ArtEx

An iOS Forensics tool for Verification, Research or Analysis from DoubleBlak.

User Guide

October 2024

www.doubleblak.com

Contents

Introduction

ArtEx is a free tool for iOS Forensics Verification, Validation, Reporting and Research from DoubleBlak.

I hope that this tool will be useful in your investigations, for research and for sparking at interest in Digital Forensics and how important it can be to investigations.

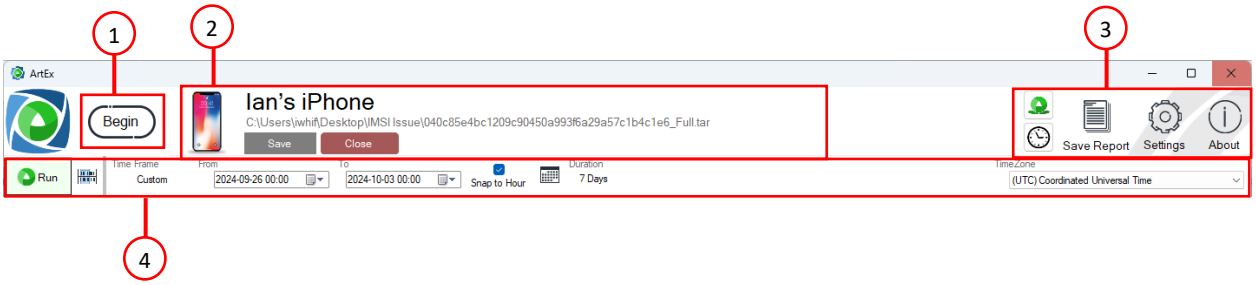
This guide will cover the features of the application and is intended to work alongside the walkthrough videos available from www.doubleblak.com.

If you have any issues or questions, please email hello@doubleblak.com.

The Interface

ArtEx is designed around a single screen which encompasses numerous tabs.

The top of the window can be broken down into 4 main parts:



1 – Begin Button
2 – Extraction Details and RTX Options
3 – Menu Buttons
4 – Time Bar Options

Begin Button

This is where all cases in ArtEx start. Press Begin to open the Extraction Finder.

Extraction Details and RTX Options

This will show the name and path of the Extraction and present the Save and Close Extraction options.

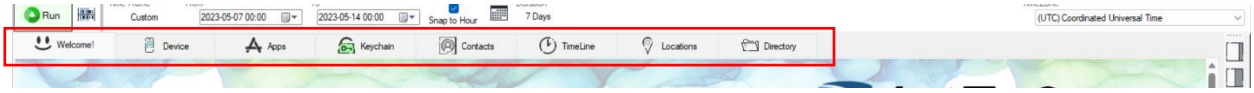
Menu Buttons

This is how to access Save Report, Settings and the About screen. You can also launch other DoubleBlak tools Epoch and Mushy.

Time Bar Options

The Time Bar controls the time period being viewed within ArtEx. It will be covered in much more detail later.

Next, are the Tabs which is where you will find all the important data. The tabs are context sensitive and may come and go depending on the data you are working with.



- Welcome
- Device
- Apps
- Keychain
- Contacts
- TimeLine
- Chats
- Gallery
- Locations
- Directory

Welcome

This user guide.

Device

The Device overview such as IMEI, Phone number, Accounts etc.

Apps

The Applications installed on the device.

Keychain

The keychain associated with the device.

Contacts

The parsed contacts from the device.

TimeLine

The events that occurred within the selected timeframe (and selected parsers).

Chats

A Chat view for selected messages.

Gallery

A Gallery view for selected media items.

Locations

A dedicated Locations screen.

Directory

A directory view of the extraction.

Each tab will be covered in more detail in its appropriate section.

Finally, there is the Right Pane, minimized against the right side of the screen.

The Right Pane is used to show anything you open. For example, if you open an Image, it will open in the Right Pane. If you open a database, it will open in the Right Pane. And so on.

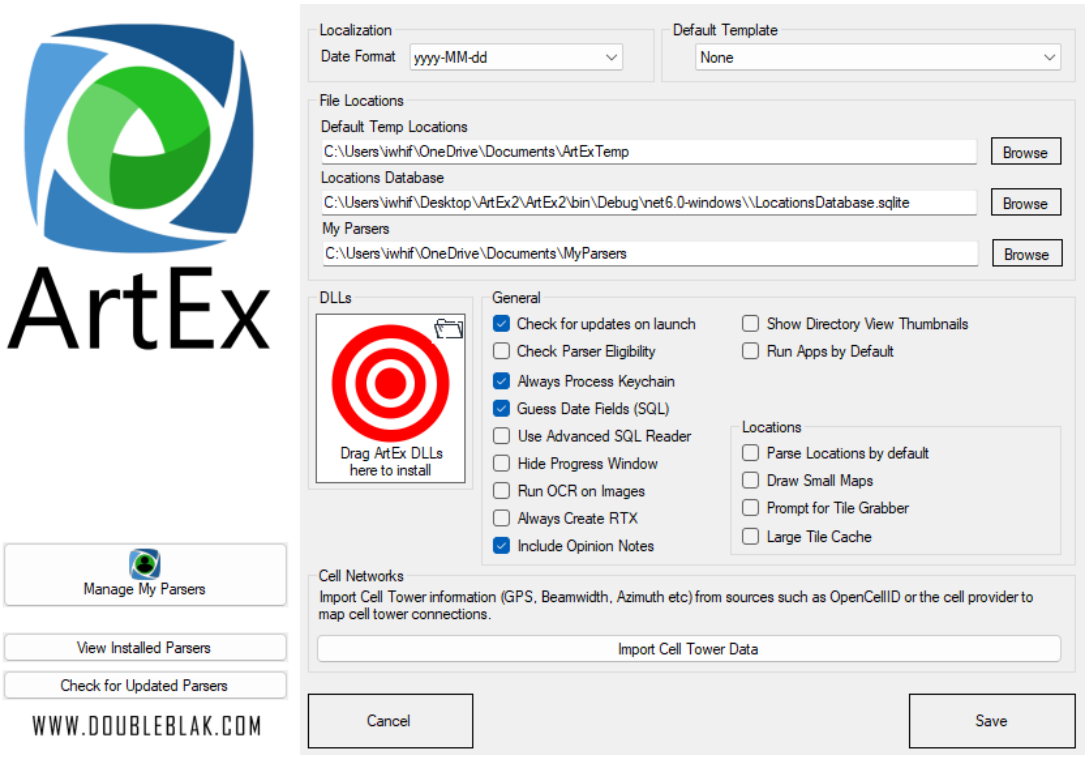
	The first icon relates to the size of the Right Pane. The darker area in the icon relates to the size of the right pane. It can easily be switched between minimized, 25% of the window or 50%. You can also drag the size to whatever you wish.
	This will close all open tabs in the Right Pane.
	This will show the Report Elements.
	This will open the Directory Viewer at the path of the file being viewed.
	This icon will open a drop down menu showing the files you have recently had open in from this extraction allowing you to quickly reopen them.
	Console View will show some of the details being logged by ArtEx. This is primarily used for trouble shooting.

Setting Up

The first time you run ArtEx you will be prompted to decide how you intend to use it. Either on or offline.

ArtEx does make use of an internet connection and is the preferred way to use the tool. Specifically, parsers can be automatically checked and updated, maps can be used, and languages translated if online (with paid licence key).

Options exist for offline use too, although they are not as convenient.



Manage My Parsers

View My Parsers. More about My Parsers can be found later in the manual.

View Installed Parsers

Show the currently installed parsers.

Check for Updated Parsers

Check online for new or updated parsers.

Localization

Date Format : Select the way you want the date to look.

Default Template

Select the default template that should automatically load when a device is parsed.

File Locations

Default Temp Location : Where can ArtEx place temp files?

Locations Database : Where is the Locations database for storing MapTiles?

My Parsers : Where to store My Parsers?

DLLs

Target : Drag individual DLLs or DLL Packages here to install new parsers manually.
Folder : Click to open the DLLs folder.

General

Check for updates on launch : Always check online for software or parser updates.
Check Parser Eligibility : When opening an extraction, check which parsers will run against it.
Always Process Keychain : Always process the keychain if available.
Guess Date Fields (SQL) : In SQL Viewer, attempt to recognize which fields are date stamps.
Use Advanced SQL Reader : Run ArtEx's custom advanced SQL code for freepage recovery.
Hide Progress Window : Minimize the progress window by default.
Run OCR on Images : Always process images using OCR.
Always Create RTX : Always create an RTX when processing.
Include Opinion Notes : Show the opinion notes; i.e. Information provided by parser author.
Show Directory View Thumbnails : Show thumbnails in the Directory View.
Run Apps by Default : Automatically run the App Parser during initial processing.

Locations

Parse Locations by default : Automatically run the Locations parser during initial processing.
Draw Small Maps : When drawing maps, draw smaller maps in the timeline.
Prompt for Tile Grabber : If ArtEx is offline, do you want prompted to manually download map tiles?
Large Tile Cache : When processing map data, this option will download more map tiles than needed.
it takes longer to begin with but will begin to pay off as the cache increases.

Cell Networks

Import Cell Tower Data : Allows you to import cell tower information for mapping connected cell towers.

Installing OCR

OCR in ArtEx utilizes Tesseract, an Open Source OCR Engine (https://github.com/tesseract-ocr/tesseract).

It is not bundled with the application itself and requires downloading from github

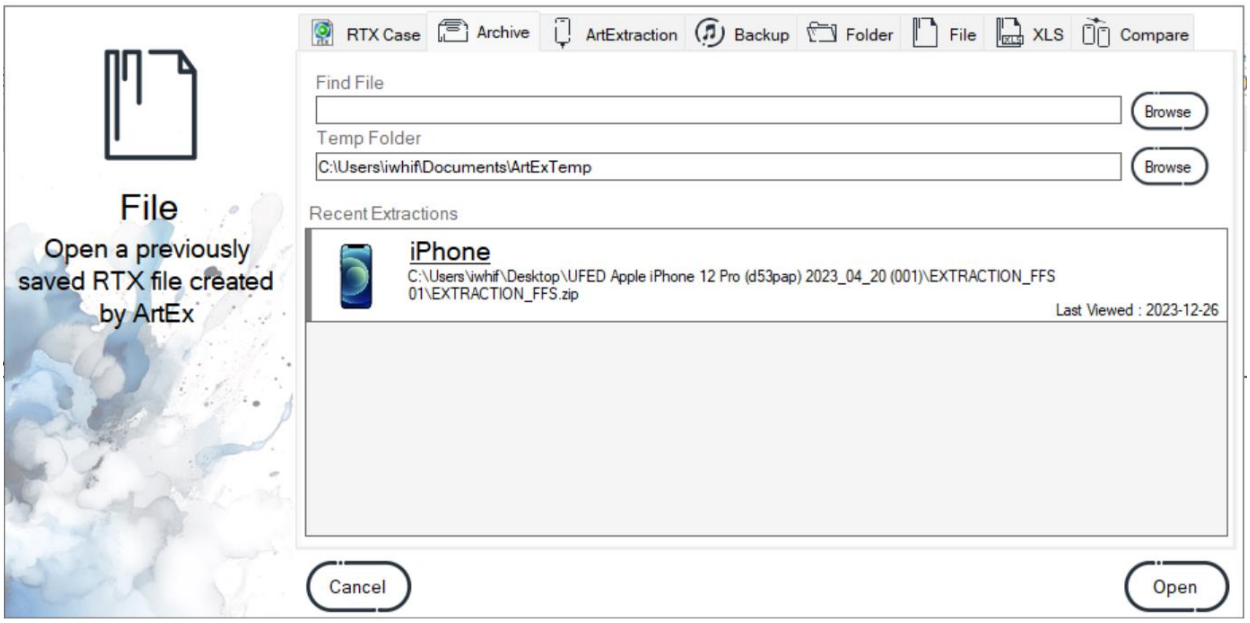
https://github.com/tesseract-ocr/tessdata_fast.

Once downloaded, the **tessdata_fast-main.zip** file should be dropped into the Target area of the settings screen normally reserved for DLLs.

Opening an Extraction

Regardless of the type of extraction you have, start by pressing the Begin button to open the Extraction Finder.

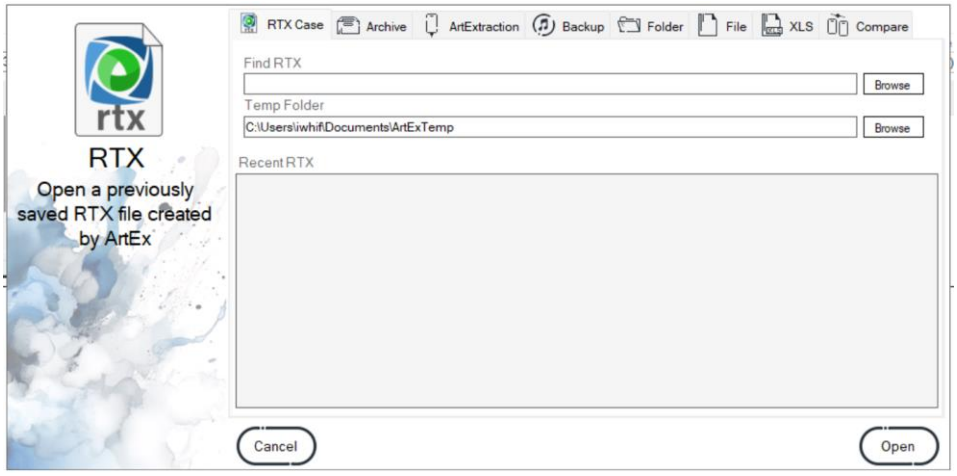
The Extraction Finder has several tabs for opening different types of extractions.



RTX Case	**RTX** Files are ArtEx's own DB format for remembering parsed extractions.
Archive	**Archives** are the typical ZIP and TAR files from most extraction tools. Archives can also be used to read UFDR files – Note that ONLY the files will be accessed. The parsed data within the UFDR is not utilized.
ArtExtraction	**ArtExtraction** is ArtEx's own connection method for connecting to jailbroken devices via SSH. This screen can also be used for creating iTunes Backups of a connected iOS device.
Backup	**Backup** allows you to read encrypted or unencrypted backups from iTunes or apps such as 3u Tools.
Folder	**Folder** allows you to process the contents of a folder as though it was an extraction.
File	**File** allows you to process a single file as though it was part of an extraction.
XLS	**XLS** has several scripts for making XLS documents into databases that can be parsed by ArtEx.
Compare	Compare creates a list of files on the device, tables in databases and fields within tables. This can then be used to compare against another device.

RTX Case

RTX files are SQLite databases that store information such as the extraction's file structure, parsed records and thumbnails. Utilizing RTX is an optional feature to allow faster reloading of an extraction.

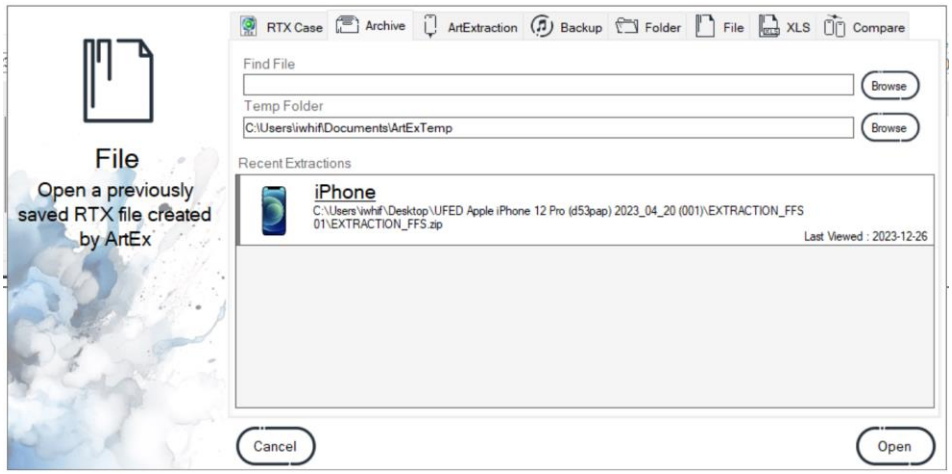


The RTX tab has a simple interface consisting of only 3 paths.

RTX File	The path of the RTX file you want to open
Temp Folder	The path that ArtEx can use as a scratch folder.
Recent	A list of recent (and accessible) RTX files. Note that loading a Recent file will use the same Temp Folder as was used previously.

Archive

Archives are the main type of extraction you will encounter. ZIP, TAR and UFDR are supported.



The Archive tab also has a simple interface consisting of only 3 paths.

Find File	The path of the Extraction Archive file you want to open (ZIP, TAR or UFDR).
Temp Folder	The path that ArtEx can use as a scratch folder.
Recent	A list of recent (and accessible) Extractions. Note that loading a Recent file will use the same Temp Folder as was used previously.

ArtExtraction

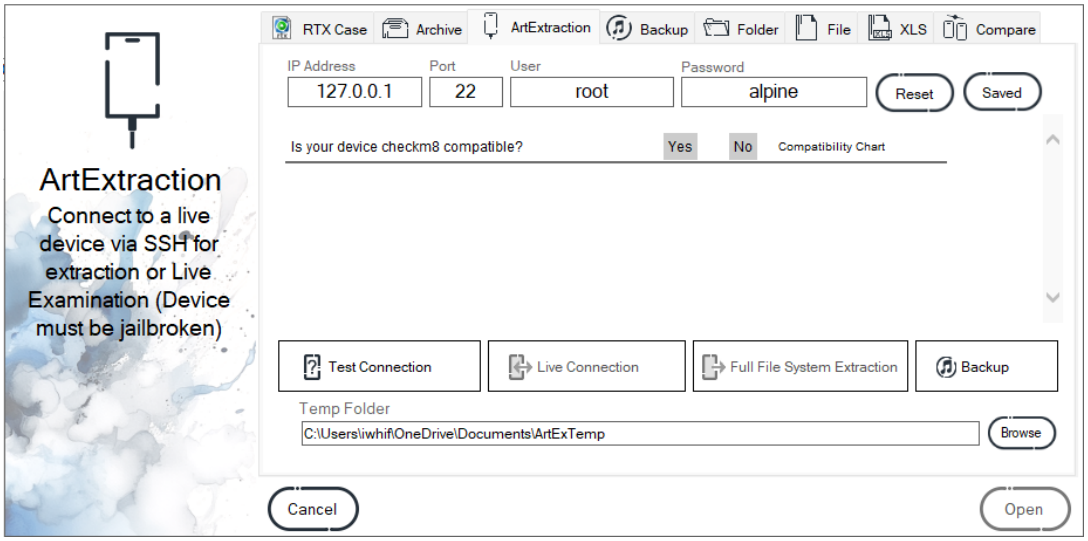
The ArtExtraction tab introduces a few new options.

As mentioned earlier, ArtExtraction is used to connect to a jailbroken iPhone/iPad via SSH and can be used to either extract the device or connect and process in real time which is great for research purposes.

The default LocalHost IP address, Port and User Credentials are loaded with the assumption you will be using a SSH Tunnel via a tool such as 3u Tools.

It is possible to run ArtExtraction over WiFi by entering the appropriate IP Address, but it is considerably slower.

ArtEx also includes instructions for jailbreaking and setting up for SSH although **ArtEx will not perform the jailbreak.**



Either enter the IP Address, Port and Credentials and press **Test Connection**.

Alternatively, select the appropriate connection from the **Saved** dropdown menu.

Assuming the connection is successful, the button will turn Green and the Live Connection and Full File System Extraction button will become enabled.

Use the Live Connection to process the device in real time or the Full File System Extraction to save the extraction.

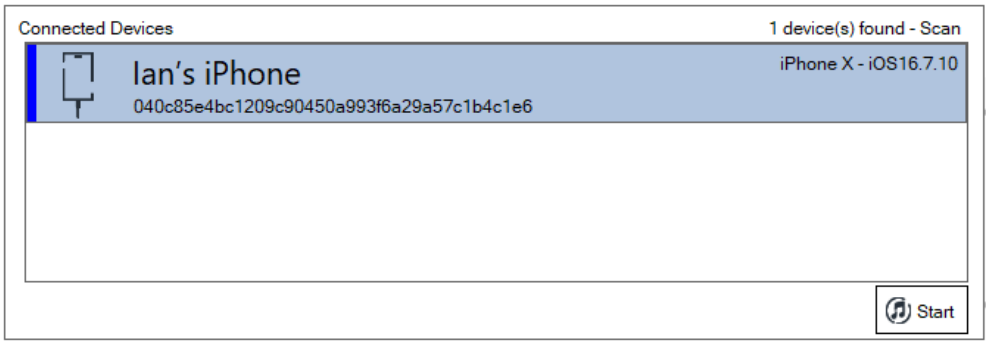
The Temp Folder path is used to specify the path that can be used as a scratch folder.

More information on ArtExtraction can be found later in the manual.

Creating an iTunes Backup

Use the **Backup** button to search your computer for a connected iOS device.

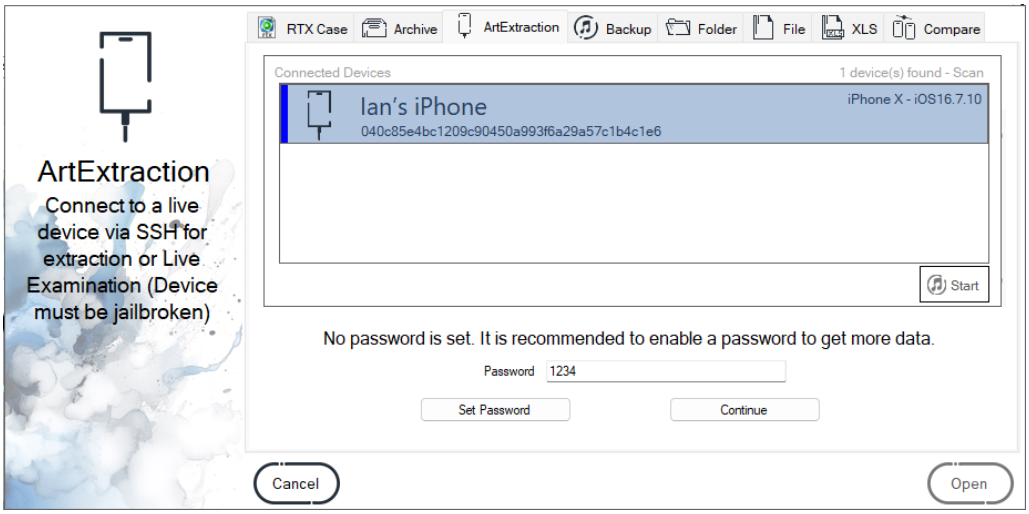
Assuming the device is found, it will be listed in the Connected Devices window. Use the **Scan** button in the top right to search again.



Select the device you want to extract and press **Start**.

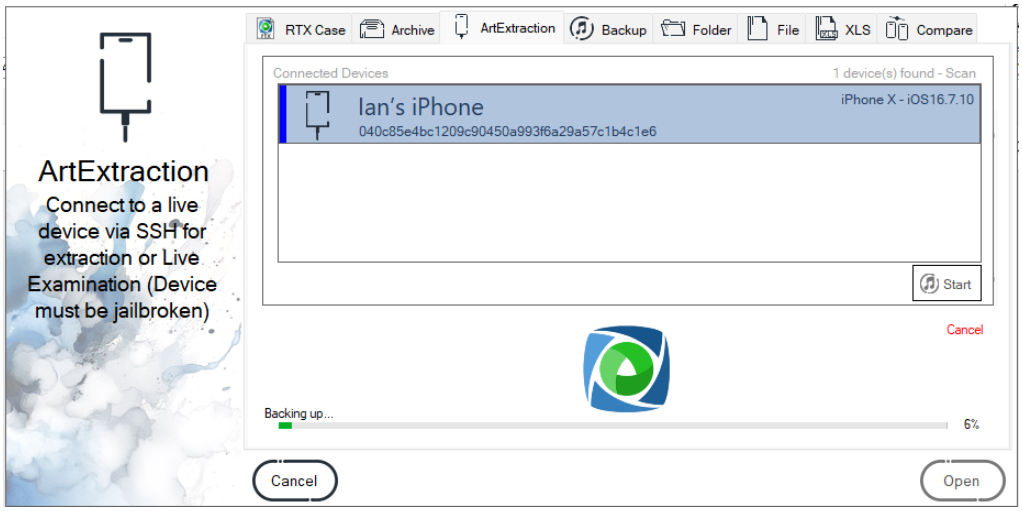
ArtEx will prompt for the target location to save to.

If the device has a backup password set, you will be asked for it. If it doesn't, you will be prompted to create one.



Pressing **Set Password** will set the password, or pressing **Continue** will start the extraction without a password.

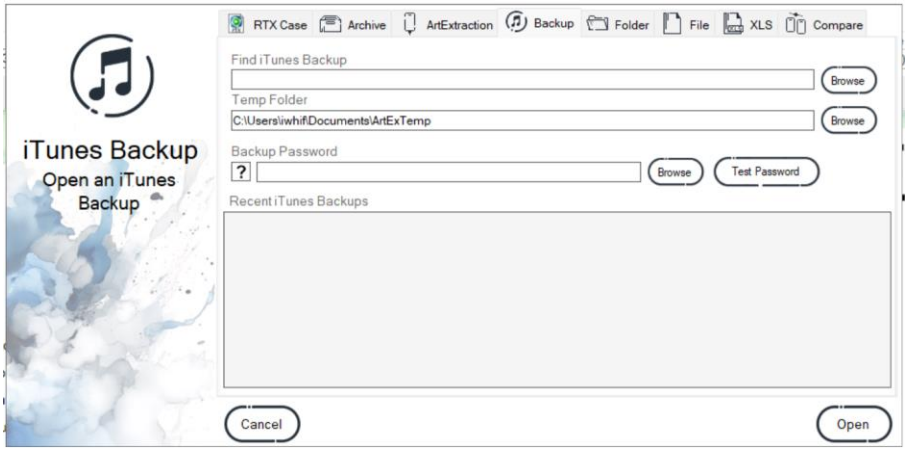
The backup will begin



When the extraction is completed, the data will begin parsing.

Backup

Backup will accept encrypted or unencrypted iTunes backups.



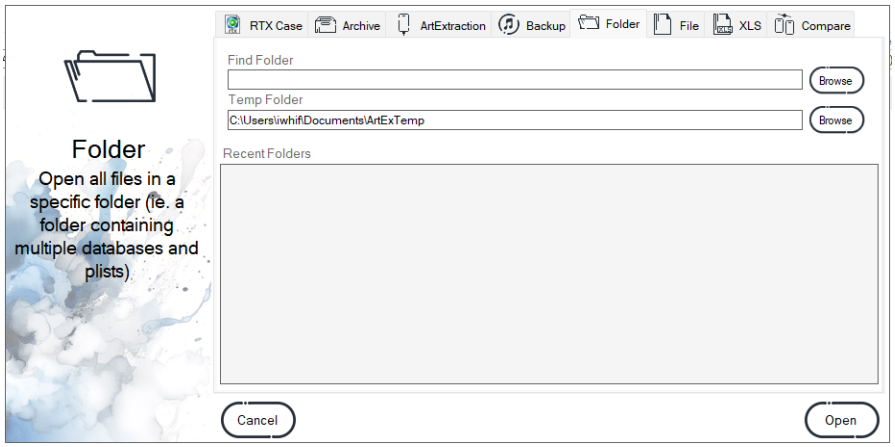
Find iTunes Backup	The path of the backup you want to open
Temp Folder	The path that ArtEx can use as a scratch folder
Backup Password	The password required to decrypt the backup OR the path to a dictionary file.:
Recent	A list of recent (and accessible) Extractions. Note that loading a Recent file will use the same Temp Folder as was used previously.

Notes

- For Encrypted iTunes backups, enter the password/load a dictionary and press Test Password. Once the password if found, the ? icon will change to a green tick (or a red cross in the case of failure) and the case can then be loaded.
- The default password of 1234 will be tested without prompting.
- If a UFD file is present with the same name as the extraction, the password will be used without prompting.
- The password will be remembered in the future if loading a Recent Case.

Folder

Using the Folder Tab allows you to point ArtEx at any folder on your computer and read the contents as though it is an extraction. The specific paths don't matter too much in this case.



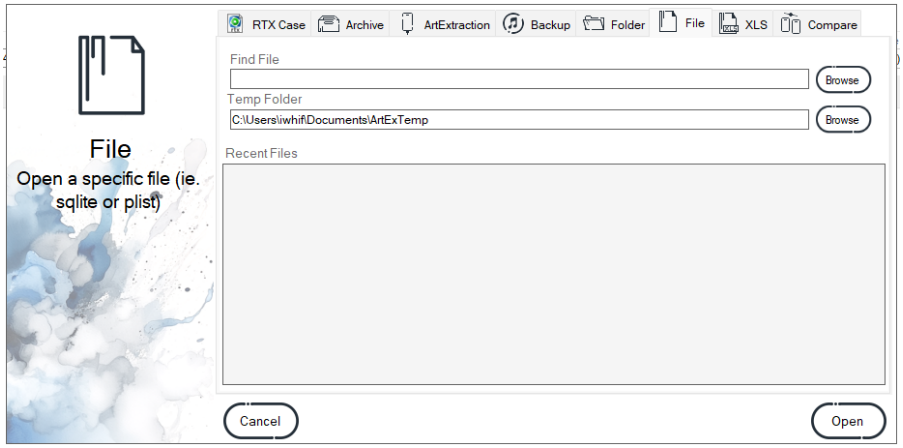
For example, as long as ArtEx finds a file with the name it understands, it will parse it as though the extraction is intact.

