IRIS LLC

2026 CELLEBRITE READER

QUICK START GUIDE

Essential Guide to Cellebrite Reports

irisinvestigations.com

QUICK START USER GUIDE FOR CELLEBRITE EXTRACTION REPORTS

Introduction

This Quick Start Guide is designed to assist criminal defense teams in the accurate and efficient review of cell phone extraction reports generated using Cellebrite software. It provides investigators and attorneys with clear, step-by-step guidance on how to open, navigate, search, and analyze extraction data using the Cellebrite Reader application. The guide also addresses how to identify hidden or missing data, recognize analytical limitations, and generate customized reports for investigation, litigation, and trial.

By the defense, for the defense

Developed by cross-trained criminal defense investigators at IRIS LLC and presented in support of the Digital Innocence Initiative, this guide is grounded in real-world defense casework. It reflects recurring digital evidence issues encountered in criminal cases, where incomplete disclosures, misunderstood data, or misinterpretation of mobile device evidence can materially affect case outcomes, including contributing to wrongful convictions.

This guide has been updated to reflect the current version of the Cellebrite Reader application. For assistance with prior versions, please contact IRIS LLC at 860-522-0001. The most recent Cellebrite Reader Manual is available at **digitalevidencetoolbox.com**.

© 2026 IRIS LLC

All rights reserved. This book or any portion thereof
may not be reproduced or used in any manner whatsoever
without the express written permission of the publisher
except for the use of brief quotations in a book review

TABLE OF CONTENTS

1. Opening Reports and Setting Time Zones

Cellebrite Reader, reports and components……..…..... 4
Opening reports…….……..... 5
Time zone settings……..……..…..... 7

2. Dashboard, Data Tabs and Basic Navigation

Dashboard View and Detail View ……..……..…..... 8
Data display areas.....……..……...…..... 9
Extraction information and device details ……..……...…..... 10
Navigating the dashboard ……..……...…..... 10

3. Getting Started and Keeping Organized

Preliminary device report ……..……...…..... 11
Using the investigator checklist ……..……...…..... 11

4. Searching & Filtering

Timeline search and checking settings……..……..... 12
Global, advanced and individual tab searches..... 14
Applying filters……..…..... 15
Location data..... 16

5. Tagging, Saving and Reporting

Tagging and bookmarking data…….…..... 16
Saving a project session file……..... 19
Loading multiple extractions……. 19
Creating custom reports……..... 20

6. Extraction Levels, Hidden Data and Requesting Reports

Forensic process.....……..... 23
Understanding different extraction levels .....……. 23
Uncovering hidden data 23
Requesting reports…….……..... 24

7. Expediting Analysis and Working with Experts

Investigator Checklist..... 25
Glossary..... 26
Tips to expedite..... 29

1. OPENING REPORTS AND SETTING TIME ZONES

Cellebrite Reader Program

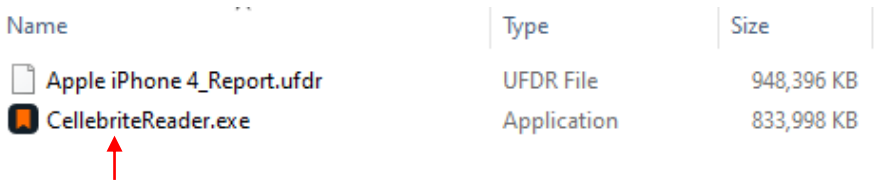
The Cellebrite UFED (Universal Forensic Extraction Device) software allows forensic examiners to create a searchable copy of the original extraction in a format for law enforcement called a Cellebrite Reader report. For more information about the forensic extraction process and different levels of extraction, see page **23**.

The Cellebrite Reader program is needed to open the forensic extraction file in a custom dashboard that allows the user to conduct advanced searches, filtering, and timeline queries. Data of interest can be tagged, project session can be saved to pick up where you left off, and custom reports can be generated.

Cellebrite Reader Report Components

The Cellebrite Reader report is a file with file extension (.ufdr). The Cellebrite Reader application (.exe) opens the UFDR report file.

Example



Opening Report - Step by Step Process

Step 1: Click on the Cellebrite Reader program icon.
Step 2: Click through opening prompts.
Step 3: Verify time settings.

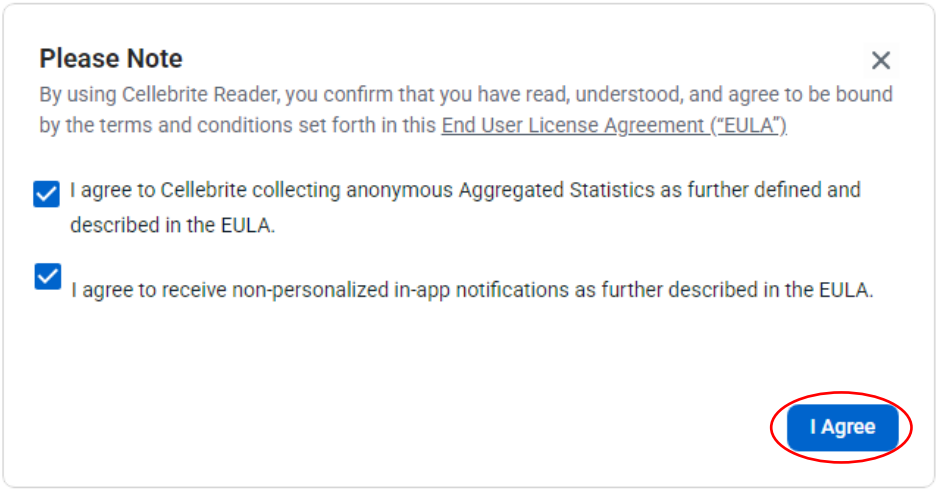
Step 1: Launch Reader Program

Click on the Cellebrite Reader application CellebriteReader and the application will begin to open. This is a large program and may take up to a minute or more to open. A progress bar at the bottom of the application screen will indicate the status.

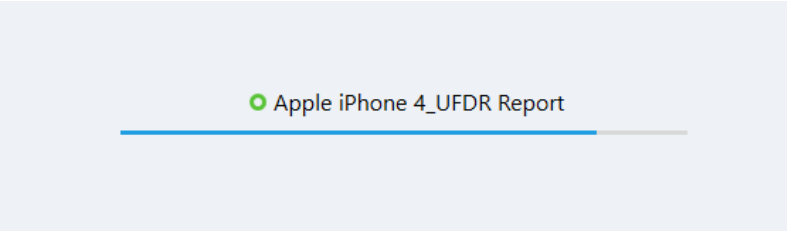
Step 2: Click Through Opening Prompts

Terms and Conditions Prompt

Click "***I Agree***"

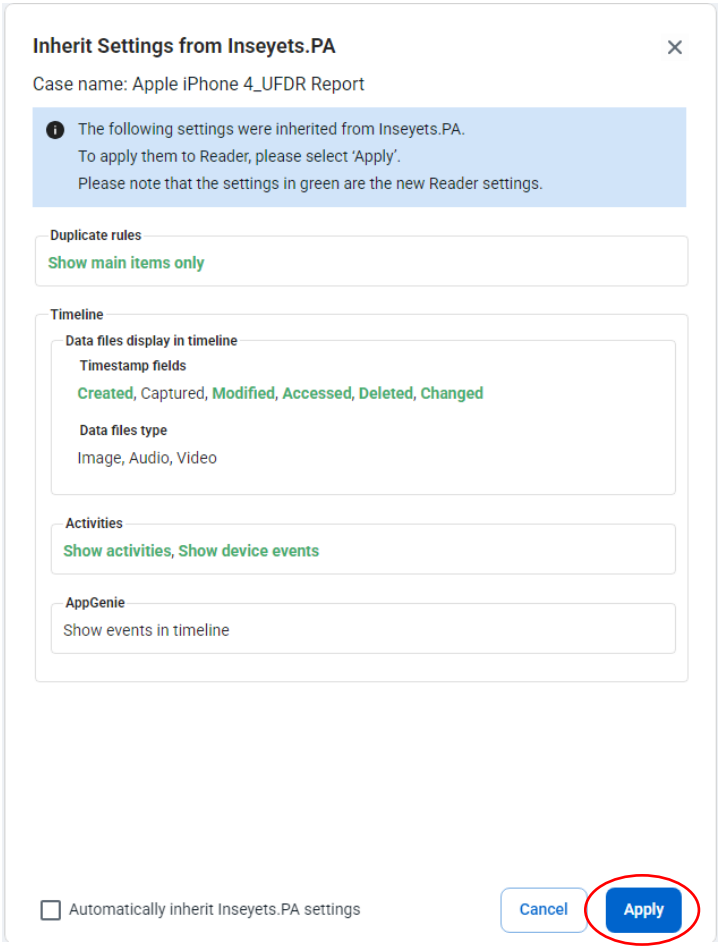


After the Cellebrite Reader application opens, the UFDR report file in the same folder will open, but could take several minutes for the report to open depending on the amount of data.



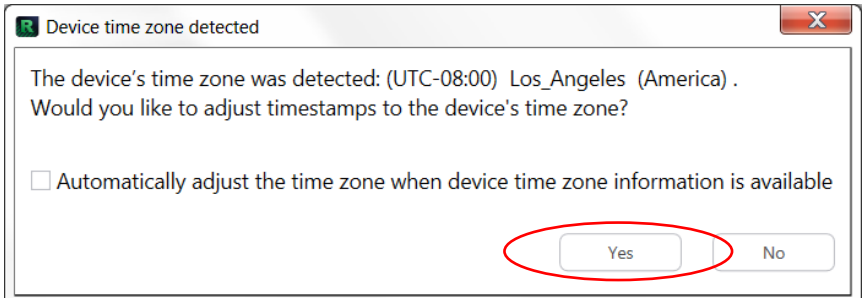
Inherit Settings Prompt

To inherit Inseyets PA settings click "***Apply***".



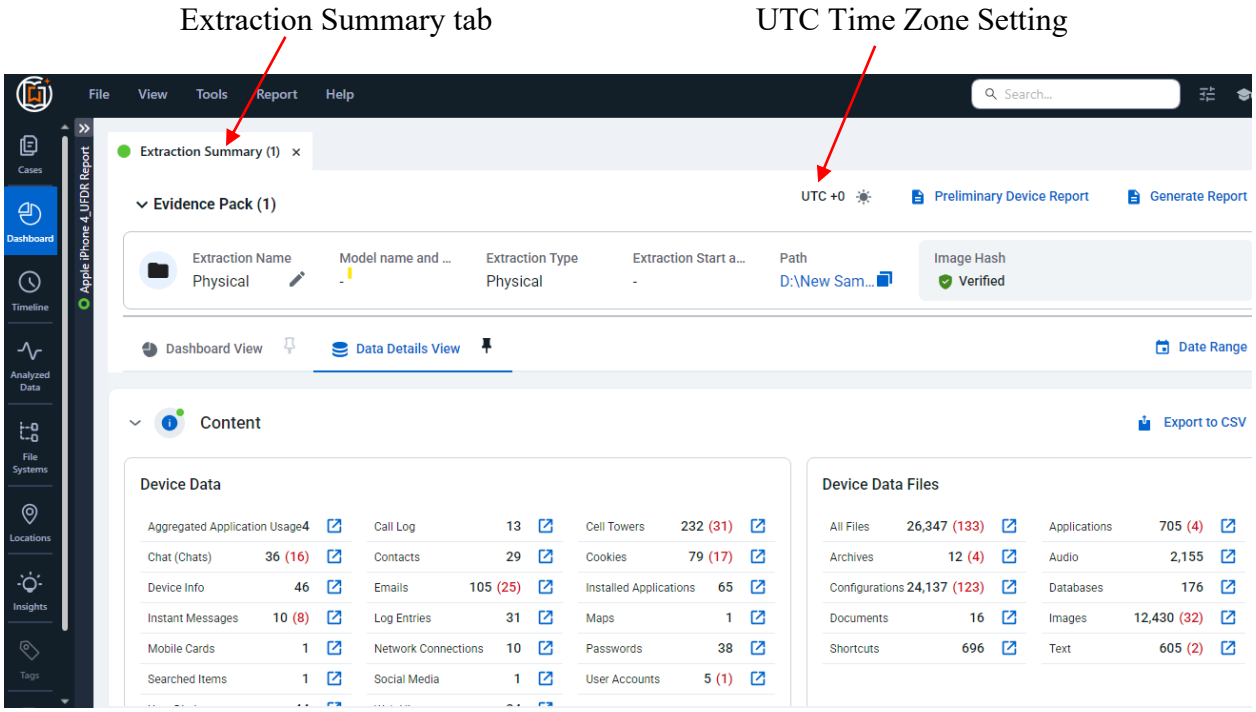
Automatic Time Zone Detection Prompt

Many mobile devices store the last time zone setting used. **If** present, Cellebrite will detect this information and indicate the time zone detected - the following prompt will appear. Click *"**yes**"* and the Dashboard will open.



