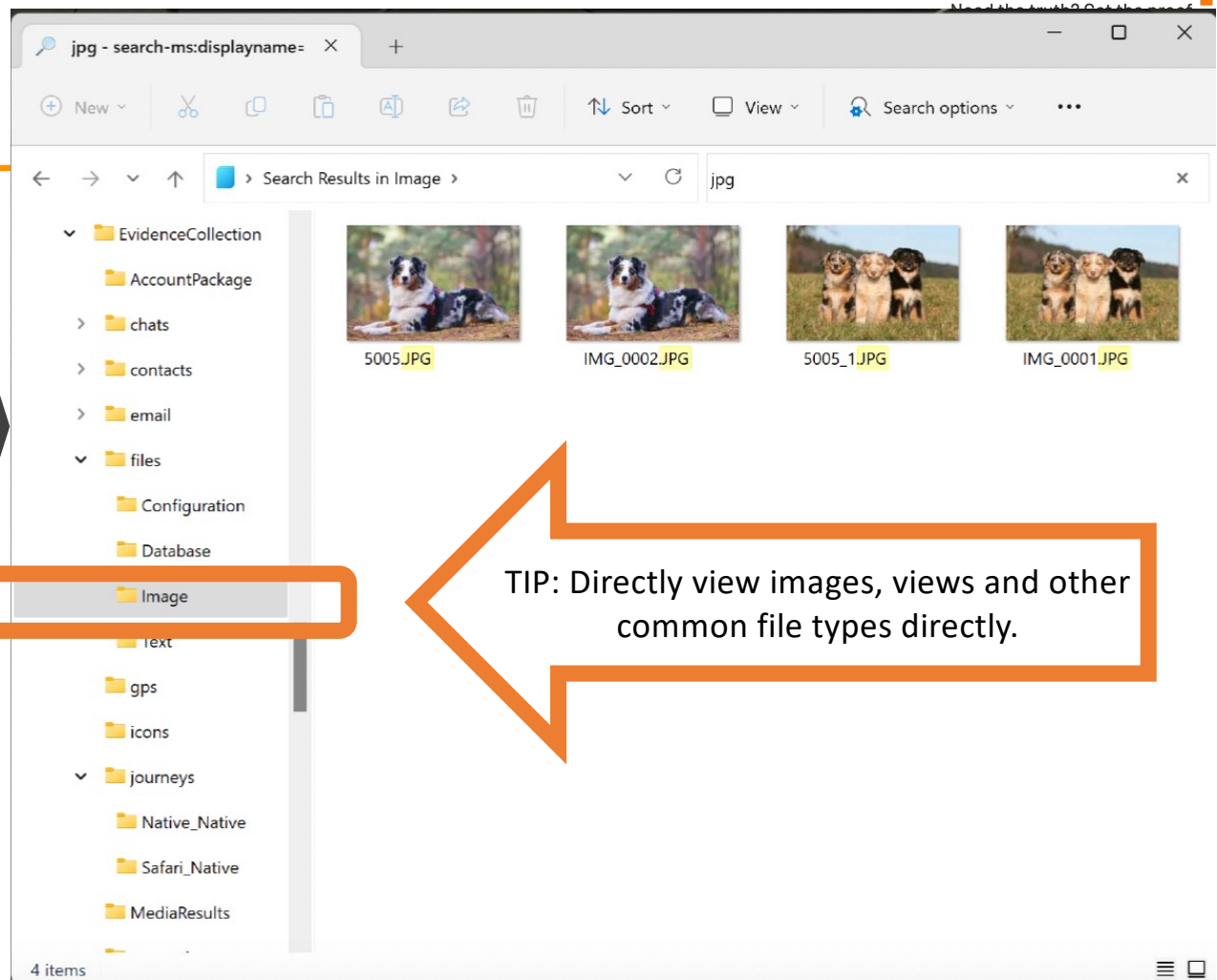
Cellebrite Cell Phone Reports

- Support various report formats
 - Excel
 - PDF
 - Cellebrite Reader(*.UFDR)
 - Others
- PDF
 - Easy to search
 - Use PDF Reader
 - Web Browser default not recommended
 - Difficult to customize for disclosure
 - Slow searching for large page counts (Few pages to many thousands)

