INTRO TO UNIVERSAL CONVERTER

UC Help Documentation

Consilio®
Together. Stronger.

Table of Contents

What is Universal Converter

23 billion text messages are sent each day worldwide. That's nearly 270,000 per second. 5 billion people globally send and receive text messages, which is about 65% of the world's population. The average response from a text message is 90 seconds, while an email's average response time is 90 minutes. It is predicted that by 2022, mobile data traffic will account for 77.47 exabytes (1 exabyte = 1 billion GB) of data.

Universal Converter (UC) is an innovative solution developed to make reviewing mobile data easier than ever before. Previously, the industry norm was to review text messages and chats as rows in Excel. Multimedia would often exist as separate documents and understanding the relationship between messages and attachments was often difficult. Making both review and production workflows challenging to navigate.

UC, however, threads text messages and chats into conversations and allows for them to be displayed in message bubbles – making the experience as close as possible to viewing them on the mobile device itself. Photos and audio/video sent as attachments to text messages and chats also display in-line with the messages, making the association clearer to understand.

Universal Converter:

- Takes Cellebrite UFDR exports and converts into an easily reviewable format
- Displays the data the way it looks like on the mobile device
- Normalizes chats from multiple sources including:
    - SMS
    - Facebook Messenger
    - WhatsApp
    - Snapchat
    - Skype & more
- Threads individual messages to display relationship-based communication between two or more parties
- Allows for use of analytics

If an unsupported audio/video/file is unable to be embedded into a thread, a message will be displayed in the bubble alerting the reviewer and directing them to the child attachment. It is also advised to view the html threads using the Google Chrome browser, as it is the supported browser.

Non-chat user data such as GPS locations, wi-fi networks and web history, can also be reviewed as separate documents, but by default they are filtered out as "Other". The output of UC can have Consilio analytics used to reduce and prioritize the review of mobile data.

Using Universal Converter

Universal Converter relies on a Cellebrite image of a mobile device in order to parse the information and display it for review. In these cases, you will need to engage Consilio's Digital Forensic Team to assist in the proper collection of mobile data so it can be used in UC. Once the data has been collected using Cellebrite by a Consilio Digital Forensic team member, it can then be parsed with the Universal Converter to be loaded into a review platform for searching, tagging and, ultimately, production.

What information is needed?

The following information is needed to provide the most data rich experiencing with UC:

- The Phone Number of the device and the Owner Name of the device
- The Custodian Name and Custodian Number provided will be used to help UC supply details to show direction via the "To" and "From" labels in messages
- The Region the phone was collected in, so the phone numbers are properly normalized
- Time zone should be indicated; otherwise UC will default to using the UTC Time zone
- Threading method: by Relationship or Conversation
- Unitization method: Split by Day or Split by Gap in Conversation (specified in hours)

Phone Number and Custodian Data

The information provided with respect to phone number and custodian will be utilized in the threading of documents. It is common for the individual text messages to only list who it was "from" or "to" - but not both. The thread will display Phone number and Custodian Name to help show the incoming or outgoing direction of communications based on the message residing on the phone. If for some reason the phone number is unknown, we advise entering the words "Phone Owner" into that field. This will cause UC to display "Phone Owner" and the Custodian name of the indicated phone or smart device in the message threads.

Threading Methods

The different threading methods determine how text messages and chat threads are organized from a relationship perspective. Once a threading method is selected, it cannot be changed without re-exporting a job which could lead to a loss of work product. The two available threading methods are: Relationship and Conversation (default).

Relationship

Threads with different communication types are threaded together into a single conversation between the phone owner and one of their contacts. This means you can see all the SMS & MMS messages, phone calls, voicemails (iPhone only) and chats, including communications from third party apps (such as WhatsApp and SnapChat) in a single thread.

Conversation (default)

Threading messages are grouped using two methods. If the messages are part of a 3rd party chat application, like WhatsApp, then that chat is used as the thread. If there is no thread, then messages are threaded based on the collection of the people involved and the application that they are using in common. This means that using the Conversation method, there are no phone owner threads. The party that sent the first incoming message in the conversation will be considered the author and have their name (or other identifying data) stored in the 'From' field.

There are fewer duplicate messages with Conversation threading. All communications will be threaded together but unitized based on the chat application utilized. For example, an SMS conversation between three individuals will be exported as a thread, while a different conversation among the same people using WhatsApp would be a separate thread. Be advised that in Conversation threading, SMS and MMS messages between the same participants are kept together. iMessage's will not be grouped together with SMS\MMS but be separately threaded.

Threading Options

Export Master Threads: This option is on by default and will export the Grandparent thread. A Grandparent thread contains all the communications of a thread that were stored by the phone owner. Note: If a thread did not go more than 24 hours there will be no grandparent thread generated and only a parent thread created.