Note: **If** this prompt does not automatically appear before the dashboard opens, the Time zone settings must be checked in the dashboard before reviewing data.

The Cellebrite Reader dashboard will open to display the **Extraction Summary** tab with the UTC setting displayed in the toolbar shown below.



UTC Time Zone

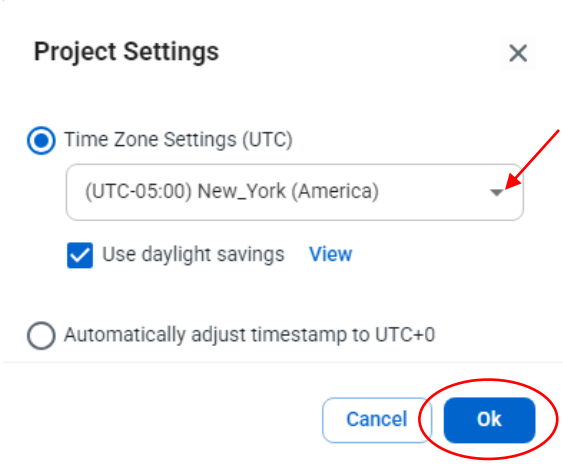
Modern mobile devices obtain accurate date and time information from internet time servers. This data is in UTC and is adjusted by the device to display in the time in the local time zone from information received from the service provider. Cellebrite Reader allows the data to be viewed in UTC or adjusted to any time zone. It is usually beneficial to set the data to be reviewed in the user's local time.

What is UTC Time Zone

UTC (Coordinated Universal Time) is the world's primary time standard, serving as the base for all other time zones, represented as UTC+0, located at the Prime Meridian (0° longitude) through Greenwich, UK, and is used for global coordination, with local times calculated by adding or subtracting hours (e.g., New York is UTC-5 or -4 with DST)

Step 3: Time Zone Settings

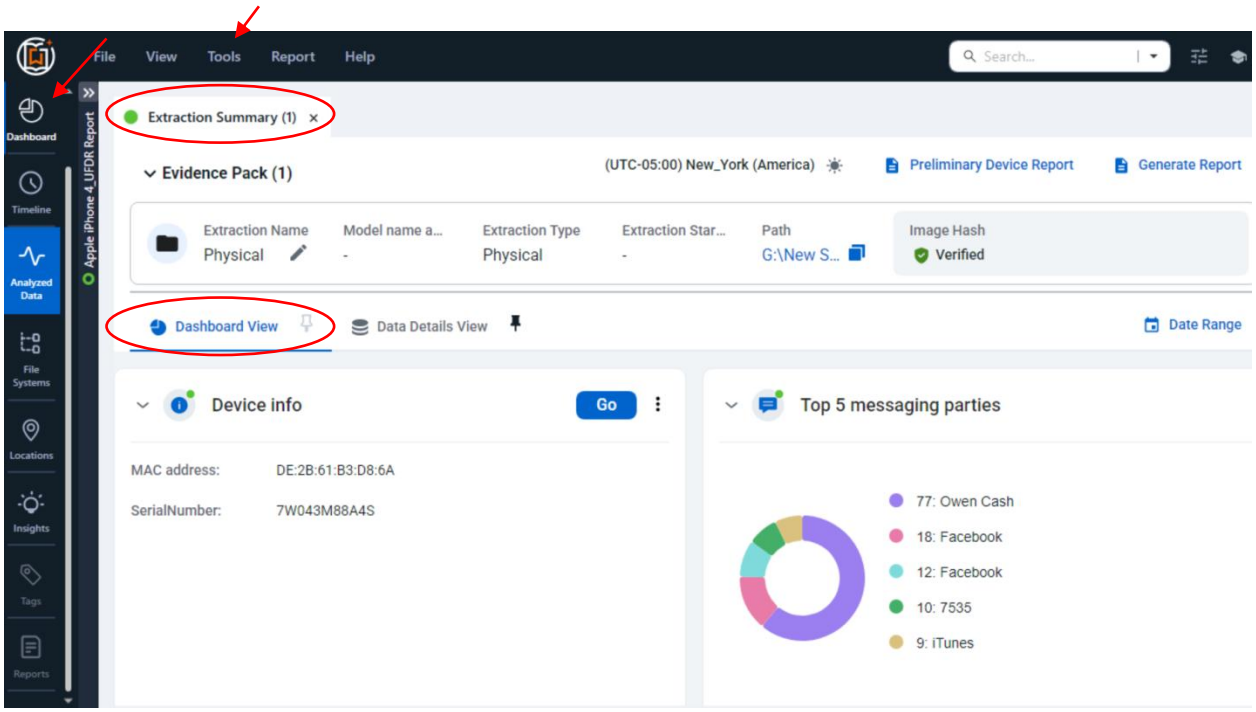
Click on the UTC icon UTC +0 to check and adjust the UTC time. Adjust UTC time zone setting, then check box for day light savings and click ok.



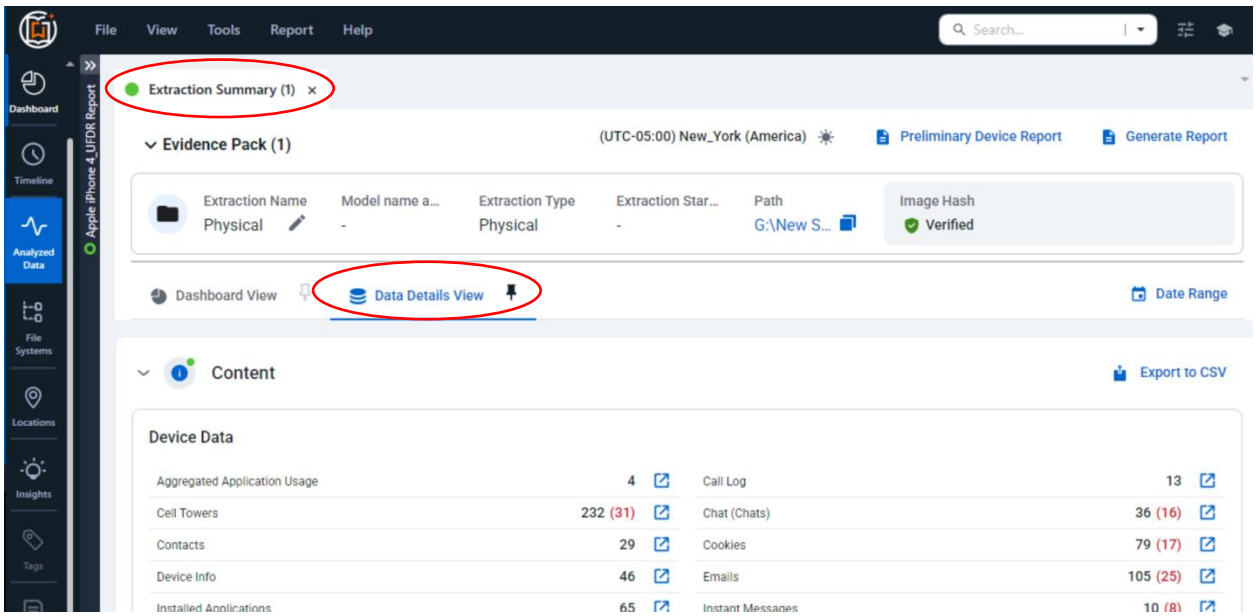
2. Dashboard Layout, Extraction Summary and Basic Navigation

Dashboard View

The Cellebrite Reader dashboard will open to an **Extraction Summary** data tab with an overview of the data displayed in two different overview formats. **Dashboard View** and **Data Detail View**. Both views have more details if you scroll down and have a toolbar along the top of the screen, and a navigation bar on the left.

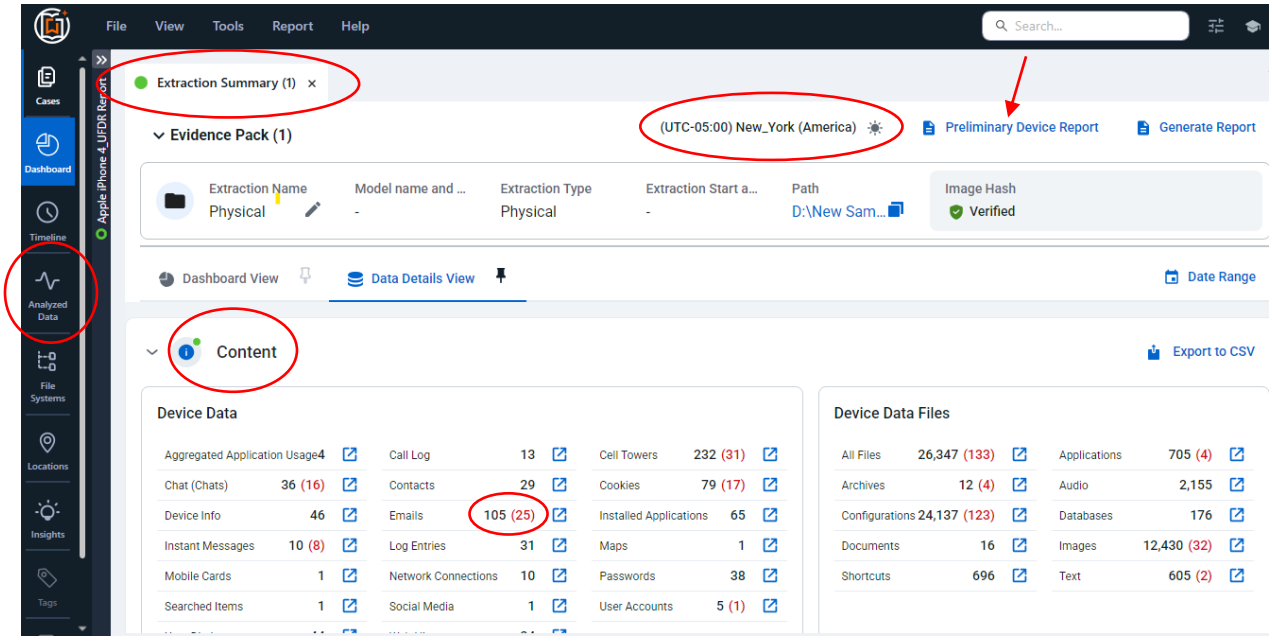


Data Detail View



Data Display Areas and Navigation

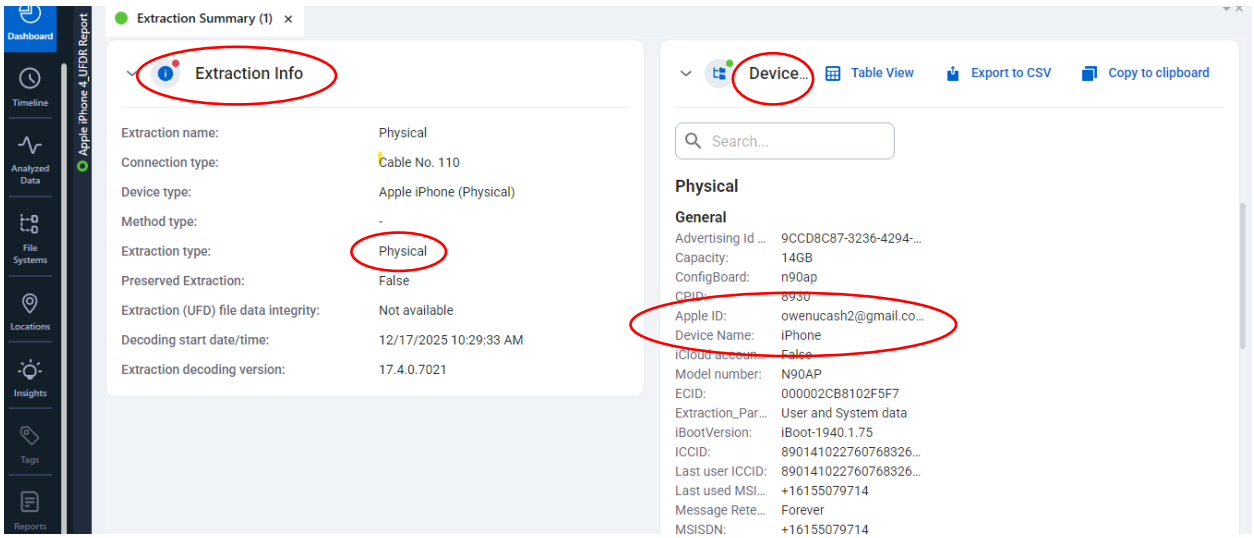
The Cellebrite Reader application has an index under **Analyzed Data** in the left Navigation pane and a quick navigation area under **Content** on the **Extraction Summary** tab. The time zone settings are displayed along the top of the dashboard next to the link to generate a preliminary device report.