Cellebrite PDF Report File Structure

Name	Date modified	Type	Size
AccountPackage	8/25/2023 11:57 PM	File folder	
chats	8/25/2023 11:38 PM	File folder	
contacts	8/25/2023 11:38 PM	File folder	
email	8/25/2023 11:38 PM	File folder	
files	8/25/2023 11:38 PM	File folder	
gps	8/25/2023 11:52 PM	File folder	
icons	8/25/2023 11:50 PM	File folder	
journeys	8/25/2023 11:38 PM	File folder	
MediaResults	8/25/2023 11:39 PM	File folder	
party_photos	8/25/2023 11:38 PM	File folder	
Passwords	8/25/2023 11:52 PM	File folder	
resources	8/25/2023 11:52 PM	File folder	
thumbnails	8/25/2023 11:38 PM	File folder	
 CellebriteReader.exe	8/1/2023 12:30 PM	Application	565,952 KB
 Forensics4U Demo.pdf	8/25/2023 11:57 PM	Firefox PDF Document	101,226 KB
 Forensics4U Demo.ufdr	8/25/2023 11:50 PM	UFDR File	3,084,060 KB

Cellebrite PDF Report File Structure



Sample Cell Phone Extraction Report

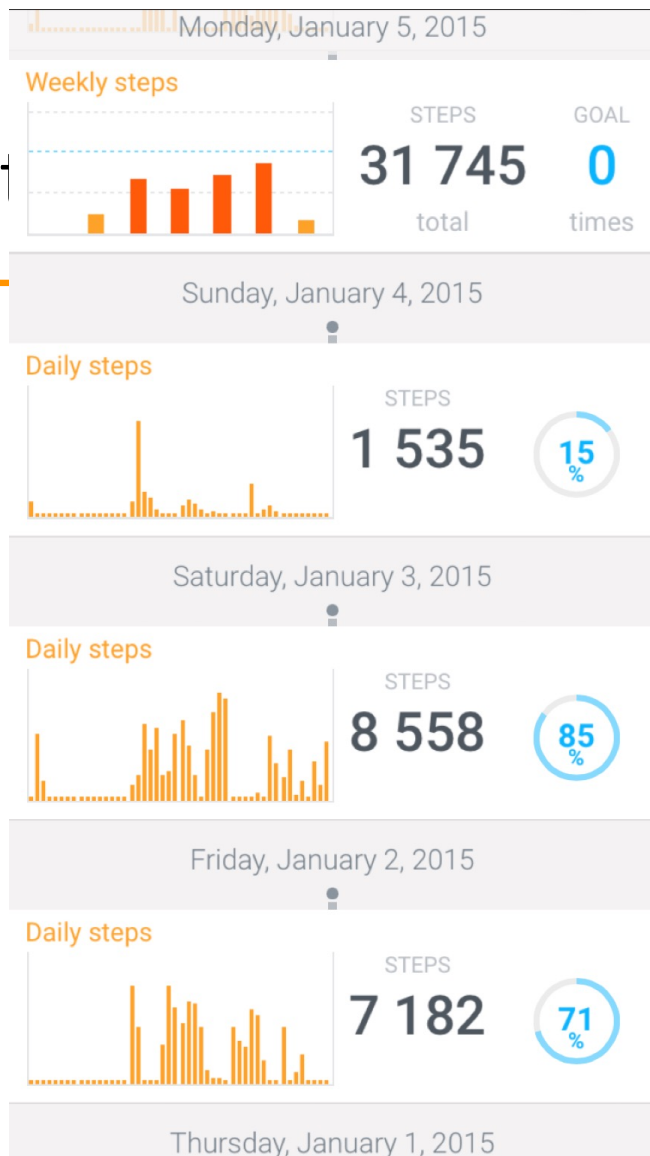
Summary

Cellebrite Physical Analyzer version	7.54.1.7
Report creation time	2/5/2022 12:03:39 PM -07:00
Time zone settings (UTC)	(UTC-07:00) Phoenix (America)
Examiner name	Examiner


