This can be great for running parsers against a specific few files, or for quickly loading a collection of files.

Find Path	The path of the Extraction folder you want to open.
Temp Folder	The path that ArtEx can use as a scratch folder.
Recent	A list of recent (and accessible) Folders. Note that loading a Recent Folder will use the same Temp Folder as was used previously.

File

Using the File Tab allows you to point ArtEx at any single file on your computer and read the contents as though it is an extraction. The specific path doesn't matter at all in this case.



As with the Folder extraction type, as long as ArtEx finds a file with the name it understands, it will parse it as though the extraction is intact.

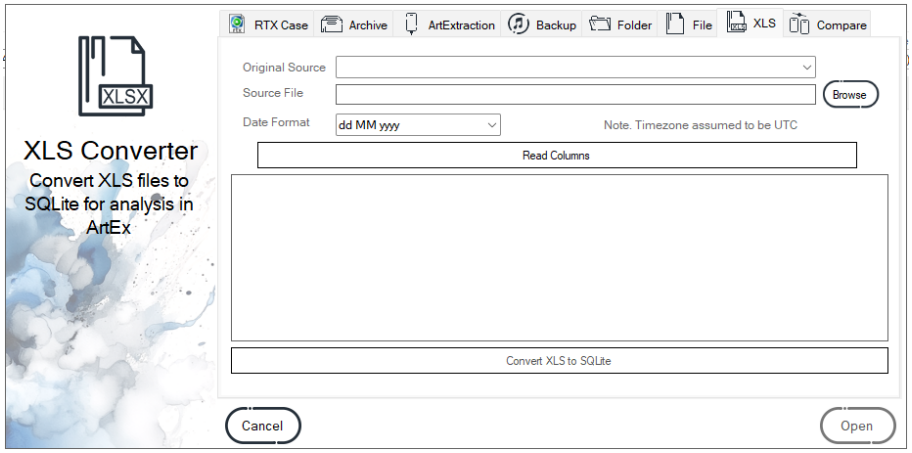
This can be great for running parsers against a specific file, or for loading a single files.

Note that loading a SQLite file will also incorporate the WAL if present.

Find File	The path of the Extraction file you want to open
Temp Folder	The path that ArtEx can use as a scratch folder
Recent	A list of recent (and accessible) Files. Note that loading a Recent File will use the same Temp Folder as was used previously.

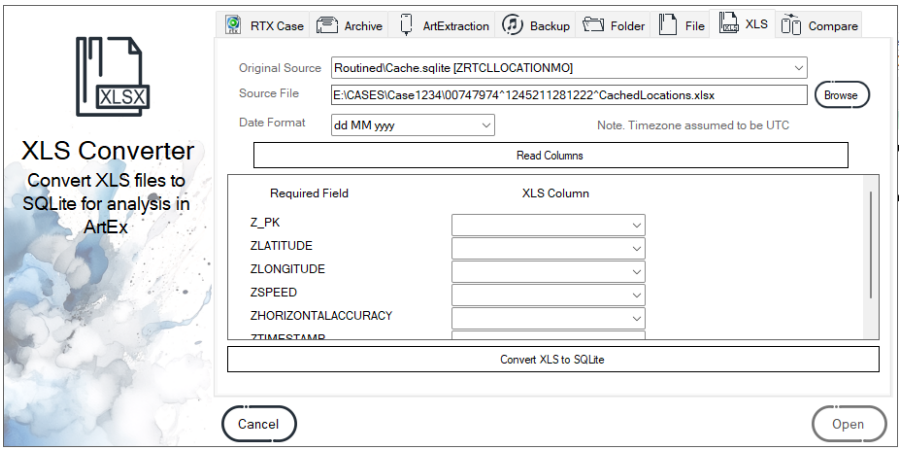
XLS

The XLS tab gives the option to convert XLS Spreadsheets made via reports in other forensics tools and convert them back into a database for processing.



It like goes without saying, but is important to note that the database generated will be limited to only the data from the spreadsheet.

As an example, if you have a Cached Locations spreadsheet from Axiom, you can convert it back into a Cache.sqlite ZRTCLLOCATIONMO table for processing in ArtEx.



Original Source	Select the appropriate source that you want to convert the spreadsheet back into.
Source File	The path to the XLS file.
Date Format	The date format used in the XLS file.

Press **Read Columns**. This will populate a list of table columns which are required. Use the dropdown list to select the equivalent column from the XML file.

Press **Convert XLS to SQLite** to attempt conversion.

Upon completion, the file will be automatically parsed and will appear as a **Recent File**.

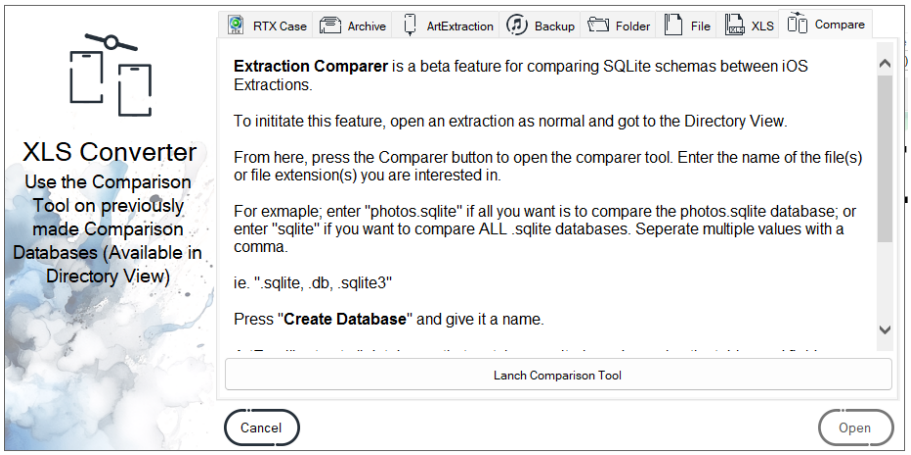
Comparison

The Compare feature is designed to identify differences between extractions. However, it is NOT designed to identify differences between contents of the extraction.

A use case for this could be to compare the SQLite schema of a database.

- Does the database exist in both extractions?

- Do both databases have the same tables?
- Do all tables have the same fields?



The Comparison Tool is explained in greater detail late.

Drag and Drop

Most extraction types that ArtEx supports can also be opened by Dragging and Dropping into the main window.

Supported Extraction types for Drag & Drop include;

- Archive
- Backup
- Folder
- File

Initial Processing

Whatever type of extraction you open, the initial process is near identical.

Step 1 : The file system is identified and mapped out.

Step 2 : Parsers are checked to see if they are relevant. (if selected).

Step 3 : Device Details / Contacts / Keychain and Locations (if selected).

No timeline parsers are run at this stage. This results in a fast initial processing time but means that additional parse time will be required during examination.

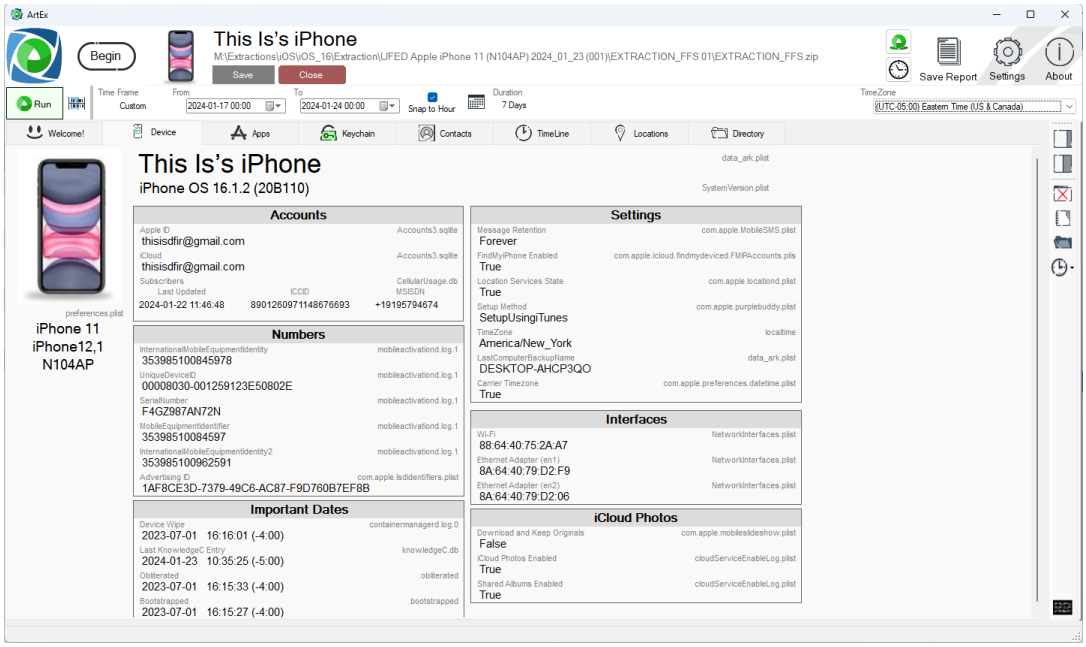
Starting an Examination

In this section, we will start at the point that an extraction is opened and work through the various tabs within ArtEx and look at each in depth.

Device Details

This tab will show the overview the extraction you have open.

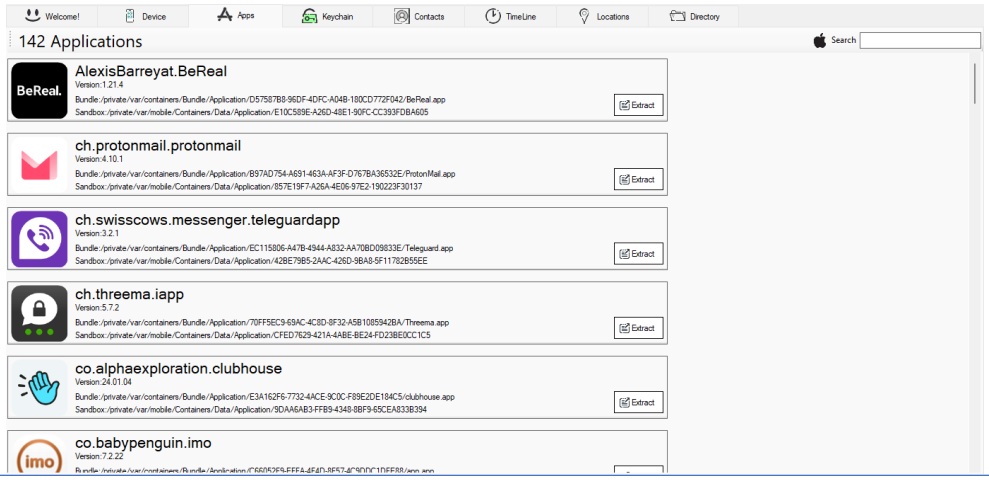
It includes important information such as the Device Name, Model, SIM and Account information and settings etc.



Any important value can be copied to clipboard simply by clicking it. Clicking the filename will open the file in the Right Pane.

Apps

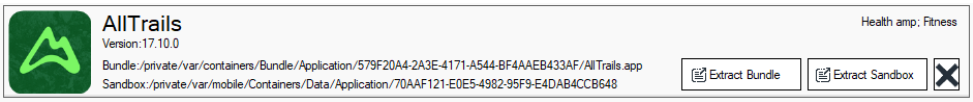
This tab will list the applications installed on the device. It can be run automatically during the initial process or run separately afterwards.



By default, all Apple Native applications are hidden. These can be shown by turning on the Apple button next to the Search box.

Searching installed Apps is possible by typing in the app name in the top right corner of the window.

Each application will show its icon and app name as well as it's Bundle and Sandbox path. These paths can be clicked to jump directly to the appropriate folder in the Directory View.



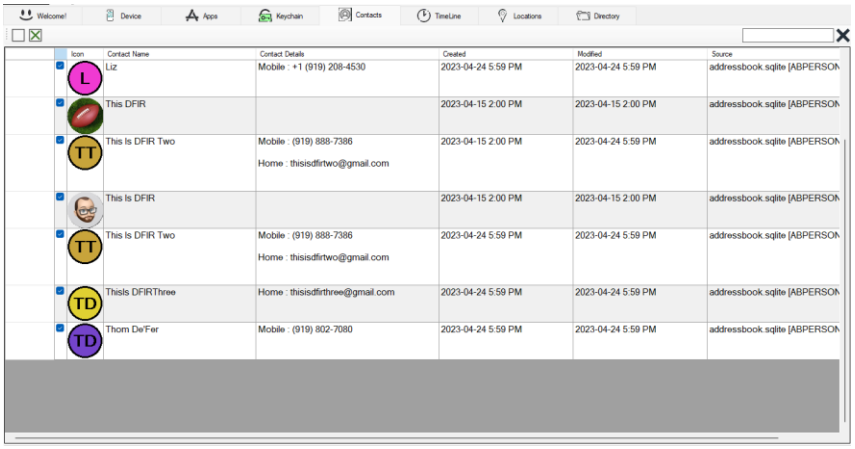
*Note that in cases such as Backups where the path may not be available, ArtEx will either make the link inactive, or will navigate to the equivalent path within the backup.

Each application also has an Extract button which allows you to save the contents of the Bundle or Sandbox directly.

Note that the icon is derived from the images on the extraction and may appear in odd colours.

Contacts

Once an extraction is parsed, the native contacts will be displayed in this table.



If the contact has an icon, it will be displayed. If there is no icon associated to the user, ArtEx will create one using the initials of the contact.

Note that parsing a communications app such as Discord or Snapchat will result in additional contacts being added to the Contacts tab.

Users can be searched using the textbox in the top right corner of the window.

Selecting and Deselecting Contacts will alter which contacts are included in any subsequent report.

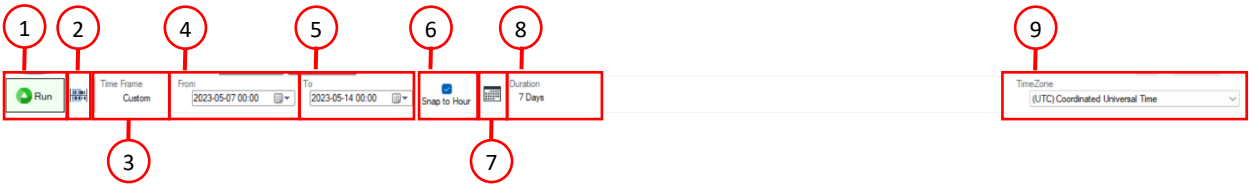
Blocked Contacts will be shown as "Blocked Number" or "Blocked Email".

TimeLine

The TimeLine is the main feature of ArtEx. It allows you to view all processed data chronologically to easily see how artifacts interact and overlap with each other.

For example, you can see when the device receives a notification, the display illuminates, the user opens the chat application sends a reply. Each step leaves its mark and ArtEx will show you this data.

The TimeLine tab is dependant on the Time Bar options at the top of the screen and we need to go over these in detail.



1 – Run Button
2 – Times of Interest (TOI)
3 – Time Frame
4 – From Time
5 – To Time
6 – Snap to Hour
7 – Save Time Frame
8 – Duration
9 – Time Zone Setting

Run Button
Reprocess the case with the new time or parser settings.

Times of Interest (TOI)
Set a Time of Interest – Explained in more detail later.

Time Frame
Select a predefined time frame such as “All Time”, “This Month” or “This Week”.

From Time
Select a custom start of the time of the time period you want to view.

To Time
Select a custom end of the time of the time period you want to view.

Snap to Hour
Snap time period to complete hours or allow minutes.

Save Time Frame
Save the time setting for this case.

Duration
The calculated duration between the Start and End timestamps.

Time Zone Setting
The Time Zone Setting in use.

Most of these are self explanatory, but some require further explanation which will be covered shortly.

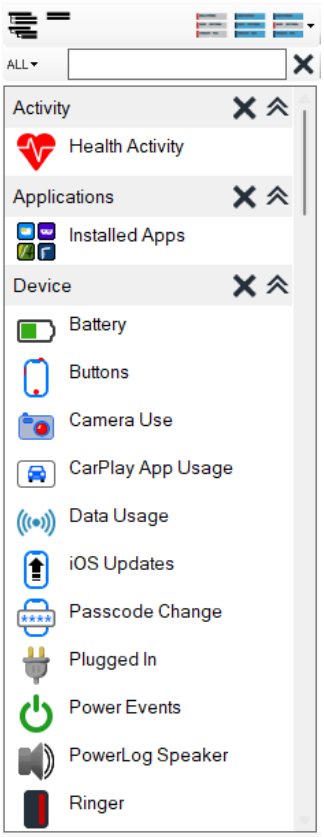
Generally, once a device is parsed, the time period will default to the last week of data before the extraction occurred. However, there are caveats to this and it may not occur every single time.

The left side of the window will show the list of available parsers.

Note that if you have the “Check for Parser Eligibility” checked in the settings, ArtEx will have taken a little longer during the initial parse to verify what files exist on the extraction and which parsers will be able to run. For example, if no Snapchat data files exist on the extraction, then the Snapchat parser will not be present in the list.

However, if you have this option turned off, you will be presented with all parsers, regardless of whether the data files exist or not.

The Parser List contains several parts;

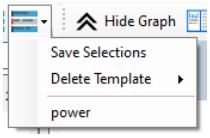


At the very top are 5 icons.

The first two  will expand or collapse all parser groups.

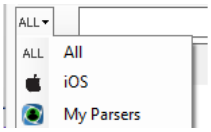
The second two  will select or deselect all parsers.

The Final icon will allow you to save the selections you currently have as a template for quicker selection in the future.



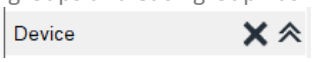
These templates are referred to on the Settings screen and allow you to choose a template to parse by default.

The second tool bar row contains a drop-down menu for selecting parser type.



There is also a search box, allowing you to search for the name of the parser you want to find along with a Clear Search button.

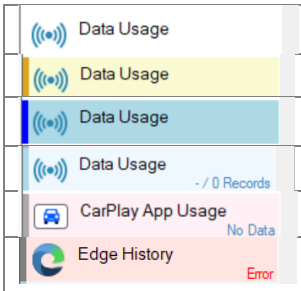
The parsers are arranged into groups and each group has its own Header bar.



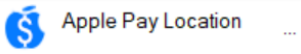
The Header bar contains the name of the group on the left and the expand/collapse button on the far right.

Clicking on the header title will select all parsers in the group and clicking the ✕ button will deselect all parsers in the group.

Lastly, each parser has its entry which can be selected/deselected by clicking. The item is colour coded as follows;

	White = Unprocessed parser. Gold = Currently highlighted parser. Blue = Selected parser. Light Blue = Disabled parser. Light Red = No data (ie. Files do not exist) Red = Parser error. This usually occurs due to the source file not being as expected.

Some parsers have additional options, as seen by the ellipsis on the right side of the button.



The ellipsis will open a mini menu for that parser.

Mini Menu's typically contain options such as:

- Show Media - Show the thumbnails of media files.
- Map All/Map<200m - Create a map for ALL location records or just those with accuracies better than 200m.
- Show Course - Show Course/Heading information on the drawn map.
- Add Password - Add a password or password list for the specific parser.
- Allow Download – Allow ArtEx to go online to download media if it cannot be found on the extraction.

Run ArtEx

Once you have selected the appropriate time frame and parsers the that you are interested in, press the 

button from the Time Bar and ArtEx will begin processing.

The first time a parser runs, the entire data source is processed. This may take some time depending on how much data there is. The data is cached however for faster use in the future.

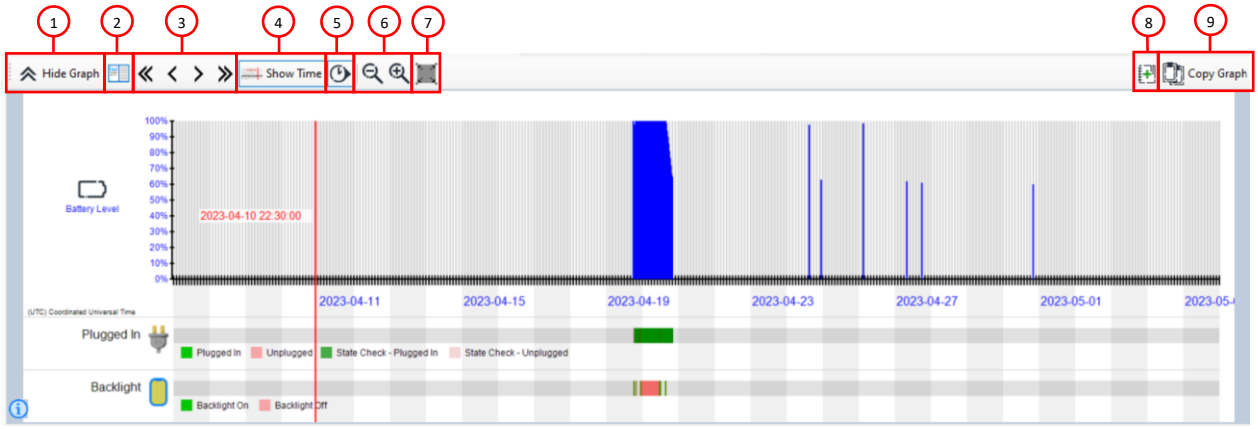
Note that although the entire dataset is processed at this time, only the dependant files needed for the selected time period will be processed.

For example; if processing Photos for a 1 month time period, the entire database will be processed, but only the single month of images will be processed.

If you then choose to process a different month, although the database does not need to be processed again, the new images will be and therefore, additional processing time may be required.

The TimeLine Graph

If your time period is less than 32 days, your parsed data will be shown in a Gantt chart. This view allows you to see all activity for the selected parsers in a quick, visual way.



1 – Hide Graph
2 – Change Layout
3 – Nudge Time Period
4 – Show Time
5 – Auto Apply
6 – Graph Zoom
7 – Graph Reset
8 – Save Graph to Report
9 – Copy to Clipboard

Hide Graph

Show or Hide the graph pane.

Change Layout

Change the layout between Horizontally or Vertically stacked panes.

Nudge Time Period

Change the selected time period. A single arrow < will nudge forward or backwards 1 hour whereas a double arrow « will nudge forward or backwards by 24 hours.

Show Time

Turn on or off the red line and time label shown on the graph as you move your mouse around.

Auto Apply

ArtEx will automatically run after any changes applied to the selected time period. With this turned off, you are required to press Run after any change.

Graph Zoom

These controls allow you to zoom in or out of the Graph image.

Graph Reset

Reset the zoom level of the graph image and recentre it.

Save Graph

Add the graph image as a Report Element.

Copy to Clipboard

Copy the graph image to the clipboard.

As well as the buttons listed above, the graph can be interacted with in a number of other ways as well.

Single Left Click
Scroll the table view to the closest record chronologically to the selected time on the graph.

Left Click & Drag
Set the Time Period using the graph. Left click sets the start, letting go sets the end.

Left Click & Drag on Parser Name Up/Down
Will allow you to reorder the parsers in the graph.

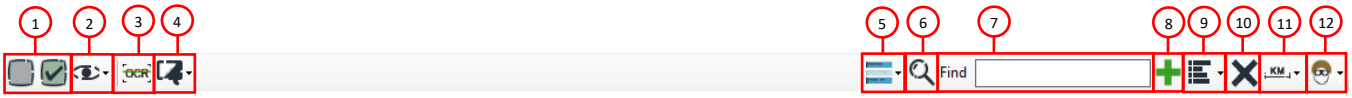
Mouse Wheel
Scroll the Time Period 1 hour forwards or backwards.

Mouse Wheel + Ctrl
Zooms in to the selected time. 1 hour is added to the start time and subtracted from the end time.

Mouse Wheel + Shift
Will zoom in/out of the graph image.

The TimeLine Table

Regardless of the length of selected time period, the Time Table will show all records chronologically.



1 – Deselect/Select all records.
2 – View Settings
3 - OCR
4 – Translation settings
5 – Show/Hide parser results
6 – Search
7 – Filter Text
8 – Add to Filter Text
9 – Filters & Conditions
10 – Clear Filter
11 – Filter Locations by accuracy
12 – Filter media by descriptors

Deselect/Select all records
Causes all visible records to be either selected or deselected.

View Settings
Change the view settings which includes either viewing ONLY the selected/deselected or changing the font size.

Translation settings
Translates the parsed messages.
Note that this requires additional configuration which is discussed later.

Show/Hide parser results
This option will allow you to turn on/off specific parsers from the table view similar to turning items off from the Parser List. The record will be removed from the table view but **not** from the graph.

Search
Search the Timeline Table for a specific word.

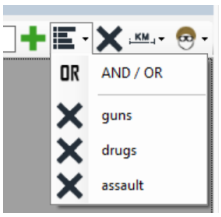
Filter Text
Filter the Timeline Table by a specific word.

Add to Filter Text

Pressing the button will add the current Filter Text to a list and allow you enter another filter term. Using this allows you to build a more complex filter.

Filters & Conditions

This dropdown will include the mode of the filter and all the terms you entered using the Add to Filter button.



The very top item is the AND / OR operator. Pressing it will switch the search between AND or OR conditions.

All other items are the search terms entered.

In the example shown, ArtEx is in **OR** mode and so the results will include any record that includes any of the terms included.

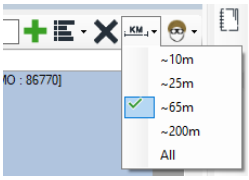
Pressing the top item will change the mode to **AND** mode and so the results will only include any records that includes ALL the terms included.

Pressing the term itself will remove it from the list.

Clear Filter

Clears all applied filters from the Text Filter list.

Filter Locations by Accuracy



This filter allows you to remove location records from the timeline that have low accuracy.

For example, selecting the 65m from the list will remove all records from the timeline that have an accuracy higher than 65m or records that don't include accuracy information.

Note that use of this filter will also remove non-location records.

Filter Media by Descriptors

This filter allows you to filter media items by using person descriptors such as Male or Female, Adult or Child, Bald or wearing Glasses etc.

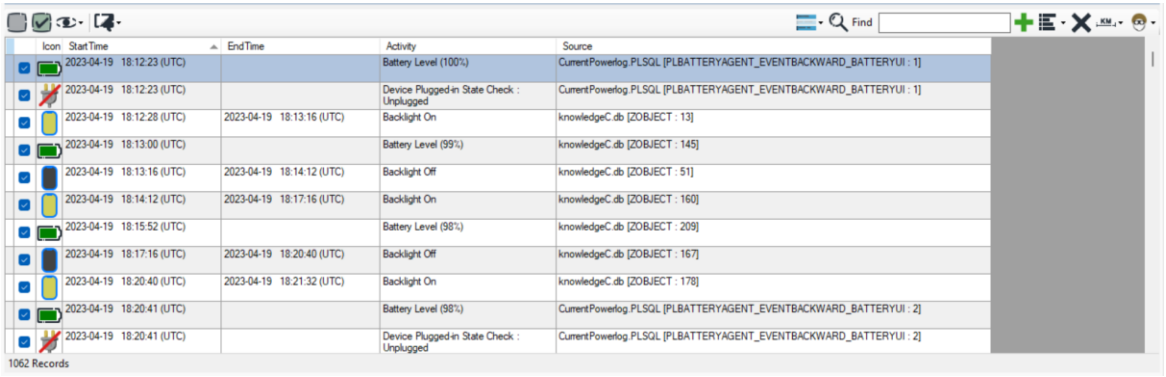
These descriptors are based on Apple's native media classifications.

Note that use of this filter will also remove non-media records.

The Table itself contains numerous standard columns including;

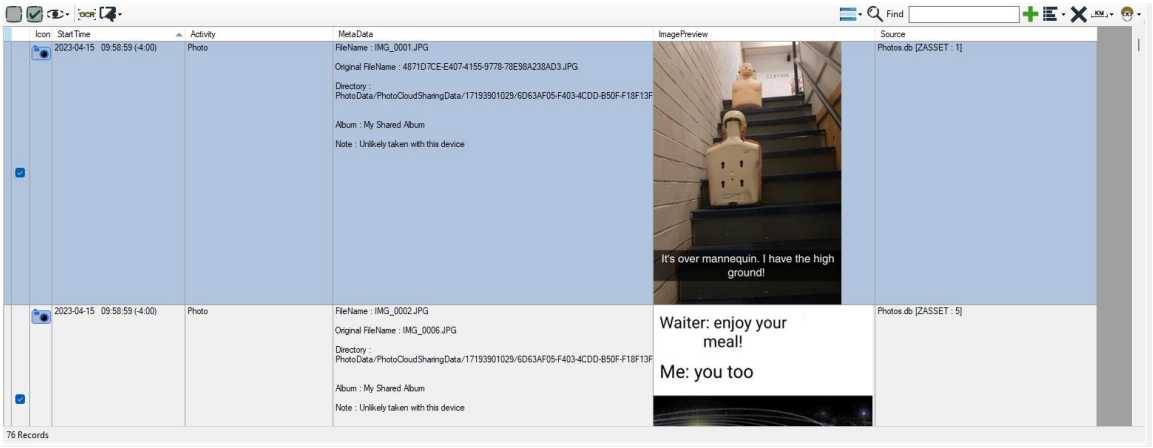
- **Time Of Interest Indicator** – The very first column will be coloured to reflect TOI information.
- **Selection State** - if the item will show in a report.
- **Icon** - A graphical representation of the activity.
- **Start Time** - The Start Time / only time related to the record.
- **End Time** - The End Time of the record (if applicable).
- **Activity** – A description of the record.