The device data and device data files display the number of files in black font with the number of deleted and recovered files in red font.

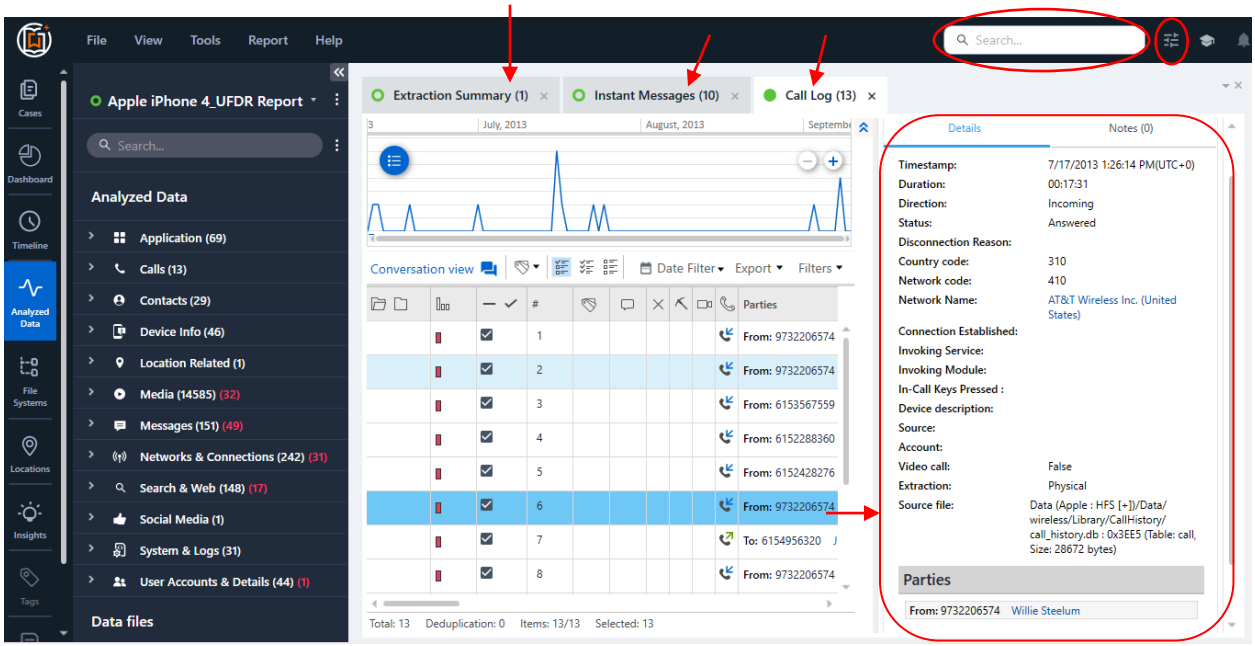
Extraction Information and Device Details

Scroll further down on the **Extraction Summary** tab to see the level of extraction that was used and the details device. **Note:** There are different levels of forensic extraction that are available depending on the device. Because different extraction levels can recover different amounts of data it is critical to know what level of extraction was used and what is currently available. For more information about levels of extraction see page **23**.



Navigating the Dashboard

In the following example, two tabs for **Call Log** and **Instant Messages** are open next to the **Extraction Summary** tab. The **Global Search** box is displayed in the upper right toolbar next to the **Advanced Search** button. Also displayed are the details from the highlighted call from the call log tab in the center, with the call detail displayed along the right bar.



3. Getting Started and Keeping Organized

Preliminary Device Report

The preliminary device report should be one of the first things to generate because it will contain information needed to complete the investigators check list and will expedite integration with digital forensic experts without having to go back to re-open the extraction report.

Device Info (46)

#	Category	Name	Value
1	General	SerialNumber	7W043M88A4S
2	General	ECID	000002CB8102F5F7
3	General	ConfigBoard	n90ap
4	General	iBootVersion	iBoot-1940.1.75
5	General	CPID	8930
6	General	Capacity	14GB
7	General	Passcode	cbrox
8	General	Extraction_Partition	User and System data
9	General	Device Name	iPhone
10	General	Model number	N90AP
11	General	Last user ICCID	89014102276076832607
12	General	Last used MSISDN	+16155079714
13	General	Apple ID	owenucash2@gmail.com
14	General	iCloud account present	False
15	General	Advertising Id (IDFA) #1	9CCD8C87-3236-4294-B0D4-910675755ECB
16	General	MSISDN	+16155079714
17	General	ICCID	89014102276076832607
18	General	Message Retention Duration	Forever
19	Metadata	DeviceInfoOSType	iOS
20	Network Interfaces	Wi-Fi MAC address	DC:2B:61:B3:D8:69
21	Network Interfaces	MAC address	DE:2B:61:B3:D8:6A
22	Phone Settings	Activation State	WildcardActivated
23	Phone Settings	Locale language	en_US
24	Phone Settings	Cloud Backup Enabled	False
25	Phone Settings	Automatic date & time	True
26	Phone Settings	Automatic time zone	True
27	Phone Settings	Location Services Enabled	True
28	Sync Data	Sync host name	STUDENT06

Using the Investigator Checklist

The investigator checklist will help you keep organized, help uncover hidden data and will expedite integration with digital forensic experts by having details you may be asked for without having to go back and re-open the extraction report.

Extraction Level

- Logical/Advanced Logical_____(Lowest Level)
- Full File System_____(Medium Level)
- Gray Key_____(Medium Level)
- Physical_____(Highest Level)

Seizure Date _____ Extraction Date_____

Device Make_____ Model_____

Owners_____ Op. System/Version_____

Phone Number_____ Service Provider _____

UTC Settings_____ UTC Validation_____

Time Period of Use_____ of Interest_____

Installed Apps._____

Missing data _____

Cloud/backups_____ Cell Provider Records_____

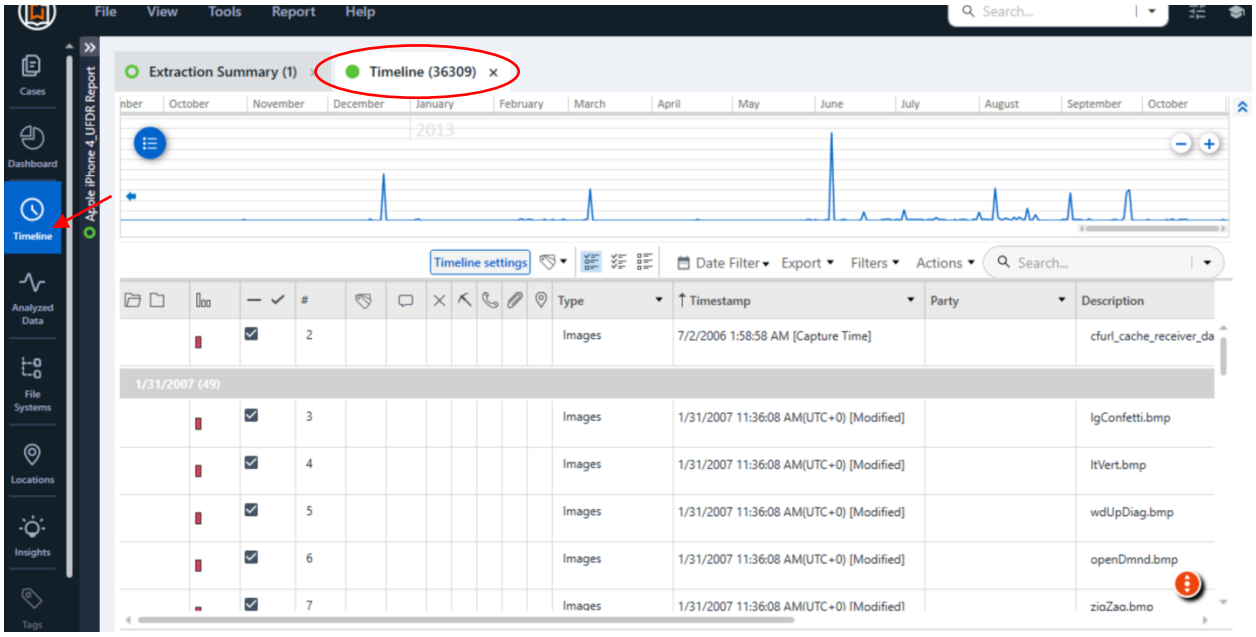
4. Searching, filtering and Location Data

Time Line Search

The Cellebrite Reader Timeline tab puts all data with timestamps into an aggregated, chronological view. Timeline view is a powerful tool that enables you to analyze data in order, apply data filters and sort. Click on the timeline button along the left toolbar and a separate data tab will open for the timeline next to the extraction summary.

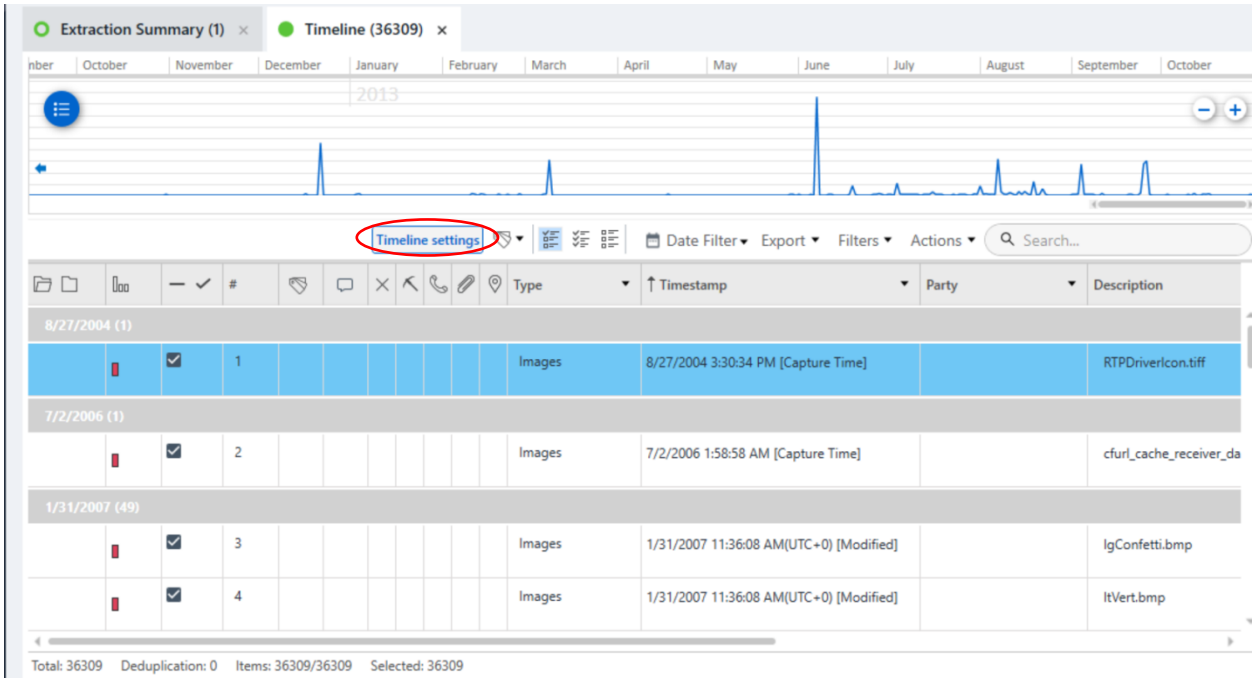
TIP: This should be one of the first things you do as part of the early stages of your investigation.