Export Standalone Files: This option is on by default. This will export all files that are stored on the phone such as - but not limited to - photo's, videos, audio, office files, and adobe files.

Unitization Method

By default, UC will generate a "master thread" HTML file for each conversation that contains the full thread regardless of unitization and threading methods. The master thread is identified as a "Grandparent" in the family relation metadata fields in Relativity and Sightline.

The unitization method determines how text message and chat threads are organized from a date/time perspective, allowing the "master thread" to be unitized into smaller chunks of time to facilitate both review and production. The unitized portions of the thread are called "Parents".

The available options are:

- Split per Day (default)
- Conversation Gap

- Single Item (for Conversation threading ONLY)

Split per Day, our default setting, unitizes each master thread to span a calendar day (12 am to 11:59 pm). This is a logical way to review conversations, and, unless otherwise requested, Cellebrite data will be processed in this fashion.

However, if conversations are expected to either be exceedingly long (hundreds of messages/day) or exceedingly spread out (single conversations can span a 1 month+), reviewing by calendar day may prove tedious. The Conversation Gap method allows you to specify how master threads should be unitized based on a specific amount of time (anywhere between 1 hour to 72 hours). Once that conversation gap is reached, a new thread will start.

Note: For Cellebrite projects that will require date culling of messages, it is best to select either the Split per Day methodology or utilize a Conversation Gap that is shorter than 1 calendar day - as anything longer than 1 calendar day will cause difficulty in accurately identifying communications from specific date periods.

Single Item: This option should only be used in line with Conversation threading. Do not use with Relationship threading as it will create duplicate messages. The intended result is to get a grandparent conversation threading with single messages.

Phone Number Normalization

The applications listed below have been identified as data points that do not contain a phone number identifier; therefore, UC will not attempt to normalize the phone number. Any unknown applications will be attempted to be normalized by phone number.

Known Applications Not Normalized by Phone Number

- Facebook Messenger
- Facebook
- com.facebook.Facebook
- Snapchat - Friend Stories
- Snapchat
- KakaoTalk
- WeChat
- Kik Messenger
- Line
- Telegram

File Types and Data Types

Universal Converter can support all communication types that Cellebrite can collect and include in its report. Common chat applications that are supported are:

- Hangouts
- iMessage
- QQ Messenger
- Skype
- SnapChat
- Tango
- Viber
- WeChat
- WhatsApp
- Yahoo Messenger

Supported data types are:

- Call logs and voicemail (iPhone only)
- SMS and MMS messages
- Both stand alone and attached to MMS/chat/calendar items:
    - Documents
    - Image, audio and video files
    - Contacts
- User accounts and passwords
- Activity logs, cookies, bookmarks and web history
- Device and Bluetooth information
- Configurations and application data
- Wireless networks

Emoji's

Emoji's are rendered based on what Cellebrite can image from the device. If the Emoji displays in Cellebrite's UFED Reader, then the Emoji will render in threads. It is not uncommon to see strange characters that show up in thread. In some instances, you can do keyword searches for emoji's through copy and paste. Do be aware that false positive hits when searching is common.

Trash Can

If Cellebrite recovers a deleted message the Threads will denote this by displaying a trash can icon in the lower right corner of the message bubble.

Threaded attachments

Universal Converter can thread audio, images, and videos. If it is a file type that cannot be threaded, a message will be displayed in bubble "<filename> - This file type is not supported for embedded threading. See attached child.".

Message attachments

Whenever possible, audio, video, and images will be threaded and able to be viewed directly in thread. There are many chat applications and audio, video, image formats can change and vary widely between them.

Any supported attachments that were included as part of the sent or received message will be processed and included as part of a threaded communication. The attachment will be both embedded into the Grandparent and Parent threads and included in the threaded communication document set as its own “Child” document. If it is not a supported format, you will be informed with the following message, "<Filename> - This file type is not supported for embedded threading, see attached child."

Note: In situations where files are sent, you will have this message presented as we do not want to embed files. For example, if a PDF file was sent, it will be included as an attachment and not embedded in thread.

Deduplication

Deduplication only occurs with standalone files. The standard method of MD5 Hash is used to deduplicate standalone files. Duplicate messages are expected to occur with Relationship threading, because of the design. If it is desired not to duplicate messages, it is recommended to use Conversation threading.

Exclusions

The following file categories are excluded automatically:

- Configuration
- Text
- Database
- Application
- Uncategorized
- Other Files
- Plist files

Emails are also excluded, as it is commonplace to only find the email stub, which will end up being incomplete and contain little value for review. Should you need to review emails, we suggest you contact our Forensics team to collect the email account from its source.