- **Source** – Details of where the record originated.



Depending on the type of record, it may also include;

- **MetaData** – Important information about the record. This could be anything such as location coordinates, message group information, media descriptions etc.
- **Message Body** – The message contents that were sent as part of the activity.
- **Media Preview** – The image related to the record. This could be an image from the device, or a map generated by ArtEx to show the location record.



Double Clicking on a cell may open the right pane.

- Double clicking on the **MetaData** or **MessageBody** cell will open a right pane with a breakdown of the MetaData information for easier copying.
- Double Clicking on the **Image Preview** cell will open the media item up for interaction such as zoom, rotate, export or OCR.
- Double clicking the **Source** cell will open the data source for the record; databases will open to the specific record if possible.

Time Zones

Similar to all other forensic applications, ArtEx parses most timestamps as UTC. This UTC value is held as the parsed records timestamp.

The time zone of the case can be changed using the dropdown menu in the top right corner of the screen. When this is changed, the timestamps shown (in the table, graph and databases) will be shown in the appropriate time zone.

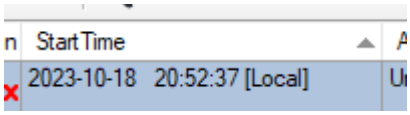
However, some records are not stored in UTC and ArtEx handles these differently to what you may be used to.

Records found in logs are often saved with Local timestamp information that may or may not include the time zone offset.

If the record does include the offset, then the parser will convert the timestamp UTC and all further calculations in the UI will be handled as though it was a UTC timestamp in the first place.

If the record does NOT include the offset, then ArtEx has no choice but to treat it as a “Local” timestamp.

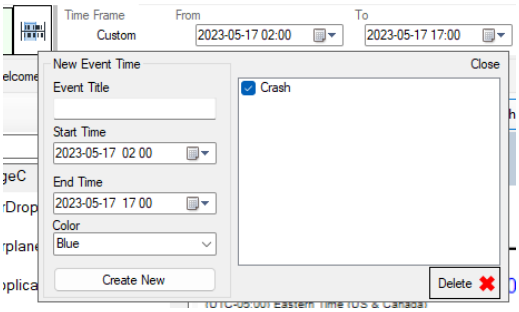
This will appear as a timestamp in the table with **[Local]** written next to it.



The time shown in a [Local] record will never change regardless of the time zone you have selected. It’s location within the chronology of the table should always be correct however.

Time of Interest (TOI)

The Time of Interest feature allows you to enter details about a refined time period you are particularly interested in such as the time of a crash or the time that a crime occurred.



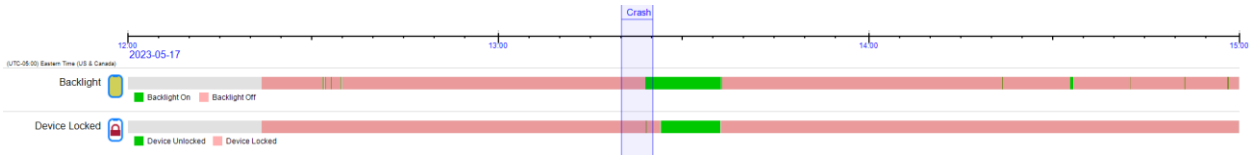
Enter a title, select the start and end dates and choose a colour from the pre-defined list. Then press **Create New**. You will see it gets created in the list on the right.

From here, you can turn the TOI on/off or delete it. Once you are happy with your TOI’s, press Close in the top right corner.

The TOI information will be shown in several locations, designed to make examinations easier, including;

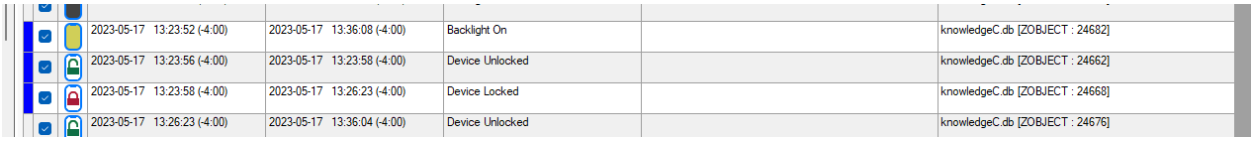
Graph

The TOI will be displayed on the graph so that you can easily see the time that you are interested in and compare it to actions on the device at that time.



Table

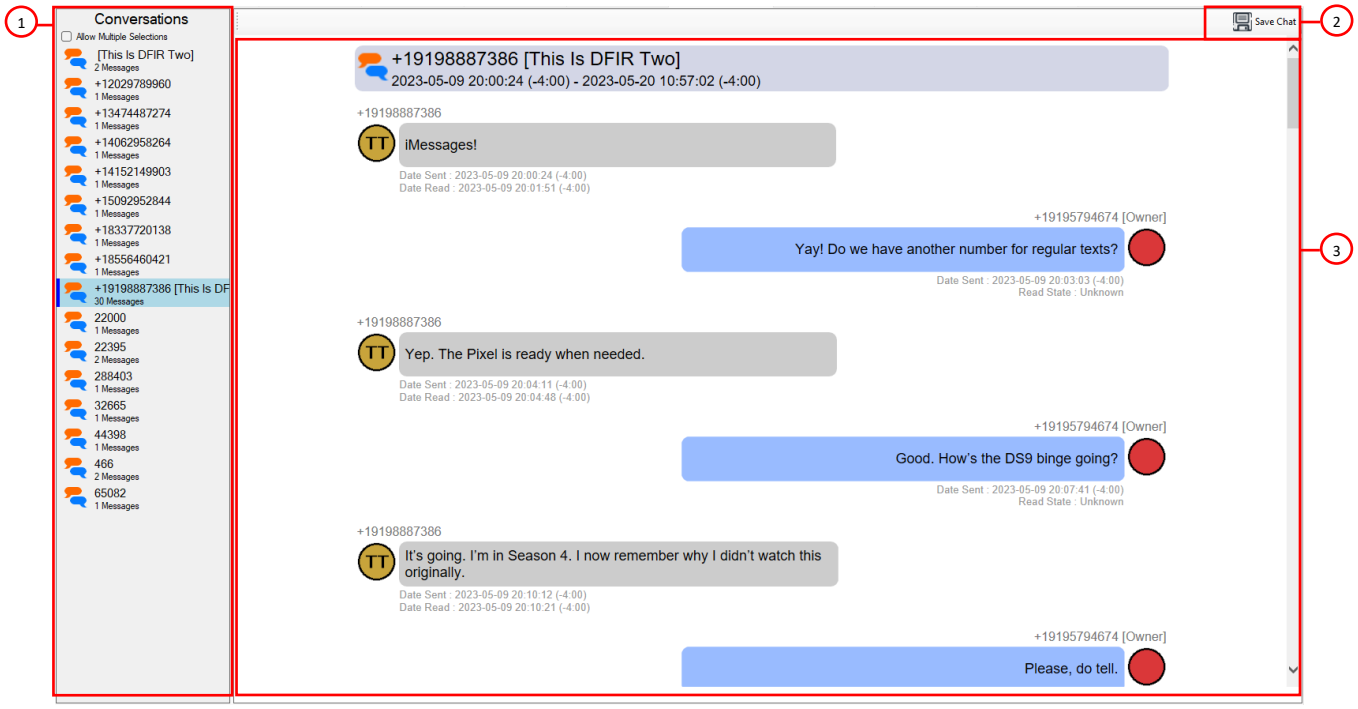
The TOI will also display as a coloured bar on left side of the table view to indicate that this action occurred during the TOI event.



2023-05-17 13:23:52 (-4:00)	2023-05-17 13:36:08 (-4:00)	Backlight On		knowledgeC.db [ZOBJECT : 24682]
2023-05-17 13:23:56 (-4:00)	2023-05-17 13:23:58 (-4:00)	Device Unlocked		knowledgeC.db [ZOBJECT : 24662]
2023-05-17 13:23:58 (-4:00)	2023-05-17 13:26:23 (-4:00)	Device Locked		knowledgeC.db [ZOBJECT : 24668]
2023-05-17 13:26:23 (-4:00)	2023-05-17 13:36:04 (-4:00)	Device Unlocked		knowledgeC.db [ZOBJECT : 24676]

Chat

If the timeline data you are viewing includes Chat Messages, the Chat tab will appear and provide another way to view the message data.



1 – Conversations
2 – Save Chat Pane
3 – Chat Pane

Conversations

This pane will list all conversations found within the selected time period.

By default, only one conversation can be selected at a time and clicking the conversation will load it into the Chat Pane.

The checkbox "Allow Multiple Selections" will allow you to select multiple conversations and show them on screen consecutively.

Save Chat Pane

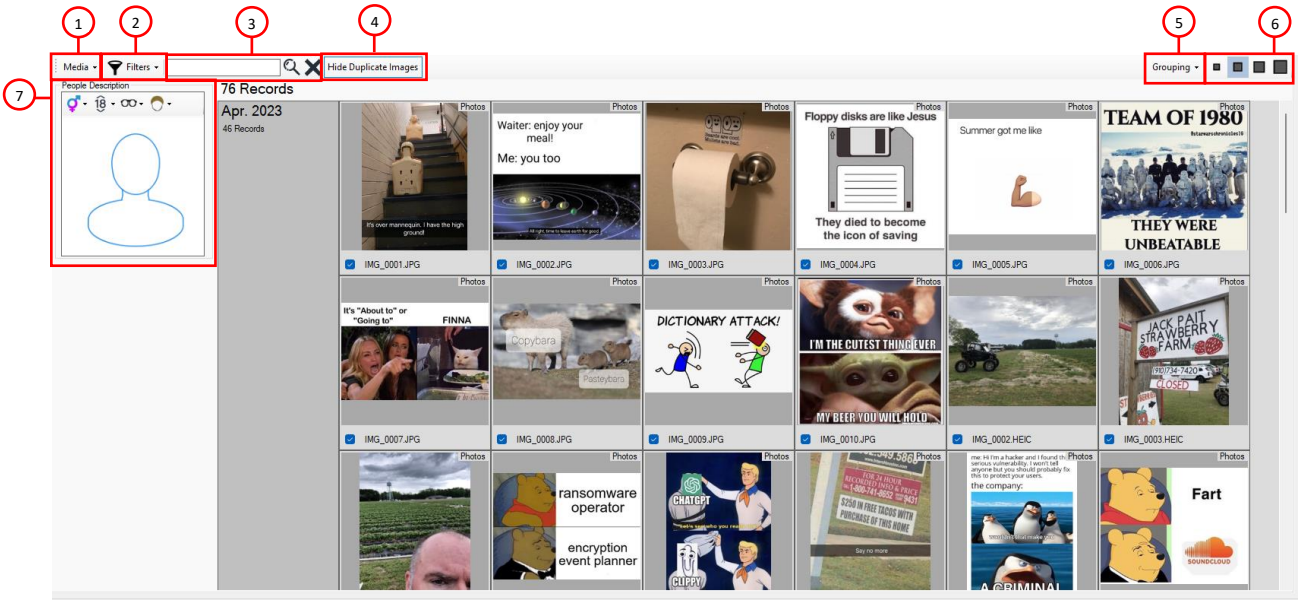
This button will allow you to save the current chat pane contents as HTML.

Chat Pane

This pane contains the chat messages which are part of the currently selected chat.

Gallery

The Gallery tab will show media items from the timeline in a thumbnail view.



1 – Media Types
2 – Filter Options
3 – Search
4 – Duplicate Options
5 – Grouping
6 – Thumbnail Size
7 – Person Descriptor

Media Types

This menu allows you to refine the filter for the type of media being shown in the Gallery View. You can choose to Show or Hide Photos, Live Photos, Videos, Screenshots, Attachments or images from Apps.

Filter Options

The Filter Options includes more filters including items that include people, are part of a specific Album or Moment or are believed to be taken with the device being examined.

Search

A simple search for specific text along with the Clear search option.

Duplicate Options

ArtEx can show or hide duplicate images.

Grouping

Choose how to Group the messages. Options include by Day, Month, Year or Moment, Album or App.

Thumbnail Size

Choose the size of the thumbnail image.

Person Descriptor

Similar to the Person Descriptor on the Timeline, you can use this to build a person description and filter the images being shown.

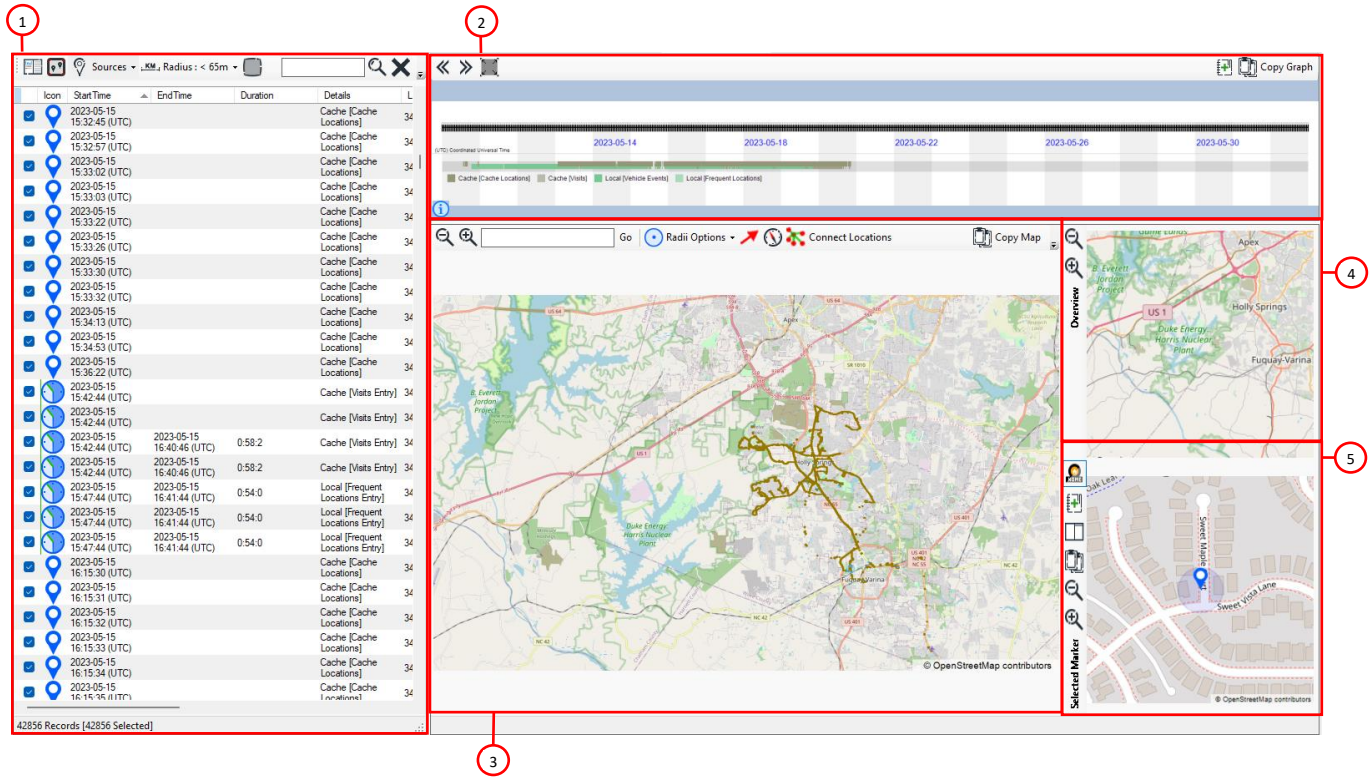
Double clicking a thumbnail will load the image to the Right Pane.

Locations

The Locations tab is a dedicated view for location data and will show all items on one large map instead of the thumbnail maps used in the timeline.

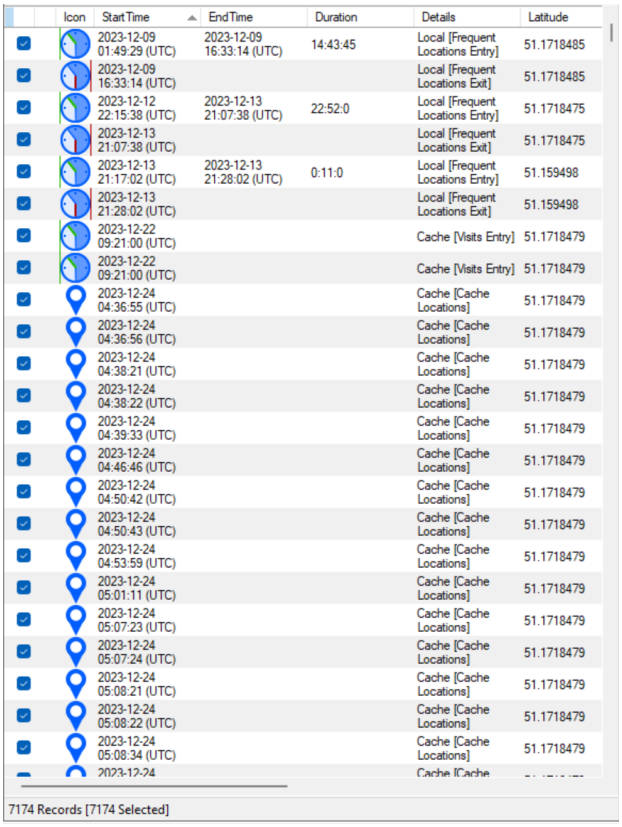
Locations parsing can take a significant amount of time. For this reason, ArtEx given you the choice of running the Locations parser as part of the initial decode or to opt to run it manually.

The Locations tab is broken into several panes:



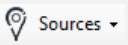
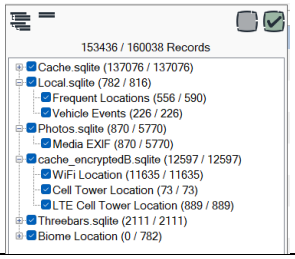
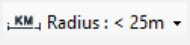
1 – The Locations Table View
2 – The Locations Timeline Graph
3 – Location Main Map
4 – High level overview
5 – Selected Record Close-Up

The Locations Table View



This table view includes all Locations record within the selected time period, including;

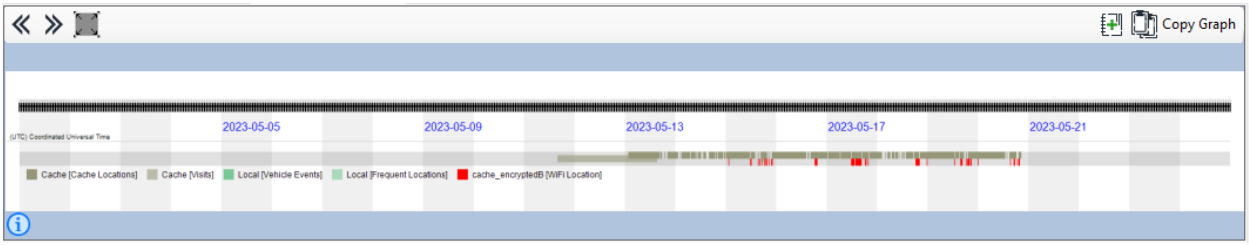
- Selection State
- Label
- Start Time
- End Time (if available)
- Duration (if applicable)
- Details (such as the origin of the record or MAC address etc)
- Latitude & Longitude
- Accuracy
- Speed (If available)
- Course (if available)
- Source ID (Typically the ROWID from the database)
- Parser name

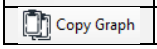
	**Switch Layout** will reorganize the view between horizontally or vertically stacked panes.
	**Match Bounds** will filter the records in the table to match the bounds of the map being viewed.
	**Sources** will open to show the Locations records that were found and allow you to turn on or off any of the sources.  Each Source may have a sub-source and each can be turned on or off independently. Each item has 2 numbers next to it within parenthesis. The first number is the number of items withing your selected time period. The second number is the total number of records found.
	**Radius Selection** will filter the records being shown by their Accuracy value, allowing you to focus on just the higher accuracy records.
	**Select All** and **Deselect All** will select or deselect all records in the table. The selection state of the records in the table will be reflected in the markers shown on the map.
	**Create Flipbook** will create an animated view of the selected location records and is covered in more detail later on.
	**Export to CSV** will export the contents of the Table View into a CSV file.

	**Label Marker** will include the timestamp of the record on the map alongside the marker. Only the records selected in the table will be affected. More details can be found shortly.
	**Search and Clear** can be used to manually filter the table or clear the search.

The Locations Graph

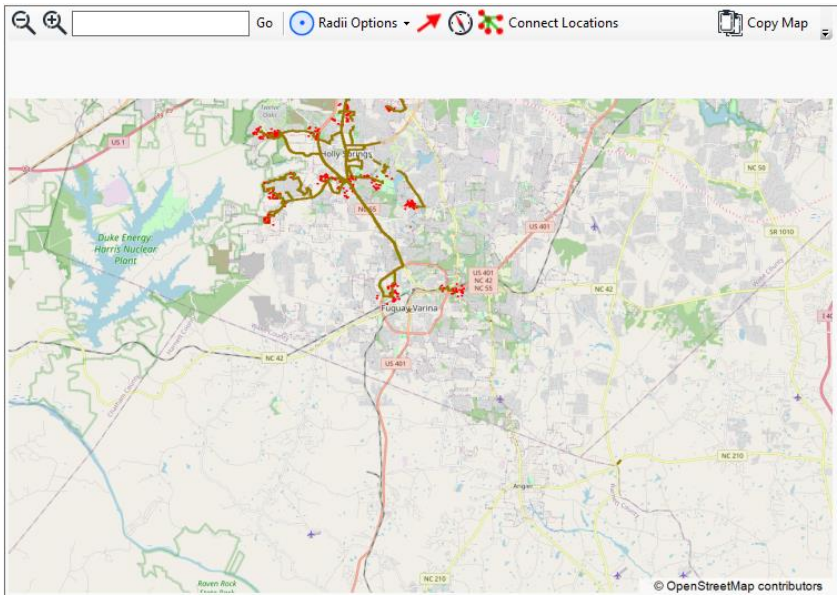
The Locations Graph is functionally similar to the TimeLine graph.

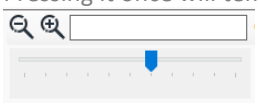


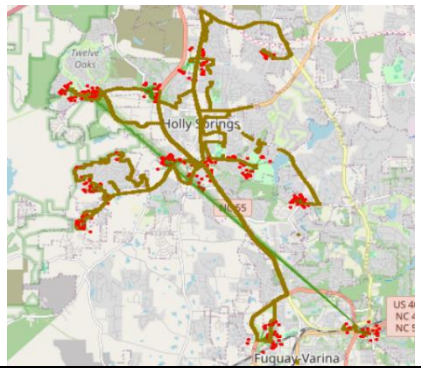
	**Nudge** 24hrs forwards or backwards. This will affect the overall Time Period being viewed.
	**Reset View** will reset the state of the graph.
	**Add Element** will add the graph image to the Report Elements.
	**Copy Graph** will copy the graph image to the clipboard.

As with the TimeLine graph, you can use the mouse to refine the time period or scroll forward/backwards in time.

The Main Map



	**Map Zoom** can be used to zoom in or out of the map. Pressing it once will temporarily open a slider for faster zoom controls 

Go	**Jump to Location** lets you directly enter GPS Coordinates (decimal format) and immediately jump to that location.
Radii Options	**Radii Options** allows you to change the opacity of the Accuracy Radius or hide it altogether.
	Highlight Marker will draw an arrow to the record(s) you have selected in the Table View. 
	Course will draw an arrow on the map to indicate the direction of travel for each marker on the map (if available). 
Connect Locations	**Connect Locations** will draw a line between the Wifi and Cell Tower Locations found in the Cache_EncryptedB database and the temporally closest record from the cache.sqlite database.  The initial reason for this feature was to demonstrate why the cache_encryptedB records could not be trusted as the location of the device at the time shown.
Custom Markers	**Custom Markers** allow you to add custom locations to the map and are discussed in more detail lower down.
	Clear Drop Pin will remove any drop pins you have added to the map. Drop pins are discussed shortly.
Copy Map	**Copy Map** will copy the map image to the clipboard.

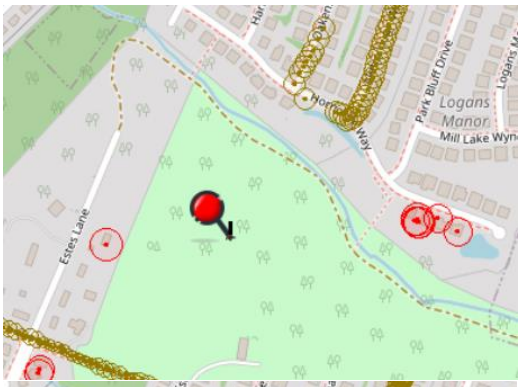
Map Navigation

There are several options for navigating the map aside from the simple zoom options in the tool bar.

1 – Double Clicking on a record in the Table View will center the record in the main map.
2 - The Mouse Wheel can be used for zooming in and Out of the map relative to the location of the mouse pointer.
3 – Single Left clicking anywhere on the map will recenter the map around the selected location.
4 – Left Click and Drag will create a box to zoom to.
5 – Keyboard cursor keys can be used to move the map around.

Map Tools

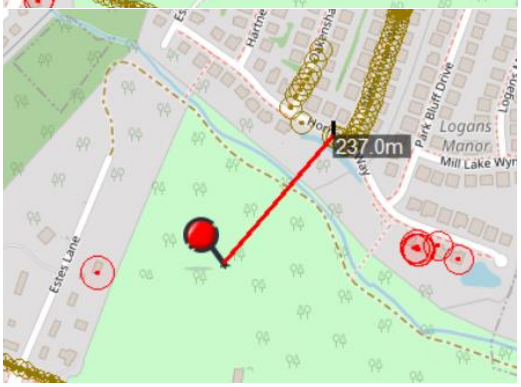
Drop Pin – Pressing SHIFT while Left clicking on the map will drop a pin. This is a way to temporarily mark a location of note.



Measure – Once a pin is dropped, continuing to hold SHIFT while moving the mouse will draw a measurement on screen between the Pin and the current location of the mouse pointer.

Releasing SHIFT will stop drawing the measurement and will leave it in its current state.

Press  to remove both the drop pin and the measurement.



Find Record – Hold CTRL and click on a marker on the map to jump to the appropriate record in the table view.

Markers Labels

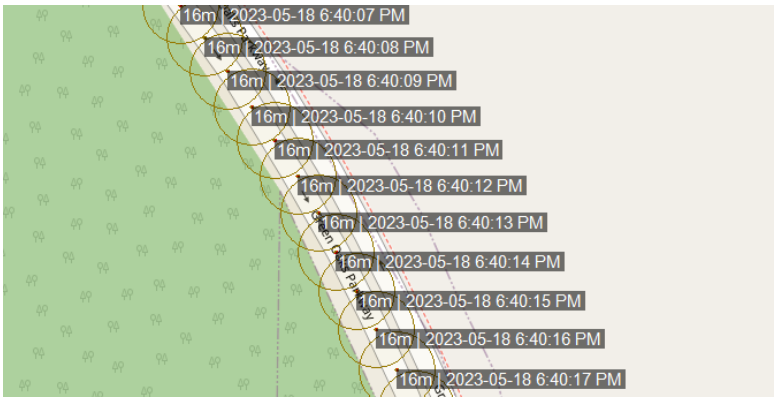
There are several options for labelling markers on the main map.

Option 1

The first, and simplest option is to select the records you are interested in on the Location Table and press the  button.

This will turn the Timestamp label on for all selected records. This is indicated in the Table view with a  icon in the second column.

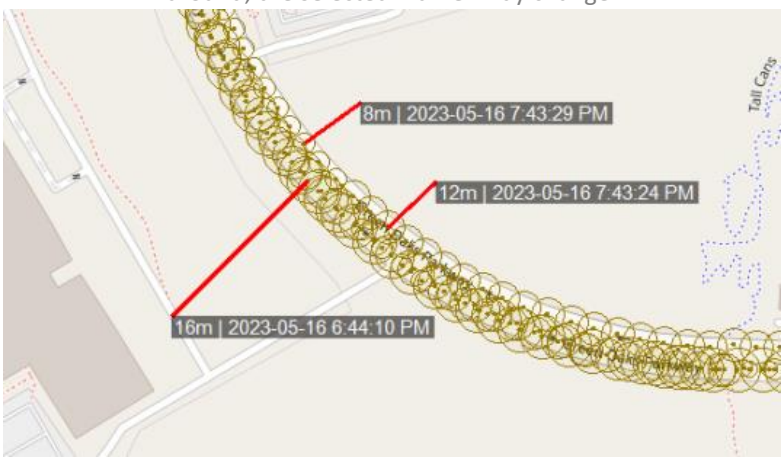
It will also place the Timestamp label on the map in the default location next to the appropriate marker.