By looking at the time and navigating to the date and time of the alleged incident, you can get a sense of the activities that occurred on the device in the time leading up to, during and after the alleged incident. This will provide the context of events, additional leads, identify witnesses or areas of investigation.

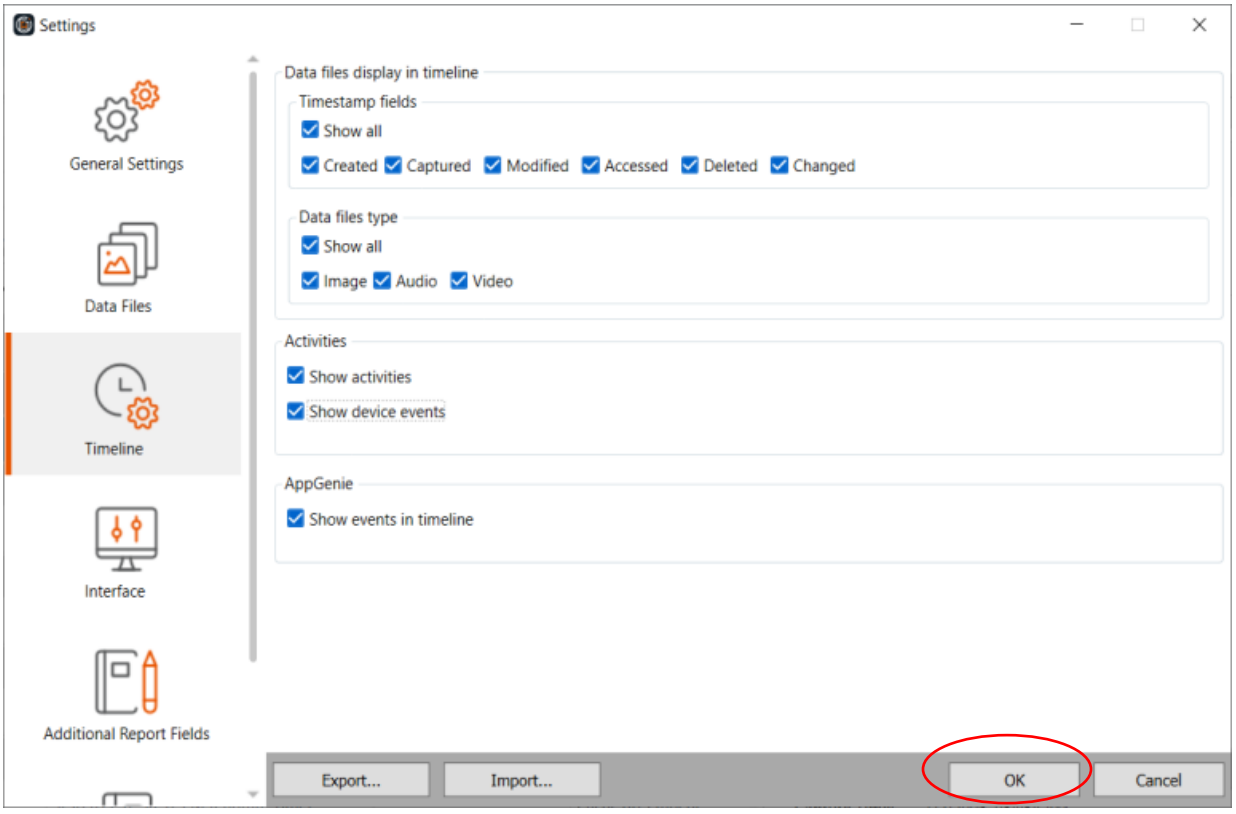


Timeline Settings

By default, not all data timestamps are shown in the timeline view. To choose what data is included and displayed in the timeline and to ensure you see everything, click the **Timeline Settings** button to double check.

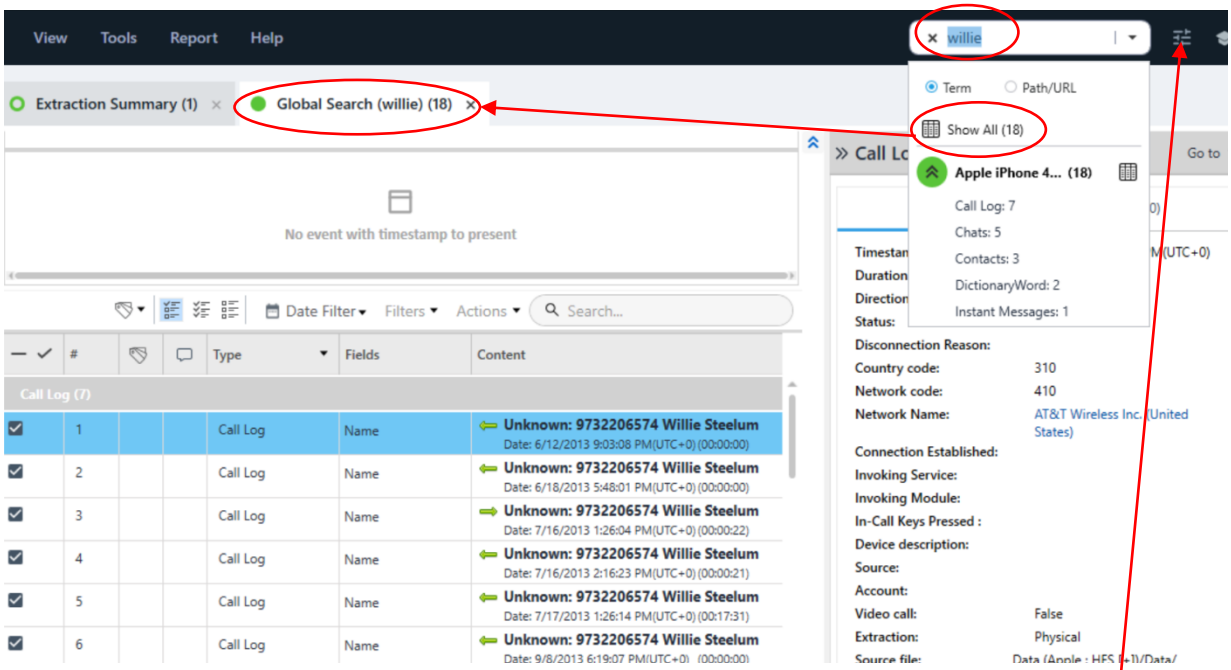


Select all items displayed in the timeline settings window and click "**OK**".



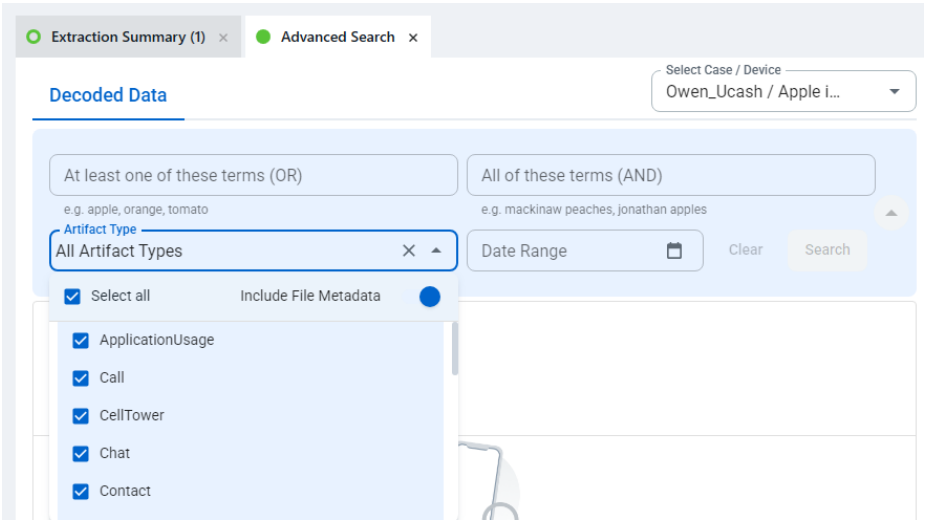
Global Search

This search will expedite the investigation by quickly searching the entire extraction by name, number, stored contact, keyword or phrase. Enter the search term in the global search box in the header as shown below. This will display a listing of the results and the data tabs where the search term was located. **TIP:** Clicking on "***Show All***" will display the search hits in their own data tab, creating a comprehensive roadmap to follow.



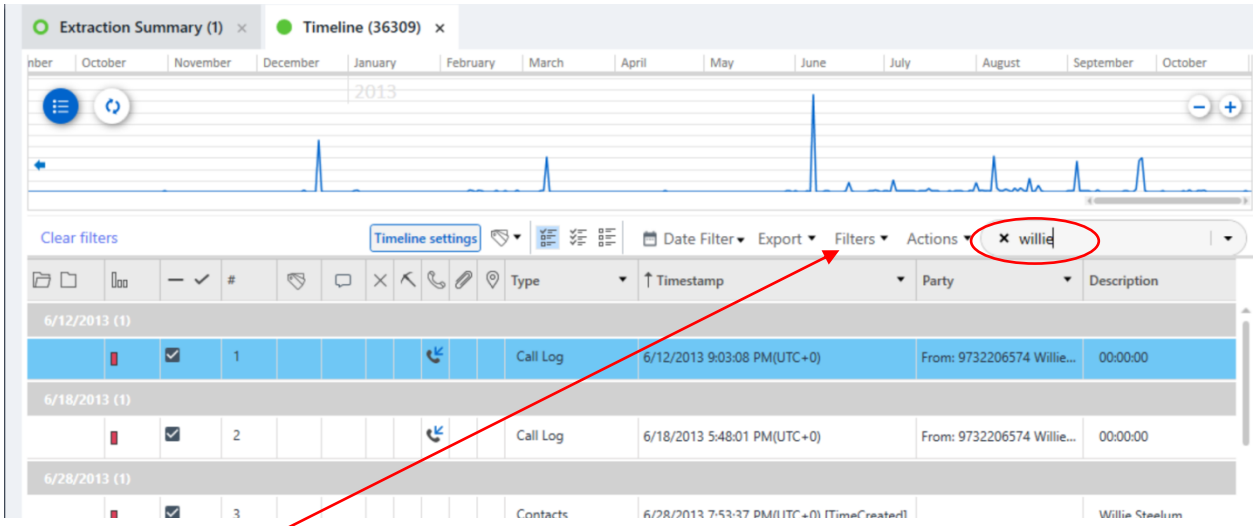
Advanced Search

Apply filters to global searches using the advanced search option.



Individual Data Tab Search

Enter the search term in the search window shown below. The data table updates to display the results of the search. Below is an example of a keyword search for ***"Willie"*** in the individual timeline tab.

