



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

User Guide

October 2024



## Contents

Introduction	3
The Interface	4
Setting Up	7
Opening an Extraction	9
RTX / Archive	10
ArtExtraction	11
Backup / Folder	13
File / XLS	14
Comparison	15
Drag & Drop / Initial Processing	16
Starting an Examination	17
Device Details / Apps	17
Contacts	18
Timeline	19
Timeline Graph	22
Timeline Table	23
Time Zones	25
Times of Interest	26
Chats	27
Media Gallery	28
Locations	29
Мар	29
Map Tools	33
Custom Markers	35
Flipbooks	36
Offline Use	38
Directory	39
Right Pane	44
Hex Viewer	44
Media Viewer	46
Text Viewer / SQL Viewer	47
Encrypted Databases	54
SQL & WAL Explorer	55
Deserialised View	59
SEGB Viewer	61
ArtExtraction	62
Reports	66
Report Elements	70
Closing an Extraction	71
RTX Files	71
Comparison	72

## 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 <u>hello@doubleblak.com</u>.

## 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:



#### **Begin Button**

This is where all cases in ArtEx start. Press (Bogin) 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.

🔾 Run 🔛	Custom	2023-05-07 00:00	2023-05-14 00:00	Snap to Hour	7 Days				 (UTC) Coordinated Universal Time	
U Welcome!	Device	A Apps	Keychain	Contacts	() TimeLine	9	Locations 🕈	Directory		
			1-	- All	X	-	D		_	î
	٠	Welcome				•	TimeLine	е		
	٠	Device				•	Chats			
	٠	Apps				•	Gallery			
	٠	Keychain				•	Location	IS		
	•	Contacts				•	Director	y		

#### 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.
X	This will close all open tabs in the Right Pane.
1	This will show the Report Elements.
	This will open the Directory Viewer at the path of the file being viewed.
0	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.
232 232	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.

	Localization			Default 1	Template		
	Date Format	yyyy-MM-d	d v	Non	e		~
ArtEx	File Locations Default Temp C:\Users\wh Locations Dat C:\Users\wh My Parsers C:\Users\wh DLLs	Locations if\OneDrive' abase if\Desktop\ if\OneDrive if\OneDrive if\OneDrive	AtEx2\ArtEx2\bin\Debug\ne AtEx2\ArtEx2\bin\Debug\ne Documents\MyParsers General Check for updates on la Check Parser Eligibility Always Process Keycha Guess Date Fields (SQ) Use Advanced SQL Re Hide Progress Window	aunch ain L) eader	<ul> <li>ws\\LocationsDatabase sqite</li> <li>Show Directory View Thi</li> <li>Run Apps by Default</li> <li>Locations</li> <li>Parse Locations by defaul</li> <li>Draw Small Mans</li> </ul>	unt	Browse Browse Browse
Manage My Parsers	Cell Networks Import Cell To map cell towe	wer informati r connection	Aur OCR on Images     Aways Create RTX     Include Opinion Notes     Include Opinion Notes     ion (GPS, Beamwidth, Azimuth     s.	h etc) from	Prompt for Tile Grabber     Large Tile Cache sources such as OpenCellID or	the cell provid	Jer to
View Installed Parsers			Import	Cell Tower	Data		
Check for Updated Parsers							
WWW.DOUBLEBLAK.COM	Cance	ł				Save	•

#### **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.



Archive	<b>Archives</b> 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	<b>ArtExtraction</b> 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	<b>Backup</b> 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	<b>XLS</b> 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.

	RTX Case 🚍 Archive 🗍 ArtExtraction 🍘 Backup 🗂 Folder 📙 File 🔛 XLS 🛅 Compare	F
	Find RTX	_
HT Y	Temp Folder	
TLX	C:\Users\iwhiftDocuments\ArtExTemp Browse	,
RTX	RecentRTX	
Open a previously saved RTX file created		
by ArtEx		
5270		
Contraction of the		
5 Carlins		
A P -		
and Vie	Cancel	n

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.

<u> </u>	RTX Case Archive D ArtExtraction D Backup T Folder File L XLS T Compare
	Temp Folder
File	C:UsersliwhiftDocumentslArtExTemp Browse Recent Extractions
Open a previously saved RTX file created	iPhone C:\Users'\whif\Desktop\UFED Apple iPhone 12 Pro (d53pap) 2023_04_20 (001)\EXTRACTION_FFS 01\EXTRACTION_FFS.zip Last Viewed : 2023-12-26
S I I I	
C. S. J.	
S Sugar	
is a Th	(Cancel Open

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.** 

[=]	👰 RTX Case 🚍 Archive 🗍 ArtExtraction 😥 Backup 🗂 Folder 🖺 File 🛄 XLS 📋 Compare
	IP Address     Port     User     Password       127.0.0.1     22     root     alpine     Reset
<b>T</b> elesson	Is your device checkm8 compatible? Yes No Compatibility Chart
ArtExtraction	
Connect to a live device via SSH for extraction or Live	
Examination (Device	$\sim$
must be jailbroken)	Test Connection
a star	Temp Folder
a ser an	C:\Users\iwhiflOneDrive\Documents\ArtExTemp Browse
Star Th	Cancel

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 Build Live Connection and Brull File System Extraction button will become enabled.

Use the B<sup>Live Connection</sup> to process the device in real time or the <sup>Connection</sup> 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.

Connected	Devices	1 device(s) found - Scan
Ţ	lan's iPhone 040c85e4bc1209c90450a993f6a29a57c1b4c1e6	iPhone X - iOS16.7.10
		() Start

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.

<b>[–</b> ]	👰 RTX Case 🚍 Archive 🖟 ArtExtraction 🏟 Backup 🗂 Folder 🖺 File 🔜 XLS 🛅 Compare
	Connected Devices 1 device(s) found - Scan
	Ian's iPhone         iPhone X - iOS16.7.10           040c85e4bc1209c90450a993f6a29a57c1b4c1e6         iPhone X - iOS16.7.10
ArtExtraction	
Connect to a live device via SSH for extraction or Live	
Examination (Device	(j) Start
must be jailbroken)	No password is set. It is recommended to enable a password to get more data.           Password         1234           Set Password         Continue
Star Th	Cancel Open

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

The backup will begin

[-]	👰 RTX Case 🝙 Archive 🗍 ArtExtraction 🍙 Backup 🗂 Folder 📗 File 🛄 XLS	Compare
	Connected Devices 1 devices	(s) found - Scan
	Ian's iPhone <sup>iPhone</sup> 040c85e4bc1209c90450a993f6a29a57c1b4c1e6	X - iOS16.7.10
ArtExtraction		
Connect to a live device via SSH for		
Examination (Device		(f) Start
must be jailbroken)		Cancel
a Service	Backing up	6%
and T	Cancel	Open

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

## Backup

Backup will accept encrypted or unencrypted iTunes backups.

	Find Tunes Backup
	Temp Folder CWaenlicht#Dermo
Tunes Backup	Backup Password
Open an iTunes Backup	Recent iTunes Backups
Callin	
224	
Strange	
Sel Cont	
and me	

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 (Tex Personer). 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.

	👰 RTX Case 🚍 Archive 🗍 ArtExtraction 🧑 Backup 🗂 Folder 🖺 File 🔜 XLS 🛅 Compare
	Find Folder  Temp Folder  Cut tending the formation of th
Folder	Cosessiwini bocuments vitex remp
Open all files in a specific folder (ie. a folder containing multiple databases and plists)	
ACRA TH	Cancel Open

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.

	🕅 RTX Case 🕼 Archive 🗍 ArtExtraction 🧭 Backup 🗂 Folder 🖺 File 🔜 XLS (	Compare
<u> </u>	Find File	Browse
	Temp Folder	
File	Closersiwmit/Documenistance.remp Recent Files	browse
Open a specific file (ie.		
squite or plist)		
San In		
321-J-1		
Dor and		
3 Cardena		
and with		
Mark Vi.	( Cancel )	( Open )

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.

	👰 RTX Case 🚍 Archive 🗓 AnExtraction 🧊 Backup 🗂 Folder 📗 File 🛄 XLS 🛅 Compare	
	Original Source	)
	Date Format dd MM yyy  V Note. Timezone assumed to be UTC	
XLS Converter	Read Columns	
Convert XLS files to SQLite for analysis in ArtEx		
2 Cardens	Convert XLS to SQLite	
server of	Cancel	)

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.

	RTX Case     The Archive     Original Source     Source File     Date Format     dd MM yyy	ArtExtraction (2) Backup C Folder C File C XLS he.sqlite [ZRTCLLOCATIONMO] e1234\00747974^1245211281222^CachedLocations.xlsx	Compare			
ALS Converter		Read Columns				
Convert XLS files to SQLite for analysis in	Required Field	XLS Column				
ArtEx	Z_PK	✓				
AILEA	ZLATITUDE					
	798550	`				
Production P		Y	'			
The second	ZHORIZONTALACCURACY					
	7TIMESTAMD					
Convert XLS to SQLite						
and the second						
CASTA TO THE						
Marke Vie	(Cancel)		( Open )			
E. I.	<u> </u>					

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?