Source Extraction

Advanced Logical	
Extraction start date/time	2/5/2022 11:28:54 AM(UTC-7)
Extraction end date/time	2/5/2022 11:29:44 AM(UTC-7)
Unit identifier	467644795
UFED version	7.54.0.444
Internal version	7.54.0.444
Selected manufacturer	Apple
Selected device name	iPhone XR (A1984)
Machine name	DESKTOP-S855FCA
Connection type	Cable No. 210
Is encrypted	Encrypted by Physical/Logical Analyzer during the extraction process for user credentials information
Backup password	1234
Extraction type	Advanced Logical
Extraction ID	C3DFAAAF-8807-4135-B671-F7325C774233
Extraction (UFD) file data integrity	Intact

Act



Contents

Type	Included in report	Total
 Activity Sensor Data	2	2
 Calendar	156	156
 Contacts	1	1
 Cookies	127	127
 Device Connectivity	35	35
 Installed Applications	489	489
 Instant Messages	1	1
 Journeys	11	11
 Locations	915	915
 Notes	6 (2 Deleted)	6 (2 Deleted)
 Passwords	29	29
 Recordings	6	6
 Searched Items	83	83
 User Accounts	2	2
 Web Bookmarks	7	7
 Web History	129	129
 Timeline	1428 (3 Deleted)	1428 (3 Deleted)
 Data Files	836	836
 Audio	7	7
 Configurations	473	473
 Databases	99	99
 Images	126	126
 Text	3	3
 Uncategorized	110	110
 Videos	18	18

Home

Tools

Apple_iPhone XR.... x

?🔔

💾★🔄🖨️🗨️↶↷

182 / 485

👉🤲⊖⊕100%

📐📄💬✍️🎨🗑️↺🔗

📁

Bookmarks ×
☰🔒

🔖 Summary

🔖 Source Extraction

🔖 Device Information

🔖 Image Hash Details

🔖 Plugins

🔖 Contents

🔖 Activity Sensor Data

🔖 Calendar

🔖 Contacts

🔖 Cookies

🔖 Device Connectivity

🔖 Installed Applications

🔖 Instant Messages

🔖 GPS

🔖 Journeys

🔖 Locations

🔖 Notes

🔖 Passwords

Locations (915)

🌐 Open in Google Earth

📍 Open in Google Maps

#	Origin	Position	Info	Confidence	Category	Deleted
1		(33.625525, -111.913961)	Description: com.apple.locationd.bundle-/System/Library/LocationBundles/Routine.bundle Time: 7/5/2022 9:26:36 AM(UTC-7) Source: Source file: iPhone/root/Library/Caches/locationd/con-solidated.db : 0x8FD7 (Table: Fences; Size: 53248 bytes)		Reminder Locations	
2		(33.625525, -111.913961)	Type: Reminder Precision: 250 Time: 7/5/2022 9:26:36 AM(UTC-7) Source: Source file: iPhone/root/Library/Caches/locationd/con-solidated.db : 0x8FD7 (Table: Fences; Size: 53248 bytes)		Reminder Locations	
3		(33.625300, -111.913900, 450.591)	Time: 7/1/2022 3:31:13 PM(UTC-7) Elevation (meters): 450.59 Source: Source file: iPhone/mobile/Media/DCIM/100APPLE/I MG_0021.MOV : 0x138DCB (Size: 1282699 bytes)		Media Locations	
4		(33.625300, -111.913900, 451.365)	Time: 7/1/2022 3:31:01 PM(UTC-7) Elevation (meters): 451.37 Source: Source file: iPhone/mobile/Media/DCIM/100APPLE/I MG_0020.MOV : 0x881A40 (Size: 8920832 bytes)		Media Locations	
5		(33.625300, -111.913900, 450.644)	Time: 7/1/2022 3:30:18 PM(UTC-7) Elevation (meters): 450.64 Source: Source file: iPhone/mobile/Media/DCIM/100APPLE/I MG_0019.MOV : 0x4CBA4E (Size: 530046 bytes)		Media Locations	