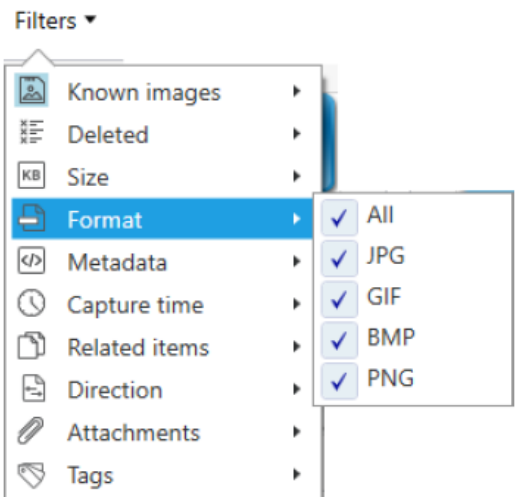


Filters

Filters can be applied to the time line and data tabs and can help expedite the investigation by reducing the amount data to be searched by date, file type or images recognizable by AI like a person, a gun or a vehicle. **TIP:** Use filters to search images to exclude stock images, choose dates, file types or for specific items.

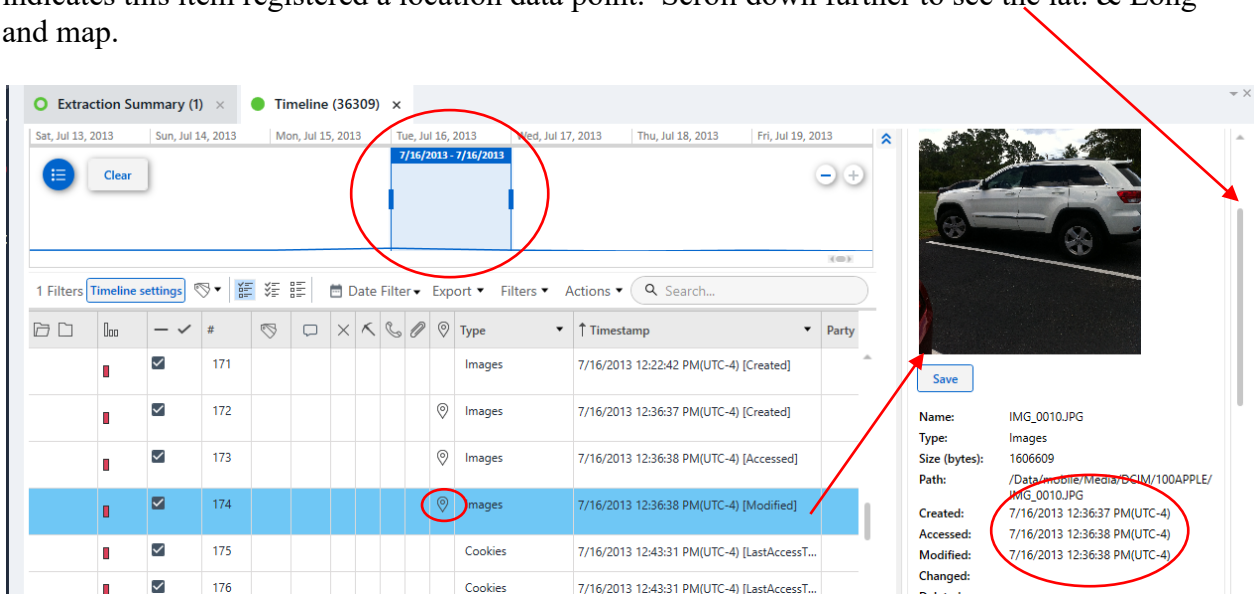
<u>Using the Quick Filter</u>

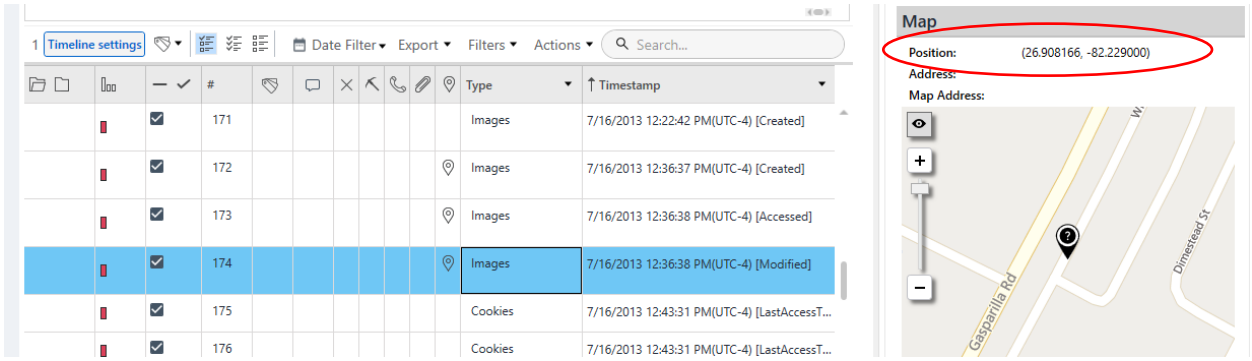
To improve accessibility the filters are now grouped under simple menus.



Location Data

The following example shows the timeline with a filter for one day, with an image highlighted showing a photo of a white Jeep, taken on 7/16/2013 at 12:36 p.m. The location data icon indicates this item registered a location data point. Scroll down further to see the lat. & Long and map.





5. Tagging, Saving and Reporting

Tags and Bookmarks

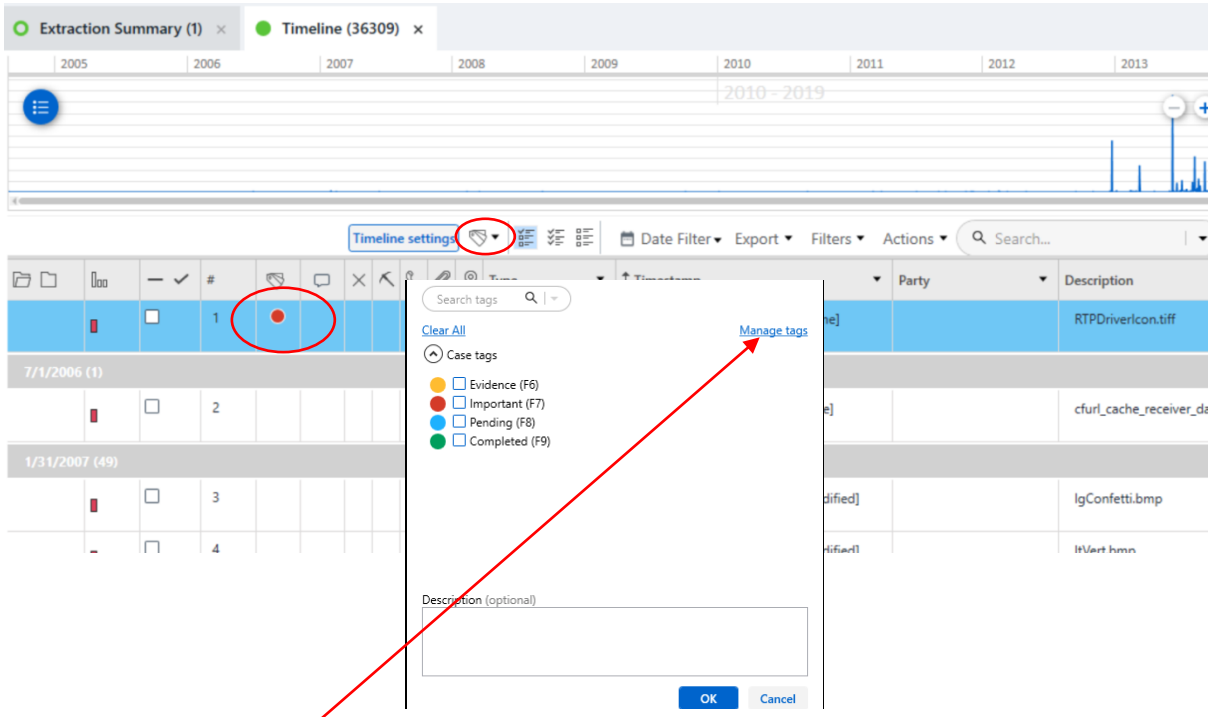
Data of interest can be tagged with tags that can be customized and bookmarked to find the items fast, keep organized and for inclusion in reports or generate custom reports.

Tags

The investigator can tag items for future reference and quickly generate a report from tagged items. Each item can have multiple tags.

To add a tag to data items

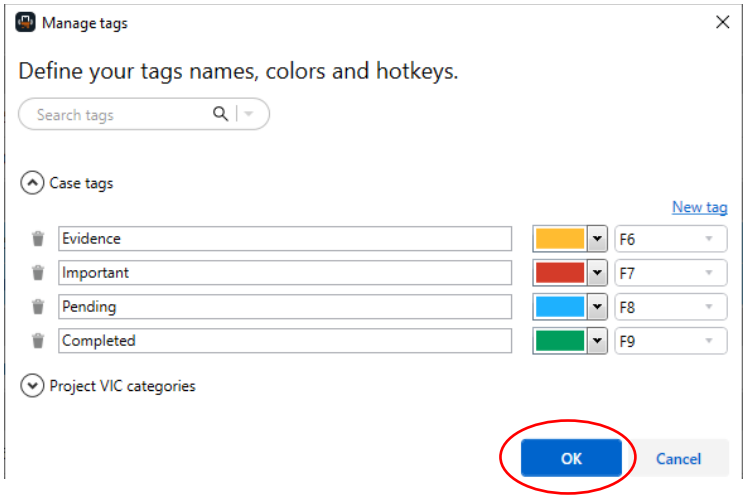
1. Select one or more rows in the data table.
2. Click the tag icon.
3. Select *Tag*.
4. Select the desired tags.
5. Click OK.



Managing Tags

Tag properties can be changed and new tags created using Manage tags:
1. Click the tag icon.
2. Select *Manage tags*.
3. In the Manage tags window you can:

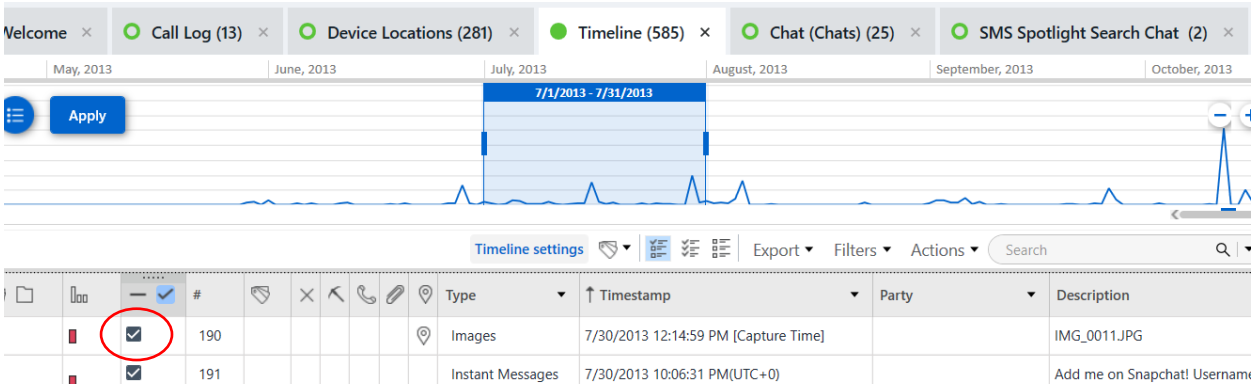
- Search tags.
- Rename existing tags.
- Delete tags.
- Define tag color.
- Define tag hotkey.
- Create a new tag by clicking new tag.



4. Click Ok.

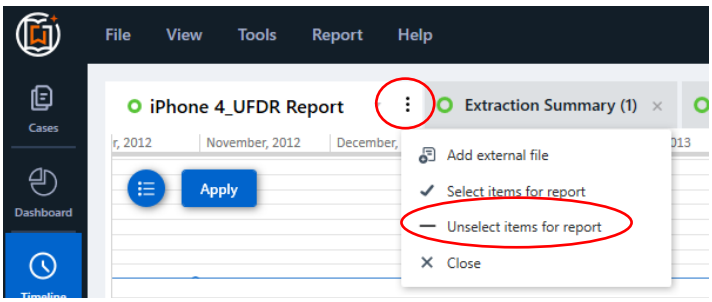
Bookmarks

Relevant data identified can be bookmarked for inclusion in the report by checking or un-checking individual items in the data table. To include items in a report, the check box next to the data item(s) must be selected with a check in the box:



Selecting or Unselecting All Items

By default, all items are bookmarked for inclusion in a report. However, you may want to generate a report based on selected data. To deselect all items, click on the three dots in the extraction summary, then **Unselect items for report**.