~	👰 RTX Case 🖻 Archive 🗍 ArtExtraction 🕖 Backup 🗂 Folder 📗 File 🛄 XLS 🛅 Compare						
	Extraction Comparer is a beta feature for comparing SQLite schemas between iOS Extractions.	^					
	To inititate this feature, open an extraction as normal and got to the Directory View.						
XLS Converter Use the Comparison	From here, press the Comparer button to open the comparer tool. Enter the name of the file(s) or file extension(s) you are interested in.						
Tool on previously made Comparison	For exmaple; enter "photos sqlite" if all you want is to compare the photos sqlite database; or enter "sqlite" if you want to compare ALL .sqlite databases. Seperate multiple values with a						
Databases (Available in Directory View)	ie. ".sqlite, .db, .sqlite3"						
Contra .	Press "Create Database" and give it a name.	~					
C. C. C.	· · · · · · · · · · · · · · · · · · ·						
and the second	Lanch Comparison Tool						
and The	Cancel	$\Box$					

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.

🔕 ArtEx									- 0	×
Begin	)	Is's iPhone	on\UFED Apple iPhone	∋ 11 (N104AP) 2024_01_23 (0I	01)\EXTRACTION_FF	S 01\EXTRACTION_FFS.	S.zip	Save Report	© Settings	() About
Cus Time Fram	tom 2024-01-17 00:00	To 2024-01-24 00:00	Snap to Hour	Duration 7 Days			TimeZone (UTC-05:00	) Eastern Time (US	& Canada)	] ~
U Welcome!	Device 🗛 Ap	ops 🔓 Keych	ain 🛞 Contact	s 🕑 TimeLine		Directory				
	This Is's iP	hone				data_ark.plist				
	IFTIONE 03 10.1.2 (2	208110)				System version prist	1			
	Anala D	Accounts	A securita 2 and a	Nessage Detection	Settings	com apple Meble SUS plat				
	thisisdfir@gmail.com		Accountes.eque	Forever		contapple.mobile.om.o.pilst				<b>1</b>
	iCloud thisisdfir@gmail.com		Accounts3.sqlite	FindMyiPhone Enabled True	com.apple.icloud.findm	rydeviced.FMIPAccounts.plis				(h).
	Subscribers	ICCID	CellularUsage.db	Location Services State		com.apple.locationd.plist				
preferences pist	2024-01-22 11:46:48 89	01260971148676693	+19195794674	Setup Method		com.apple.purplebuddy.plist				
iPhone 11		Numbers		SetupUsingi lunes TimeZone		localtime				
iPhone12,1	InternationalMobileEquipmentIdenti	ity	mobileactivationd.log.1	America/New_York		data, ark plist				
N104AP	353985100845978 UniqueDeviceID		mobileactivationd.log.1	DESKTOP-AHCP3QO		Gata_an.pist				
	00008030-001259123E5 SerialNumber	60802E	mobileactivationd log 1	Carrier Timezone True	com.app	le.preferences.datetime.plist				
	F4GZ987AN72N				Interfaces		1			
	MobileEquipmentidentifier 35398510084597		mobileactivationd.log.1	Wi-Fi	intoindood	NetworkInterfaces.plist				
	InternationalMobileEquipmentIdenti 353985100962591	ity2	mobileactivationd.log.1	Ethernet Adapter (en1)		NetworkInterfaces.plist				
	Advertising E 14F8CF3D-7379-49C6-		m.apple.lsdidentifiers.plist	8A:64:40:79:D2:F9 Ethernet Adapter (en2)		NetworkInterfaces.plist				
	In	noortant Dates		8A:64:40:79:D2:06						
	Device Wipe		containermanagerd.log.0	Download and Keen Originals	iCloud Photos	annia mobilas idas bow pist				
	2023-07-01 16:16:01 (-4 Last KnowledgeC Entry	4.00)	knowledgeC.db	False	con					
	2024-01-23 10:35:25 (-	5:00)	obliterated	iCloud Photos Enabled True		cloudServiceEnableLog.plist				
	2023-07-01 16:15:33 (-4	4:00)	.ouworaled	Shared Albums Enabled		cloudServiceEnableLog.plist				
	Bootstrapped 2023-07-01 16:15:27 (-4	4:00)	.bootstrapped				1			

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.

A.	AllTrails	Health amp; Fitness
A	Venant 77.000 Bundle:/private/var/containers/Bundle/Application/579F20A4-2A3E-4171-A544-BF4AAEB433AF/AITrails.app Sandbox:/private/var/mobile/Containers/Data/Application/70AAF121-E0E5-4982-95F9-E4DAB4CCB648	🖺 Extract Bundle

\*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.

U Welcome!	Device 🗛 Apps	🗟 Keychain 🔘 Contacts	TimeLine 🖓 Locations	Directory	
					>
loon	Contact Name	Contact Details	Created	Modified	Source
· ·	Liz	Mobile : +1 (919) 208-4530	2023-04-24 5:59 PM	2023-04-24 5:59 PM	addressbook.sqlite [ABPERSON
* 🦉	This DFIR		2023-04-15 2:00 PM	2023-04-15 2:00 PM	addressbook.sqlite [ABPERSON
	This Is DFIR Two	Mobile : (919) 888-7386 Home : thisisdfirtwo@gmail.com	2023-04-15 2:00 PM	2023-04-24 5:59 PM	addressbook.sqlite [ABPERSON
• 😔	This Is DFIR		2023-04-15 2:00 PM	2023-04-15 2:00 PM	addressbook.sqlite [ABPERSON
•	This Is DFIR Two	Mobile : (919) 888-7386 Home : thisisdfirtwo@gmail.com	2023-04-24 5:59 PM	2023-04-24 5:59 PM	addressbook.sqlite [ABPERSON
<b>•</b>	ThisIs DFIRThree	Home : thisisdfirthree@gmail.com	2023-04-24 5:59 PM	2023-04-24 5:59 PM	addressbook.sqlite [ABPERSON
•	Thom De'Fer	Mobile : (919) 802-7080	2023-04-24 5:59 PM	2023-04-24 5:59 PM	addressbook.sqlite [ABPERSON

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 dependent on the Time Bar options at the top of the screen and we need to go over these in detail.



#### **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.
ALL-	The first two 🚝 will expand or collapse all parser groups.
Activity X 🗙	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
Applications X 🛠	Hide Graph
Installed Apps	Save Selections
Device X 🛠	power
Battery	
Buttons	These templates are referred to on the Settings screen and allow you to choose a template to parse by default.
Camera Use	
😭 CarPlay App Usage	The second tool har row contains a dron-down menu for selecting parser type
(((•))) Data Usage	
iOS Updates	
Passcode Change	My Parsers
🐈 Plugged In	There is also a search box, allowing you to search for the name of the parser you want
O Power Events	to find along with a Clear Search button.
PowerLog Speaker	
Ringer	The parsers are arranged into groups and each group has its own Header bar.
	Device 🗙 🛠
	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;

(((•))) Data Usage	White = Unprocessed parser.
(((•))) Data Usage	Gold = Currently highlighted parser.
(((•))) Data Usage	Blue = Selected parser.
(((•))) Data Usage	Light Blue = Disabled parser.
CarPlay App Usage	Light Red = No data (ie. Files do not exist)
C Edge History	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.





#### **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 requir

#### **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 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.

	<b>Ф- I</b>	•			- Q Find	+ E · X -
lco	n StartTime		▲ EndTime	Activity	Source	
	2023-04-19	18:12:23 (UTC)		Battery Level (100%)	CurrentPowerlog.PLSQL [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 1]	
• 🎽	2023-04-19	18:12:23 (UTC)		Device Plugged-in State Check : Unplugged	CurrentPowerlog.PLSQL [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 1]	
2	2023-04-19	18:12:28 (UTC)	2023-04-19 18:13:16 (UTC)	Backlight On	knowledgeC.db [2OBJECT : 13]	
-	D 2023-04-19	18:13:00 (UTC)		Battery Level (99%)	knowledgeC.db [ZOBJECT : 145]	
•	2023-04-19	18:13:16 (UTC)	2023-04-19 18:14:12 (UTC)	Backlight Off	knowledgeC.db [20BJECT : 51]	
•	2023-04-19	18:14:12 (UTC)	2023-04-19 18:17:16 (UTC)	Backlight On	knowledgeC.db [ZOBJECT : 160]	
<b>•</b>	2023-04-19	18:15:52 (UTC)		Battery Level (98%)	knowledgeC.db [ZOBJECT : 209]	
2	2023-04-19	18:17:16 (UTC)	2023-04-19 18:20:40 (UTC)	Backlight Off	knowledgeC.db [20BJECT : 167]	
•	2023-04-19	18:20:40 (UTC)	2023-04-19 18:21:32 (UTC)	Backlight On	knowledgeC.db [20BJECT : 178]	
☑ 📻	2023-04-19	18:20:41 (UTC)		Battery Level (98%)	CurrentPowerlog.PLSQL [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 2]	
• 🎽	2023-04-19	18:20:41 (UTC)		Device Plugged in State Check : Unplugged	CurrentPowerlog.PLSQL [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 2]	

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.

lcor	n Start Time	Activity	MetaData	ImagePreview	Source
2	2023-04-15 08-58-59 (4-00)	Photo	FielName: IMS_0001.JPG Organal FlexInter: 44711075E-64774155-977878E38A238AD3.JPG Detectory: PhotoData/PhotoDoudSharingData/17193901029/6063AF05F4034CDD-850FF18F13F Album: My Shared Album Note: Unlikely taken with this device:	Pis over mannequin. I have the high ground!	Protos do [ZASET : 1]
2	2023-04-15 09-58-59 (4:00)	Photo	FleName: IMS_0002.PFG Original FleName: IMS_0005.JPG Directory PhotoData/PhotoCloudShampData/17193901029/6063AF05.F403-4CDD-850F-F18F13F Album: My Shared Album Note: Unlikely taken with this device	Waiter: enjoy your meal! Me: you too	Photos do (ZASSET : S)

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.

n	StartTime		A
×	2023-10-18	20:52:37 [Local]	U

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.