Apple_iPhone XR.pdf

HomeToolsApple_iPhone XR.... x

182 / 485

100%

Open in Google EarthOpen in Google Maps

Bookmarks

SummarySource ExtractionDevice InformationImage Hash DetailsPluginsContentsActivity Sensor DataCalendarContactsCookiesDevice ConnectivityInstalled ApplicationsInstant MessagesGPSJourneysLocationsNotesPasswords

Locations (915)

#	Origin	Position	Info	Confidence	Category	Deleted
1		(33.625525, -111.913961)	Description: com.apple.locationd.bundle- /System/Library/LocationBundles/Routine. bundle Time: 7/5/2022 9:26:36 AM(UTC-7) Source: Source file: iPhone/root/Library/Caches/locationd/con solidated.db : 0x8FD7 (Table: Fences; Size: 53248 bytes)		Reminder Locations	
2		(33.625525, -111.913961)	Type: Reminder Precision: 250		Reminder Locations	

33.625525, -111.913961

33.625300, -111.913900

Base map

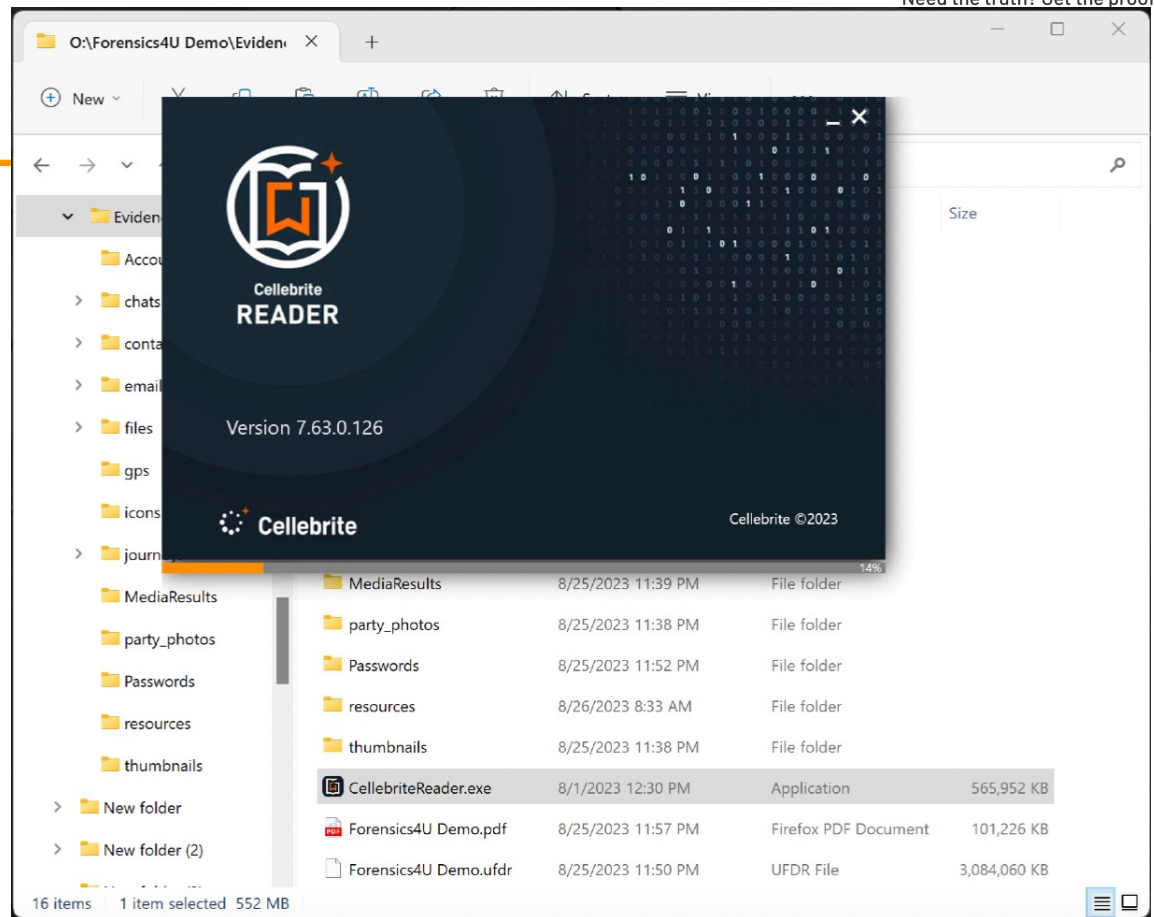
R & D Precision Welding & FabUS Tax

E Greenway Rd

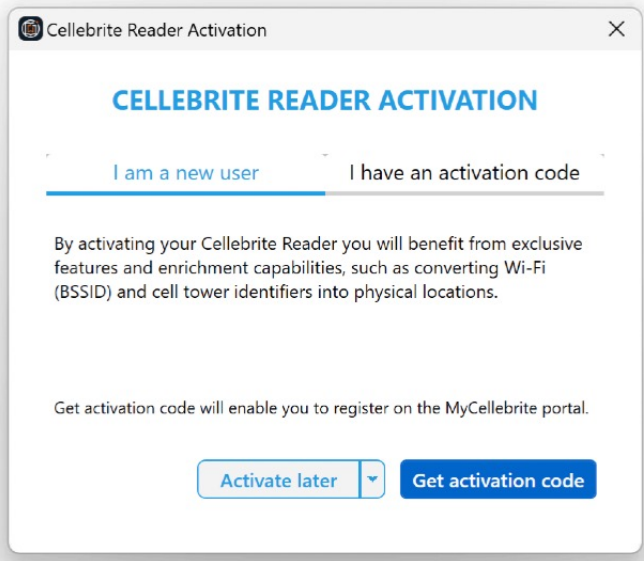
Cellebrite Reader

- File extension *.UFDR
- Requires Cellebrite Reader
 - Included with UFDR file