Pressing again on a record that already has Marker Labels turned on, will turn the marker label off.

Option 2

Move your mouse over (or close) to a marker while holding SHIFT and CONTROL to show the timestamp of that specific marker. The selected marker will be whichever is the closest to the mouse cursor and you move around, the selected marker may change.



Left Clicking while still holding SHIFT + CONTROL will lock the timestamp label in place and you will see the icon appear in the Table view on the appropriate record.

Option 3

If you know the specific marker on the table you want to highlight but cannot find It on the map view (or it is obscured by other records), double clicking the row in the table while pressing CONTROL and SHIFT will lock in your chosen record and you will see that the record shows "…" where you normally see the icon.

Now, with SHIFT + CONTROL pressed down, you can move your mouse anywhere on the map and the label will always point to your selected record. Left click to lock in the location of the label on the map.

Option 4

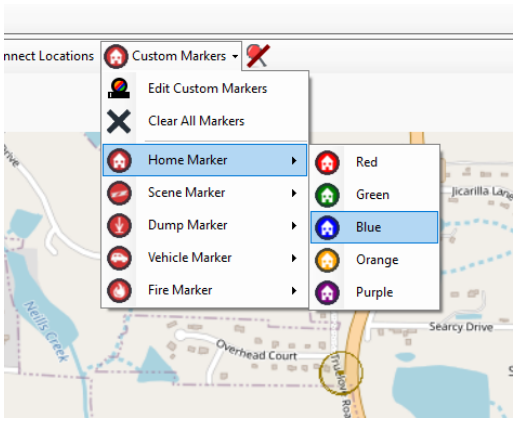
Press the Right Mouse Button on a map marker while holding SHIFT + CONTROL will result in a similar outcome as option 3. The associated record will show "…" and now regardless of where you move your mouse, the timestamp label will always point back to the selected record.

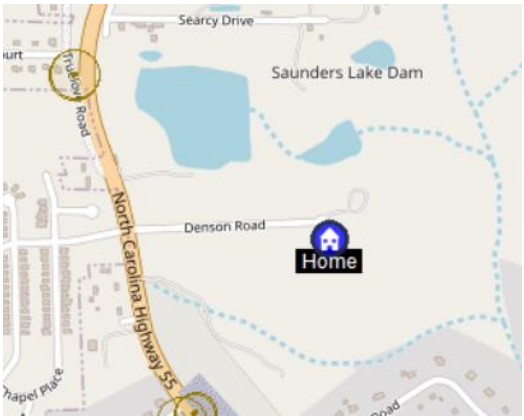
Custom Markers

Custom Markers allow you to place a more permanent marker in a location relevant to your case.

Current Marker options include **House**, **Car**, **Scene**, **Fire**, **Dump Site**, and each marker can be shown in a different colour; either Red, Blue, Green, Purple or Orange.

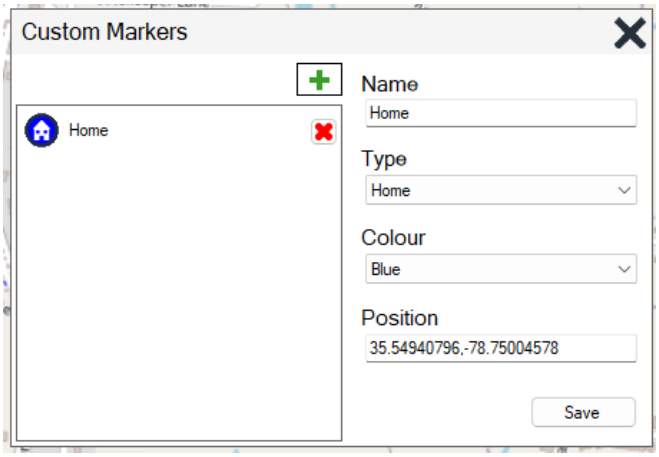
Select a marker type and color and click on the map to place.



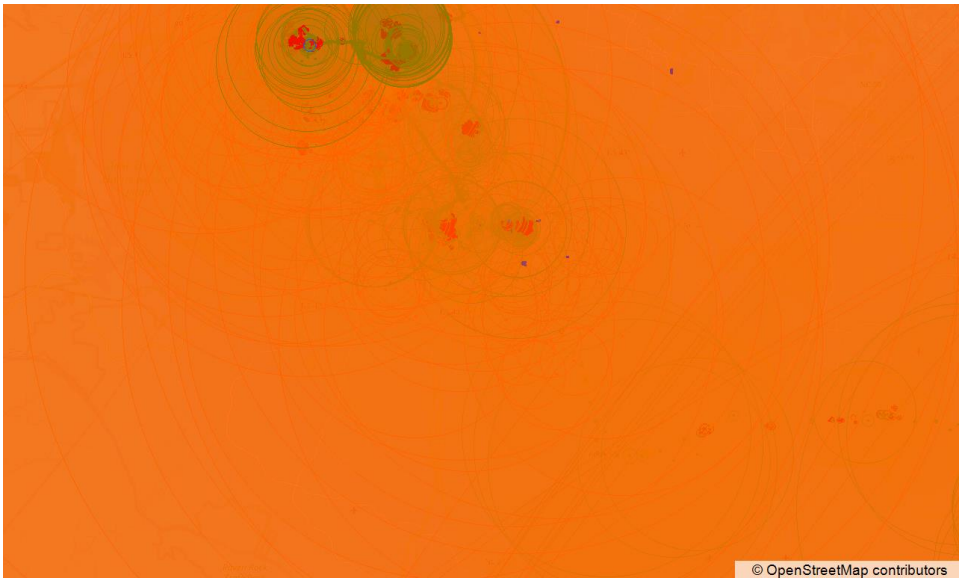


This marker will remain persistently in the selected location.

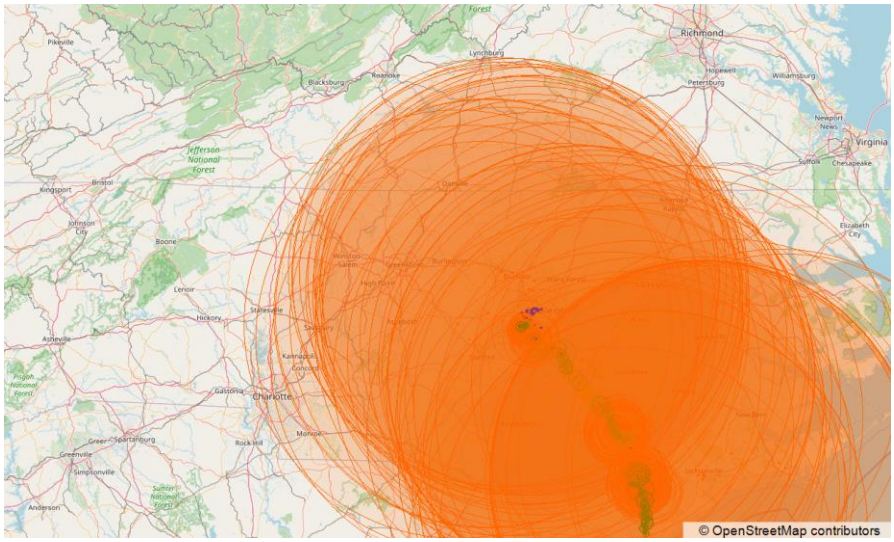
To alter or rename the marker, press Custom Markers > Edit.



It is quite common that upon first loading the Locations screen, the entire map will be presented in a mass of orange.



This is not an error but reflects the number of records parsed. Zooming out will give a clearer picture of what the cause of the orange screen is:

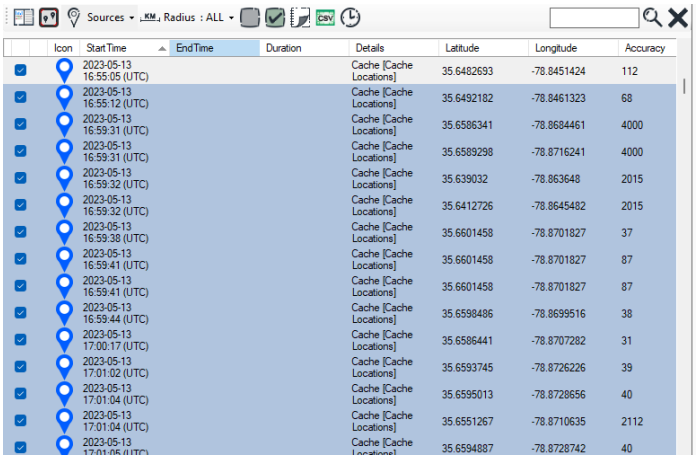


Reducing the Sources or changing the Accuracy Filter is a good way to remove these low accuracy and troublesome records.

Creating a Flipbook

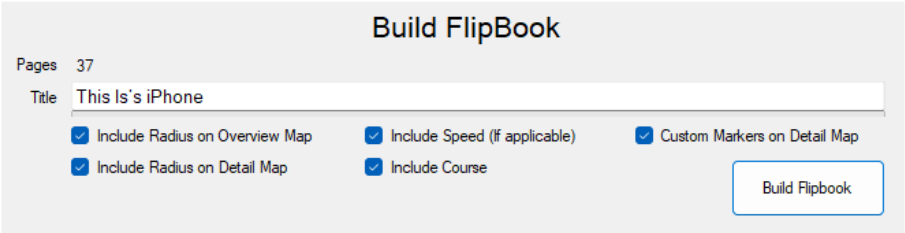
A Flipbook is an animation of the location data that can be either presented as a HTML document to scroll through or as an MP4 video.

Start by highlighting the records you want to include in the Flipbook.



The press the Create Flipbook button  .

A new tab will open within the Locations tab and will present the FlipBook options.

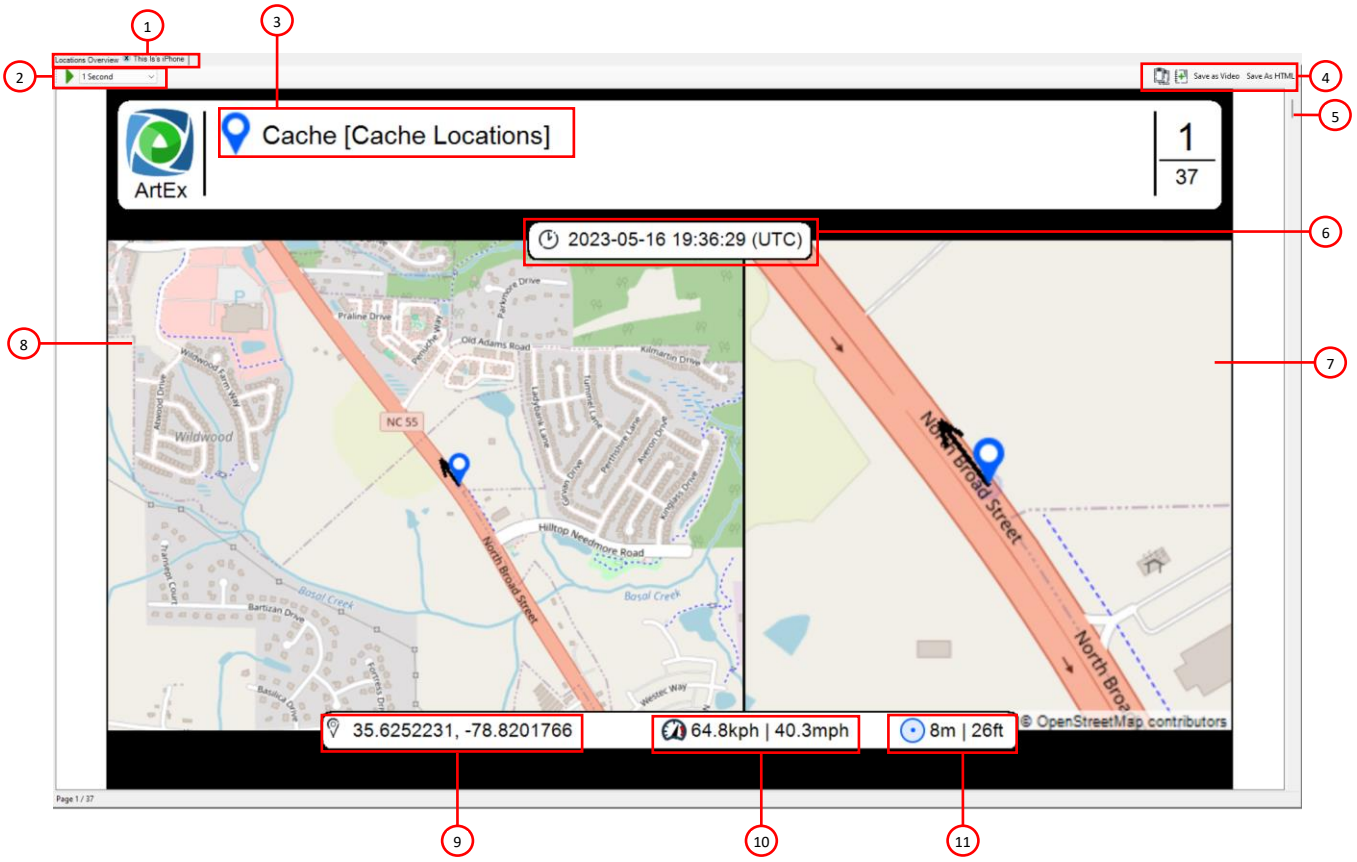


This window informs you of the number of pages in the flipbook (relative to the number of records highlighted) and gives the opportunity to give the Flipbook a title.

You then have some options:

1 – Include Radius on Overview
2 – Include Radius on Detail Map
3 – Include Speed (if applicable)
4 – Include Course
5 – Custom Markers on Detail Map

When you build the Flipbook the tab will update with the results.



1 – Locations Tabs
2 – Play/Pause and Play Speed will auto-scroll though the pages.
3 – Parser Name
4 – Save Options (Copy to Clipboard, Save to HTML, Save as MP4)
5 – Manual Scroll.
6 – Timestamp of the current record
7 – Detail Map shows a close view of the current record.
8 – Overview Maps shows a higher level view of the current record.
9 – Coordinates of the current record.
10 – Accuracy of the current record.
11 - Accuracy of the current record.

Saving Flipbook

Flipbooks can be saved as either an interactive HTML report or MP4 video using the buttons shown in the image as item 4.

To save as an MP4, you will need to have FFMPG installed at the default location on your C drive (C:\FFmpeg). Download FFMPG from https://ffmpeg.org/download.html.

Offline Use

As an offline user, you have two options to make use of Map data.

Tile Grabber

When you try to use maps in ArtEx while offline, you will be prompted to use Tile Grabber by inserting a USB Drive and selecting the drive from the list.

ArtEx will copy a small tool to the USB along with a list of required map tiles. Once finished, take the USB to an internet connected computer and run the TileGrabber.exe.

TileGrabber will download all required tiles and once finished, return the USB to the original computer for ingestion.

Custom Tile Server

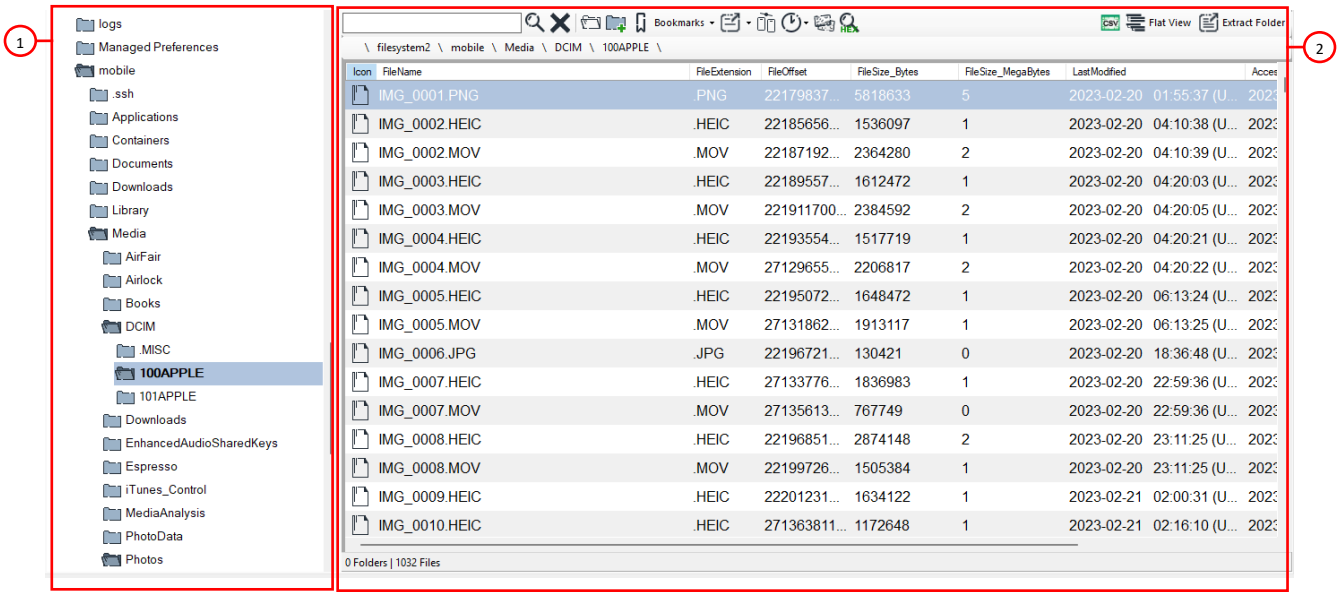
Setting up your own OpenStreetMaps server on the inside of your network is another alternative.

Create a text file called **CustomMapTileServer.txt** which contains only the URL of your server. Save this file in the root directory of ArtEx.

Directory

The directory view allows you to navigate the file structure that has been parsed.

It is split into 2 main sections: Tree View and Table View.

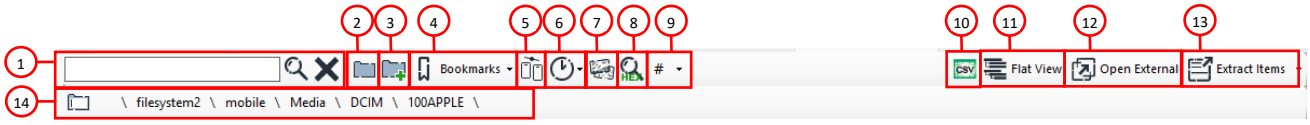


1 – Tree View
2 – Table View

The Tree View shows only folders in an open or closed state. Clicking on a folder to open it will show all folders inside and will also update the table view to show all items inside it.

Clicking on an open folder will close it.

The Table View will show all items inside the currently selected folder.



1 – Search Options
2 – Show Folders in Table
3 – Open New Directory Tab
4 – Bookmarks
5 – Extraction Comparison
6 – Time Filter
7 – Show Thumbnails
8 – Hex Search
9 – Hash Files
10 – Export to CSV
11 – Flat View
12 – Extract Folder
13 – Extract Items
14 – Breadcrumb Path

Search Options

Type in the name of the file or folder you are interested in and press 🔍.
Press ✖ to clear the search.
Note that using the Search feature will disable the Tree View until ✖ is pressed.

Show Folders in Table

This option will turn on/off folders from showing in the main Table View.

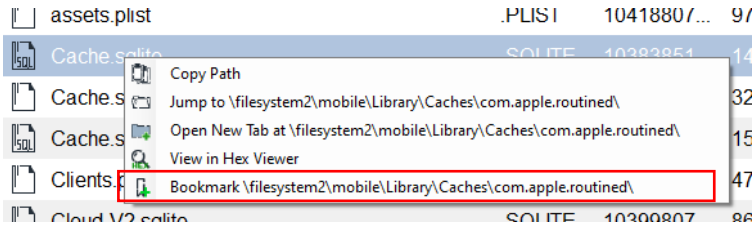
Open a New Directory Tab

This will open another directory tab, allowing you to work in multiple paths at once.

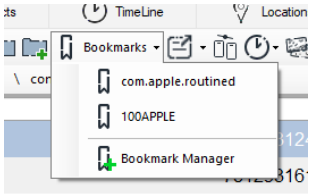
Bookmarks

Bookmarks allows you to save common paths that are interesting and quickly navigate to them in the future.

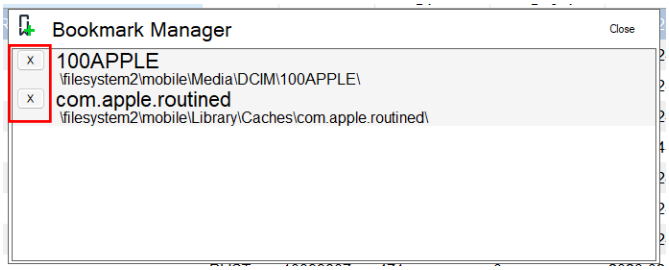
Add Bookmarks by right clicking on a file and select the “Bookmark” option.



The path will be added as a Bookmark that can now be used at any point to jump straight to the bookmarked path.



Use the Bookmark Manager to remove Bookmarks that are no longer required.



Extraction Comparison

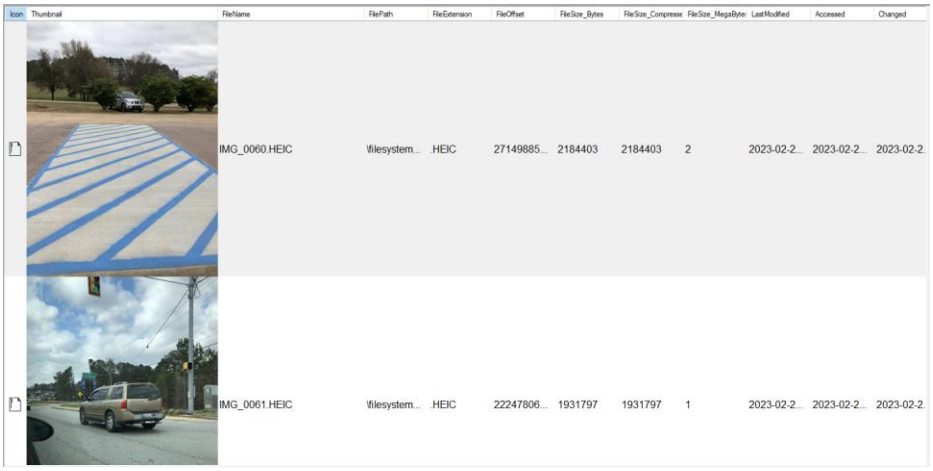
This will be explained more in a separate section of this manual.

Time Filter

This option allows you to apply the selected time period to the files in the Directory View. i.e. The files visible in the Directory View will only be the files that were Created, Modified, Accessed or Changed (depending on your selection) within the time period selected. Note that you can only choose one timestamp at a time as a filter.

Show Thumbnails

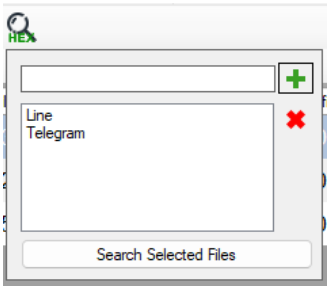
This button will turn on/off the thumbnail view of media files within the Directory View.



Note that each directory will be processed at the time the directory is accessed and will potentially take a long time depending on the amount of files present. Thumbnails will be cached to enable faster reloading.

Hex Search

ArtEx allows you to search all selected files for specific terms. More about Hex View will be discussed later.



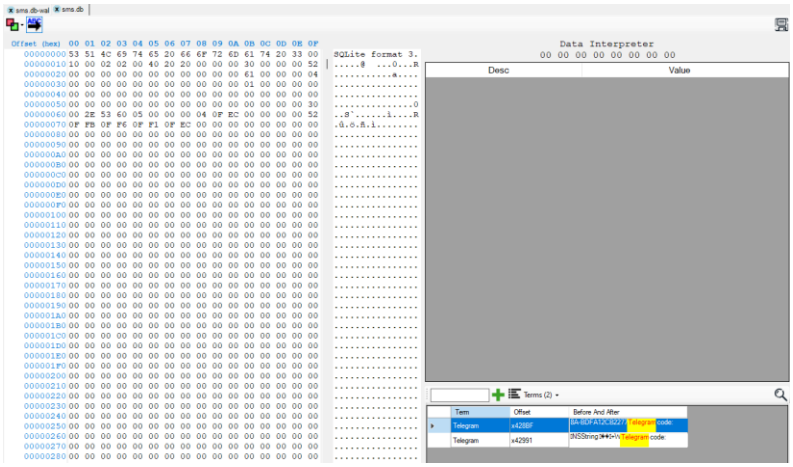
Enter the search term and press the ➕ to add the item to the list.

Select an item and press ✖ to remove it from the list.

*Note that this is case sensitive.

Press ‘Search Selected Files’ to search the currently selected files.

This will search the selected files and open each file up to highlight the results.



Hashing

Pressing this button will has the selected files which will be shown in the table view.
Pressing the down arrow on this button will give the choice to hash all files in the view.

Export to CSV

This button will save the information in the current view to a CSV file.

Flat View

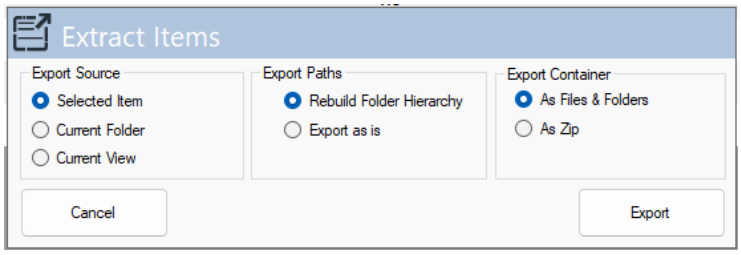
View all files in and below the currently selected folder regardless of the directory structure.

Open External

Extract the file and launch it in the default windows application.

Extract Items

Pressing Extract Items will open the Extract Files window to give you options and control over how the data is exported.



Export Source

- Selected Item(s) – Extract ONLY the selected item(s)
- Current Folder – Extract all items in the current folder.
- Current View - Extract all items in the current view.

Export Path

- Rebuild Folder Hierarchy – Maintain the file path of the extracted items.
- Export as is – Ignore the hierarchy and just export the files.

Export Container

- As Files & Folder – export the files/folders to the desktop as files and folders.
- As Zip – Save the exported data in a zip file.

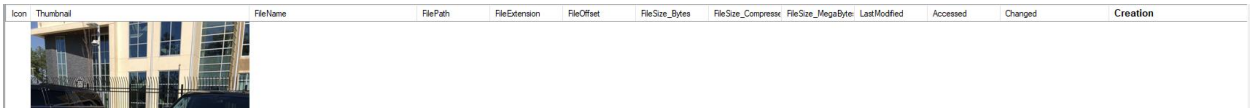
Breadcrumb Path

The breadcrumb path will show each folder in the path to the currently selected file and allows you to jump to any folder by clicking on the specific part of the breadcrumb path you are interested in.

Clicking on the folder at the start of the breadcrumb trail will allow you manually enter the path you want to visit.

The Table View

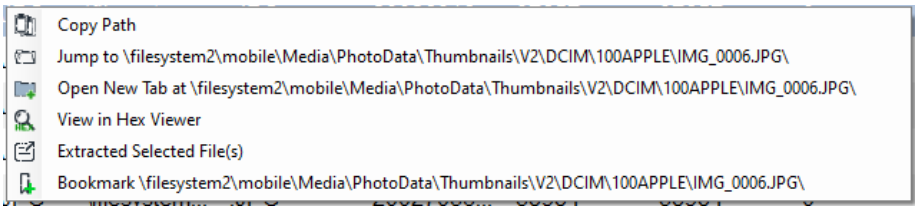
The Table itself contains numerous fields although not all fields are visible at all times. It often depends on the type of extraction and the options selected.



Icon – An icon representative of the type of record (Folder, File, SQLite, Symbolic Link etc).
Thumbnail – The thumbnail view of the file (if applicable and selected).
FileName – The name of the file.
FilePath – The path of the file.
LinkPath – The symbolic link path (if applicable).
OriginalPath – The Original path (applicable to backups or UFDR).
FileExtension – The extension of the file.
FileOffset – The offset of the file (applicable to archives).
FileSize_Bytes – The size of the file in Bytes.
FileSize_Compressed – The compressed size of the file (in Bytes).
FileSize_MegaBytes – The size of the file (in MegaBytes).
LastModified – The Last Modified timestamp of the file (if available).
Accessed – The Accessed timestamp of the file (if available).
Changed – The Changed timestamp of the file (if available).
Creation – The Creation timestamp of the file (if available).

Mouse Clicks

Left clicking on a record will select it.
Double Clicking on a record will attempt to open the file in the Right Pane. By default, ArtEx will try to open the file in the appropriate viewer but will default to Hex.
Right Clicking on a record will present a Context Menu.



Copy Path will simply copy the path of the file (including filename) to the clipboard.
Jump to will navigate the Directory View to the selected file; this is most useful when used in conjunction with the Search feature.
Open new Tab will open a secondary Directory View tab at the path shown.
View in Hex Viewer will open the file in ArtEx's Hex Viewer.
Extract Selected File(s) will launch the Extract Items view.
Bookmark will add the path of the file to the Bookmark list.