<b>–</b>				-	
	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.

		Save Chat
This Is DFIR Two]     2Messages     +12029789960	+19198887386 [This Is DFIR Two] 2023-05-09 20:00:24 (-4:00) - 2023-05-20 10:57:02 (-4:00)	Â
1 Messages +13474487274 1 Messages +14062958264 1 Messages	+19198887386 IMessages!	
<ul> <li>+14152149903</li> <li>1 Messages</li> <li>+15022952844</li> <li>1 Messages</li> <li>+18337720138</li> </ul>	Date Sent : 2023-05-09 20:00 24 (-4:00) Date Read : 2023-05-09 20:01:51 (-4:00) +19195794674 [Own	ner]
1 Messages + 18556460421 1 Messages + 19198887386 [This is DE	Yay! Do we have another number for regular texts?	
30 Messages 22000 1 Messages 22395	+19198887386	
2 Messages 288403 1 Messages 22665	Date Read : 2023-05-09 20.04.41 (-4.00) Date Read : 2023-05-09 20.04.48 (-4.00)	
1 Messages 44398 1 Messages 466	+19195794674 [Own Good. How's the DS9 binge going?	ner]
2 Messages 65082 1 Messages	Date Sent : 2023-05-09 20 07-41 (-4.00) Read State : Unknown	
	+19198887386 It's going. I'm in Season 4. I now remember why I didn't watch this originally. Date Sent : 2023-05-09 20:10:12 (-4:00) Date Read : 2023-05-09 20:10:21 (-4:00)	
	+19195794674 [Ow	ner]

- 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.



- 3 Search
- 4 Duplicate Options

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

	lcon	StartTime	EndTime	Duration	Details	Latitude
~		2023-12-09 01:49:29 (UTC)	2023-12-09 16:33:14 (UTC)	14:43:45	Local [Frequent Locations Entry]	51.1718485
<u>~</u>		2023-12-09 16:33:14 (UTC)			Local [Frequent Locations Exit]	51.1718485
$\sim$		2023-12-12 22:15:38 (UTC)	2023-12-13 21:07:38 (UTC)	22:52:0	Local [Frequent Locations Entry]	51.1718475
		2023-12-13 21:07:38 (UTC)			Local [Frequent Locations Exit]	51.1718475
~		2023-12-13 21:17:02 (UTC)	2023-12-13 21:28:02 (UTC)	0:11:0	Local [Frequent Locations Entry]	51.159498
<u>~</u>		2023-12-13 21:28:02 (UTC)			Local [Frequent Locations Exit]	51.159498
~		2023-12-22 09:21:00 (UTC)			Cache [Visits Entry]	51.1718479
~		2023-12-22 09:21:00 (UTC)			Cache [Visits Entry]	51.1718479
~	9	2023-12-24 04:36:55 (UTC)			Cache [Cache Locations]	51.1718479
~	•	2023-12-24 04:36:56 (UTC)			Cache [Cache Locations]	51.1718479
~	9	2023-12-24 04:38:21 (UTC)			Cache [Cache Locations]	51.1718479
<u>~</u>	•	2023-12-24 04:38:22 (UTC)			Cache [Cache Locations]	51.1718479
~	9	2023-12-24 04:39:33 (UTC)			Cache [Cache Locations]	51.1718479
	9	2023-12-24 04:46:46 (UTC)			Cache [Cache Locations]	51.1718479
~	<b>Q</b>	2023-12-24 04:50:42 (UTC)			Cache [Cache Locations]	51.1718479
~	9	2023-12-24 04:50:43 (UTC)			Cache [Cache Locations]	51.1718479
~	<b>Q</b>	2023-12-24 04:53:59 (UTC)			Cache [Cache Locations]	51.1718479
~	9	2023-12-24 05:01:11 (UTC)			Cache [Cache Locations]	51.1718479
<u>~</u>	9	2023-12-24 05:07:23 (UTC)			Cache [Cache Locations]	51.1718479
~	9	2023-12-24 05:07:24 (UTC)			Cache [Cache Locations]	51.1718479
~	9	2023-12-24 05:08:21 (UTC)			Cache [Cache Locations]	51.1718479
~	9	2023-12-24 05:08:22 (UTC)			Cache [Cache Locations]	51.1718479
~	9	2023-12-24 05:08:34 (UTC)			Cache [Cache Locations]	51.1718479
-	Ó	2023-12-24			Cache (Cache	

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.					
٩٩	Match Bounds will filter the viewed.	Match Bounds will filter the records in the table to match the bounds of the map being viewed.				
Sources +	Sources will open to show or off any of the sources. 153436 / 160038 Records Cache sqite (137076 / 137076) Cache sqite (137076 / 137076) Cache sqite (137076 / 137076) Cache sqite (870 / 5700) Photos sqite (870 / 5770) Cache encyrted8 sqite (7287 / 12597) WiFi Location (11635 / 11635) Cache oncyrted8 sqite (7287 / 12597) Catl Tower Location (73 / 73) Catl Tower Location (71 / 782)	the Locations records that were found and allow you to turn on 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.				
; KM_I Radius : < 25m →	<b>Radius Selection</b> 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.					
	<b>Create Flipbook</b> will create an animated view of the selected location records and is covered in more detail later on.					
CSV	Export to CSV will export to	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.

« » 🔳					🛃 <u> </u> Copy Graph
(UTC) Coordinated Universal Time	2023-05-05	2023-05-09	2023-05-13	2023-05-17	2023-05-21
Cache [Cache Locations] Cache [Visits	Local [Vehicle Events] 📃 Local [Frequent	Locations) 📕 cache_encryptedB (WiFi Location)			
<b>()</b>					

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





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.		
	Noly Steing		
(V)	Course will draw an arrow on the map to indicate the direction of travel for each marker		
	on the map (if available).		
	En Entra		
	the second se		
	and the second states		
Connect Locations	Connect Leasting will draw a line between the Wifi and Call Towar Leastions found in		
Connect Educations	the Cache. EncryptedB database and the temporally closest record from the cache solite		
	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.		
	US4 NC4		
	NC Fugua Varina		
😡 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.		
( <b>2</b> ).	Drop pins are discussed shortly.		
🛄 Сору Мар	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.

Annon Mit Lake Wyn Control of Con

**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

### Gbutton.

This will turn the Timestamp label on for all selected records. This is indicated in the Table view with a  $^{\textcircled{0}}$  icon in the second column.

	,
<ul> <li>2023-05-16</li> <li>18:51:56 (UTC)</li> </ul>	Cache [Cache 35.6161227 Locations]
<ul> <li>2023-05-16</li> <li>18:51:57 (UTC)</li> </ul>	Cache [Cache 35.6159879 Locations]
<ul> <li>2023-05-16</li> <li>18:51:58 (UTC)</li> </ul>	Cache [Cache 35.6158427 Locations]
<ul> <li>O 2023-05-16</li> <li>18:51:59 (UTC)</li> </ul>	Cache [Cache 35.6157121 Locations]
2023-05-16 18:52:00 (UTC)	Cache [Cache 35.6155757 Locations] 35.6155757

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  $\bigcirc$  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.