 - Enables custom report generation in any of Cellebrite's supported formats
 - Fast searching
 - Perpetual Tagging Supported
 - *May need to set time zone.*
 - *Deselect "Check All"*

Launch
Cellebrite
Reader



POP-UP:
“Activate
Later”



The screenshot shows a web browser window titled "Cellebrite Reader Activation". The page has a header "CELLEBRITE READER ACTIVATION" in blue. Below the header are two tabs: "I am a new user" (selected) and "I have an activation code". The main text explains that activating the reader provides exclusive features like converting Wi-Fi (BSSID) and cell tower identifiers into physical locations. At the bottom, there are two buttons: "Activate later" (with a dropdown arrow) and "Get activation code".

Cellebrite Reader Activation

CELLEBRITE READER ACTIVATION

[I am a new user](#) | [I have an activation code](#)

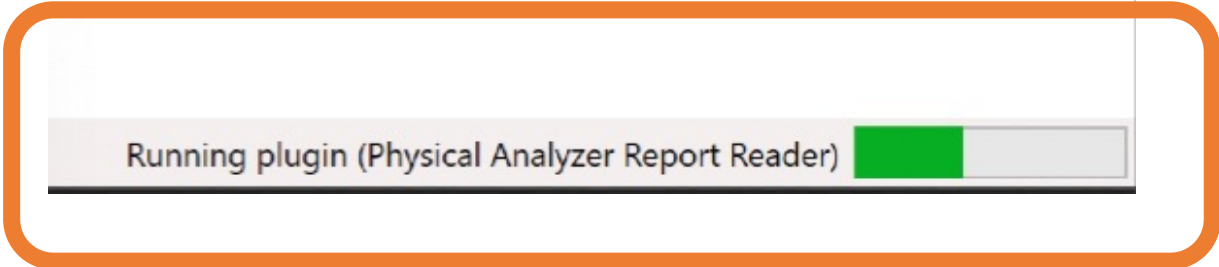
By activating your Cellebrite Reader you will benefit from exclusive features and enrichment capabilities, such as converting Wi-Fi (BSSID) and cell tower identifiers into physical locations.