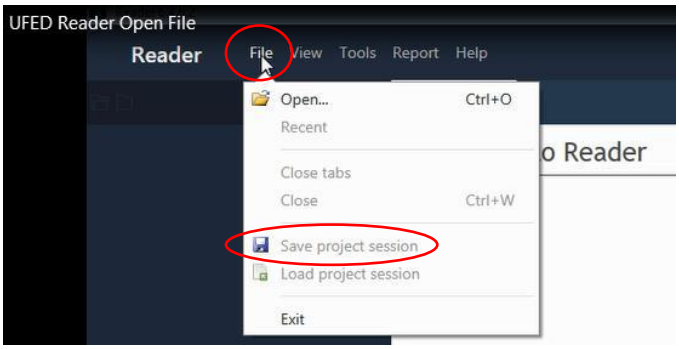


Saving Project Session Files

Saving a project session allows the investigator to pick up where they left off in the review of the Cellebrite Reader report. A project session and will retain bookmarks, tags and view settings which can be applied the next time the UFED Reader Report is opened.

TIP: Always check extractions generated by law enforcement that may have been from their project session file and could contain their tags and bookmarks.

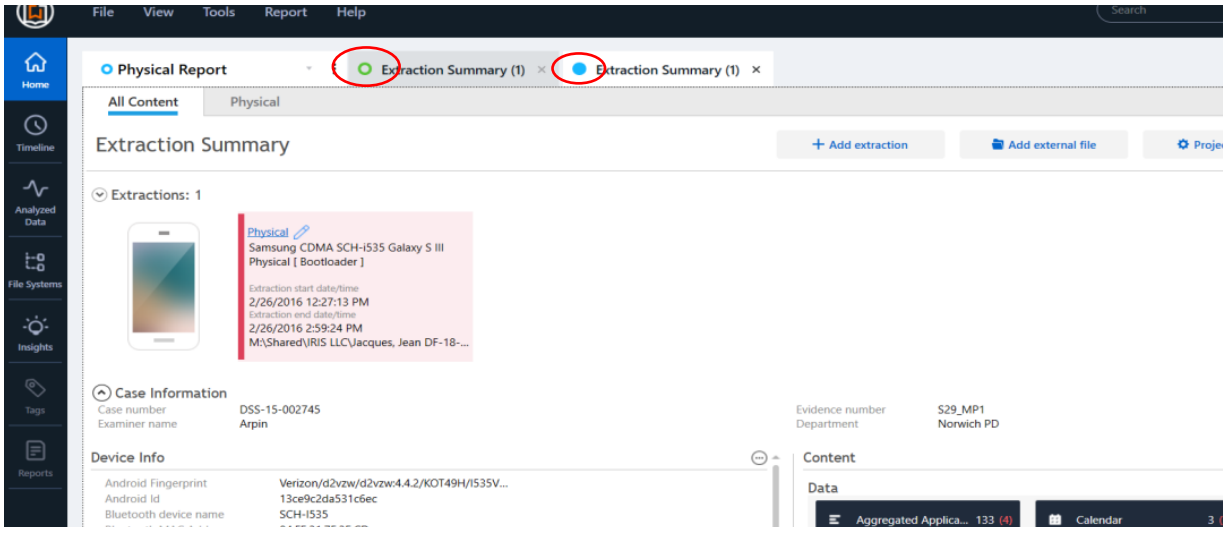
To save a project session, from the File menu, select Save project session, and follow the prompts to name and save the project session file:



The next time the Cellebrite Reader report is opened, you will be prompted that a session file exists for this report.

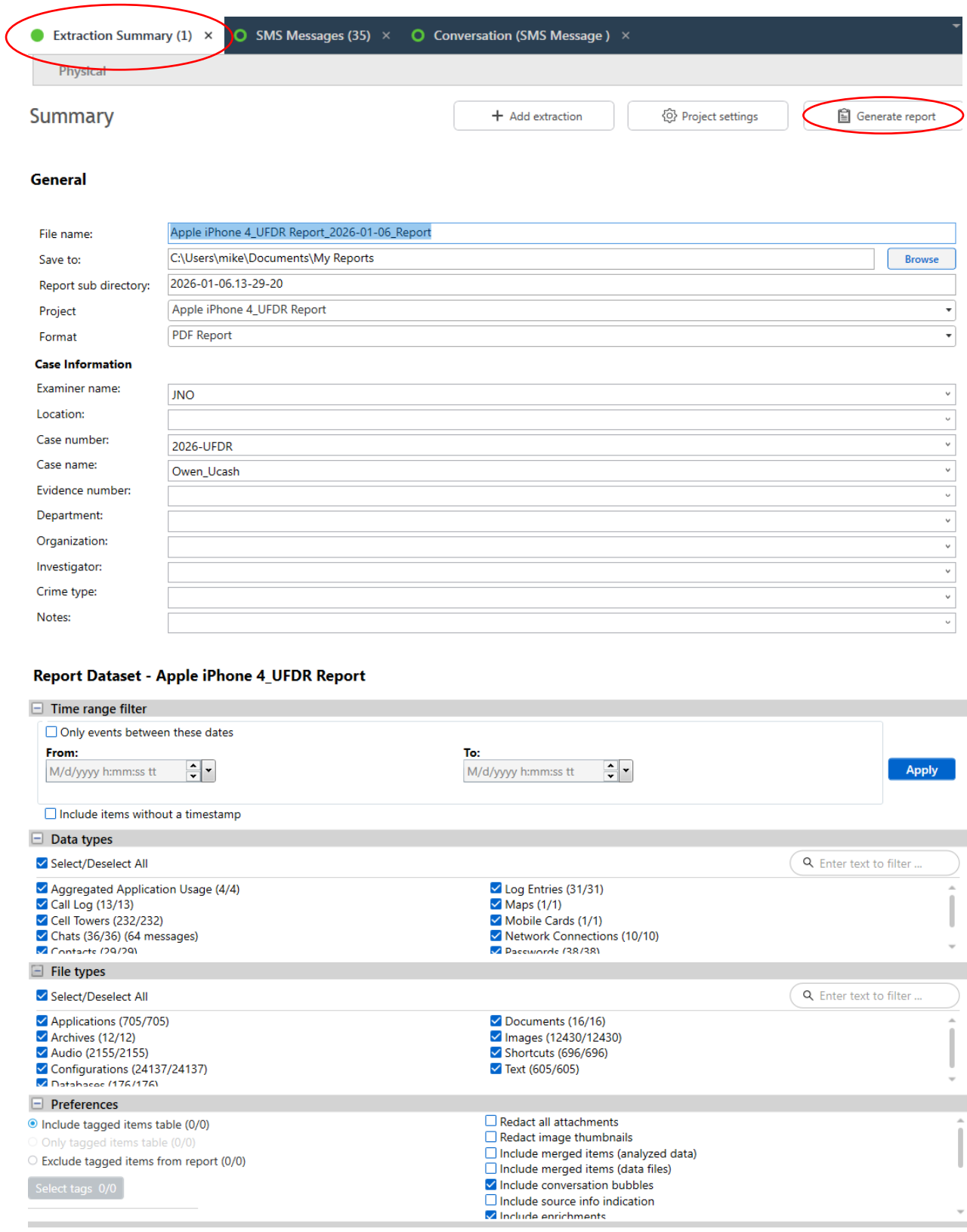
Loading Multiple Extractions

Expedite the searching, analysis and reporting of multiple related extraction reports by loading them into one UFED Reader dashboard. Global searches can be conducted on multiple open extractions simultaneously and custom reports can be generated from data from several reports at the same time. Use the *File>open* and navigate to the UFDR file to open two or more Reader reports.



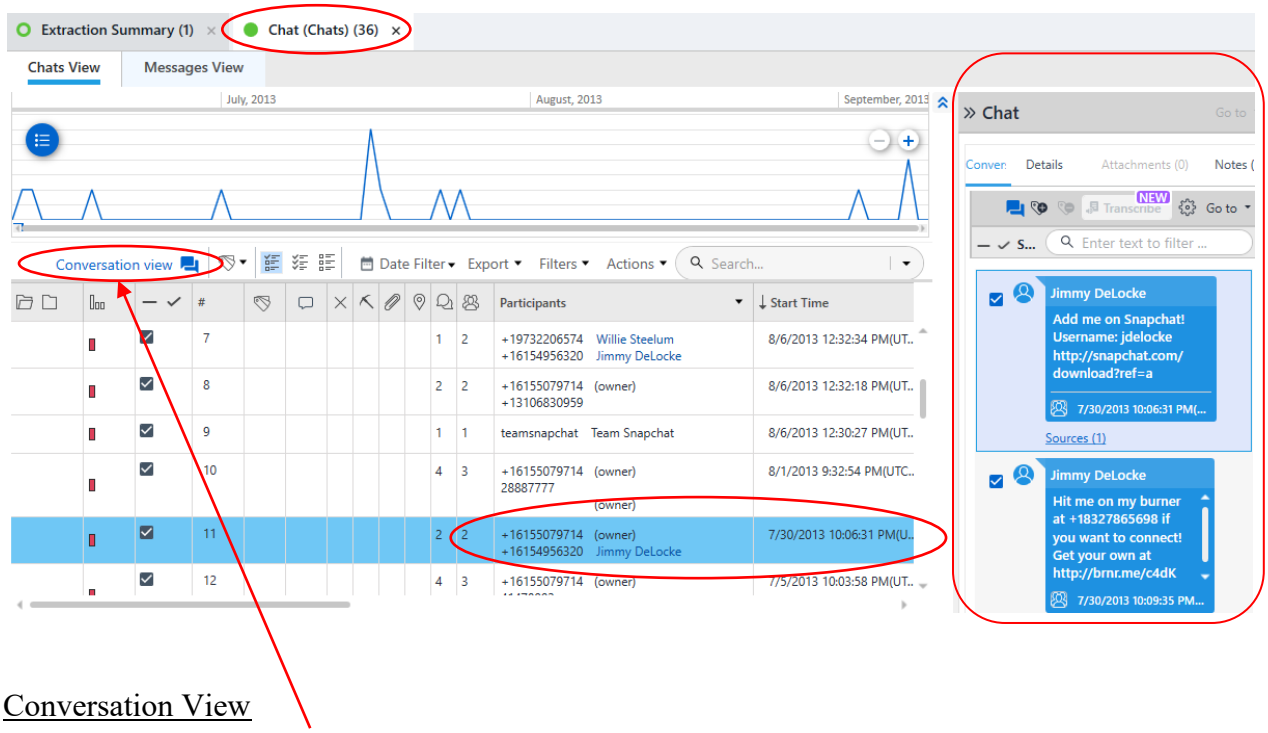
Creating Custom Reports

Using the UFED Reader application, any relevant data identified can be bookmarked for inclusion in the report. A new report is created from the **Extraction Summary** tab.