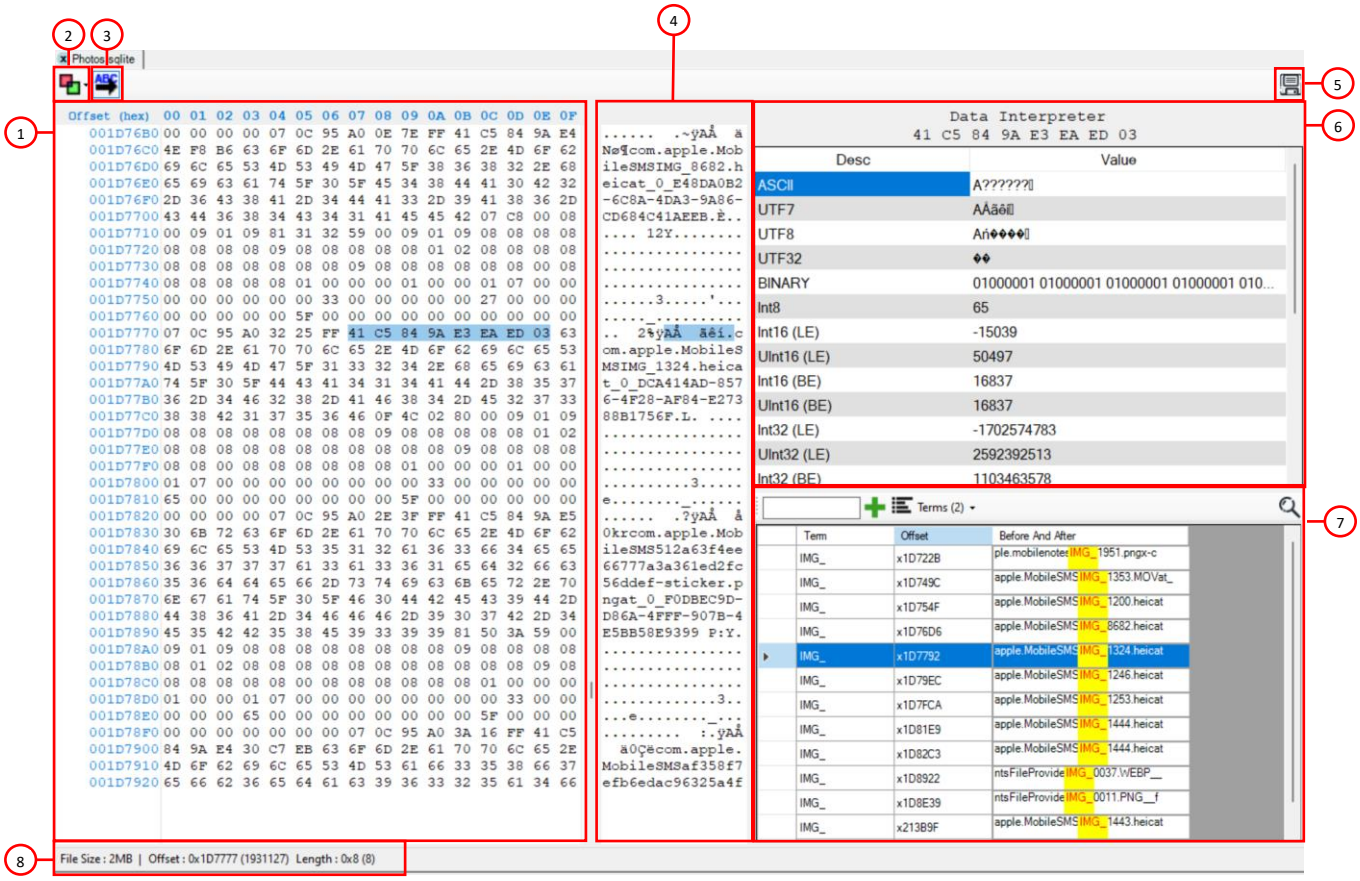
Right Pane

The Right Pane can be used to open files of many different types. Each type will present in context to the file type.

Hex View

The Hex View can be launched by Right Clicking on a file and selecting View in Hex Viewer. It will also be the default view when opening a file that ArtEx cannot automatically recognize.

The Hex Viewer can be split into 4 parts: Hex View, ASCII View, Data Interpreter and Search.

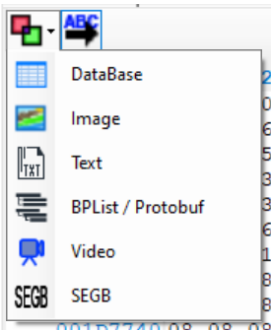


1 – Hex View
2 – Load As
3 – Extended ASCII
4 – ASCII View
5 – Save File will save the file.
6 – Data Interpreter
7 – Search View
8 – File & Selection Information

Hex View

The main window will show the contents of the file in a HEX view.

Load As



The Load As menu allows you to tell ArtEx how to open a file.
Supported types are;

- Database
- Image
- Text
- BPlist/Protobuf (Serialized Data)
- Video
- SEGB (iOS Biome) file

Any of these options will open the file in the requested viewer while keeping the Hex view also open.

Extended ASCII

This option turns on or off the Extended ASCII characters for the ASCII View.

ASCII View

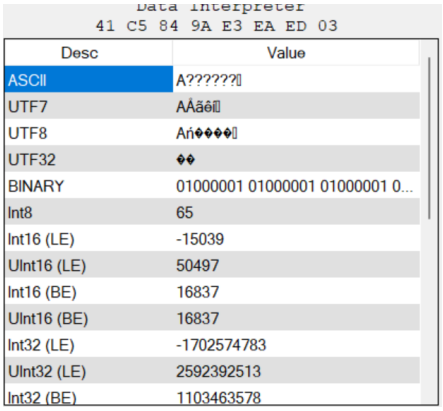
Shows the ASCII view of the file (in extended or basic ASCII)

Save File

Save the file to your local computer.

Data Interpreter

Shows different ways to interpret the data you have selected in the Hex View.



The Data Interpreter area will show how the bytes you have selected in the Hex or ASCII view look using different interpreters.

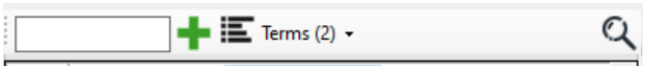
Currently supported interpreters are:

- ASCII
- UTF7
- UTF8
- UTF32
- BINARY
- Int8
- Int16 (LE)
- UInt16 (LE)
- Int16 (BE)
- UInt16 (BE)
- Int32 (LE)
- UInt32 (LE)
- Int32 (BE)
- UInt32 (LE)
- Int64 (LE)
- UInt64 (LE)
- Int64 (BE)
- UInt64 (LE)
- Single (LE)
- Single (BE)
- Double (LE)
- Double (BE)
- Mac Absolute
- Mac Millisecond

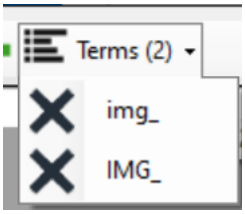
Search View

Allows you to perform searches against the file for specific words.

Entering a search term into the text box and pressing ✚ will add the search term to the Terms list.

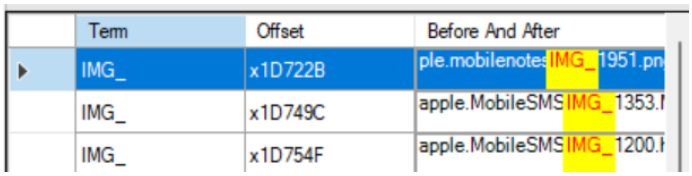


Clicking on the Terms button will show all terms currently in the list and these can be removed by pressing the associated ✕.



Once all search terms have been entered, press  to perform the search.

The results will show the offset and the Term found, the offset and the surrounding bytes.



	Term	Offset	Before And After
▶	IMG_	x1D722B	ple.mobilenotes IMG_1951.pn
	IMG_	x1D749C	apple.MobileSMS IMG_1353.I
	IMG_	x1D754F	apple.MobileSMS IMG_1200.I

Double clicking on a result will jump to the appropriate offset in the Hex View.

Note that Search is case sensitive and currently only searches the ASCII content. Byte searches is not supported.

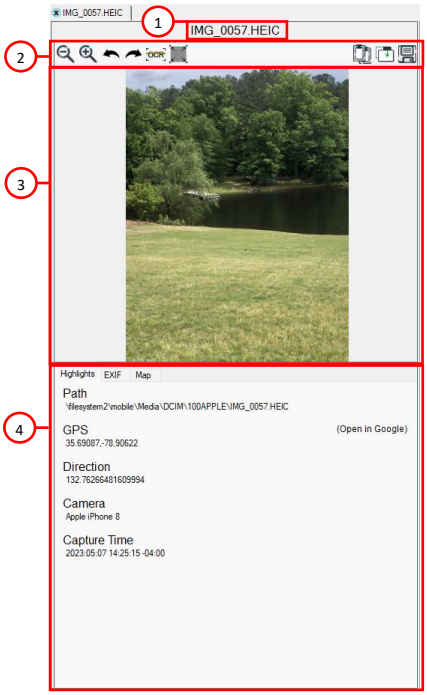
File & Selection Information

Shows file size, current offset, and selection size.

Media View

Media View can be launched either by double clicking on the Thumbnail of a record in the Timeline View, From Directory View or from the Hex Viewer.

The top of the pane will display the media item itself, and the bottom of the pane will show information related to the item.



1 – Media Title

2 – Tool Bar

	Zoom in/Out of the image
	Rotate the image 90°
	Run OCR on this image
	Reset Image
	Replay (Context sensitive)
	Copy image to Clipboard
	Open in External App
	Save Media

3 – Media Content

4 – Info Tab

Highlights	Important information.
EXIF	Exif Data for the item.
Map	Rendered map.
OCR	OCR content if relevant.

Text View

Text View can be launched either by double clicking on the source column in Timeline View, From Directory View or from the Hex Viewer.

This is a simple Text viewer with options of text size and word wrap.

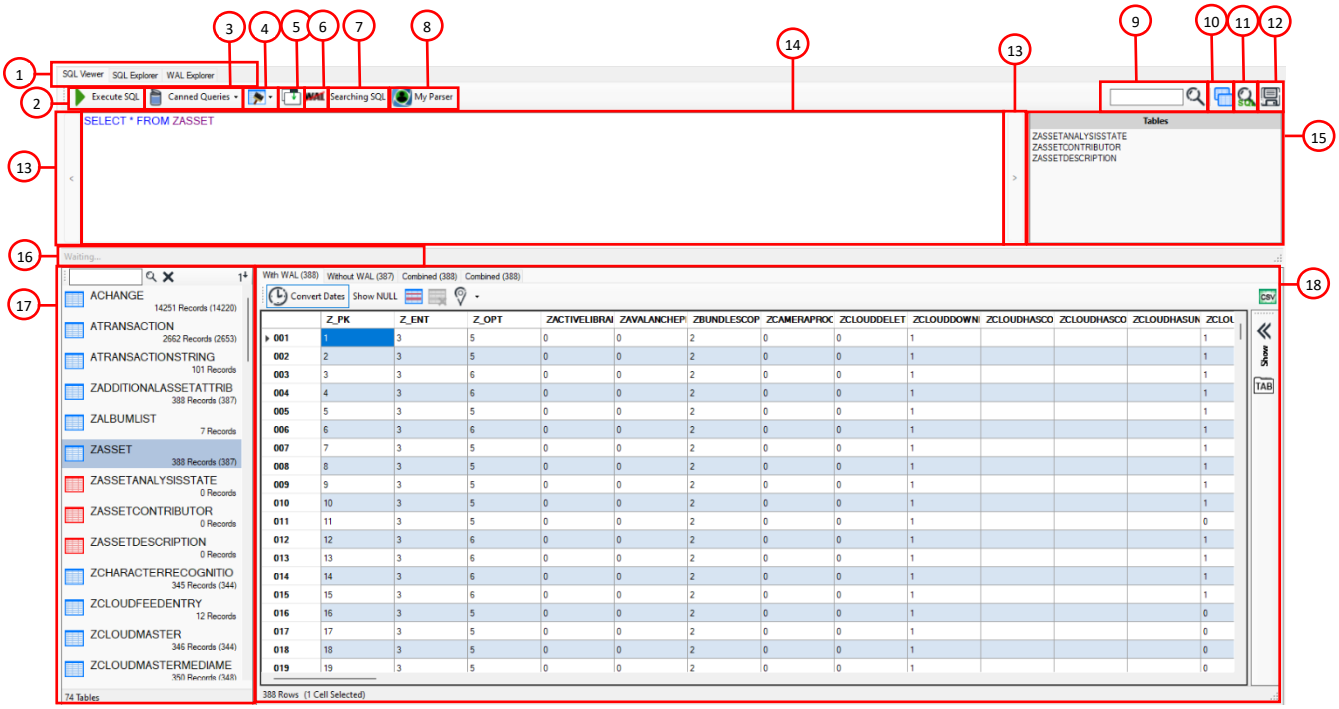
1 – Tool Bar

A A	Font Size Shrink/Grow
	Open in External App
WordWrap	Word wrap
	Save File
	Search

2 – Text View

SQL Databases

ArtEx has a built-in SQLite viewer to aid with validation and research an also includes a SQLite and WAL Explorer feature.



1- SQLView or Explorer Tabs
2 - Run Query
3 - Canned Queries
4 - Table Definitions
5 - Undock Database
6 - WAL Comparison
7 - Search Style
8 – My Parsers
9 - Search
10 - Reopen Database
11 - SQL Recovery / Advanced SQL
12 - Save Database
13 – SQL Navigation
14 - SQL Query Textbox
15 – SQL Suggestions
16 - Query Feedback
17 - Tables List
14 - Database Table View

SQLView or Explorer Tabs

This allows you to switch between features. The SQL and WAL Explorer features are described in the next section.

Run Query

Run the query that is written in the SQL Query Textbox.

Canned Queries

Canned Queries allows you to save the query that is written in the SQL Query Textbox and reuse it later.

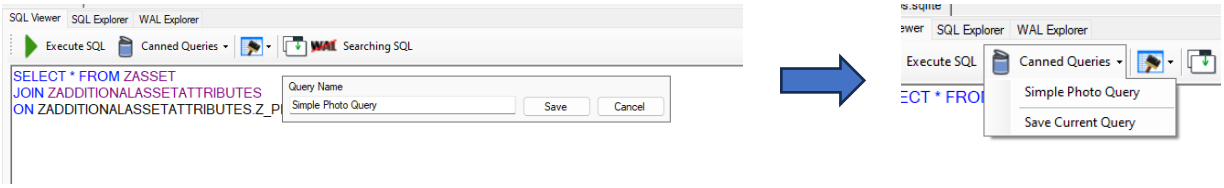
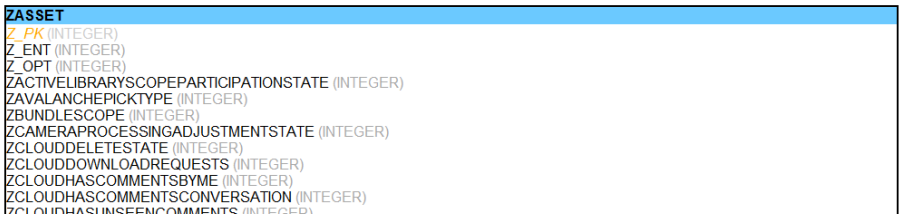


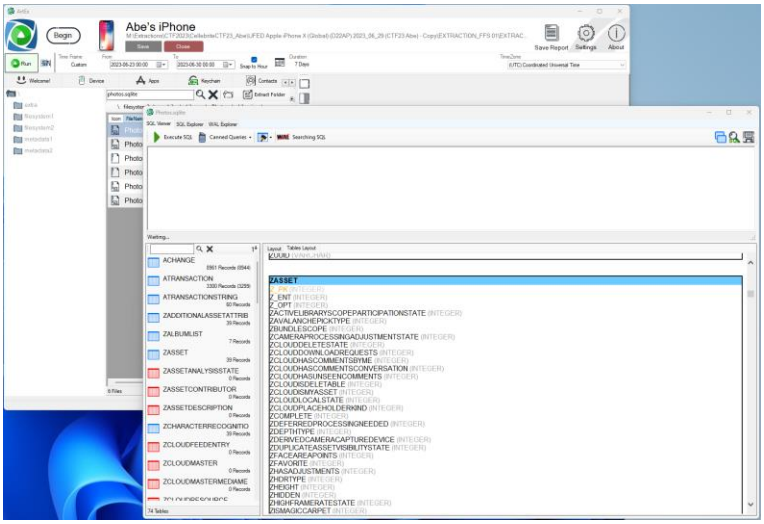
Table Definitions

You can use this feature to list out the database or table schema.



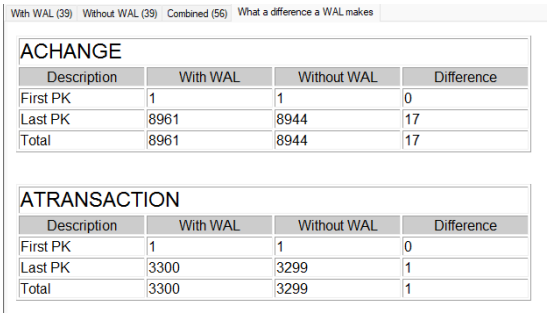
Undock Database

The Undock Database button will create a new window containing the database being viewed which is separate from the main ArtEx interface.



WAL Comparison

WAL Comparison will compare the database with the WAL applied and without the WAL applied to give you an idea of how much affect the WAL file has.



Wth WAL (39) Without WAL (39) Combined (56) What a difference a WAL makes

ACHANGE

Description	With WAL	Without WAL	Difference
First PK	1	1	0
Last PK	8961	8944	17
Total	8961	8944	17

ATRANSACTION

Description	With WAL	Without WAL	Difference
First PK	1	1	0
Last PK	3300	3299	1
Total	3300	3299	1

Search Style

Search Style allows you to choose between searching the database or what is visible in the table.

My Parsers

Launches the MyParser (beta) tool covered in more detail later in the manual.

Search

The search tool allows quick searching of the entire database or table.

- If there is no table selected, every table in the database will be searched.
- If a table is selected, only that table will be searched.

Reopen Database

This button will reopen the database in a separate tab, allowing you to run multiple instances and multiple queries.

SQL Recovery / Advanced SQL

The SQL Recovery is the same as the “Run Advanced SQL” in the Settings.

This is custom code which analyzes each freepages of the database and tries to associate the recovered data to the appropriate table by using pattern matching of the number of fields and data types.

If a freepage is found that matches multiple tables, the page is ignored, rather than possibly associate it to the incorrect table. In some cases, this can mean that Advanced Recovery may present less data than without the advanced recovery running. However, this only affects the database view as parsers will run the normal SQL database without recovery regardless of if Advanced Recovery is selected or not.

See SQL and WAL Explorer section for more information.

Save Database

Save the database to your computer.

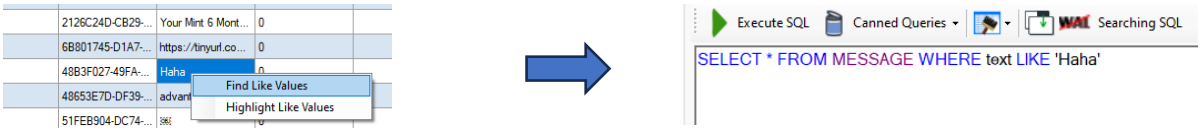
SQL Navigation

SQL Navigation buttons < and > can be used to navigate through all queries run in this session.

SQL Query Textbox

A free textbox to allow you to type in any SQL query you want. Logic is applied as you type to highlight keywords or table names.

Note that you can quickly create a SQL command by right clicking on a table record and selecting **Find Like Values**. This will build you a query to find content matching the selected cell.



This feature will create a SQL Query and run it based upon the column selected and the contents of the cell.

SQL Suggestions

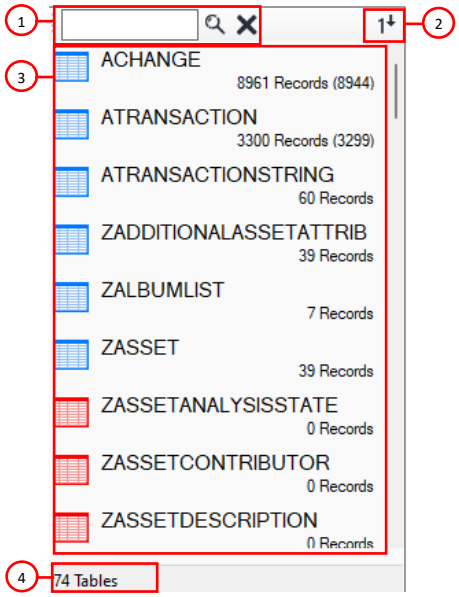
SQL Suggestions will try to suggest tables and fields to make writing SQL statements easier.

Query Feedback

This status bar will give feedback on your query.

Tables List

This panel lists all tables within the database.



1 - Table Search and Clear Search

2 - Sort tables either alphabetically or by number of records.

3 - The tables.
Each table in the list contains important information, starting with the icon.

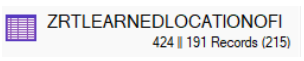
	Normal table.
	Empty or erroneous table.
	Recovery has been run on table.
	Table has been decrypted. There is more about encrypted databases later.

In normal operation, it is likely you will see the number of Records followed by a number inside brackets like this:

The first number represents the number of records in the table when the WAL is applied.

The bracketed number represents the number of records in the table if the WAL is not applied.

When running SQL Recovery, a further number is added before a "||". This number represents the results of the recovery process.



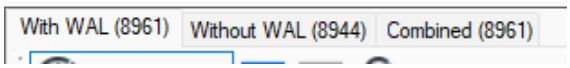
This example shows that Recovery found 424 records, reading the database with the WAL found 191 and reading the database without the WAL found 215.

Clicking a table will load it to the Database Table View.

4 - Table Count

Database Table View

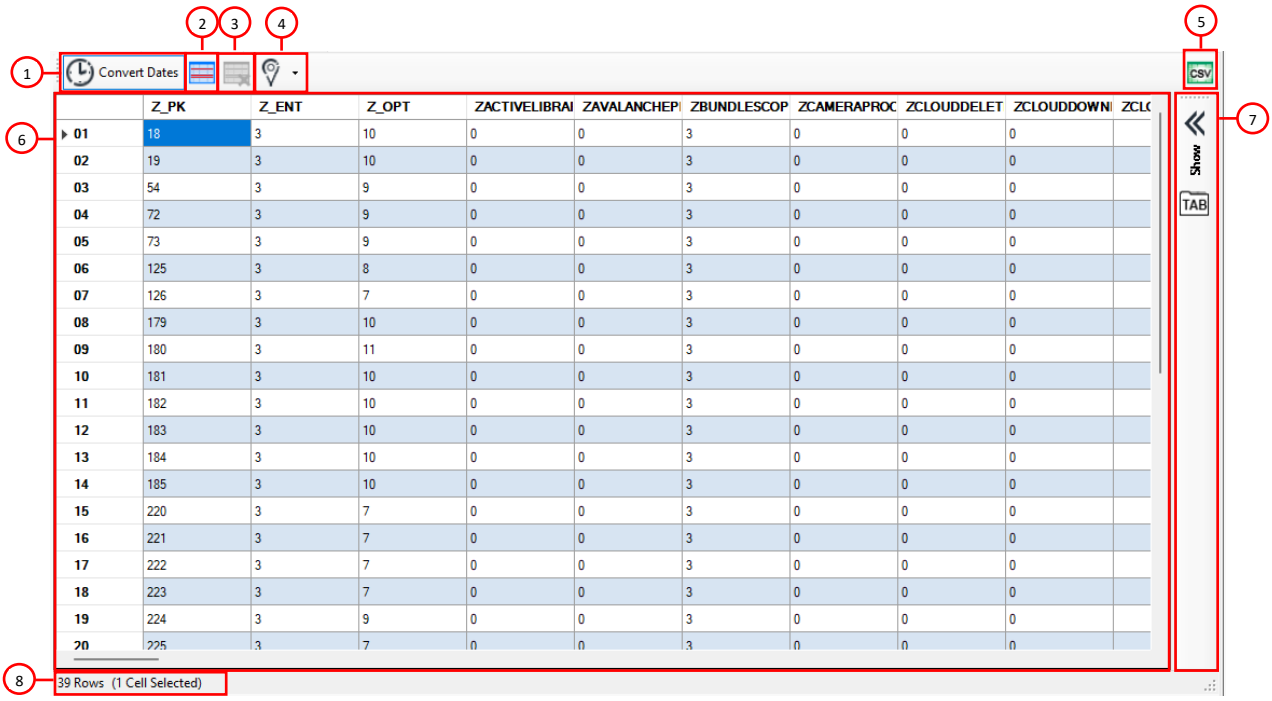
The Database Table View pane is made up of several tabs, each tab representing a unique way to view the database table.



With WAL will show the database table with the WAL applied.
Without WAL will show the database table without the WAL applied.
Combined will show a combination view of With and Without WAL. Duplicates records are not included.
Recovery may also show here for databases where Advanced Recovery was utilized.

Any table you load or query you run will be applied to all views (With/Without WAL, Combined & Recovery).

Each tab contains the same layout.

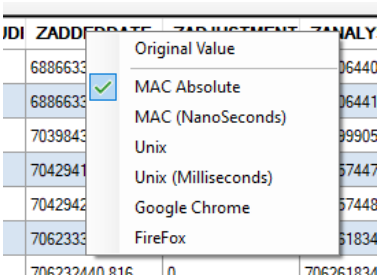


1 - Convert Dates
2 - Find Missing Rows
3 - Clear Row Highlights
4 - Map Custom Rows
5 - Save table to CSV
6 - Table
7 - Database View Right Pane
8 - Table information

Convert Dates

ArtEx will automatically try to recognize timestamps in the table and will show the appropriate fields as timestamps. This can be turned on or off permanently in the Settings or temporarily by using this button.

Note that you can also manually specify the appropriate timestamp to use by right clicking on the header and selecting from the list. Selecting **Original Value** will remove the Timestamp format and return to showing a number.



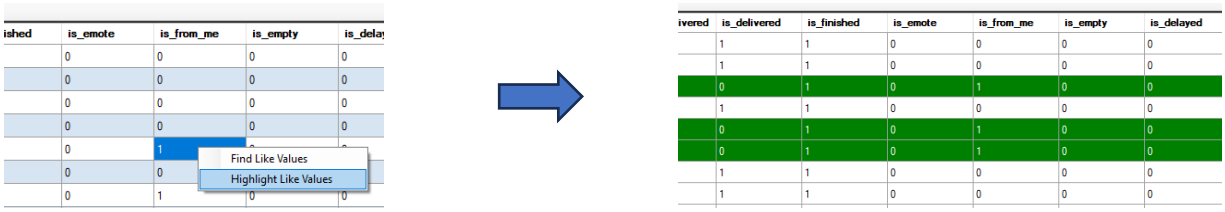
Find Missing Rows

Find Missing Rows will use the primary key to try to identify missing records. It is not attempting any type of recovery, just highlighting that the numbers are non-sequential by creating an empty, red coloured record.

	ROWID	guid	text	replace	service_center	handle_id
028	28	F708427C-FDC3-...	Hi	0		11
029	29	E9F88B9E-D895-...	Or else	0		9
030	30					
031	31	B5BA46F0-708C-...	The command yo...	0		1
032	32	B58DEC93-D223...	Hey! I've been us...	0		12
033	33	4E54B44C-2E57-...	Snapchat: Check...	0		13
034	34	53646798-BD02-...	Menu	0		1
035	35	52625CD2-8A56-...	Reply with any of...	0		1
036	36	A89997BB-DDB7...	Data	0		1
037	37	486262E3-27BD-...	Balance	0		1

Clear Row Highlights

Right clicking on a cell will give an option to “Highlight like value”. This is similar to running a query, but the non-conforming records aren’t removed.



This feature will highlight all records where the “is_from_me” field = 1.

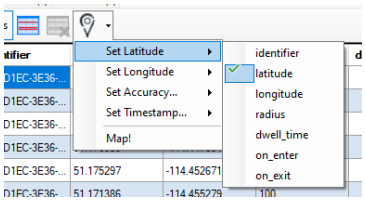
The Clear Row Highlights button will remove this formatting feature.

Map Custom Rows

There may be times that you find a database that contains location data that is unparsed by ArtEx but you would like to see it on the Location tab.

The Database Mapping feature allows you to specify the Latitude, Longitude, Accuracy and Timestamp to map out.

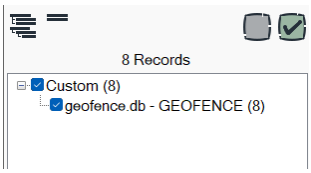
Simply select each of the fields and select from the list of fields. Note that ArtEx may have prepopulated this for you if it recognizes appropriate data.



Accuracy and Timestamp are not mandatory, but will affect the output as it may result in records with impossible timestamps.

Once you have assigned the required fields, press **Map!**

Your data will be listed as a Location Data Source under the Custom node and plotted onto the map.



Save table to CSV

Simply save the current view to a CSV.

Table

This is the table itself with row and columns as expected. Alternating rows are coloured white and blue.