Custom Markers	×
	+ Name
A Home	Home
<b>v</b>	Турө
	Home ~
	Colour
	Blue ~
7	Position
	35.54940796,-78.75004578
	Save

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.
	00 (v	) Sources + 📧	🖽 Radius : ALL 👻 🦲	) 🖌 🖌 🖾	G			<u>्</u> र
	lcon	StartTime	<ul> <li>EndTime</li> </ul>	Duration	Details	Latitude	Longitude	Accuracy
<u>~</u>	9	2023-05-13 16:55:05 (UTC)			Cache [Cache Locations]	35.6482693	-78.8451424	112
	•	2023-05-13 16:55:12 (UTC)			Cache [Cache Locations]	35.6492182	-78.8461323	68
	•	2023-05-13 16:59:31 (UTC)			Cache [Cache Locations]	35.6586341	-78.8684461	4000
	•	2023-05-13 16:59:31 (UTC)			Cache [Cache Locations]	35.6589298	-78.8716241	4000
	•	2023-05-13 16:59:32 (UTC)			Cache [Cache Locations]	35.639032	-78.863648	2015
	•	2023-05-13 16:59:32 (UTC)			Cache [Cache Locations]	35.6412726	-78.8645482	2015
	<b>Q</b>	2023-05-13 16:59:38 (UTC)			Cache [Cache Locations]	35.6601458	-78.8701827	37
	<b>Q</b>	2023-05-13 16:59:41 (UTC)			Cache [Cache Locations]	35.6601458	-78.8701827	87
	<b>Q</b>	2023-05-13 16:59:41 (UTC)			Cache [Cache Locations]	35.6601458	-78.8701827	87
	<b>Q</b>	2023-05-13 16:59:44 (UTC)			Cache [Cache Locations]	35.6598486	-78.8699516	38
	0	2023-05-13 17:00:17 (UTC)			Cache [Cache Locations]	35.6586441	-78.8707282	31
	Ý	2023-05-13 17:01:02 (UTC)			Cache [Cache Locations]	35.6593745	-78.8726226	39
	Ý	2023-05-13 17:01:04 (UTC)			Cache [Cache Locations]	35.6595013	-78.8728656	40
	Ŷ	2023-05-13 17:01:04 (UTC)			Cache [Cache Locations]	35.6551267	-78.8710635	2112
	Ó	2023-05-13 17:01:05 (UTC)			Cache [Cache	35.6594887	-78.8728742	40

The press the Create Flipbook button 辽 .

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

		Build FlipBook	
Pages	37		
Title This Is's iPhone			
	Include Radius on Overview Man	Include Second (Kapplicable)	Custom Madram an Datail Man
	Include madua on overview map	Include Speed (il applicable)	Custom Markers on Detail Map

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.



<sup>2 –</sup> Play/Pause and Play Speed will auto-scroll though the pages.

5 – Manual Scroll.

- 4 Save Options (Copy to Clipboard, Save to HTML, Save as MP4)
- 9 Coordinates of the current record.10 Accuracy of the current record.

8 – Overview Maps shows a higher level view of the current record.

11 - Accuracy of the current record.

6 – Timestamp 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 <u>https://ffmpeg.org/download.html</u>.

# **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.

<sup>3 –</sup> Parser Name

#### **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.

logs	<u></u> વ 🗙	🕅 🛄 🕻 Bookmarks • 🗹 •	ñ ()• 👒	2		csy 📜	Flat View 👔 Extract Fo
Managed Preferences	\ filesystem2 \ mobile \ Media \ DO	\ filesystem2 \ mobile \ Media \ DCIM \ 100APPLE \					
🚰 mobile	Icon FileName	FileExtension	FileOffset	FileSize_Bytes	FileSize_MegaBytes	LastModified	Acc
.ssh	IMG_0001.PNG						
Applications	MG_0002.HEIC	.HEIC	22185656	1536097	1	2023-02-20	04:10:38 (U 202
Containers	IMG_0002.MOV	.MOV	22187192	2364280	2	2023-02-20	04:10:39 (U 202
Documents	□ IMG 0003.HEIC	.HEIC	22189557	1612472	1	2023-02-20	04:20:03 (U 202
Library		.MOV	221911700	2384592	2	2023-02-20	04:20:05 (U 202
Media	MG 0004.HEIC	.HEIC	22193554	1517719	1	2023-02-20	04:20:21 (U 202
AirFair		.MOV	27129655	2206817	2	2023-02-20	04:20:22 (U 202
Airlock		HEIC	22105072	1648472	- 1	2023 02 20	06:13:24 (U 20)
Books		MOV	22133072	1040472	1	2023-02-20	06:13:24 (0 202
		.INOV	27131002	120424	1	2023-02-20	10:26:49 (11 202
		JPG	22190721	130421	0	2023-02-20	10.30.40 (U 202
101APPLE	IMG_0007.HEIC	.HEIC	2/133//0	1830983	1	2023-02-20	22.59.36 (0 202
Downloads	IMG_0007.MOV	.MOV	27135613	767749	0	2023-02-20	22:59:36 (U 202
EnhancedAudioSharedKeys	MG_0008.HEIC	.HEIC	22196851	2874148	2	2023-02-20	23:11:25 (U 202
Espresso	MG_0008.MOV	.MOV	22199726	1505384	1	2023-02-20	23:11:25 (U 202
iTunes_Control	MG_0009.HEIC	.HEIC	22201231	1634122	1	2023-02-21	02:00:31 (U 202
MediaAnalysis	MG_0010.HEIC	HEIC	271363811	. 1172648	1	2023-02-21	02:16:10 (U 202
Photos	0 Folders   1032 Files						

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.



## Search Options

Type in the name of the file or folder you are interested in and press  $\overset{\circ}{\times}$ . Press  $\overset{\leftarrow}{\times}$  to clear the search. Note that using the Search feature will disable the Tree View until  $\overset{\leftarrow}{\times}$  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.

Ľ	assets.plist		.PLIST	10418807	97
SOL	Cache.selite	Comu Dath		10383851	14
	Cache.s	Jump to \filesystem2\mobile\Library\Caches\	com.apple.routi	ned\	32
SQL	Cache.s	Open New Tab at \filesystem2\mobile\Library	\Caches\com.ap	ople.routined\	15
	8	View in Hex Viewer			
Ľ	Clients.	Bookmark \filesystem2\mobile\Library\Cache	s\com.apple.ro	utined\	47
ll - N	Cloud V/2 co	lito		10300807	86

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.

🖟 Bookmark Manager	Close
X 100APPLE Vilesystem2/mobile/Media/E com.apple.routined Vilesystem2/mobile/Library/0	l

### **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.

R						
	Line Telegram	*				
	Search Selected Files					

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.

FileExtension FileOffset FileSize Bytes FileSize Compresse FileSize MegaByte LastModified Accessed Changed



Creation

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
- Jump to \filesystem2\mobile\Media\PhotoData\Thumbnails\V2\DCIM\100APPLE\IMG\_0006.JPG\
- Open New Tab at \filesystem2\mobile\Media\PhotoData\Thumbnails\V2\DCIM\100APPLE\IMG\_0006.JPG\
- 🔒 View in Hex Viewer
- Extracted Selected File(s)
- Bookmark \filesystem2\mobile\Media\PhotoData\Thumbnails\V2\DCIM\100APPLE\IMG\_0006.JPG\

**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.



6 – Data Interpreter

8 - File & Selection Information

7 - Search View

- 1 Hex View
- 2 Load As
- 3 Extended ASCII
- 4 ASCII View

5 – Save File will save the file.

#### 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.

	Du	ou moorproor
41	C5	84 9A E3 EA ED 03
Desc		Value
ASCII		A?????
UTF7		AÂãôil
UTF8		Ań <b>♦♦♦</b> ♦]
UTF32		<b>*</b> *
BINARY		01000001 01000001 01000001 0
Int8		65
Int16 (LE)		-15039
UInt16 (LE)		50497
Int16 (BE)		16837
UInt16 (BE)		16837
Int32 (LE)		-1702574783
UInt32 (LE)		2592392513
Int32 (BE)		1103463578

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	<ul> <li>UInt32 (LE)</li> </ul>			
• UTF7	<ul> <li>Int32 (BE)</li> </ul>			
• UTF8	<ul> <li>UInt32 (LE)</li> </ul>			
• UTF32	<ul> <li>Int64 (LE)</li> </ul>			
<ul> <li>BINARY</li> </ul>	<ul> <li>UInt64 (LE)</li> </ul>			
• Int8	<ul> <li>Int64 (BE)</li> </ul>			
<ul> <li>Int16 (LE)</li> </ul>	<ul> <li>UInt64 (LE)</li> </ul>			
<ul> <li>UInt16 (LE)</li> </ul>	<ul> <li>Single (LE)</li> </ul>			
<ul> <li>Int16 (BE)</li> </ul>	<ul> <li>Single (BE)</li> </ul>			
<ul> <li>UInt16 (BE)</li> </ul>	<ul> <li>Double (LE)</li> </ul>			
<ul> <li>Int32 (LE)</li> </ul>	<ul> <li>Double (BE)</li> </ul>			

- 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  $\mathbf{X}$ .

•	E	erms (2) 👻	
Ī	×	img_	
	×	IMG_	

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.mobilenote: <mark>IMG_</mark> 1951.pn
	IMG_	x1D749C	apple.MobileSMS <mark>IMG_</mark> 1353.
	IMG_	x1D754F	apple.MobileSMS <mark>IMG_</mark> 1200.ł

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

Q€	Zoom in/Out of the image
<b>t</b>	Rotate the image 90°
OCR	Run OCR on this image
	Reset Image
	Replay (Context sensitive)
	Copy image to Clipboard
	Open in External App
٥q	Save Media

3 – Media Content

4 – Info Tab

Highlights	Important information.			
EXIF	Exif Data for the item.			
Мар	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.