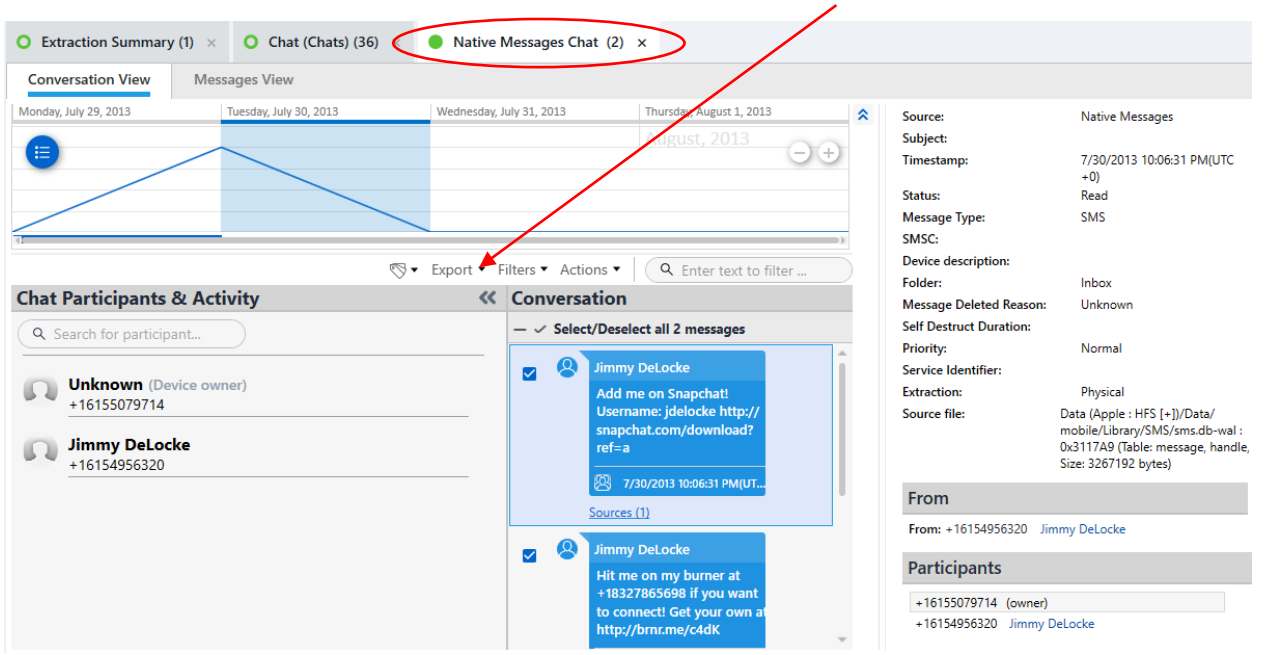
Exporting Single Items

Selected items can be exported as a report from a data tab view. Single item reports are quick, easy and in some cases small enough to email. The following example shows a text in the chat tab and displayed in conversation view along the right column.

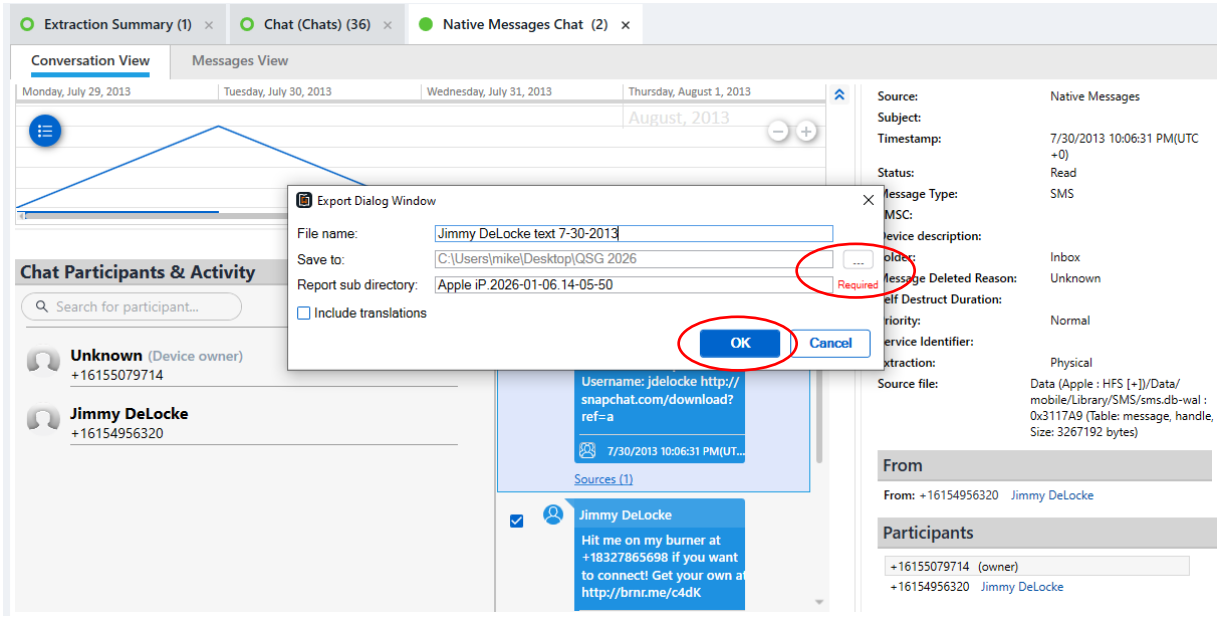


Conversation View

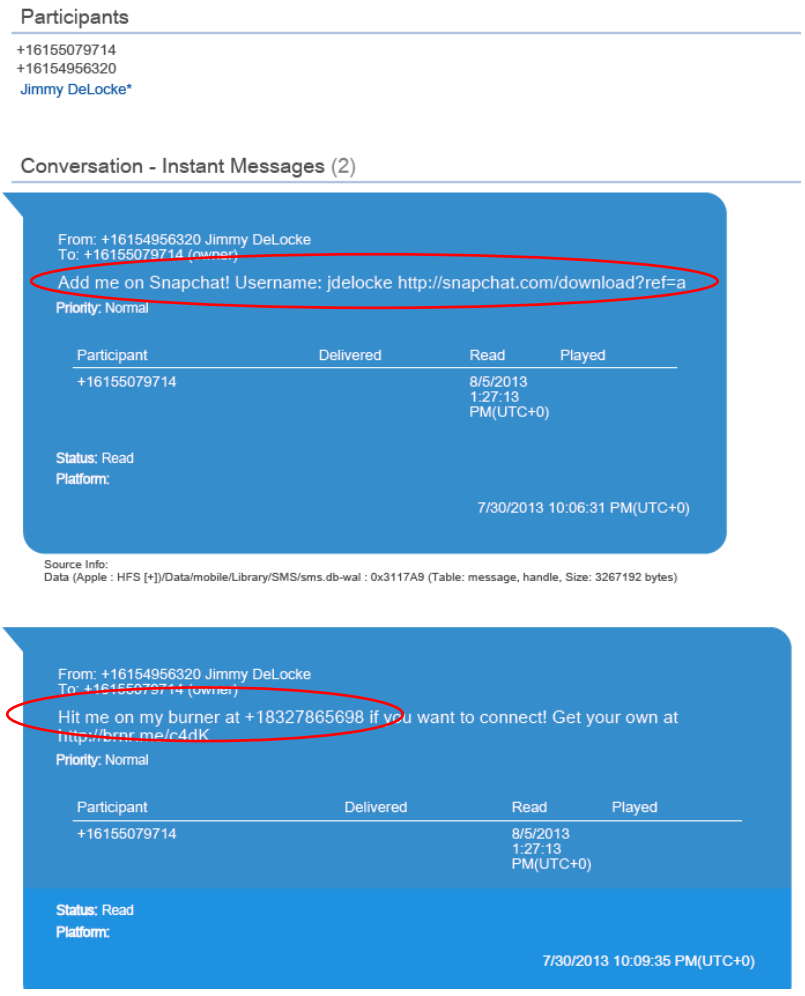
Click on **Conversation View** button to open an individual data tab, then click **Export** to generate a single item report in conversation view that resemble what the user would see on their device.



Choose File Name & Destination



Example: PDF Report of Single Item



Participants

+16155079714
+16154956320
Jimmy DeLocke*

Conversation - Instant Messages (2)

From: +16154956320 Jimmy DeLocke
To: +16155079714 (owner)
Add me on Snapchat! Username: jdelocke http://snapchat.com/download?ref=a
Priority: Normal

Participant	Delivered	Read	Played
+16155079714		8/5/2013 1:27:13 PM(UTC+0)	

Status: Read
Platform:
7/30/2013 10:06:31 PM(UTC+0)

Source Info:
Data (Apple : HFS [+])/Data/mobile/Library/SMS/sms.db-wal : 0x3117A9 (Table: message, handle, Size: 3267192 bytes)

From: +16154956320 Jimmy DeLocke
To: +16155079714 (owner)
Hit me on my burner at +18327865698 if you want to connect! Get your own at http://brnr.me/c4dK
Priority: Normal

Participant	Delivered	Read	Played
+16155079714		8/5/2013 1:27:13 PM(UTC+0)	

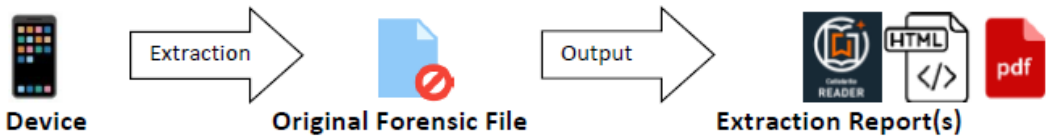
Status: Read
Platform:
7/30/2013 10:09:35 PM(UTC+0)

6. Forensic Extraction Levels, Hidden Data and Requesting Reports

Forensic Extraction

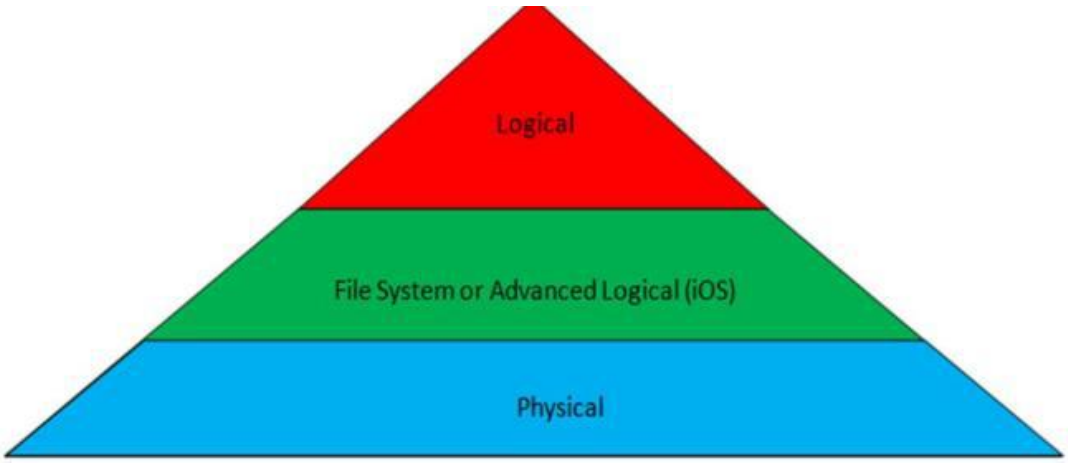
Cellebrite UFED (Universal Forensic Extraction Device) is hardware and software used to obtain the data from a mobile device. Cellebrite Physical Analyzer software decodes the extracted data into human readable form for review and analysis into the original forensic file (.UFD).

The forensic examiner can output reports of all data or selected data. The reports can be generated in several formats including PDF, HTML, Excel, Word and Cellebrite Reader format.



Levels of Extraction

There are three basic levels of forensic extraction, and it is important to know what type of extraction was conducted because each one can recover a different amount of data. Not all devices are supported for all extraction levels. As new extraction levels are developed, they can be used to re-visit older cases to recover more data.



Extraction Type	Level	Data Recovered
1. Logical	Basic level	Current data
2. File System	Intermediate level	Current and some deleted
3. Physical	Advanced level	Current data and deleted

Hidden Data

Not all the data recovered from a device will be displayed in the UFED Reader Report for various reasons listed below.

Installed Applications (Apps)

Applications, or 'Apps' are programs that can be run on the device, such as a third-party texting apps or social media apps. Apps that are supported by the forensic tool will be decoded and displayed in the extraction report. However, there are millions of applications available for smart phones and not all apps are supported.

Data from installed apps that are not supported will not automatically be included in extraction report, but may still be present in the original forensic extraction file and specific database tables for these apps.

Database Tables

Depending on many factors such as device make, model and extraction support levels, advanced analysis can recover additional data from various database tables:

1. Event logs – identifies significant device events, such as activation of airplane mode, device lock/unlock, charging, health data, etc.
2. Call and text database logs – creates numbered log of each activity.
3. Deleted data that was not recovered will leave a gap in the database log.