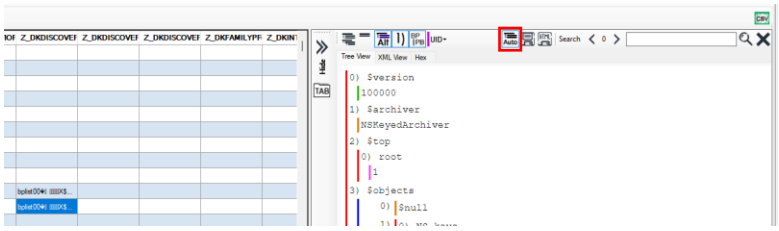
Database View Right Pane

The Database Table View has its own Right Pane for showing embedded information. This typically means Serialized Data such as BPList and Protobuf which is covered in more detail later on.

Whenever you select a cell that contains serialized data, the right pane will automatically open and display the contents. There are two features which are unique to the Database View Right Pane Deserialized View.

Auto Expand

You can use the Auto-Expand button to automatically expand the full BPList/Protobuf blob when the tab opens.



Tabbed View

By default, this right pane will only show one blob at a time. But you can have each blob open in its own tab but pressing the TAB button. Note that the tab name will come from the row number.

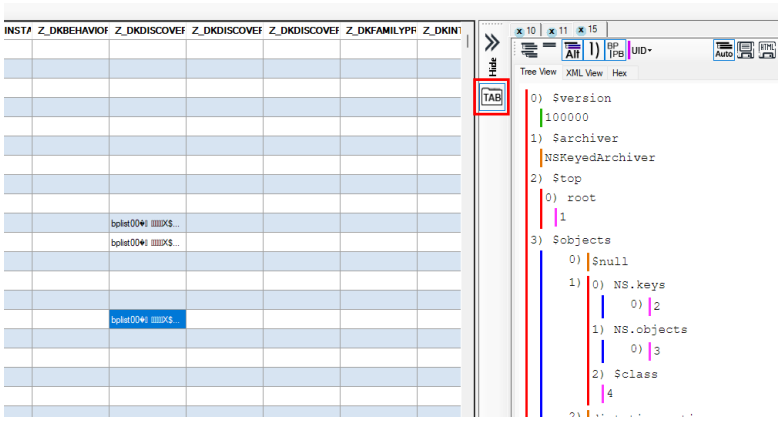


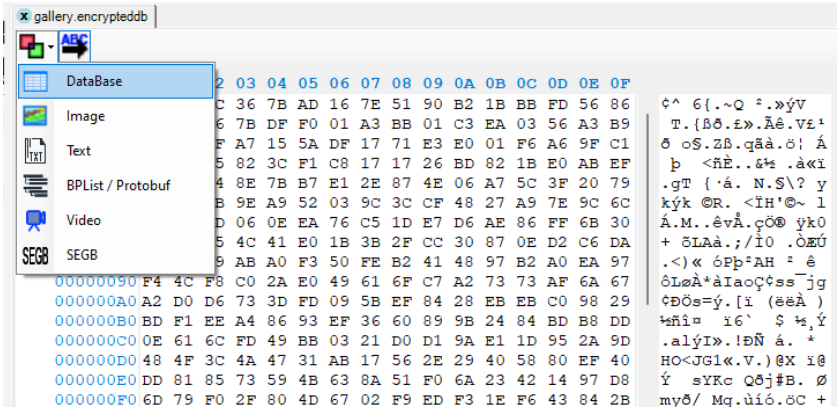
Table information

The status bar includes the number of records and number of cells selected.

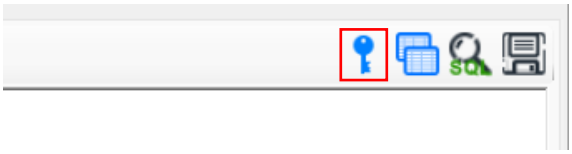
Encrypted Databases

Trying to open an encrypted database will initially fail as ArtEx struggles to recognize the format.

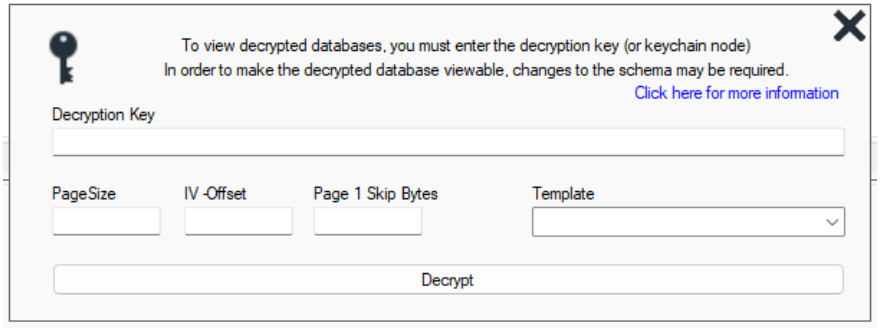
Use the “Open as” option to open the file as a Database.



This will obviously still fail to open the database properly but you will now see a new icon has appeared in the tool bar.



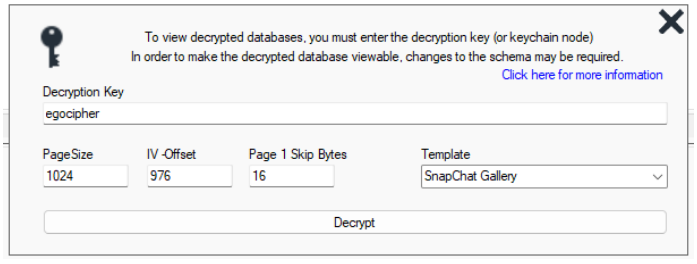
Pressing this will open the Database Decryption feature. Note that this is a limited feature and may not work for all databases.



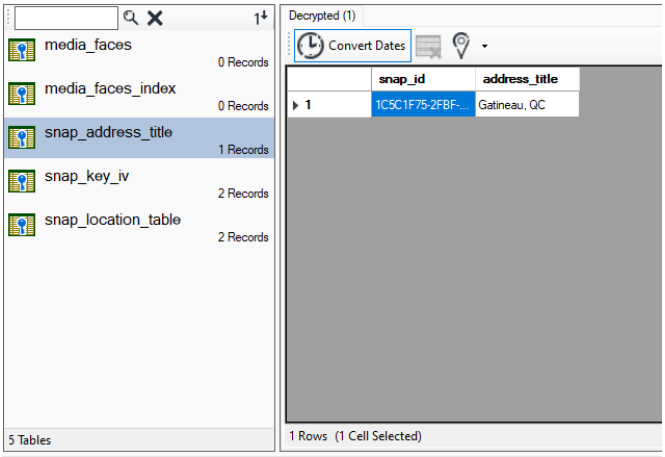
You can enter the actual decryption key or name of the decryption key in the keychain.
You must enter a page size, offset of the IV and the number of bytes to skip on page 1.

You can select from a pre-defined list of supported databases by using selecting from the Template dropdown.

This will populate the required fields for you.



Pressing Decrypt will try to decrypt the table using the given criteria and present the result.



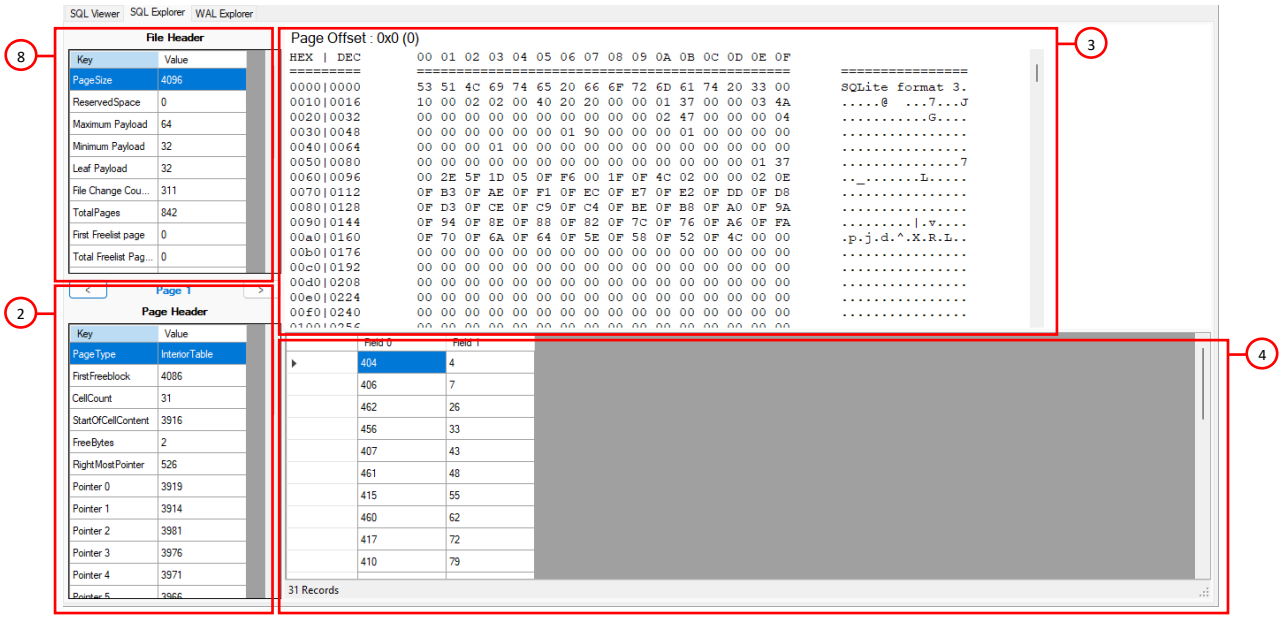
Note that in some case, minor modifications must be made to the database for it to work. This does not alter the data being parsed but is necessary to get the database to show.

SQL & WAL Explorer

This feature allows deep diving into the SQLite database and associated WAL file.
Both tools are very similar, but do have some differences.

SQL Explorer

The SQL Explorer is broken into 4 panes.



1 - Database Information (Header)
2 - Page Information
3 - Page (Hex View)
4 - Page (Table View)

Database Information (Header)

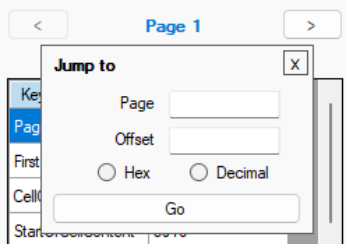
This information comes from the SQLite Header and shows the size of the pages, the total free pages etc.

Page Information

This area contains information about the specific page being viewed.

At the top of the pane are navigation buttons to allow forward and backwards navigation through the pages.

Clicking on the blue “Page” label will open the Jump To feature.



Here, you can jump to a specific page or offset within the database. Note though that jumping to a specific offset will simply load the page that encompasses that offset.

This is a really useful feature for understanding records found when doing a hex search, as exampled shortly.

The pane then lists out the Page Header information. These items can be clicked to highlight the record in the Hex View and Table View.

Page View (Hex)

This is the Hex view of the single page being viewed. It has limited functionality (no data interpretation tools) but will reflect the record that is highlighted.

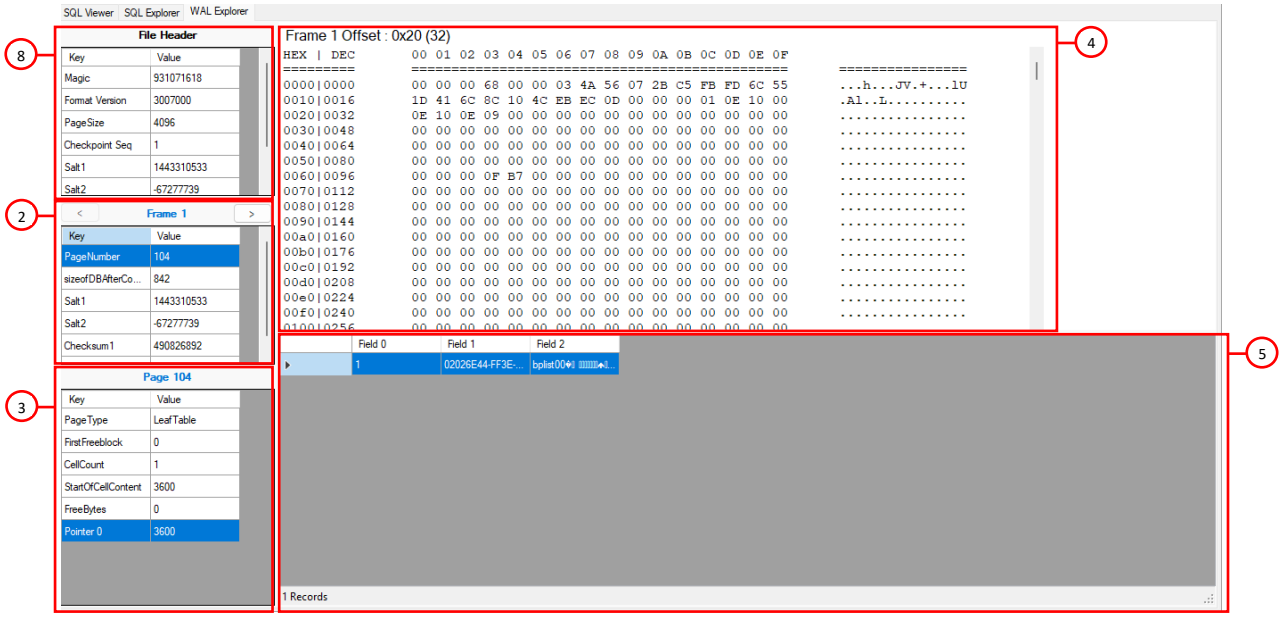
Page View (Table)

This is the table view of the single page being viewed. The feature uses the information in the record headers to identify the fields and parses the records accordingly. However, since the information presented is solely sourced from the page being viewed, the fields will not have meaningful names, instead, taking a consecutive number.

	Field 41	Field 42	Field 43	Field 44	Field 45	Field 46	Field 47	Field 48	Field 49	Field 50	Field 51
▸			49	56			0.433020114898...	0.467261453144...	0.545440985692...	0.469547578445...	0.335630688425...
			85				0	0.499494622151...	0.593265727162...	0.244921833276...	0.134232249911...
			86				0	0.458077243181...	0.805190958082...	0.133949115872...	0.114029024293...
			87				1	0.282995011115...	0.467903554439...	0.102169990539...	0.056686414134...
			88				1	0.439740661475...	0.549042865633...	0.139590471982...	0.198443198822...
			89				1	0.688593579877...	0.606211662292...	0.562224626541...	0.288803219566...
			90				0.583703517913...	0.504013755676...	0.482904195785...	0.924743950366...	0.958642936278...
			91				1	0.583998627263...	0.327932775020...	0.110649228096...	0.192167434525...

WAL Explorer

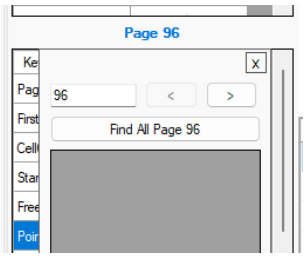
The WAL Explorer has a similar layout but with an additional pane.



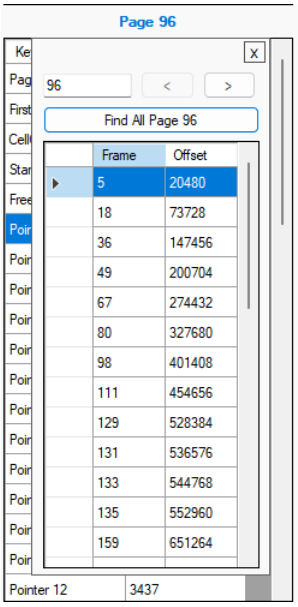
1 - Database Information (Header)
2 - Frame Information
3 - Page Information
4 - Page (Hex View)
5 - Page (Table View)

The Frame Information can now be seen between the File and Page information panes and can be used to navigate backwards and forwards between the frames and launch the Jump To feature.

Almost everything else about the WAL Explorer is identical to the SQL Explorer although there is also a “Find All Pages” feature available by clicking on the blue “Page” label.

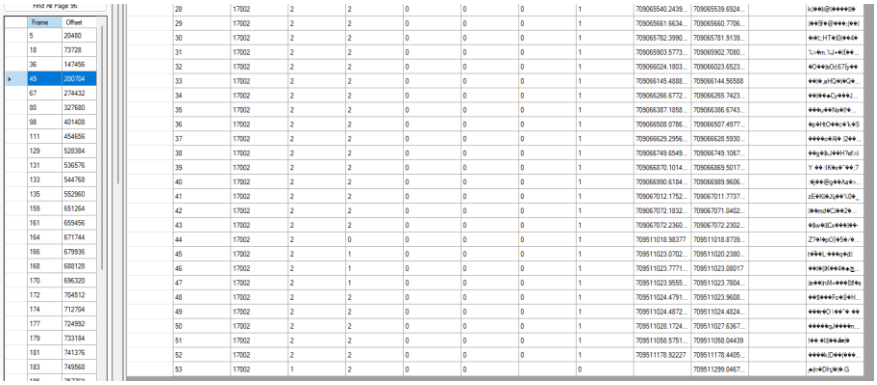


Here, you can find the next/previous or all versions of any particular page, letting you see the history of a page/record.

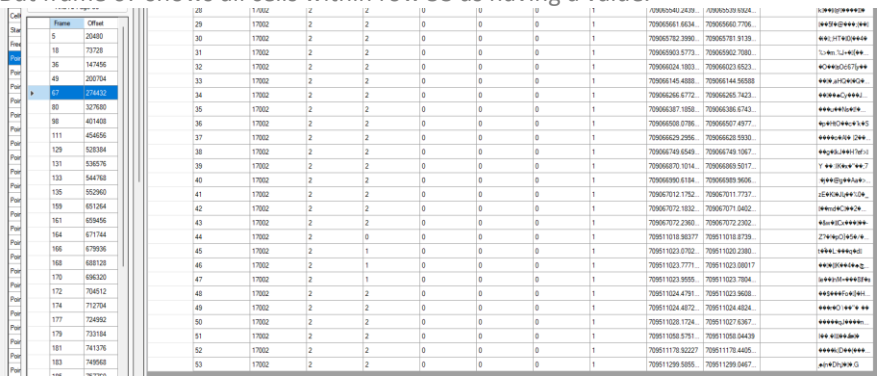


Once all pages are identified, they can quickly be navigated by clicking on the desired row.

For example, it can be seen here that Frame 49 has a record 53, but not all cells have a value.

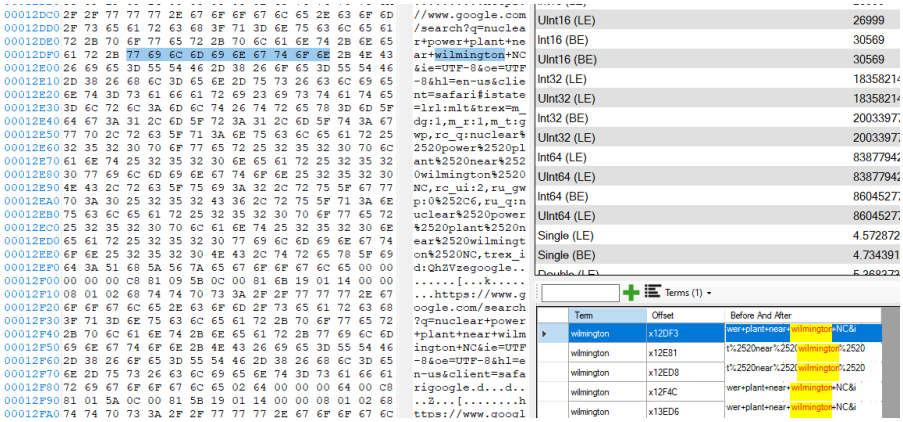


But frame 67 shows all cells within row 53 as having a value.



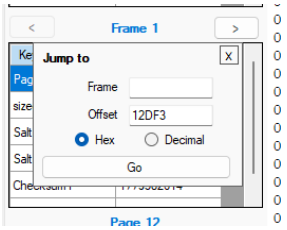
As an example of how this could be useful:

The results of a Hex search result in an offset being found within the WAL of 0x12DF3.

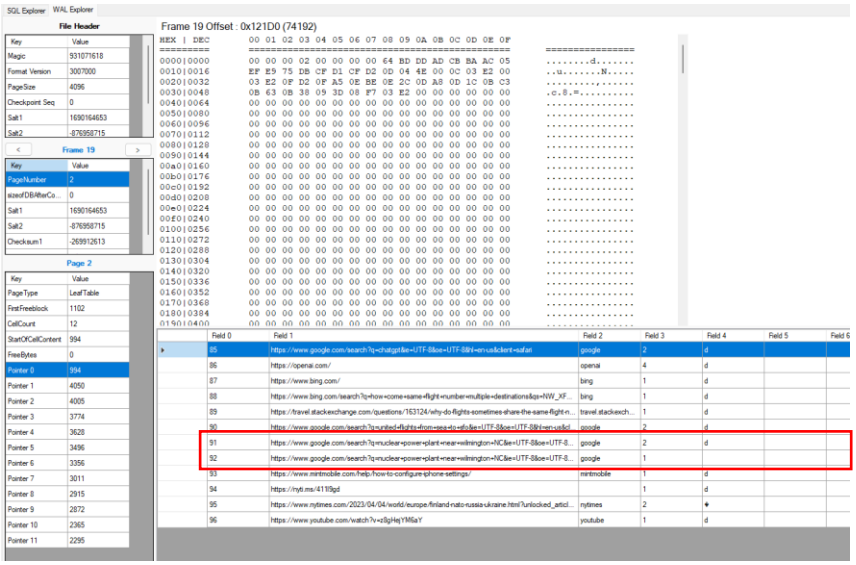


The WAL file can be opened as a Database and WAL Explorer.

The Jump To feature can be used to jump to x12DF3.



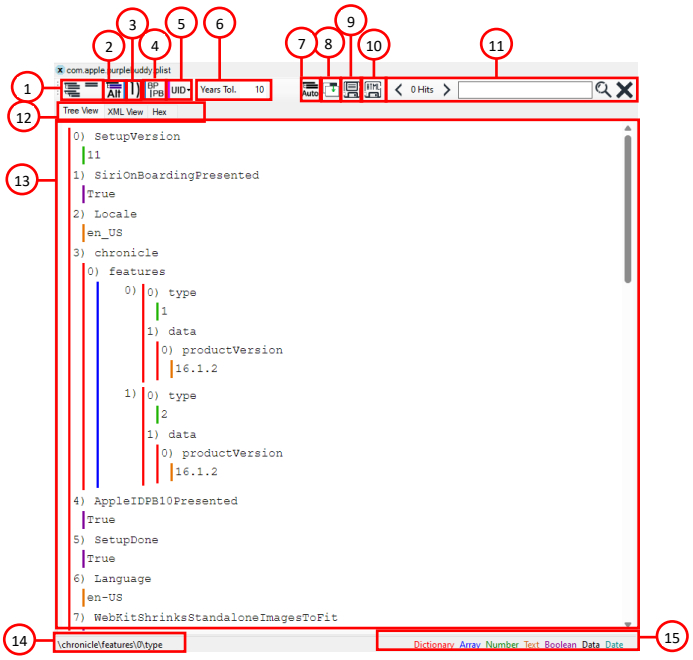
As mentioned above, the Jump To feature will navigate to the frame/page on which that offset falls and process the entire page.



Immediately we can see the record and can therefore understand much more than is available by simply looking at the Hex.

Deserialized Viewer

ArtEx includes a built in viewer for PList & Protobuf files.



1 - Expand / Collapse All nodes
2 - Show Alternate Values
3 - Show Node Numbers
4 - Attempt to process BPList blobs as protobuf
5 - UID Options
6 - Set Year Tolerance
7 - Auto-Expand Tree
8 - Undock Viewer
9 - Save File
10 - Save HTML Representation
11 - Search Options
12 - View Tabs
13 - Main Window
14 - Current Node
15 - Legend

Expand / Collapse All nodes

Expand or collapse all nodes within the serialized data tree.

Show Alternate Values

Since ArtEx is working without a protobuf schema, it has to make an educated guess at the datatype based on numerous factors. Sometimes, there are multiple possibilities and ArtEx will have to select the most likely option. This option will force ArtEx to show all alternatives.

Show Node Numbers

ArtEx can add additional numbers to the nodes for ease of viewing.

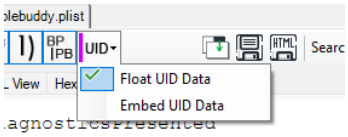
Attempt to process BPList blobs as protobuf

Some blobs within bplists may be protobuf. With this option turned on, ArtEx will attempt to decode them inline, presenting everything as one large tree.

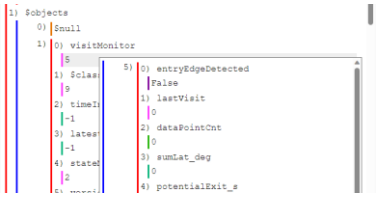
UID Options

The UID Options allows you to control how the Deserializer handles UID values.

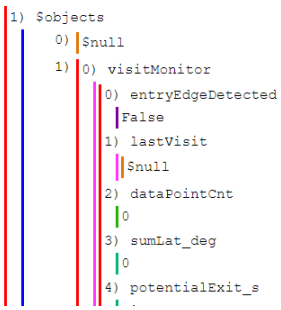
Essentially, a UID value is a pointer to another node in the file, and ArtEx allows you to choose from two options;



Float UID Data - When you hover over a UID value, a window will float to show you the resolved data at that UID Node. Here, we wee UID Value 5 brings the data from Node 5.



Embed UID Data - Will build the tree and substitute the UID value for the data it represents. Here, we see the same data as above, except instead of showing a UID Value of 5, the actual value of Node 5 is shown in its place.



Set Years Tolerance

ArtEx can check all numeric values parsed from serialized data and try to display them as timestamps. Setting a tolerance lets ArtEx know what kind of data you think is relevant.

ie. If a value is parsed with a year of 2002, you aren't interested as it's likely not really a timestamp. But if it shows 2023 then it likely is. The tolerance applies years behind and ahead of the current date.

Undock Viewer

Undock Viewer will create a new floating window with the current serialized data view.

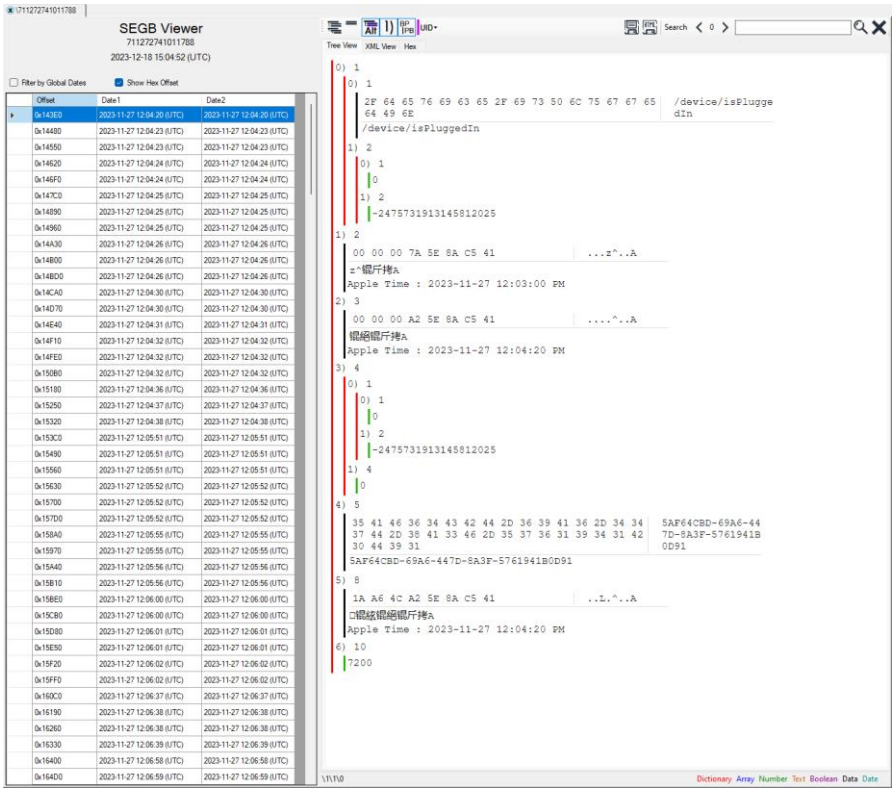
Main Window

The main window can be used to show either a structured Tree View, an XML view or a Hex View but using the tabs at the top.

Tree View	XML View	Hex View

SEGB Viewer

As an extension to the Deserialized Viewer, ArtEx provides a means to view SEBG v1 and SEGB v2 files.



Essentially, the SEGB viewer is a list of frames on the left and the normal protobuf viewer on the right. Each frame can be selected to view the protobuf blob.
You can also use the “Filter by Global Dates” checkbox to filter the SEGB results to match the Time Bar settings.

ArtExtraction

ArtExtraction is a unique feature which allows you to connect to a JailBroken iOS device and either extract the data or process it as though it was a normal extraction.