Get activation code will enable you to register on the MyCellebrite portal.

[Activate later](#) [Get activation code](#)

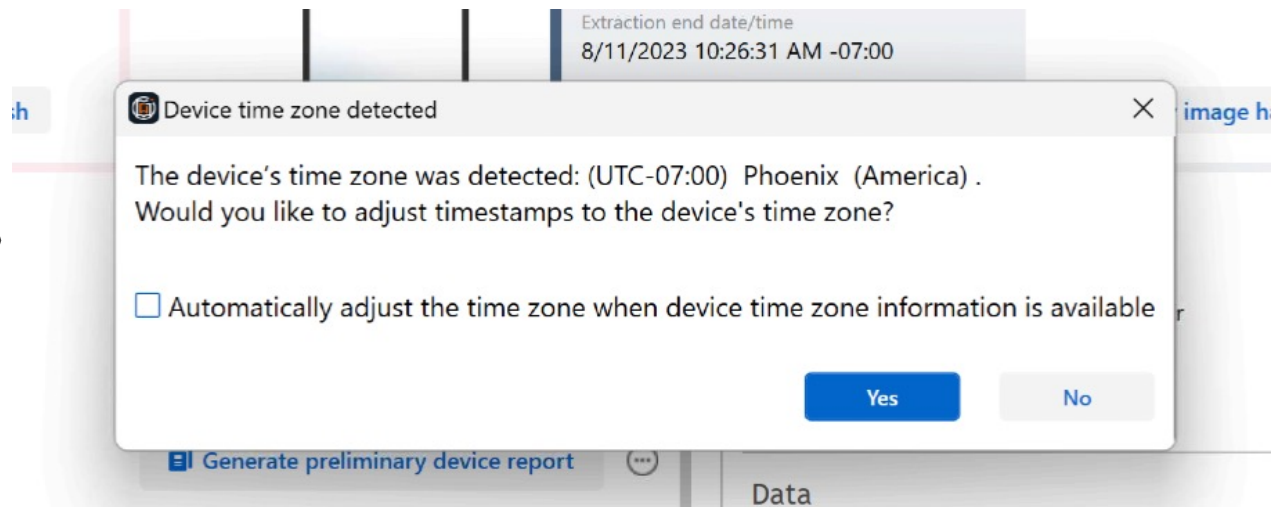
POP-UP:
“Activate
Later”

- UFDR file should load automatically
- Load progress bar – lower right corner
- May take awhile
- Minimum recommended computer hardware
 - Windows 10 / 11
 - I5 or better
 - 8 GB RAM or better