-	containemanagerd too 0	
(1)	A A 🗊 WordWrap	9
$\sim$	Tue Apr 11 07:44:50 2023 [71] <notice> (0x16dd/f0000) _containermanagerd_init: containermanagerd (</notice>	Mobil
$\sim$	Tue Apr 11 07:44:50 2023 [71] <notice> (0x16dd7f000) _containermanagerd_init: containermanagerd p</notice>	erfoi
	Tue Apr 11 07:44:50 2023 [71] <notice> (0x16dd7f000) -[MCMMigrationStatus _migrateFromManyMarkerF</notice>	iles!
$\mathbf{C}$	Tue Apr 11 07:44:50 2023 [71] <notice> (0x16dd7f000) -[MCMMigrationStatus isBuildUpgrade]: Did no</notice>	t fir
	Tue Apr 11 07:44:50 2023 [71] <notice> (0x16dd7f000) -[MCMClientConnection _regenerateAllSystemCo</notice>	ntair
	Tue Apr 11 07:44:50 2023 [71] <notice> (0x16dd7f000) -[MCMContainerMigrator _checkIfDeviceMayNeed</notice>	Syste
	Tue Apr 11 07:44:50 2023 [71]	
	<notice> (0x16dd7f000) -[MCMMigrationStatus setMigrationCompleteForType:]: Migration completed o</notice>	n 19I
	Tue Apr 11 07:44:50 2023 [71] <notice> (0x16dd7f000) -[MCMMigrationStatus writeCurrentBuildInfoTo</notice>	Disk]
	Tue Apr 11 07:44:52 2023 [71] <notice> (0x16de0b000) -[MCMContainerMigrator performDataMigratorMi</notice>	grati
	Tue Apr 11 07:44:52 2023 [71] <notice> (0x16de0b000) -[MCMContainerMigrator _performBundleContain</notice>	erOw
	Tue Apr 11 07:44:52 2023 [71] <notice> (0x16de0b000) -[MCMMigrationStatus setMigrationCompleteFor</notice>	Type:
	Tue Apr 11 07:44:52 2023 [71] <notice> (0x16de0b000) -[MCMCodeSigningMapping migrateAppGroupIdsFr</notice>	omDat
	Tue Apr 11 07:44:52 2023 [71] <notice> (0x16de0b000) - [MCMMigrationStatus setMigrationCompleteFor</notice>	Type:
	ration completed on 19D52 for GroupIdMigration	
	Tue Apr 11 07:44:52 2023 [71] <notice> (0x16de0b000) -[MCMCodeSigningMapping migrateCachedCodeSig</notice>	ningl
	Tue Apr 11 07:44:52 2023 [71] <notice> (0x16de0b000) -[MCMMigrationStatus setMigrationCompleteFor</notice>	Type:
	Tue Apr 11 07:44:52 2023 [71] <err> (0x16de0b000) - [MCMGroupManager _cleanupUnreferencedGroupCont</err>	aines
	Tue Apr 11 07:44:57 2023 [71] <notice> (0x16de97000) _containermanagerd_init_block_invoke: contai</notice>	nerma
	Tue Apr 11 07:44:58 2023 [71] <notice> (0x16de97000) containermanagerd init block invoke: con</notice>	
	tainermanagerd cleanup complete	
	Tue Apr 11 07:44:58 2023 [71] <err> (0x16de97000) server_get_process_containers: Invalid data con</err>	tain∈
	Tue Apr 11 07:44:58 2023 [71] <notice> (0x16de97000) server_get_process_containers: SB Type: 0, f</notice>	allir
	Tue Apr 11 07:45:45 2023 [71] <notice> (0x16e0c7000) -[MCMContainerMigrator performPerUserDataMig</notice>	ratic
	Tue Apr 11 07:45:45 2023 [71] <notice> (0x16e0c7000) -[MCMContainerMigrator performPerUserDataMig</notice>	ratic
	Tue Apr 11 07:45:45 2023 [71] <notice> (0x16e0c7000) -[MCMContain</notice>	
	erMigrator performPerUserDataMigrationForClientConnection;withError;] block_invoke; Completed Per	Usei
	Tue Apr 11 07:45:45 2023 [71] <notice> (0x16e0c7000) -[MCMMigrationStatus setMigrationCompleteFor</notice>	Type:
	Tue Apr 11 07:45:45 2023 [71] <notice> (0x16e0c7000) -[MCMContainerMigrator performPerUserDataMig</notice>	ratic
	Tue Apr 11 07:45:45 2023 [71] <notice> (0x16e0c7000) -[MCMContainerMigrator performPerUserDataMig</notice>	ratic
	nForClientConnection:withError:] block invoke: Completed User Data Protection Migration for <mcmu< th=""><td>serīc</td></mcmu<>	serīc
	Tue Apr 11 20:00:52 2023 [71] <err> (0x16de0b000) - [MCMClientConnection userManagedAssetsPathWith</err>	Conta
	Tue Apr 11 22:52:08 2023 [71] <err> (0x16de0b000) -[MCMClientConnection userManagedAssetsPathWith</err>	Conta
	Wed Apr 12 22:51:21 2023 [71] <err> (0x16dd7f000) -[MCMClientConnection userManagedAssetsPathWi</err>	
	thContainerIdentity:isRelative:createIfNecessary:existed:withError:]: 2491: Failed to create app	data
	Thu Apr 13 20:01:28 2023 [71] <err> (0x16de0b000) - [MCMClientConnection userManagedAssetsPathWith</err>	Conta
	Thu Apr 13 22:48:26 2023 [71] <err> (0x16dd7f000) -[MCMClientConnection userManagedAssetsPathWith</err>	Conta
	Fri Apr 14 22:48:41 2023 [71] <err> (0x16de0b000) -[MCMClientConnection userManagedAssetsPathWith</err>	Conta
	ainer for user managed assets path for com.apple.nonContainerUserManagedAssets: (21) CONTAINER NO	r foi
	Sat Apr 15 09:55:25 2023 [71] <err> (0x16de0b000) - [MCMClientConnection userManagedAssetsPathWith</err>	Conta
	Sat Apr 15 09:55:28 2023 [71] <err> (0x16dd7f000) -[MCMClientConnection userManagedAssetsPathWith</err>	Conta
	Sat Apr 15 09:58:52 2023 [71] <err> (0x16dd7f000) - [MCMClientConnection userManagedAssetsPathWith</err>	Conta
	Sat Apr 15 10:07:13 2023 [71] <err> (0x1</err>	
	6de97000) -[MCMClientConnection userManagedAssetsPathWithContainerIdentity:isRelative:createIfNec	essai
	Sat Apr 15 10:15:17 2023 [71] <err> (0x16dd7f000) - [MCMClientConnection userManagedAssetsPathWith</err>	Conta
	Sat any 15 13-17-20 2023 [71] (err) (0x16dd7f000) - [MCMClientConnection createOrLookunContainerWi	thCor.

1 – Tool Bar

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

<sup>2 –</sup> 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 Tabs7 - Se2 - Run Query8 - M3 - Canned Queries9 - Se4 - Table Definitions10 - F5 - Undock Database11 - S6 - WAL Comparison12 - S

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.

ACHANGE			
Description	With WAL	Without WAL	Difference
First PK	1	1	0
Last PK	8961	8944	17
		la a con	
Total	8961	8944	17
ATRANSAC	TION	8944	17
ATRANSAC Description	8961 TION With WAL	8944 Without WAL	Difference
Total ATRANSAC Description First PK	8961 TION With WAL	8944 Without WAL	Difference
Total ATRANSAC Description First PK Last PK	8961 TION With WAL 1 3300	8944 Without WAL 1 3299	Difference

#### 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.

2126C24D-CB29	Your M	lint 6 Mont	0	
6B801745-D1A7	https://	/tinyurl.co	0	
48B3F027-49FA	Haha		0	
48653E7D-DF39	advant	Find I	Like Values	
		Highl	light Like Values	
51FEB904-DC /4	082		U	



Execute SQL Canned Queries • To Mark Searching SQL SELECT \* FROM MESSAGE WHERE text LIKE 'Haha'

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.
2	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 (8961) Without WAL (8944) Combined (8961)

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.



4 - Map Custom Rows

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.

_				
IDI	ZADD	Orio	ginal Value	ANALY
	6886633	MA		06440
	6886633	MA	C (NanoSeconds)	06441
	7039843	Uni	ix	99905
	7042941	Uni	ix (Milliseconds)	57447
	7042942	Goo	ogle Chrome	57448
	7062333	Fire	Fox	51834
	7062324	40.816	0	706261834

### **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 nonconforming 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.

s 📰 📖	9	•					
ntifier		Set Latitude	•	•		identifier	d
D1EC-3E36		Set Longitu	de	•	~	latitude	
D1EC-3E36		Set Accurac	y	۲		longitude	
D1EC-3E36		Set Timesta	mp	*		radius	
D1EC-3E36	l	Map!				dwell_time	
D1EC-3E36	51.17	5297	-114.45	2671		on exit	
D1EC-3E36-	51 17	1386	-114 45	5279	-	100	

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 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.