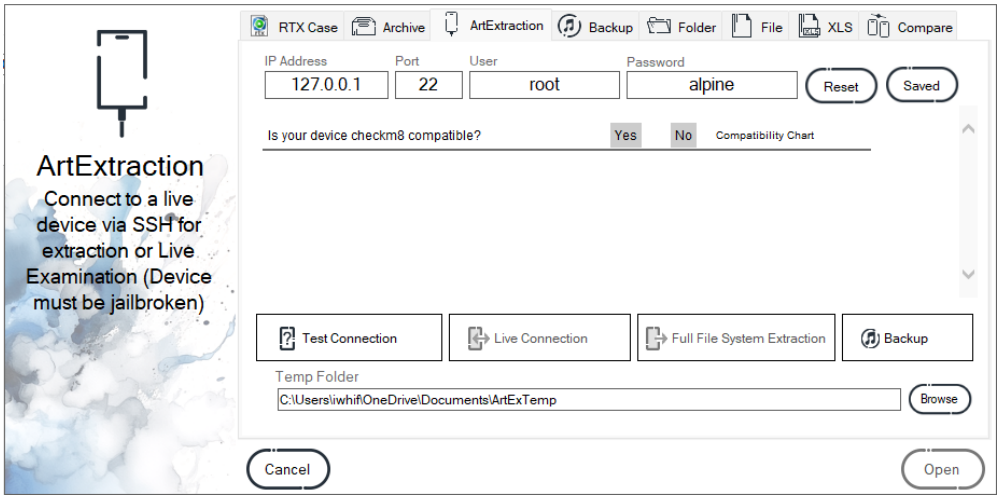
The Live Connection feature is designed to help you research what happens in the background when certain actions are taken on the device.

View in near real time as you send a message or navigate to a webpage and see how the database looks immediately without having to extract.

ArtEx will not do the jailbreaking for you. You must have a pre-jailbroken device with SSH installed as per the instructions on the ArtExtraction screen.

Once you have a jailbroken device you can choose to connect via either wifi or a SSH Tunnel via a tool such as 3u Tools.

An SSH Tunnel is much faster than wifi and is the recommended way to proceed.

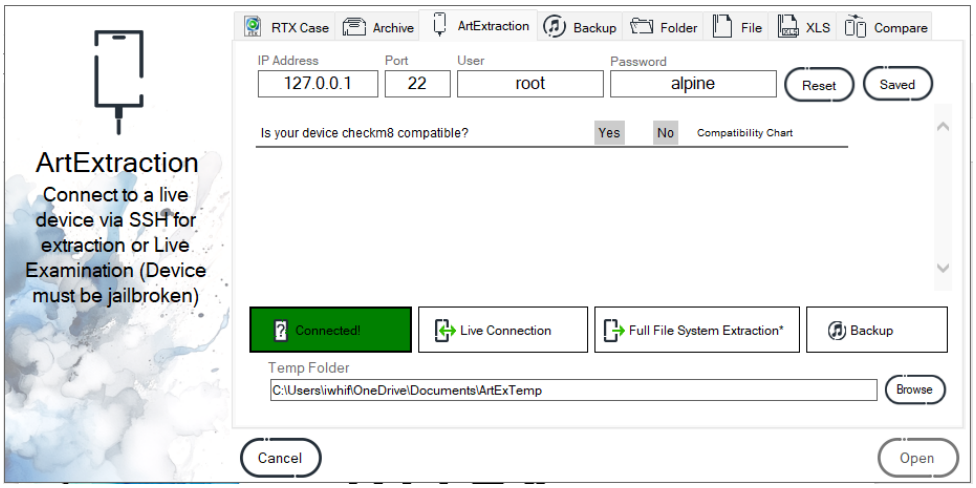


You will see that the default connection options are already filled in but these can be changed if necessary.

You can also click the **Saved** button to see previously used connection settings.

Once you are ready to connect, press the Test Connection button.

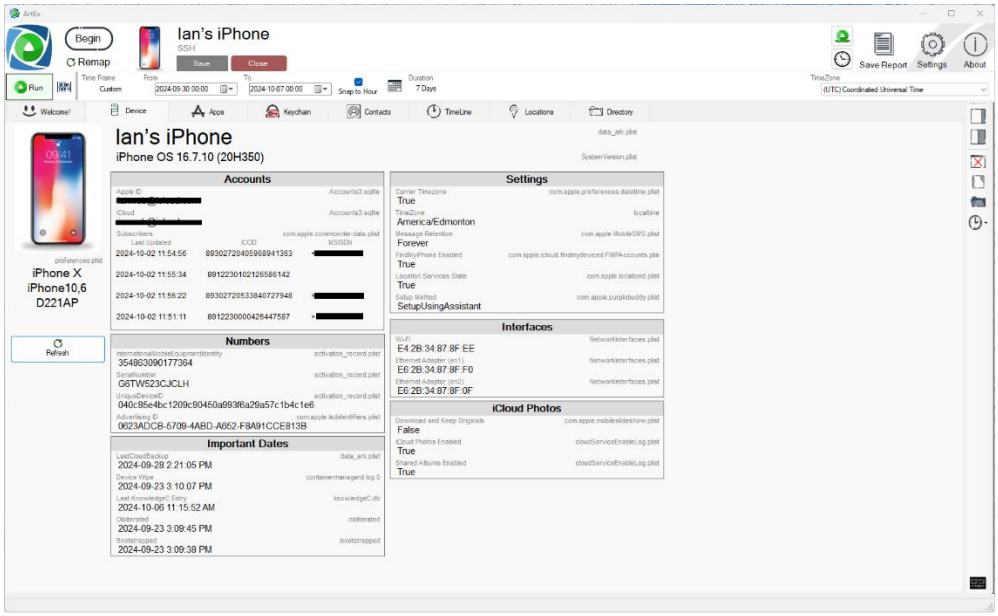
Assuming the connection succeeds, the button will change to green.



You can now choose to start a Live Connection or do a Full File System Extraction (keychain is not included).

The Full File System Extraction will extract the data and save to a .tar file, immediately processing the extraction upon completion.

The Live Connection will treat the device just like an extraction and map the directories and get device information as normal.



At this point, you can use ArtEx as normal, processing different parsers or opening files via the Directory Browser.

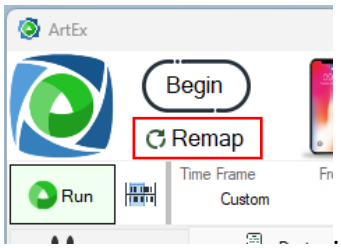
There are several things to be aware of when using Live Connection;

a) Every time you run the parsers, the latest information will be extracted from the device. This means that the data is not cached like normal and will subsequently take more time to process.
b) Every time you open a file from the Directory Browser, the latest version of the file is extracted. Again, this can result in slightly longer load times compared to a cached file.

c) The directory structure is not updated automatically. For example, if a file is created on the device after the initial processing, it will not be visible in the directory view or timeline. A great example would be if you were testing the Camera application and took a photograph. As the photos.sqlite database is refreshed when opened (either manually via the Directory Browser or via parser) then the newly created record will show up. However, as far as ArtEx is concerned the photo itself doesn't exist as a file in the directory structure.
d) The Device Details tab will not be automatically updated if something on the device changes.

To address these issues, some buttons within ArtEx will only be displayed when connected via Live Connection.

Firstly, underneath the Begin button there is "Remap" button.

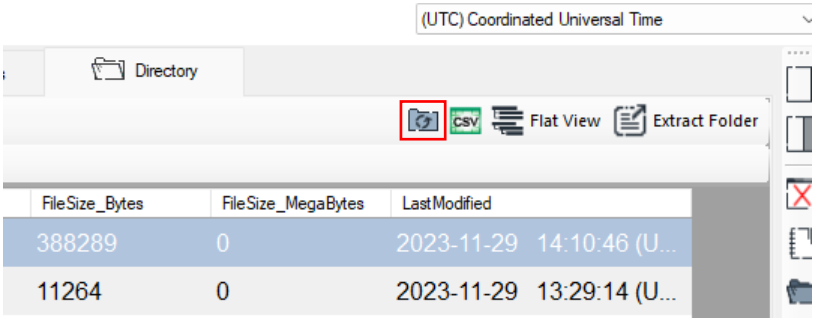


The "Remap" button will remap the entire device, ensuring that you can see the latest files added since the last time the device was mapped.

Although this will ensure that you are not missing any new files at all, it is a cumbersome approach if you know the directory where a file is created.

To return to the Camera example, if you take a photograph, you know that it will be in the DCIM folder.

In this case, you can navigate to the appropriate file within the Directory Browser and use the button to remap only that folder and it's children.

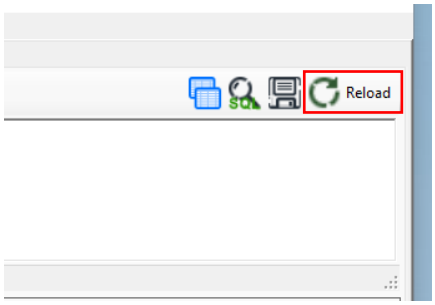


This new mapping will be used by the parsers and is quicker than remapping the entire device.

The Device Details pane will now include a new Refresh Button which will reprocess the Device Details and update the tab.

Finally, making changes to a file (plist or database etc) is typically only reflected by closing and reopening the file in question but this can be an interruption.

Instead, you will find a “Reload” button has appeared within the files’ viewer window.

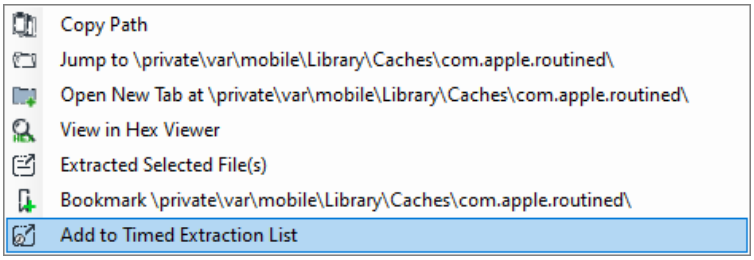


This button will close and reopen the current database and rerun your current SQL query, making this this quickest and easiest way to see updated information.

Timed Extractions

To assist with research, ArtEx has a Timed Extraction feature.

From the Directory View, Right Click on the file you want to extract and select “Add to Timed Extraction List”.



This will open up a pane at the bottom of the screen.

Repeat for all the files you want to extract which will be listed in the middle of the loaded screen.

Use the Target field to select a folder to extract the files to and use the drop down menu to select the extraction frequency.

This will cause ArtEx to extract the selected files at the selected frequency and save them with the appropriate timestamp

This is useful to see how a file may change over time.

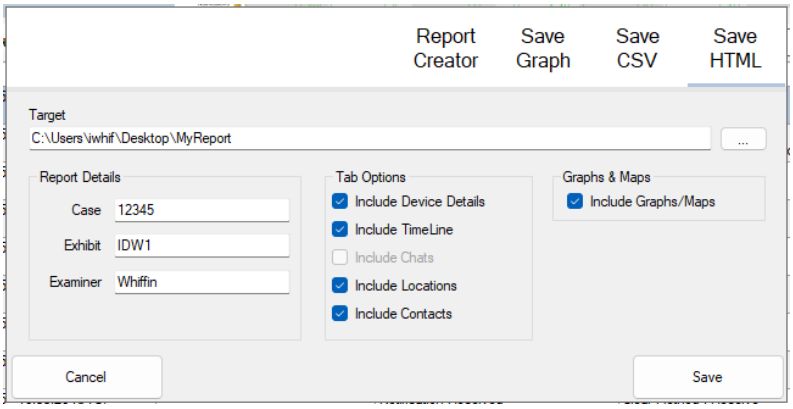
	This button will remove the currently selected file from the Timed Extraction queue.
	This button will add the currently selected file from the Directory Browser to the Timed Extraction Queue.
	These options will Start and Pause the Extraction timer.
	This button will ignore the timer and do an immediate extraction.

Reports

ArtEx has several options for creating reports, all accessible from the 

button in the top right of the window.

This will launch the Report feature.



Four reporting options are available; Save HTML, Save CSV, Save Graph and Report Creator.

In all cases, the Target field is used to specify the location to save the file to.

The option available options are contextual based on the type of report selected.

Save HTML

The HTML report is the standard option for saving the results of the analysis and it is the HTML report that most of the options refer to.

Report Details

Case : Enter the Case Number/Reference.
Exhibit : Enter the Exhibit Number/Reference.
Examiner : Enter the examiner name.

Tab Options

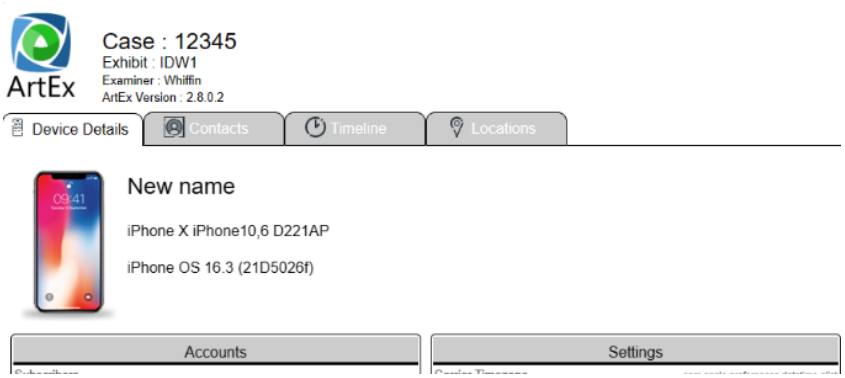
Include Device Details : Include the Device Details information as a tab in the report.
Include Timeline : Include the Timeline information tab in the report.
Include Chats : Include the Chats tab information in the report (if applicable).
Include Locations : Include the Locations information in the report (if applicable).
Include Contacts : Include the Contacts information in the report.

The HTML Report

The HTML report can be opened via the **index.html** at the root of the report.

This will immediately open the Device Details tab (if included) or timeline.

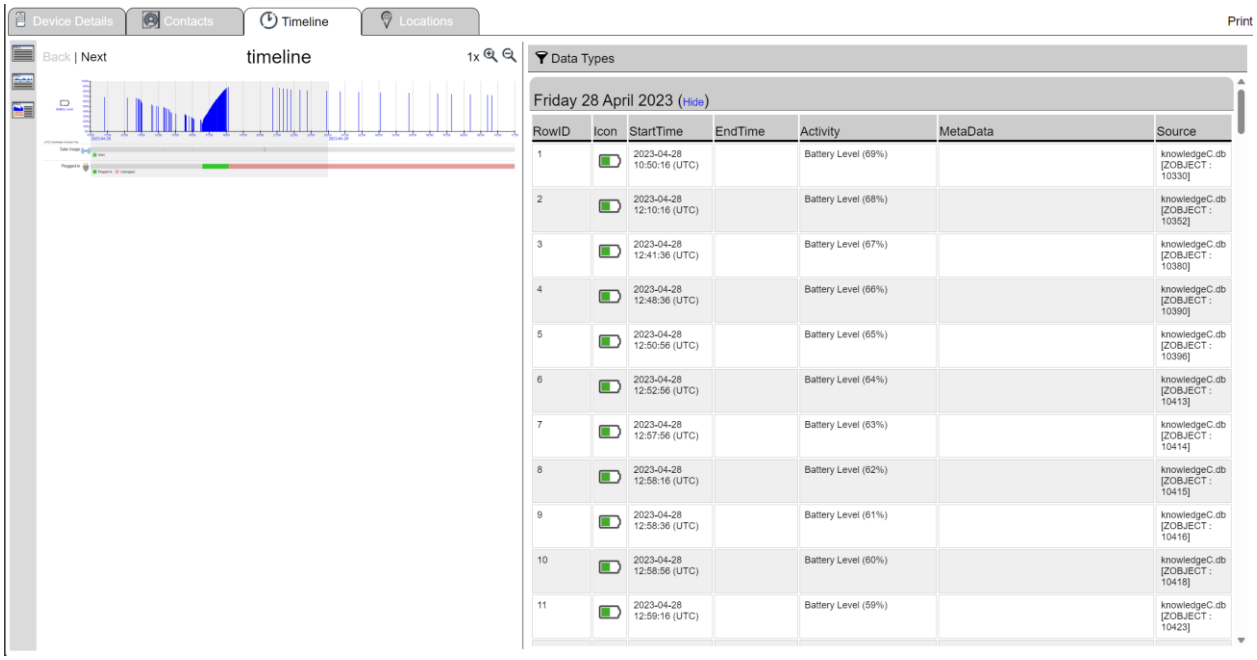
The top of the screen will include the Report Details and several tabs to access each of the different sections of the report.



The Device Details and Contacts tabs are straightforward reports based on the data in ArtEx.

Timeline and Locations are more interactive in order to handle the vast amount of information that may be contained.

Both Timeline and Locations follow the same basic structure.



1 - Reports Tabs
2 - View Options
3 - Graph / Map
4 - Graph / Map Navigation
5 - Graph / Map Zoom Controls
6 - Data Type Filter
7 - Date Table

Reports Tab

This row of tabs allows quick navigation between the sections of the report.

View Options

View Options allows you to view the table data without the graph or map, with the graph / map and table side by side (Horizontal) or Graph / Map on top and table on bottom (Vertical)

Graph / Map

The main Graph or Map image.

Graph / Map Navigation

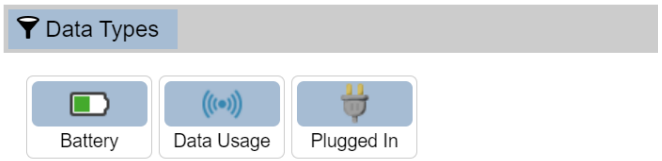
If Report Elements have been used to save additional graph and map images, they can be navigated here using the Previous and Next buttons.

Graph / Map Zoom Controls

Zoom in/out of the image.

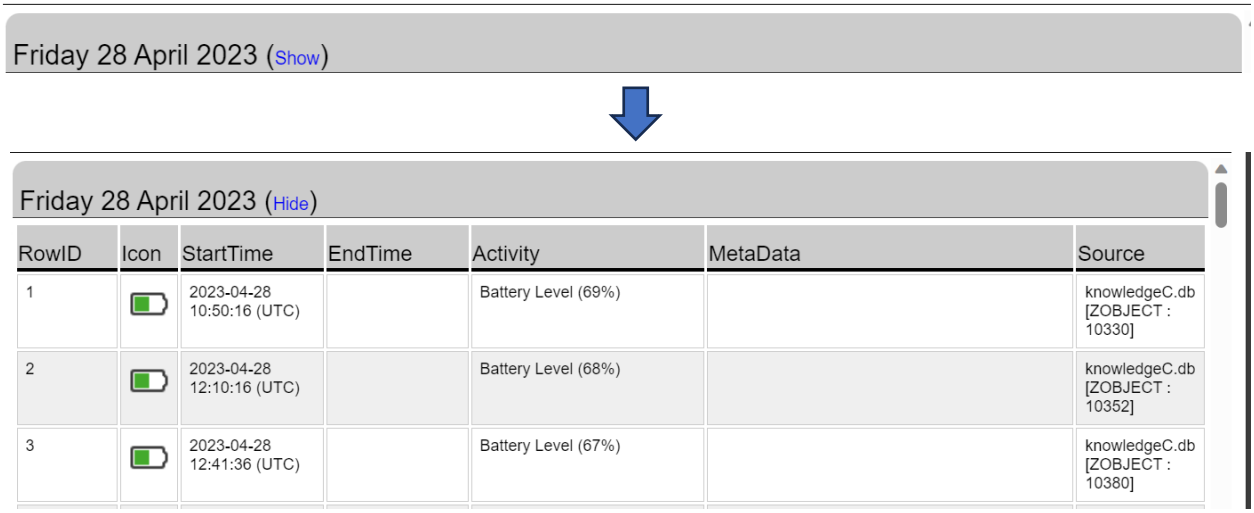
Data Type Filter

The report provides basic filtering options to remove records based on their type. Blue buttons are turned on.



Date Table

The data is broken down by date and each date of interest must be expanded by pressing the header



Save CSV

This option saves the table to a CSV file. No additional options are taken into account.

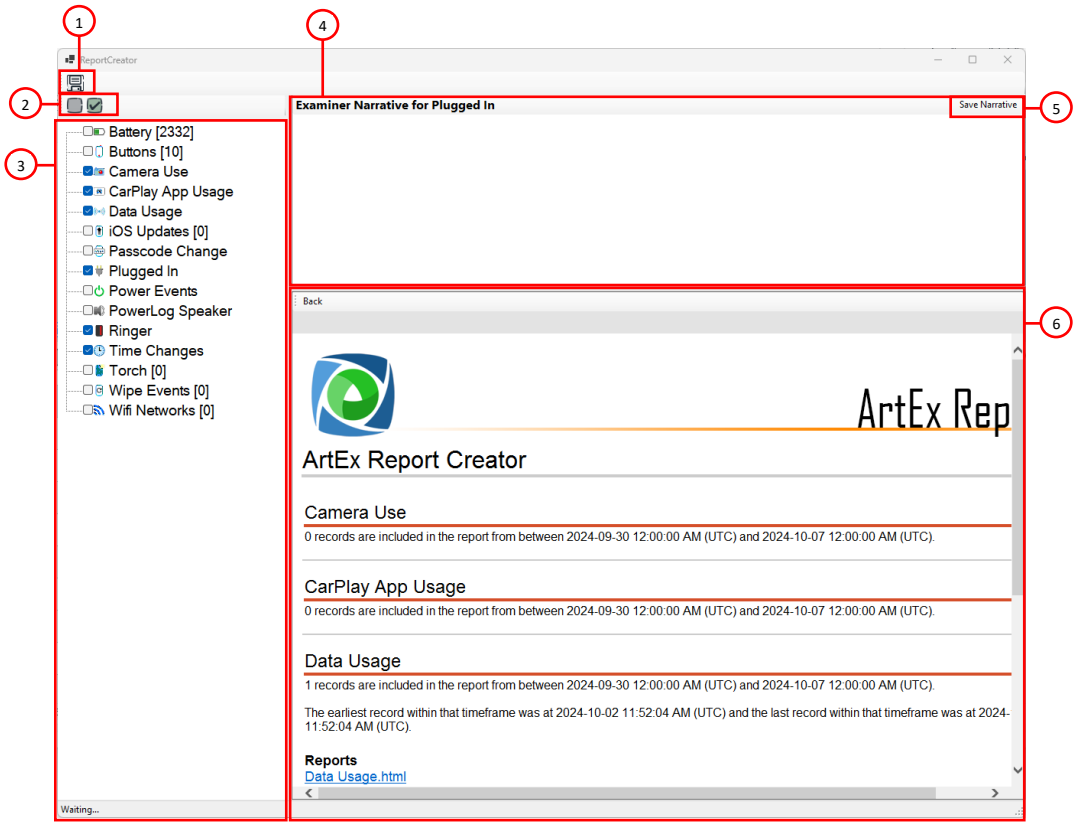
Save Graph

This option will simply save the graph image to a file.

Report Creator

The Report Creator is designed to create the barebones of an artifact centered report, listing the basic information about each artifact type and giving you the opportunity to add additional information where required.

Each artifact type included in the Report Creator report will also output an individual report for that specific artifact, linked via the main page.



1 – Save Report
2 – Select / Deselect Artifacts
3 – Artifact Tree
4 – Artifact Opinion Text
5 – Save Narrative Text
6 – Report Preview

Save Report

This will save the report that is currently presented in the preview window, along with any associated items.

Select/Deselect Artifacts

This will select or deselect all artifacts in the Artifacts Tree for inclusion or exclusion in the report.

Artifact Tree

This tree will show all artifacts processed in the TimeLine view.

Artifact Opinion Text

With an Artifact selected in the Artifact Tree, you can enter opinions about the item that you would like to include in the final report. Note that some “opinion” text will be populated automatically.

For example, the artifact will automatically include a count of the number of records of that type that were and the date of the first and last record.

Save Narrative Text

This commits your narrative text to the report. It can always be altered later if required.

Report Preview

This is the final HTML report that is being generated.

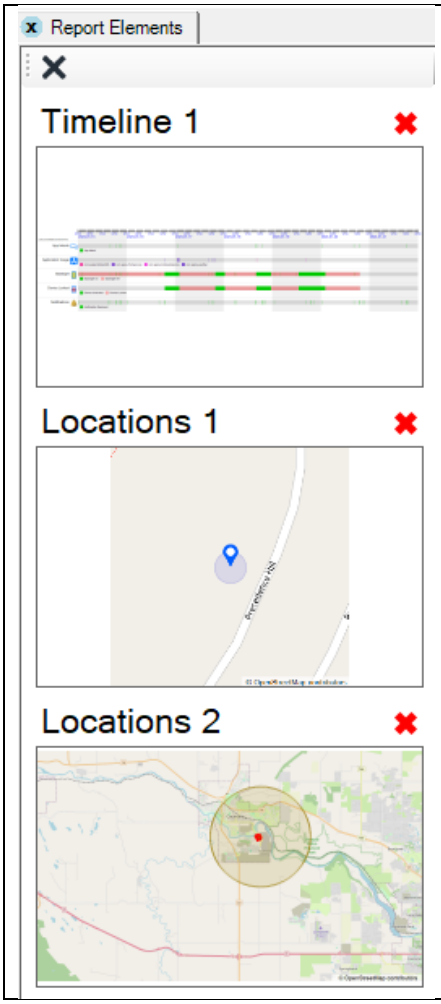
It is broken down by artifact type and each artifact will have the automatic opinion, custom opinion and report links.

Report Elements

Report Elements allows you to store and report several Timeline graph or Location map images.

Throughout ArtEx, there are several locations where you will find the “Add to Report Element” button  .

This button will add the specified image to the Report Elements which is accessible via the Right Pane.



The Report Elements feature lists all images that have been saved.

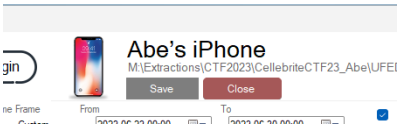
The Red cross above each item will remove the item and the Black cross at the very top will remove all items from the Report Elements tab.

Clicking an item will open it up for closer inspection.

Closing an Extraction

You have two options for closing ArtEx cases.

1) Close ArtEx window
2) Press the Close button underneath eh extraction name and path.



In either case, you will be asked if you would like to keep or remove the temporary files that were created.

Removing the temporary files is ideal to minimize the resources required by ArtEx however subsequent openings of the same extraction will be required to extract files again.

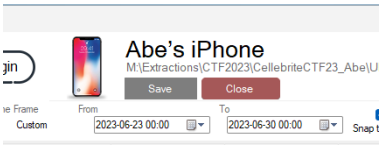
RTX

RTX (pronounced "r-tex") is designed to reduce time loading a case for the second or subsequent times.

An RTX file can be created by default whenever you Begin case by turning on the Automatic RTX Creation in the settings.

However, if this setting is turned off, there is a manual option too.

Once a case is parsed, a Save button appears underneath the extraction name and path.



At this point, the, save button is gray and the text reads "Save".

Pressing this button will change the colour to Red and the text to "Recording".

The directory structure and parsed data is immediately recorded to the RTX file and any subsequently parsed data or changes will also be automatically saved.

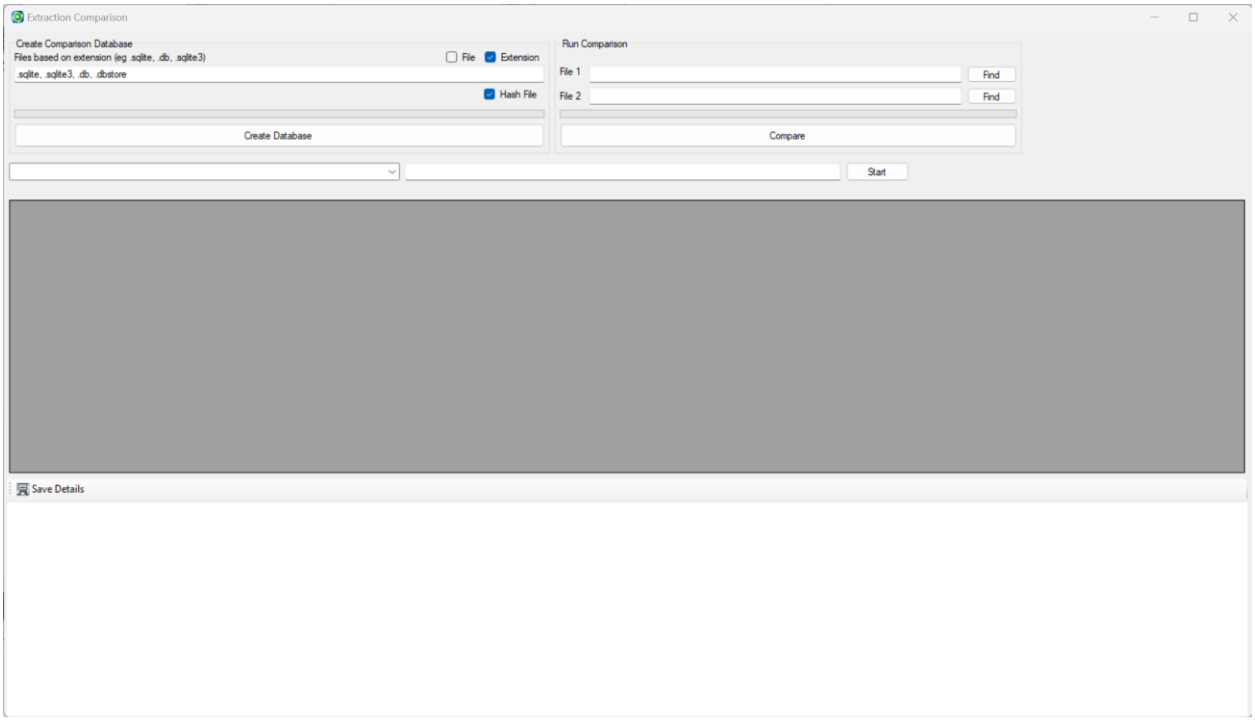
Pressing the "Recording" button again will stop the ongoing save activity.