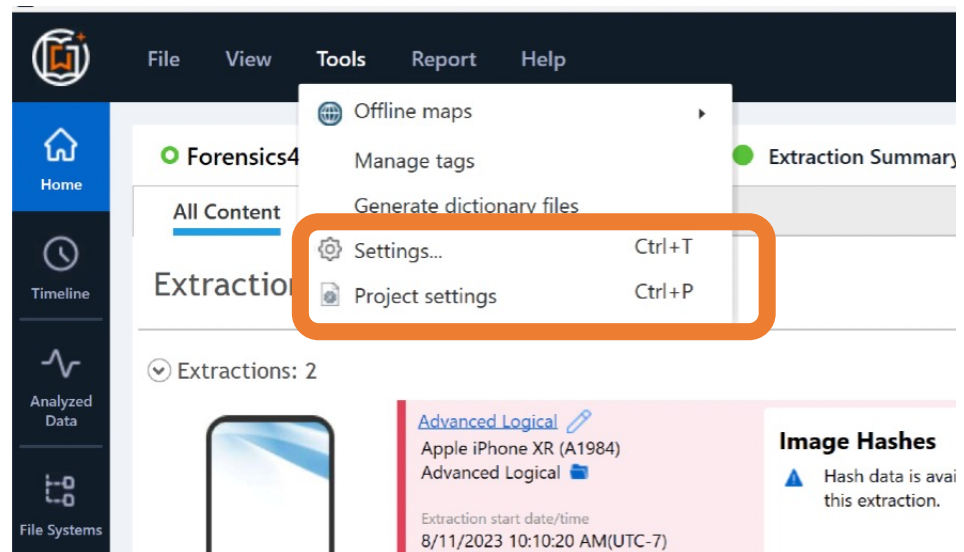


Running plugin (Physical Analyzer Report Reader)

POP-UP: Confirm Time-Zone



Tools Settings



Settings:
Check all ...

The screenshot shows the 'Settings' window of a forensic application. The left sidebar contains icons for 'General Settings' (selected), 'Data Files', 'Timeline', 'Interface', 'Additional Report Fields', and 'Report Defaults'. The main panel displays various configuration options:

- ☒ Use daylight savings (Daylight Saving Time ...)
- Duplicate rules**
 - ☒ Show main items only
 - ☐ Show group of similar items (Group secondary items under main items)
 - ☐ Show all items
- Export**
 - ☐ Adjust File and Filesystem timestamps to local machine Date and Time settings
 - CSV
 - Encoding: UTF-16
 - Separator: Tab
- Temp folder**
 - Default Location: C:\Users\compufor\AppData\Local\Temp\ (Change)
- Dictionary files**
 - Default Location: C:\Users\compufor\Documents (Change)
- Image hash verification**
 - ☐ Automatically verify images on project load
- Extractions**
 - ☒ Suggest restoring a session file when its corresponding extraction is loaded
- Thumbnail cache**
 - ☒ Save project cached thumbnails. (10)
 - ☒ Load thumbnail cache to memory
- Views** (highlighted with an orange box)
 - ☒ Check all entities by default
 - ☐ Expand all entities by default
- Map**
 - ☒ Use online maps
 - ☐ Use offline maps Port: 3000

At the bottom are buttons for 'Export...', 'Import...', 'OK', and 'Cancel'.

Settings:
Check all ...

RUN DEMO

Desired Learning Objectives

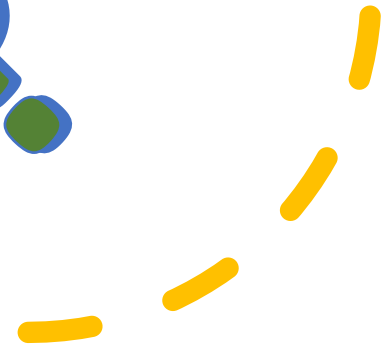
1. CDRs vs Cell Phone Extractions
2. Identify Evidence Opportunities
3. Safely Collect Evidence
4. Cell Phone Extraction Types
5. Manage Client Expectations
6. Search a Cell Phone Extraction
- 7. Generate a Filtered Cell Phone Report**

Create Report with Cellebrite Reader

- Confirm Time Zone
- Use “Tags” to “Check” records for inclusion
- Customize Report Title Page
- Use Wizard to export “Checked” records.
- Save work before exiting viewer.

Desired
Learning
Objectives

Questions ?



Forensics4U LLC – Flat Fee Forensic Images

- Forensics4U mission to enable those who need access to court-accepted forensic extractions / image of their mobile device, USB thumb drive, or computer hard drive.
- Forensics4U enables the customer to manage their own forensic data and analysis costs.
- Forensics4U makes it easy!
 - Just complete an online request form, along with a services agreement and checkout. You'll receive a prepaid shipping label to ship your device to Forensics4U.
 - You will be kept informed every step of the way. Once your device arrives at our labs, we'll perform the forensic extraction / imaging and save the results onto an external Forensics4U drive.
 - We will return your device, along with the forensic extraction, extraction process report, and a pdf report summarizing key information present on your device.
- We include our easy-to-use guide to help you perform keywords searches against the PDF report.
- Visit our website, www.Forensics4U.com, to order service.