I	🗴 gal	lery.encrypteddb															
	Ъ.	ABC															
		DataBase	2	03	04	05	06	07	08	09	0A	0в	0C	0D	0E	0F	
		Image	C	36 7B	7B	AD F0	16	7E	51 BB	90 01	B2	1B FA	BB	FD	56	86 89	¢^ 6{.~Q <sup>2</sup> .»ýV
		Text	F	A7	15	5A	DF	17	71	E3	E0	01	F6	A6	9F	C1	ð o§.Zß.qãà.ö¦ Á
	1	BPList / Protobuf	5 4	82 8E	3С 7В	F1 B7	C8 E1	17 2E	17 87	26 4E	BD 06	82 A7	1B 5C	E0 3F	AB 20	EF 79	p <ne&*₂.a≪î .gT { á. N.§\? y</ne&*₂.a≪î 
		Video	В	9E	A9	52 F2	03	9C	3C	CF F7	48 D6	27 27	A9	7E	9C	6C	kýk ©R. <ïH'©~ 1
	CEVD	SEGR	5	4C	41	E0	1B	3B	2F	CC.	30	87	0E	D2	C6	DA	+ õLAà.;/Ì0 .ÒÆÚ
	SEGD	SEGD	9	AB	A0	F3	50	FE	B2	41	48	97	B2	A0	EA	97	.<)« óPþ²AH ² ê
		00000090 F4 4C	F8	72	2A 2D	EU	49	61 5 D	6F.	04	A2	73	73	AF CO	6A 60	6/	oLøA*alaoçess jg
		000000B0 BD F1	EE	7.3 2.4	86	93	EF	36	60	89	20 9B	24	84	BD	B8	29	+mîî¤ ï6` \$ + Ý
		000000C0 0E 61	6C	FD	49	BB	03	21	DO	D1	9A	E1	1D	95	2A	9D	.alýI».!ĐÑ á. *
		000000D0 48 4F	3C	4A	47	31	AB	17	56	2E	29	40	58	80	EF	40	HO <jg1«.v.)@x th="" ï@<=""></jg1«.v.)@x>
		000000E0 DD 81	85	73	59	4B	63	8A	51	F0	6A	23	42	14	97	D8	Ý sYKc Qðj#B. Ø
		000000F0 6D 79	F0	2F	80	4D	67	02	F9	ED	F3	1E	F6	43	84	2в	myð/ Mg.ùíó.öC +

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.

Decryption Key	In order to make	pted databases, you must ente the decrypted database viewa	r the decryption key (or keychain hode) ble, changes to the schema may be required. Click here for more informatic
PageSize	IV -Offset	Page 1 Skip Bytes	Template
		Decrypt	

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.

Decryption Ke	In order to make	the decrypted database viewa	ble, changes to the schema may be required. Click here for more informa
egocipher	,		
PageSize	IV -Offset	Page 1 Skip Bytes	Template
1024	976	16	SnapChat Gallery
		Decemt	

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.

ey         V           geSize         40           servedSpace         0           skimum Payload         32           af Payload         32           o Change Cou         31           talPages         84           t Freelet page         0	Value 1096 10 14 12 12 111 142 10 11 142 10 10 10 10 10 10 10 10 10 10	HEX   DE HEX   DE 	C () C	00 01 ( 53 51 4 10 00 ( 00 00 ( 00 00 ( 00 00 ( 00 00 ( 00 00 ( 00 2E 5 0F B3 (	12         0.3         0.4           12         0.2         0.2         0.2           12         0.2         0.2         0.0           10         0.0         0.0         0.0           10         0.0         0.0         0.0           10         0.0         0.0         0.0           10         0.0         0.0         0.0           10         0.0         0.0         0.0           10         0.0         0.0         0.0           10         0.0         0.0         0.0	4 05 06 4 65 20 0 40 20 0 00 00 0 00 01 0 00 00 0 00 000 0 00000000	5 07 0 0 66 6 0 20 0 0 00 0 1 90 0 0 00 0 0 00 0 0 00 0	8 09 F 72 0 00 0 00 0 00 0 00 0 00 0 00	0A 0B 6D 61 01 37 02 47 00 01 00 00	0C 0I 74 20 00 00 00 00	0E 0F 33 00 03 4A 00 04 00 00	SQLite f	format 3. 7J G	I		
gesize         4t           servedSpace         0           ximum Payload         64           imum Payload         32           af Payload         32           ac Change Cou         31           talPages         84           st Freelist page         0	1096 34 32 32 311 32 32 34 34 34 34 34 34 34 34 34 34 34 34 34		= 0 9 6 2 0 8 0 4 0 6 0 2 0 8 0 8 0 8 0 8 0 8 0 8 0 8 0 8 0 9 8 0 9 8 0 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	53 51 4 10 00 ( 00 00 ( 00 00 ( 00 00 ( 00 00 ( 00 2E 5 0F B3 (	4C 69 74 02 02 00 00 00 00 00 00 00 00 01 00 00 00 00 5F 1D 05	4 65 20 0 40 20 0 00 00 0 00 01 0 00 00 0 00 00	0 66 6 0 20 0 0 00 0 1 90 0 0 00 0	F 72 0 00 0 00 0 00 0 00 0 00 0 00	6D 61 01 37 02 47 00 01 00 00	74 20 00 00 00 00 00 00	33 00 03 4A 00 04 00 00	======= SQLite f 0	format 3. 7J G			
servedSpace 0 ximum Payload 64 nimum Payload 32 af Payload 32 change Cou 31 talPages 84 xt Freelist page 0 tal Emplit Page 0	) 34 32 32 311 342 342 3	0000 000 0010 001 0020 003 0030 004 0040 006 0050 008 0060 009 0070 011 0080 012 0050 014	6 2 0 8 0 6 0 6 0 8 0 8 0	53 51 6 10 00 ( 00 00 ( 00 00 ( 00 00 ( 00 2E 5 0F B3 (	2 02 02 00 00 00 00 00 00 00 00 01 00 00 00 00 5F 1D 05	+ 65 20 0 40 20 0 00 00 0 00 01 0 00 00 0 00 00 0 00 00 0 00 00 0 00 00	0 66 6 0 20 0 0 00 0 1 90 0 0 00 0	P 72 0 00 0 00 0 00 0 00 0 00	01 37 02 47 00 01 00 00	74 20 00 00 00 00 00 00	03 4A 00 04 00 00	SQLITE 1				
ximum Payload 64 nimum Payload 32 af Payload 32 change Cou 31 talPages 84 st Freelist page 0	54 52 52 51 51 54 52 55 55 55 55 55 55 55 55 55 55 55 55	0020 003 0030 004 0040 006 0050 008 0060 009 0070 011 0080 012 0090 014	2 ( 8 ( 0 ( 6 ( 2 ( 8 (	00 00 ( 00 00 ( 00 00 ( 00 00 ( 00 2E 5 0F B3 (	00 00 00 00 00 00 00 01 00 00 00 00 5F 1D 0		0 00 0 L 90 0 0 00 0	0 00 0 00 0 00 0 00	02 47 00 01 00 00	00 00	00 04 00 00		G			
nimum Payload or nimum Payload 32 af Payload 32 or Change Cou 31 talPages 84 st Freelist page 0	94 92 92 91 91 942 9	0030 004 0040 006 0050 008 0060 009 0070 011 0080 012 0090 014	8 0 4 0 6 0 2 0 8 0	00 00 ( 00 00 ( 00 00 ( 00 2E 5 0F B3 (	00 00 00 00 01 00 00 00 00 5F 1D 0	0 00 01 0 00 00 0 00 00	L 90 0 0 00 0 0 00 0	0 00 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	00 01 00 00	00 00	00 00					
nimum Payload 32 af Payload 32 o Change Cou 31 talPages 84 st Freelist page 0	12 12 111 142	0040 006 0050 008 0060 009 0070 011 0080 012 0090 014	4 0 6 0 2 0 8 0	00 00 ( 00 00 ( 00 2E 5 0F B3 (	00 01 00 00 00 00 5F 1D 05	0 00 00 0 00 00 5 05 54	0 00 0	0 00 0	00 00	00.00					•	
af Payload 32 change Cou 31 talPages 84 st Freelist page 0	12 111 142	0050 008 0060 009 0070 011 0080 012 0090 014	0 0 6 0 2 0 8 0	00 00 0 00 2E 5 0F B3 0	00 00 00 5F 1D 0	00 00	0 00 0	0 00	00 00		00 00					
e Change Cou 31 talPages 84 st Freelist page 0	) ) )	0060 009 0070 011 0080 012 0090 014	6 ( 2 ( 8 (	00 2E 5 OF B3 (	5F 1D 0	5 08 84			00 00	00 00	01 37		7			
talPages 84 st Freelist page 0	)	0080 012	8 0	OF B3 (			5 00 1	F OF	4C 02	00 00	02 0E		L			
talPages 84 st Freelist page 0	)	0090 012	0 1	0	OF AE OF	F F1 OE	FECU	FE7	OF E2	OF DE	OF D8					
st Freelist page 0		00301014	A	08 94 0		P 09 01	F C4 0	F BE	OF 56	OF AU	OF SA					
tal Empliet Page 0		00.01016		01 70 0	DE 67 01	F 64 01	2 02 0 2 52 0	F 58	02 70	OF AC	00 00	n i d /	V D T.			
		00b01017	6 0	00 00 0	00 00 00	0 00 00		0 00	00 00	00 00	00 00	.p.j.a.				
tai meelist i ag v	)	00c01019	2 0	00 00 0		0 00 00	0000	0 00	00 00	00 00	00 00					
		00401020	8 (	00 00 0	00 00 00	0 00 00	0 00 0	0 00	00 00	00 00	00 00					
< Pa	age 1	00e0 022	4 (	00 00 0	00 00 00	0 00 00	0 00 0	0 00	00 00	00 00	00 00					
Page	Header	00£0 024	0 (	00 00 0	00 00 00	0 00 00	0 00 0	0 00	00 00	00 00	00 00					
ev V	Value	01001025	e 1	00 00 (	00 00 00	n nn nr	0 00 0	0 00	00 00	00.00	00.00			_		
	torio Toble		Field 0	Field												
ge i ype i m	ntenor i able	l   ▶	404	4												
stFreeblock 40	1086		406	7												
ICount 31	81		400			-										
utOfCallCantant 20	016		462	26												
artOrCellContent 33	010		456	33												
eBytes 2	2		407	13												
htMostPointer 52	526		407			-										
	010		461	48												
inter U 35	313		415	55												
inter 1 39	914		400	0		-										
inter 2 39	981		400	02		-										
			417	72												
inter 3 39	3976		410	79												
inter 4 39	971		-													
ey ge att int int int int int	Freelist Pag         F           Page         Page           Pippe         1           Treeblock         2           ColdCellContent         2           OfCellContent         2           Verse         2           er 0         2           er 1         2           er 2         2           er 3         2           er 4         2	Freelet Pag         0           Page Header         >           Value         Type           Freeblock         4085           kount         31           OfCellContent         3916           Bytes         2           Most Participant         525           rer 0         3919           er 1         3514           er 2         3981           er 3         3976           er 4         3571	Freelikt Pag         0         0005101         0005101           Vage 1         000401020         000601024         000601024           Value         Value         005010104         00501024           Value         Value         00501024         0000025           Value         Value         005010104         00501024           Value         Value         10000025         0000025           Value         Value         10000025         0000025           Value         Value         10000025         0000025           Value         20000025         0000025         0000025           Value         <	Freelik Pag     0     000010116       Page 1     000010192       000010192     000010224       000010224     000010224       000010224     000010224       000010224     000010224       000010225     01001025       Value     78800       Value     1001025       Value     1001025       Value     1001025       Value     1001025       Value     1001025       Value     405       005010111     405       <	Freelik Pag     0	Freelik Pag     0     0     0000101192     000000000000000000000000000000000000	Freelett Pag       0       000010192       000000000000000000000000000000000000	Freeder Page 1       0       00 00 10 1/8       00 00 00 00 00 00 00 00 00 00 00 00 00	Freeder Page 1       0	Freeder Page: 1       0       00000 102 16       0000 100 100 00 00 00 00 00 00 00 00 00	Freelatt Pag       0       0       00 <td>Freeder Pag 0       0       0000 02 10 2 7 6       000 00 00 00 00 00 00 00 00 00 00 00 00</td> <td>Freeder Pag.       0       <t< td=""><td>Freeder Pag.       0       <t< td=""><td>Freeder Pag       0       0       00</td><td>Freeder Fag 0       0       0000 01 1/6       000 00 00 00 00 00 00 00 00 00 00 00 00</td></t<></td></t<></td>	Freeder Pag 0       0       0000 02 10 2 7 6       000 00 00 00 00 00 00 00 00 00 00 00 00	Freeder Pag.       0 <t< td=""><td>Freeder Pag.       0       <t< td=""><td>Freeder Pag       0       0       00</td><td>Freeder Fag 0       0       0000 01 1/6       000 00 00 00 00 00 00 00 00 00 00 00 00</td></t<></td></t<>	Freeder Pag.       0 <t< td=""><td>Freeder Pag       0       0       00</td><td>Freeder Fag 0       0       0000 01 1/6       000 00 00 00 00 00 00 00 00 00 00 00 00</td></t<>	Freeder Pag       0       0       00	Freeder Fag 0       0       0000 01 1/6       000 00 00 00 00 00 00 00 00 00 00 00 00