Requesting Reports

Industry standards recommend that a full report and copy of the original extraction file and proprietary file viewer be requested.

Sample Request

1. All reports including search warrant or consent, and reports regarding the seizure and the chain of custody of the evidence.
2. The forensic examiners report detailing the tools and all procedures used to examine the device.
3. A copy of the forensic extraction in the native proprietary format. (UFD)
4. Forensic Report in UFED Reader format with UFED Reader file viewer.
5. The proprietary file viewer for the specific forensic tool used to create the extraction.

INVESTIGATOR CHECKLIST

Case Name_____ Case Number_____

Date Received_____ Evidence Number _____

Media Type (drive, disk) _____ Folder/File Size_____

Report Types and Components Included (√)

- PDF_____ (.pdf file)
- Link Files_____ (Associated with PDF)
- HTML_____ (.html file)
- Other_____ (i.e., Excel)
- UFDR_____ (.ufdr file)
- Cellebrite Reader_____ (.exe file)
- Cellebrite Reader Manual_____ (.pdf file)
- Forensic Extraction File_____ (.UFD file)
- Examiner's Report _____ (.pdf file)

Extraction Level

- Logical/Advanced Logical_____ (Lowest Level)
- Full File System_____ (Medium Level)
- Gray Key_____ (Medium Level)
- Physical_____ (Highest Level)

Seizure Date _____ Extraction Date_____

Device Make_____ Model_____

Owners_____ Op. System/Version_____

Phone Number_____ Service Provider _____

UTC Settings_____ UTC Validation_____

Time Period of Use_____ of Interest_____

Installed Apps._____

Missing data _____

Cloud/backups_____ Cell Provider Records_____

Investigator_____ Date_____

GLOSSARY

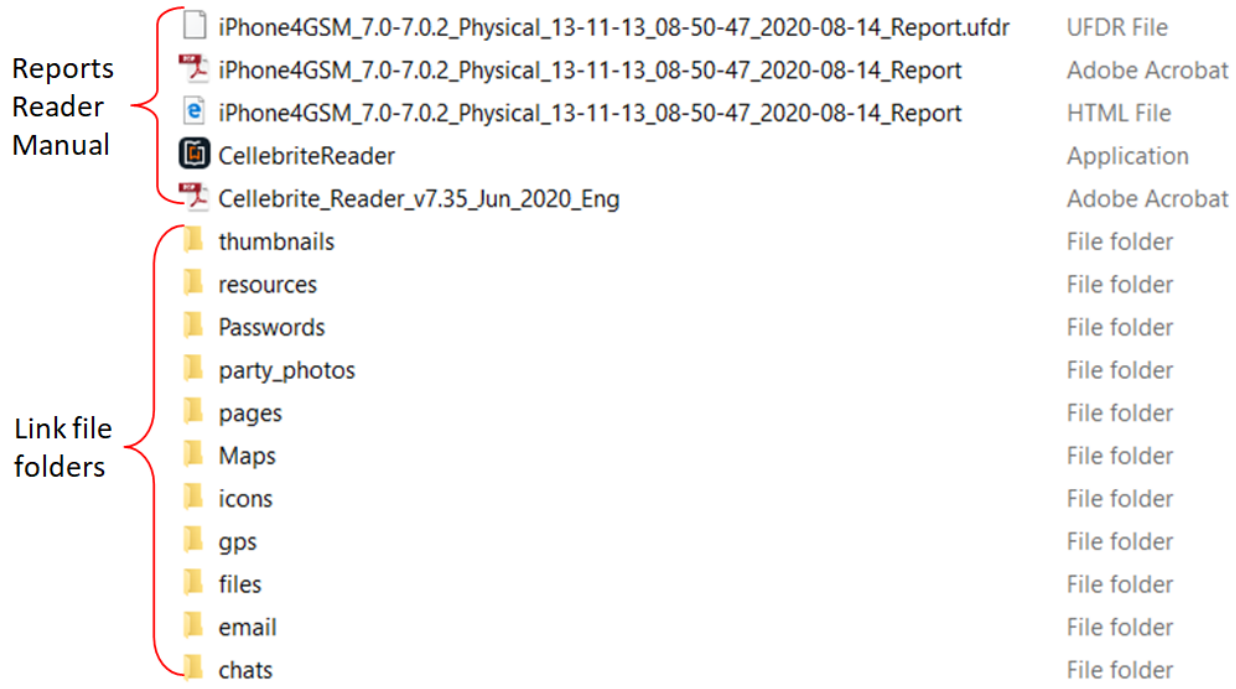
To assist with the completion of the Investigator Checklist, refer to the following definitions:

Case Information

Case Name:	Name of the client, and may be different from the device owner if owned by a witness or co-defendant.
Case Number:	Your agency case number and/or case docket number.
Date Received:	Date which the report materials were received.
Evidence Number:	Agency evidence ID or other identification information.
Media Type:	Report received on CD/DVD, USB drive, file download, etc.
Folder/File Size:	Size in bytes of the report(s). To determine the file size, 'right-click' the main report folder and choose properties from the dropdown menu. Wait for the calculation to complete and note the 'Size on disk'.

Report Types and Components Included

Open the report folder(s) to see what reports were generated and that supporting files are included. It is possible for the examiner to generate multiple report formats at one time, whereby the reports will be in a single folder, or separately resulting in multiple report folders. The following sample contains PDF, HTML and Cellebrite Reader format reports:



For each of the following, confirm the requested items were included:

PDF:	Single report in Adobe Acrobat format with .pdf file extension.
HTML:	Hyper-Text Markup Language format report which opens in an internet browser.
Link files:	If a PDF or HTML format report was generated, the link file folders containing the data files such as pictures, videos and audio files should be included as identified in the above screenshot. ***(Link file folders are not present when only a UFER Reader report is provided.)***
Other:	Although not as common for forensic use, Cellebrite can generate reports in Microsoft Word or Excel formats.
UFDR:	Cellebrite UFED Reader format report with .ufdr file extension.
Cellebrite Reader:	Cellebrite Reader application with .exe file extension, used to open the UFED Reader report file.
Reader Manual:	A Cellebrite Reader user manual in PDF format. Current versions of Cellebrite Reader no longer contain a manual.
Extraction File:	A copy of the original device extraction in a format which requires licensed forensic software to decode and review. A file created with Cellebrite UFED will typically include a file with a .ufd or .ufdx file extension. Depending on the device, the extraction may be a file with a .bin extension or in a compressed archive with a .zip or .tar file extension.
Examiners Report	Note whether a narrative report by the forensic analyst is present detailing the scope of the warrant and investigation, evidence chain of custody, forensic tools and procedures, and any filters or constraints used in the production of the report.

Extraction Level

Extraction level information for extractions conducted with Cellebrite UFED products will be listed in the extraction summary section of the UFED Reader or PDF Report or in the extraction summary tab of an HTML report. If the extraction was conducted with Gray Key or other forensic tools, the extraction summary information may not be populated. Note all extraction levels identified on the Investigator Checklist.

Other Information

The bottom section of the Investigator Checklist is used to record information about the device and the examination. This may come from the forensic report or additional sources such as the search warrant of forensic examiner's report.

Seizure Date:	Date and time the device was obtained as evidence. If the device was handled properly, it should have been isolated from the network to prevent new data or any changes after the date and time it was seized.
Extraction Date:	Date and time the extraction(s) were performed. If Cellebrite UFED products were used, this information will be listed in the extraction summary section of the UFED Reader or PDF Report or in the extraction summary tab of an HTML report. If this is not populated, refer to the forensic examiner's report.

Source Extraction

Logical	
Extraction start date/time	3/21/2019 6:24:49 PM
Extraction end date/time	3/21/2019 6:28:15 PM
Selected manufacturer	Apple
Connection type	Cable No. 220
Extraction software version	7.13.0.77
Is encrypted	Encrypted by UFED Physical/Logical Analyzer during the extraction process for user credentials information
Backup password	1234
Extraction type	Logical [Method1]
Extraction ID	d4e1c821-f6dd-4aa1-8e98-1b5fcfc5d4e9

Device Make: Manufacturer such as Apple, Samsung, ZTE, etc. Listed in *Device Information* section of the report.

Model: Model name or number such as iPhone X or Galaxy S24. The actual model number (i.e.SCH-I535RWBVZW) should be noted as it further identifies specific information about the device.

Owners: Device owner, which may be a witness or another party to the case. In addition to review of the police reports and forensic examiner's report, review the device information section of the report and compare the data to device user's data in the report.

Op System/Version: Modern devices are Android or Apple iOS, although there may still be phones running older or proprietary operating systems. This information can be located in the device information section of the forensic report.

Phone Number Telephone number used for the mobile device, listed as MSISDN (Mobile Station International Subscriber Directory Number) in the device information section of the forensic report. If the SIM card had been changed or the phone is dual SIM, there may be more than one MSISDN identified. If the SIM card was extracted separately from the phone, a SIM data tab will be present under analyzed data and will contain the MSISDN information.

Service Provider If available, will be listed under device information and identify the cellular service provider. If a separate SIM data extraction was performed, information identifying the carrier will be present and may need to be identified using on-line carrier lookup tools.

UTC Settings Are the timestamps in the report in UTC or are they adjusted to a local time zone? This information is listed in the Summary of the PDF or HTML report and can be viewed or changed in the project settings from the *Extraction Summary* tab of the Cellebrite Reader tab. ***(For more information about time settings, see page 7.***

UTC Validation It is important to validate time stamp data as device users can travel to different time zones, and they can also manually change date and time settings on the device. Efforts to identify known events to validate time stamps, such as comparing call log information to billing records should be conducted.

Time Period of Use: Determine the time the device has been actively used. In some cases, the device may have an activation date listed within device information of the forensic report. If not, review the timeline for user data. Note: Images and other items pre-installed on the device may have timestamps preceding initial use of the device. Also, if a user had purchased a new device and restored data from a backup, old files may be on the device.

Of Interest: What is the time period relevant to the investigation, and does it appear that this device was in use during that time?

Installed Apps: Look for application of interest in the Installed Application of the forensic report. In some cases, this data may not have been decoded by the forensic analysis software, but it is still in the report and further examination may be warranted.

Missing Data: Review the timeline for gaps in usage as well as review the data noting missing categories that are expected such as images or videos which were not included with generation of a report.

7. Expediting Analysis and Working with Experts

1. Save entire extraction folder to desktop to expedite opening.
2. Use Preliminary Device Report and the Investigator Checklist to baseline device settings and expedite integration with experts - without having to re-open the extraction report.
3. Uncover hidden data by knowing what extraction level was used and if new technology exists that can recover more data.
4. Be aware of the UTC time setting that was set for the report.
5. Start analysis by going to Timeline and review events around the date and time of incident.
6. Check Timeline setting button to include all, close and re-open to apply changes.
7. Expedite searches - use Global Search, click show all to open results in one data tab.
8. Develop a comprehensive keyword search list by name, number, stored contact, screen-name, phrases etc.
9. Expedite review by loading multiple reports, then use Global Search.
10. Expedite review with filters.
11. Check for installed apps, that could contain hidden data.
12. Check database tables for user activity.
13. Use tags and bookmarks to isolate, organize and create reports for data of interest.
14. Use Project Session files to save tags and bookmarks and pick up where you left off.
15. Use single item export for smaller file sizes in PDF - easy to email.
16. Take advantage of conversation view display options.
17. Get expert help to analyze findings, uncover hidden data and other areas of investigation, cloud, backups, cell provider records etc.

Training & Expert Support

This guide is designed to promote a minimum standard for defense investigators reviewing mobile device extraction reports. It helps bridge the technical knowledge gap that often exists in defense teams and provides practical tools to improve case review, strengthen investigations, and help prevent wrongful convictions.

It is intended for training and reference purposes and is not a substitute for expert digital forensic analysis. For advanced instruction, case-specific review, or expert consultation, contact us at www.irisinvestigations.com or call us directly **860-522-0001**.

For the latest UFED Reader Manual and other digital evidence resources for the defense, go to the DigitalEvidenceToolbox.com.