Opening an RTX file will load the saved directory information, parsed records and cached images to speed up the initial processing.

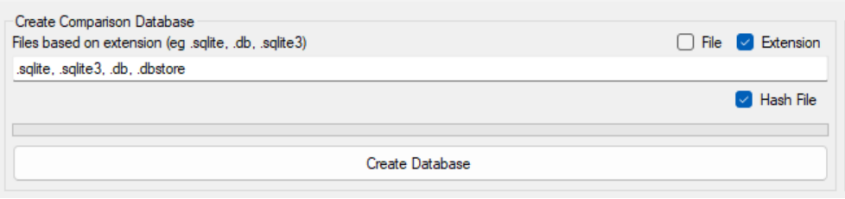
Extraction Comparison

The extraction comparison is an experimental tool designed to identify differences between file systems and database schemas of two different extractions.

It can be launched from the Directory View



The top left of the window is the Create Comparison Database frame. This is the first step in creating a comparison.



You can choose to include specific File by entering the path and selecting the File checkbox, or enter the extension of the files you want to include and choose the Extension checkbox.

You have the option to hash the file also.

Press Create Database.

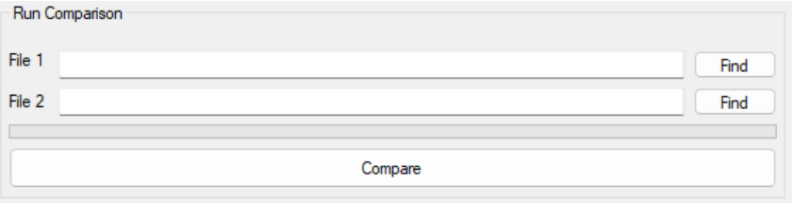
ArtEx will extract the specified files and create a database of the database, tables, fields and datatypes.

Once completed, the first step is over, and you can close the screen.

The second step is to load another extraction and launch the Comparison window again, repeating the steps from above.

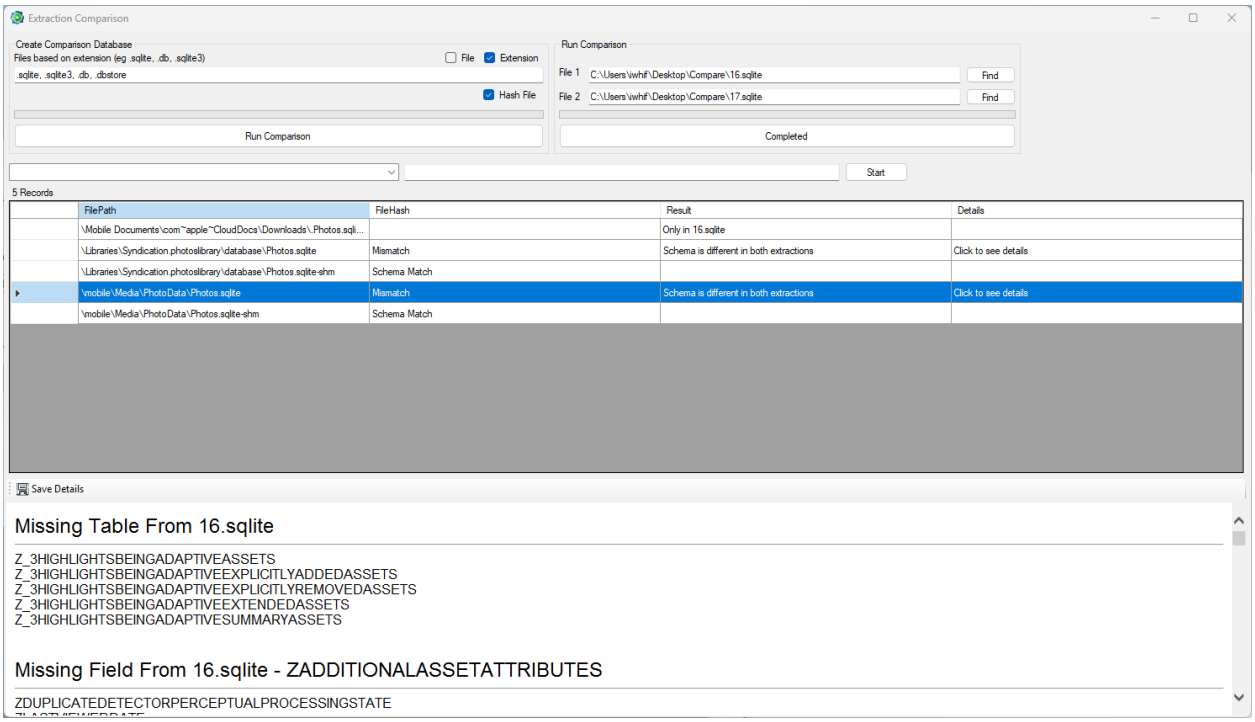
Once completed, you will have 2 databases ready for comparison. This can be done immediately from the same Comparison window, or launched from the Extraction Finder.

The top right of the Comparison Window is the Run Comparison frame.



Use the Find buttons to point to each of the database created and then press Compare.

ArtEx will compare the 2 previous outputs and provide a list of differences.



The first column provides the path.
The second column provides details of if the files hash matches.
The third column gives more information about the analysis.
The fourth column provides the most detail.

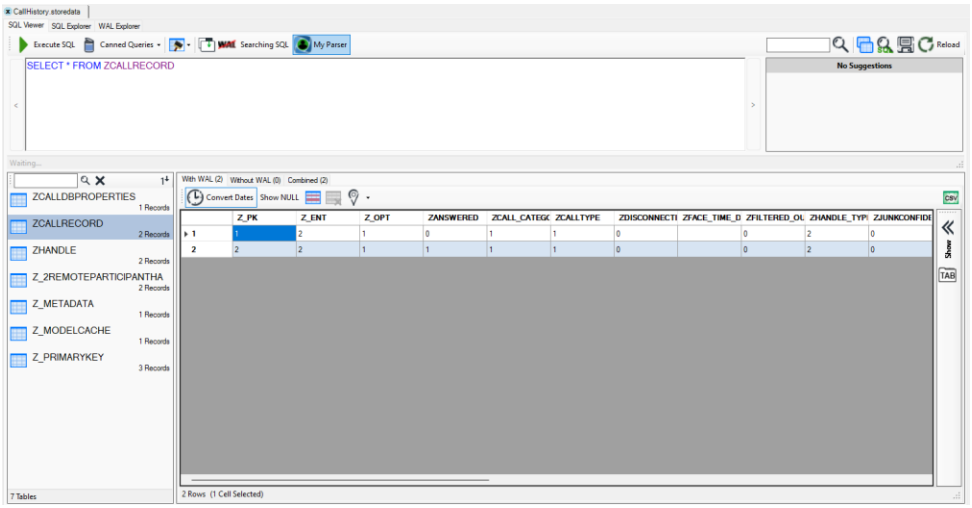
Clicking on a row may provide a more thorough breakdown of the differences between the files.

My Parsers [BETA]

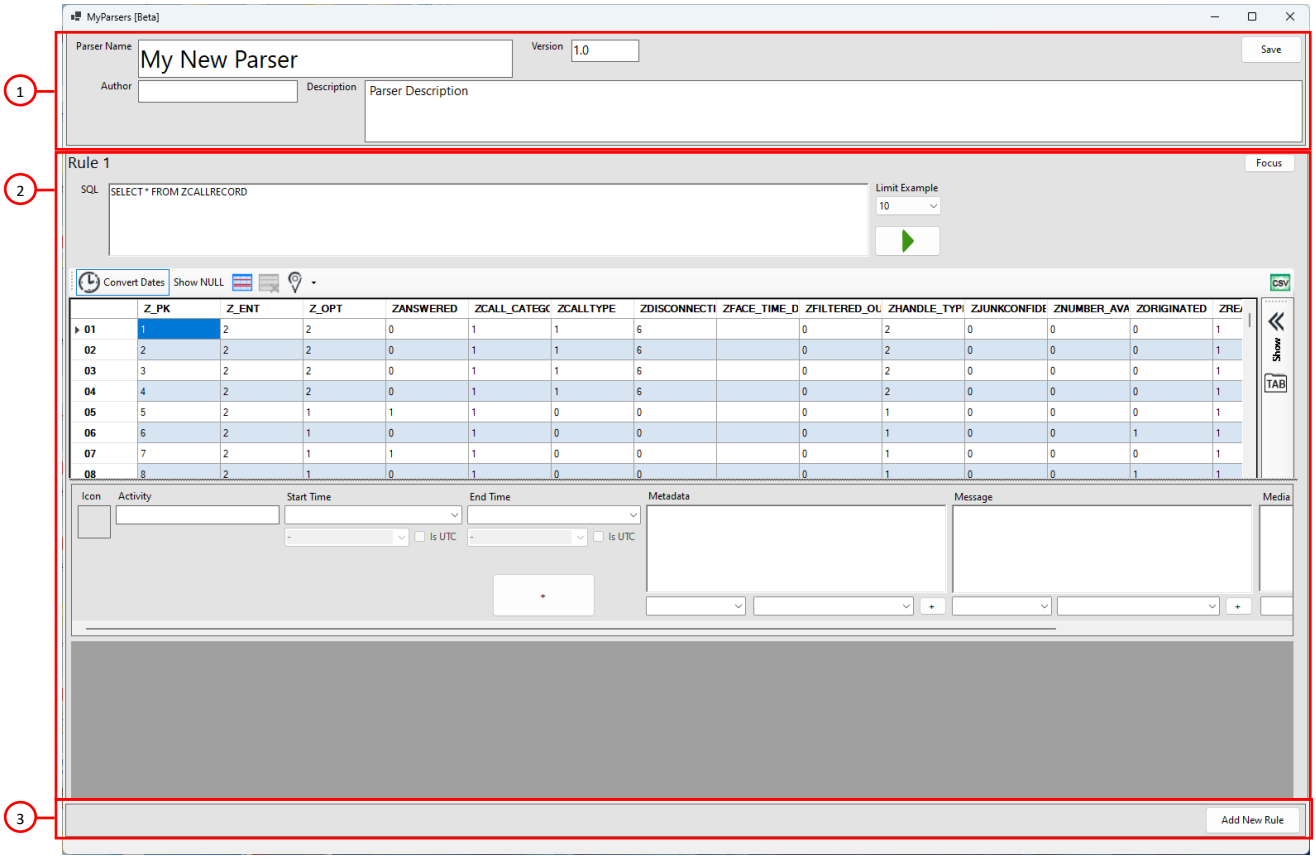
My Parsers is a new feature to allow you to utilize ArtEx's interface for reporting on your own research.
Note : It is in its initial stages and may not work entirely as expected.

Note that the release notes, like this feature, are still a work in progress.

1. Open the database you are interested in.
2. Run whatever SQL queries you want.
3. Press the My Parser button.



4. This will launch the My Parser window.



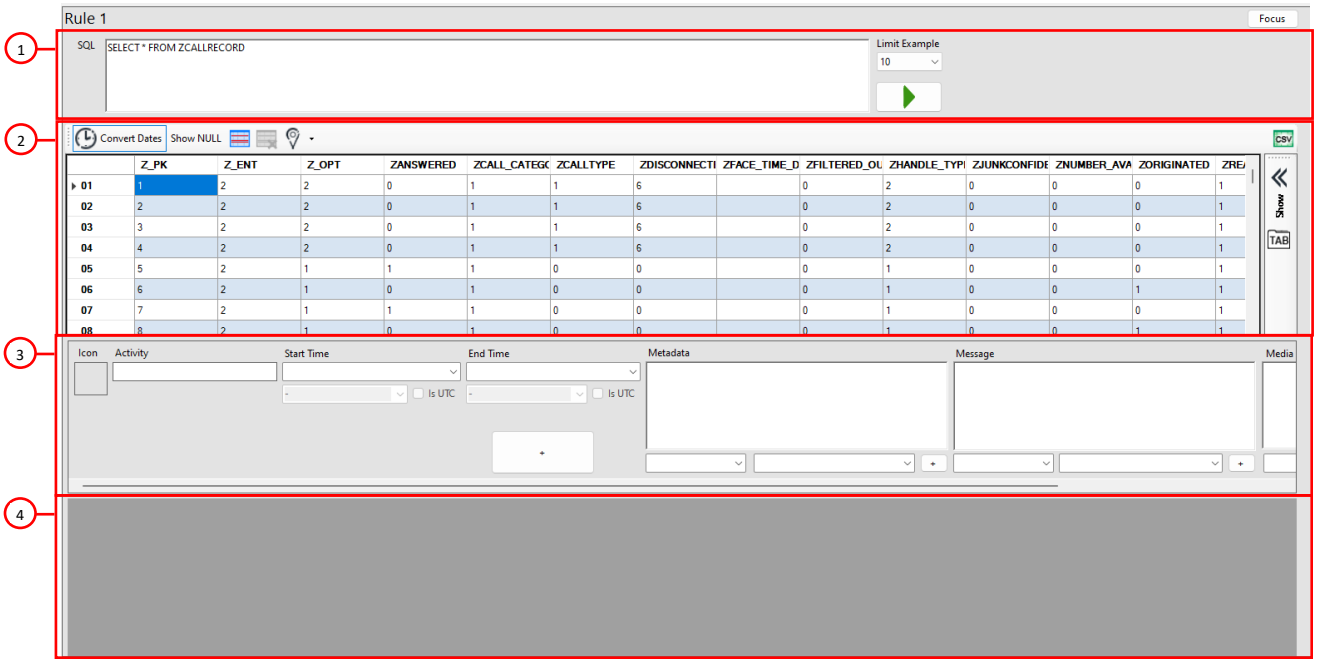
1 – Parser Details
2 – Rules
3 – Add Rule

Parser Details

The Parser Details pane allows you to enter a parser name, description and details.

Rules

Each Parser can have a maximum of 5 rules and the Rules area requires additional explanation.

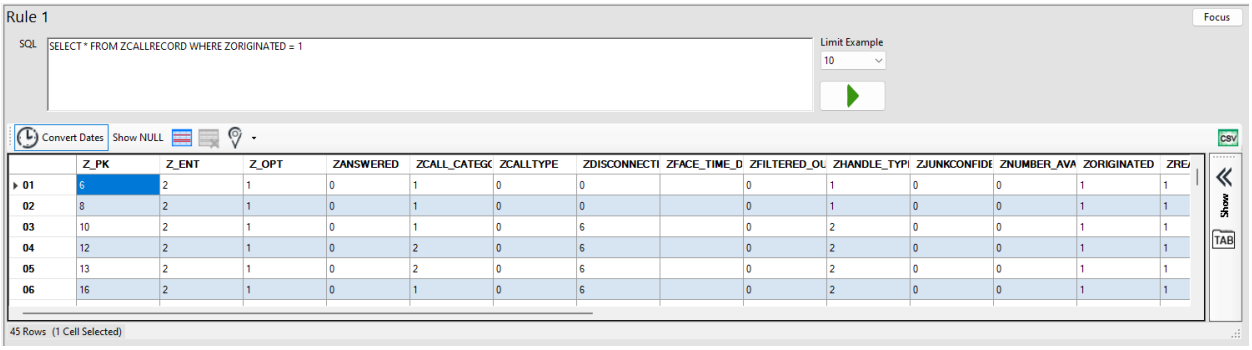


1 – SQL Statement
2 – SQL Results
3 – Parser Mapping
4 – Parser Preview

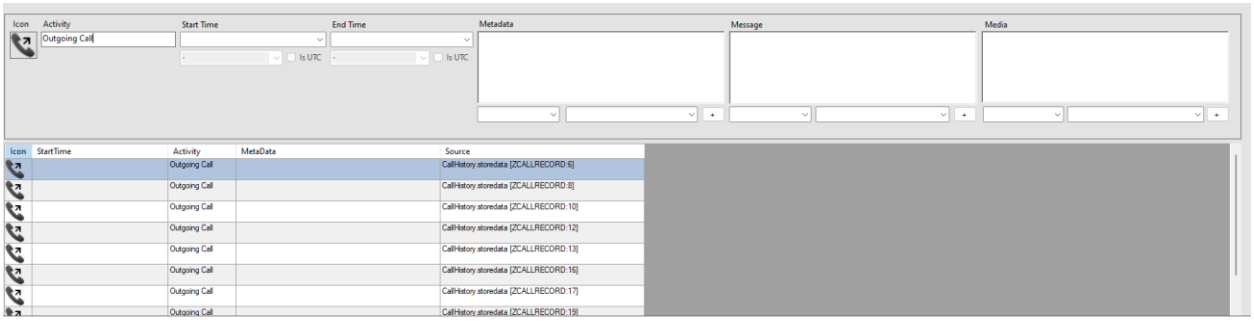
For example, entering the SQL

SELECT * FROM ZCALLRECORD WHERE ZORIGINATED = 1

Will result in a list of all outgoing calls

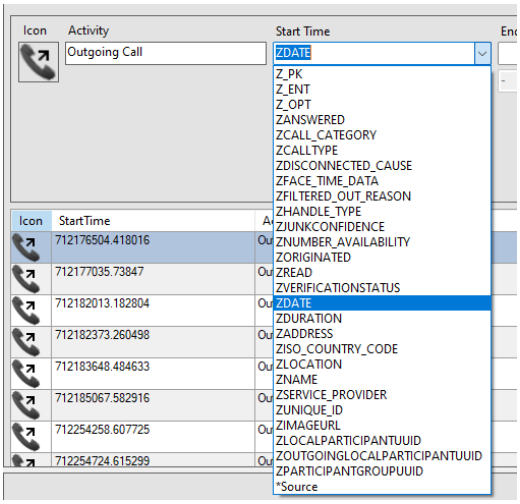


You can then begin mapping the items which will automatically update the parser preview.

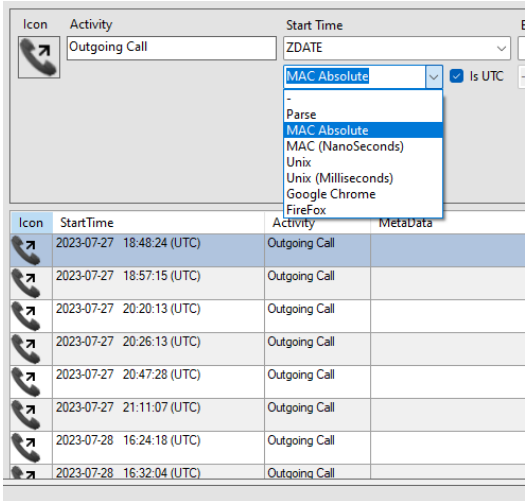


Fields such as Icon and Activity are free for you to enter whatever you want.

Some fields must be mapped to the database. For example, Start Time. In these cases, select the appropriate field from the drop down list.

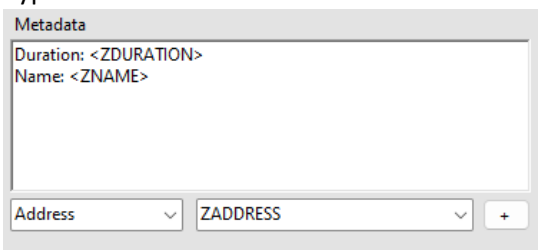


You may notice this populates the Start Time exactly as it is in the database and still requires converting to a timestamp. This can be done by selecting the appropriate epoch from the list.



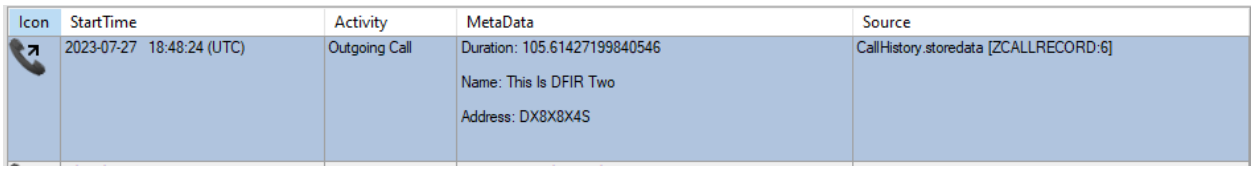
The Metadata field is a semi-custom field depending on the type of data being parsed.
In this instance, we will treat it as an open field.

Type in the name of the data and select the field from the drop down list:

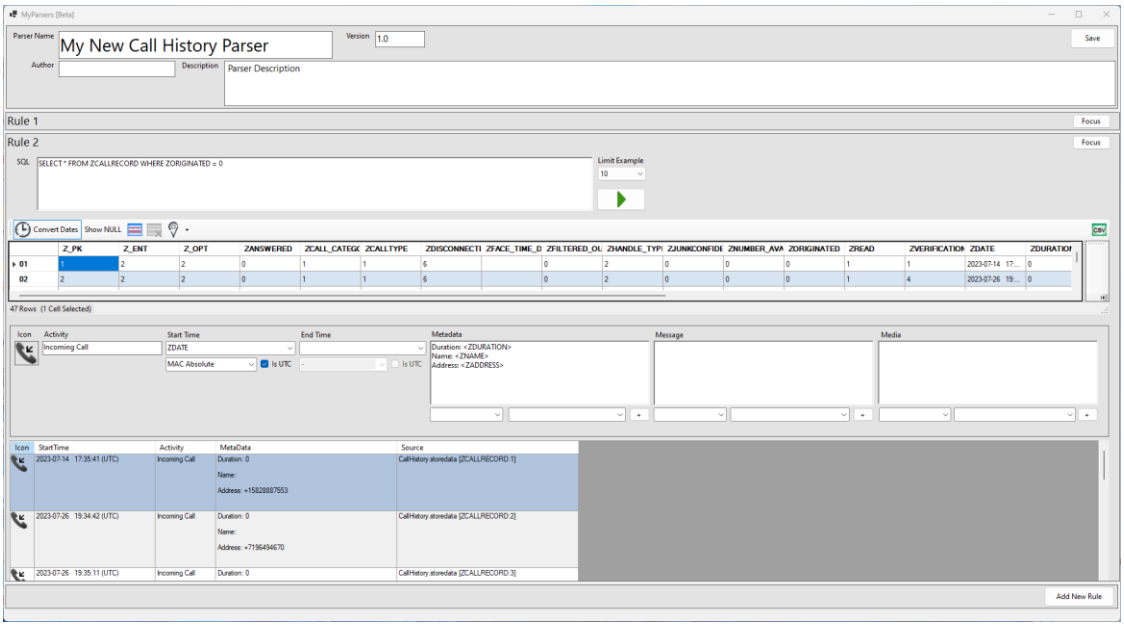


Press the + button to save the item.

This will be viewable in the Parser Preview.

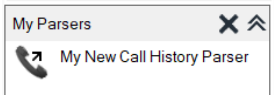


At this point, you may consider this Rule Complete and press Add New Rule where the SQL can be changed to Incoming calls.

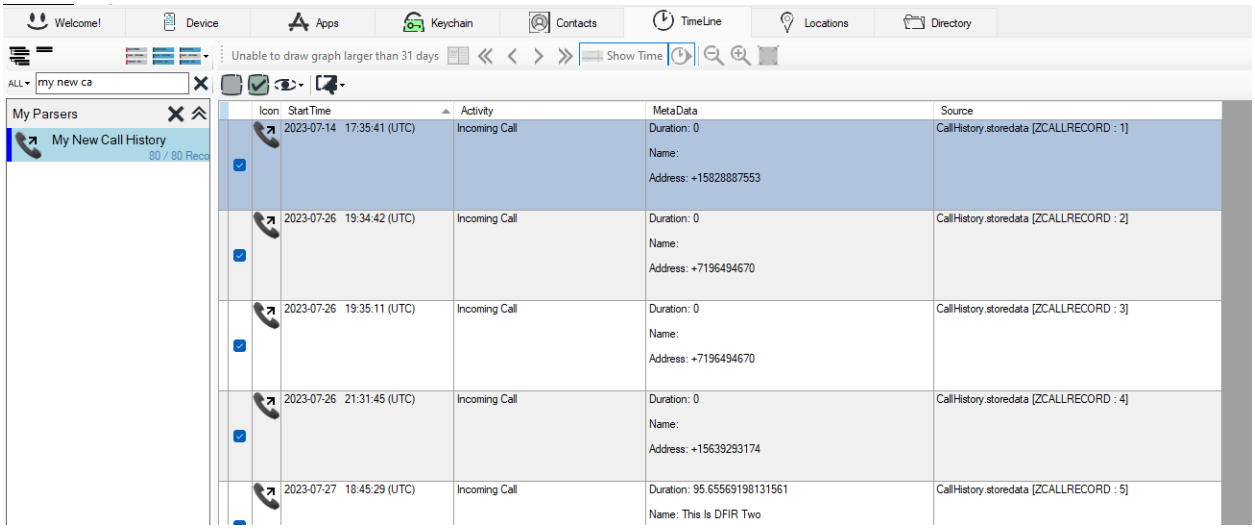


Once you have added all rules, press Save in the top right.

Your new parser will be saved to the location specified in Settings and added to the My Parsers section of the Timeline.

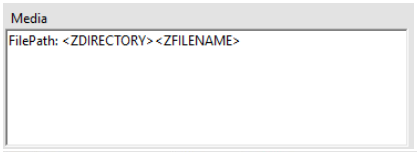


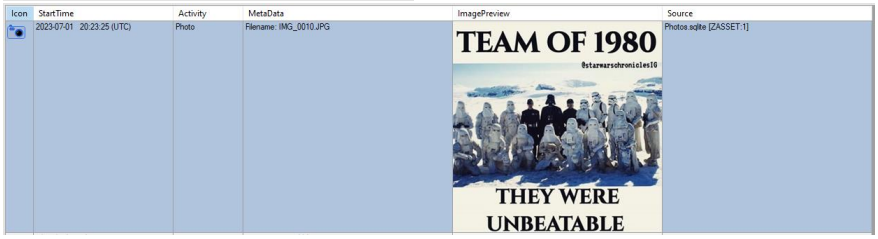
It can now be used like any other parser.



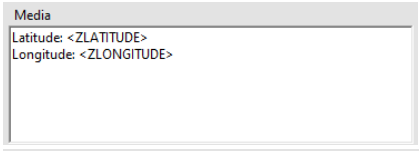
More complicated parsers can also be created by utilizing the additional options in the Rules pane.

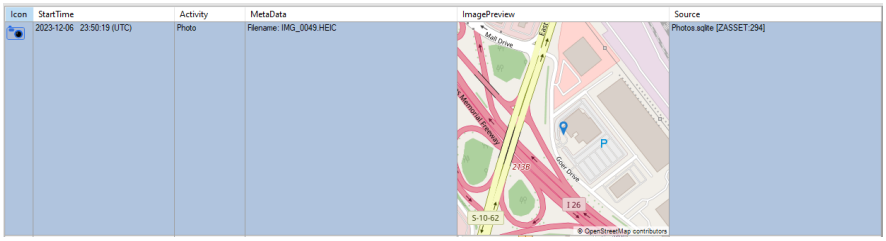
- JOINS are permitted to make more complicated SQL Queries
- More complicated Mapping such as:
  - Add Media using the Media Block



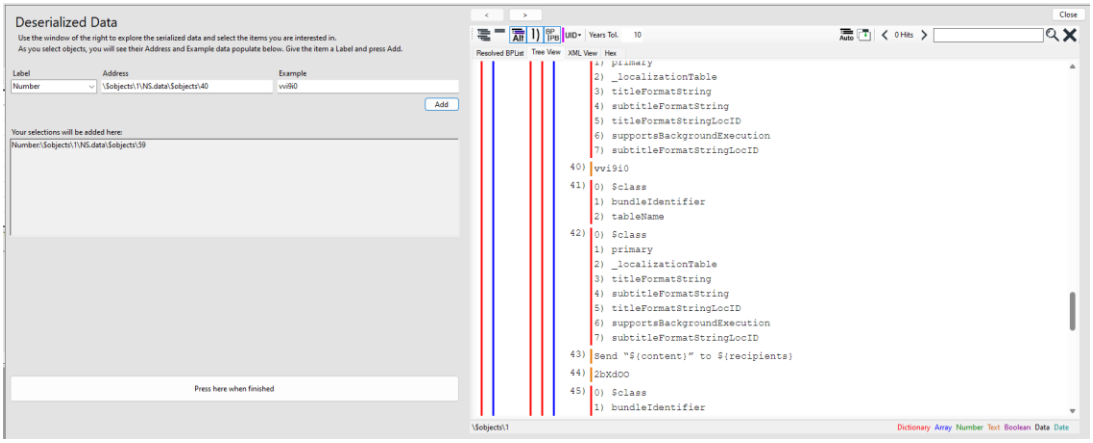


  - Add Maps using the Media Block





- Use Deserialized Data



Add the label information at the left and use the tree to find the appropriate node.