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.

May         Value         HEX         I DEC         00 01 02 0 3 04 05 06 07 08 09 0A 0B 0C 00 DE 0F           Magic         331071618         DEC         00 00 100 00         00 00 00 06 68 00 00 03 4A 56 07 2B 05 PB PD CC 55   .	by         Value         Unit         HEX         DEC         00         01         02         03         44         05         06         07         08         05         0.0         00	Key		Flame I C	Uffset : 0x20	(32)									
Magic         931071618         0001 0000         000 0 000 000 000         000 0 000 000 000         000 0 000 000 000         000 0 000 000 000         000 0 000 000 000         000 0 000 000 000 000 000         000 0 000 000 000 000 000 000 000 000         000 000 000 000 000 000 000 000 000 00	age         91071618         00000         00000         00000         0000000         00000000         0000000         0000000         0000000         0000000         0000000         0000000         0000000         00000000         00000000         00000000         00000000         00000000         00000000         000000000         0000000000         0000000000         00000000000         00000000000         000000000000000000000000000000000000		Value	HEX   DE	.c 00	01 02 0	3 04 05	06 07	08 09	0A 0B	0C 0D	OE OF	7		
Format Version       3007000       0010       010<	matt Version       9007000       0010       0010       0010       010<	Magic	931071618	00001000	== == 00 00	00 00 6	8 00 00	03 4A	56 07	2B C5	FB FD	6C 55	=====================================		
PageSize       4096         Deckpoint Seq       1         Sat1       144310533         Sat2       47277723         C       Frame 1         Sat3       000 00 00 00 00 00 00 00 00 00 00 00 00	geSize         4096         002010032         02210022         02210022         0220002         0200002         000000         0000000         0000000         0000000         00000000         000000000         000000000000000000000000000000000000	Format Version	3007000	0010 001	.6 10	41 6C 8	C 10 4C	EB EC	0D 00	00 00	01 OE	10 00	) .AlL		
Deckport Seq         1         0030 [0048]         00 00 00 00 00 00 00 00 00 00 00 00 00	extport Se       1       0030 10043       00040 00000000000000000000000000000000	PageSize	4096	00201003	12 OE	10 OE 0	9 00 00	00 00	00 00	00 00	00 00	00 00			
Sal1       144331653         Sal2       67277739          Frame 1         >       000 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	at1       1443310533         at2       47277739          Frame 1         >       006010096       000000000000000000000000000000000000	Checkpoint Sea	1	00301004	.8 00	00 00 0	0 00 00	00 00		00 00	00 00	00 00	)		
Image: Normal state         Provide State         Pr	1.100000000000000000000000000000000000	Salt1	1443310533	0050 008	0 00	00 00 0	0 00 00	00 00	00 00	00 00	00 00	00 00			
1982       (9/10) 0112       00 00 00 00 00 00 00 00 00 00 00 00 00	2       12/27733       0070 [0122]       00 00 00 00 00 00 00 00 00 00 00 00 00	C. In C.	67077700	00601009	6 00	00 00 0	F B7 00	00 00	00 00	00 00	00 00	00 00			
Key       Value         Rey       Value         Popel luridi       104         sate:0108/terCo.       842         Sati       1443310533         Sati       1600         Checkum1       45002592         Page Total       000000000000000000000000000000000000	Prame         I         >         000000000000000000000000000000000000	Satz	-6/2///39	00701011	.2 00	00 00 0	0 00 00	00 00	00 00	00 00	00 00	00 00	)		
Key         Value           ProgetAttacking         104           start         1443310533           Salt         1443310533           Salt         1443310533           Salt         1443310533           Salt         1443310533           Checkaun1         450025852           Page 104           Key         Value           Page Type         LeafTable           Field 0         Field 1         Field 2           Value         Page Type         LeafTable           Field 0         Field 1         Field 2           Value         Page Type         LeafTable           Field 0         Field 1         Field 2           Value         Page Type         LeafTable           Field 0         Field 1         Field 2           Value         Page Type         LeafTable           Field 0         Field 1         Field 2           Value         Page Type         LeafTable           Field 0         Field 1         Field 2           Value         Page Type         LeafTable           Field 0         Field 1         Field 2           Value         Value      P	gen/unitery       Value       Oda 0       010 (0 0 0       00 0	<	Frame 1	> 00901012	4 00	00 00 0	0 00 00	00 00	00 00	00 00	00 00	00 00	)		
Page1Namber         104           sized/DBAHerCo	pge1unter       104       00b0   0175       00 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Кеу	Value	00a0 016	00 00	00 00 0	0 00 00	00 00	00 00	00 00	00 00	00 00	)		
bited/D8/terCo       842         Sali       1443310533         Sali       1443310533         Sub       67277739         Checkaum1       45002592         Page 104         Key       Value         Page 104         Key       Value         Page 104         Frestfreeblock       0         GelCourt       1         Sat0CelCentert       3600         Freeblock       0         Power 0       3500	ed/DB/Her/Co	PageNumber	104	0060 017	6 00	00 00 0	0 00 00	00 00	00 00	00 00	00 00	00 00	)		
Number of National State         Data         Dista 1 (2008)         Cold Cold Cold Cold Cold Cold Cold Cold	att       1443310533         at2       47277739         at2       47277739         ecksum1       490225892         Page 104         ey       Value         geType       LealTable         atfreebook       0         atCount       1         <	sizeofDBAfterCo	842	00c0 019	2 00	00 00 0	0 00 00	00 00	00 00	00 00	00 00	00 00	)		
Sal1     143310333       Sal2     67277739       Obecksun1     49025892       Page 104     Field 0       Key     Value       PageType     LeafTable       ParFreeblock     0       Celocurit     1       SatoCelocurit     3800       FreeBytes     0       Celocurit     3600	Mt       1443003         Mt2       67277739         Mt2       67277739         Vala       Page 104         Prope       1         Vala       1         020205624/F32       batt004/10004         Mt12       1         1       020205624/F32         1       020205624/F32         1       020205624/F32         1       1         1       020205624/F32         1       1         1       1         1       1         1       1         1       1         1	C-ht	1442210522	00e01020	4 00	00 00 0	0 00 00	00 00		00 00	00 00	00 00	)		
SM2         6727739         Image: Constraint of the second	12     47277739     1       recksun1     49022582       Pege 104       ey     Value       eg/spc     LedTable       afreebiock     0       4000000000000000000000000000000000000	Satti	1443310533	00f0 024	10 00	00 00 0	0 00 00	00 00	00 00	00 00	00 00	00 00			
Drecksun1         490026892         Field 0         Field 1         Field 2           Page 104         1         020056244FF3E         toper0041         timesta           Key         Value         Page Type         Leaf Table         toper0041         timesta           Pred Freeblock         0         CelContr         1         sandtXCelContent         3600           Parter 0         3600         Image Type         Leaf Table         Image Type         Leaf Table	Page         1         D02056244 FF3E         Epidet004           *         1         00205644 FF3E         Epidet0044           #Court         1         1         00205644 FF3E         Epidet0044           #Endes         0	Salt2	-67277739	01001025	<u>ie 00</u>	00 00 0	0 00 00	00 00	00_00	00 00	00 00	00 00	)		
Page 104         I         00026E44FF3E         Isolat00+2 1000+1           Key         Value         PageType         Les/Table         Instruction of the second of the	Page 104         I         000205E44 FF2E         location(0+1)         IIIIII+1           fey         Value         I         000205E44 FF2E         location(0+2)         IIIIII+1           ige Type         Leaf Table         I         000205E44 FF2E         location(0+2)         IIIIII+1           ifferediock         0         I         Ifferediock         0         Ifferediock	Checksum1	490826892		Field 0	Field 1	Field	12	_						
Key     Value       PageType     LeaTable       Reafreeblock     0       CelCont     1       StactCelContent     3600       FreeBytes     0       Porter 0     3600	isy         Value           igeType         LealTable           stTreeblock         0           ilCourt         1           atfOrCelContert         3600           eblyes         0           irter 10         \$500		age 104		1	02026E44-F	FF3E bplist	00\$1 IIIIIIA	a						
PageType     LeafTable       FirstFireblock     0       CollCount     1       StactXCelContent     3600       FiresBytes     0       Peinter 0     3600	ge Type         Leaf Table           st Freeblock         0           40 Court         1           actOrCelContert         3600           seb/ses         0           ref 0         3500	Key	Value												
FirstFreebook     0       CelCourt     1       StartOfCelContent     3600       FreeBytes     0       Pointer 0     3600	affeeblock         0           4Count         1           4CColContert         3500           artCCelContert         3500           rter 0         3600	PageType	LeafTable												
CalCourt 1 StaCOTCelContent 3600 FreeBytes 0 0 Pointer 0 3600	Ancodexit         0           GCOunt         1           ACCCeContert         3500           refer 0         3600	FirstFreeblock	0												
SactOcalContent 3500 FineBytes 0 Pointer 0 3600	R.cdf, 1 af(CellContext 3600 ster 0 36000 ster 0 36000 ster 0 3600 ster 0 3600 ster 0 3600 ster 0 3600	CallCaunt	1												
FreeBytes 0 0 Force 0 3600	and Carlow and a set of the set o	StatOfCallContact	2600												
Preseyve 0 3600	I Records	Stattor Celicontent	0												
Porter 0 3600	inter D 3600	rreebytes	U												
	1 Records	Pointer 0	3600												
	1 Records														
	1 Records														
1 Records															
1 - Database Information (Header)	1 Batabase mornation (neader)	1 - Data	hase Inform	1 Records	ter)										

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.

L	Page 96
Ke Pag 96 First Cell Star Free Poir	Find All Page 96

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

		F	age 9	96		
Ke					X	
Pag	96			< >		
First		Find	d All Pa	ge 96		
Cell		From		Offect		
Star		rian	ne	20490		
Free		18		73728		
Poir		36		147456		1
Poir		49		200704		
Poir		67		274432		
Poir		80		327680		
Poir		98		401408		
Poir		111		454656		
Poir		129		528384		
Poir		131		536576		
Poir		133		544768		
Poir		135		552960		
Poir		159		651264		
Poir						
Pointe	er 12		3437			

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

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

10			•••		<i>•</i> •											
	HID ALL PA	ige 36	-	11		28	17002	2	2	0	0	0	1	709065540.2439	709065539.6924	k2000]@20000020
	Frame	Offset	16			29	17002	2	2	0	0	0	1	709065661.6634	709065660.7706	10000000000000000000000000000000000000
	5	20480				30	17002	2	2	0	0	0	1	709065782.3990	709065781.9139	4441;HT4(0(4444
	18	73728		Ш		31	17002	2	2	0	0	0	1	709065903.5773	709065902.7080	%> <b>♦m.%J+♦t(♦♦</b>
	36	147456		Ш		32	17002	2	2	0	0	0	1	709066024.1803	709066023.6523	+O++10667(y++
•	49	200704				33	17002	2	2	0	0	0	1	709066145.4888	709066144.56588	**!*.aHQ#!#Q*
	67	274432		Ш		34	17002	2	2	0	0	0	1	709066266.6772	709066265.7423	**(***Cy***J
	80	327680		Ш		35	17002	2	2	0	0	0	1	709065387.1858	709066386.6743	*****!!:*/**
	98	401408		Ш		36	17002	2	2	0	0	0	1	709066508.0786	709066507.4977	+p+HO++c+1+S
	111	454656		Ш		37	17002	2	2	0	0	0	1	709066629.2956	709066628.5930	**********
	129	528384		Ш		38	17002	2	2	0	0	0	1	709066749.6549	709066749.1067	eegesJeeH?ef>l
	131	536576				39	17002	2	2	0	0	0	1	709065870.1014	709066869.5017	Y 00:IK8x0100;7
	133	544768		U		40	17002	2	2	0	0	0	1	709066990.6184	709066989.9606	:#j##@g##Aa#>
	135	552960		Ш		41	17002	2	2	0	0	0	1	709067012.1752	709067011.7737	2E+KHJU++1.0+_
	159	651264		Ш		42	17002	2	2	0	0	0	1	709067072.1832	709067071.0402	189md9C18929
	161	659456		Ш		43	17002	2	2	0	0	0	1	709067072.2360	709067072.2302	+8w+3Cx+++2++-
	164	671744		Ш		44	17002	2	0	0	0	0	1	709511018.98377	709511018.8739	Z74!4pO]454/4
	166	679936		Ш		45	17002	2	1	0	0	0	1	709511023.0702	709511020.2380	teileL:eeeqed)
	168	688128	чн	Ш		46	17002	2	1	0	0	0	1	709511023.7771	709511023.08017	**:*(K**4**2
	170	696320	Ш	Ш		47	17002	2	1	0	0	0	1	709511023.9555	709511023.7804	ie++inM++++Sf+s
	172	704512	Ш	Ш		48	17002	2	2	0	0	0	1	709511024.4791	709511023.9608	**S***Fo#I #H
	174	712704	Ш	Ш		49	17002	2	2	0	0	0	1	709511024.4872	709511024.4824	*****01*****
	177	724992	Ш	Ш		50	17002	2	2	0	0	0	1	709511028.1724	709511027.6367	***** <sub>Q</sub> ]****n
	179	733184	Ш	Ш		51	17002	2	2	0	0	0	1	709511058.5751	709511058.04439	100.01200.5020
	181	741376	1	1		52	17002	2	2	0	0	0	1	709511178.92227	709511178.4405	****kJD**(***
	183	749568	Ш	Ш		53	17002	1	2	0	0		0		709511299.0467	eheDh/#I#.G
	100	161100		101												

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

				20	11005	*	*	•		·		10000004012400		Not the sector by
	Frame	Offset	1111	29	17002	2	2	0	0	0	1	709065661.6634	709065660.7706	(**5/*@***;(**)
	5	20480		30	17002	2	2	0	0	0	1	709065782.3990	709065781.9139	4442;HT4ID(4444
	18	73728		31	17002	2	2	0	0	0	1	709065903.5773	709065902.7080	%> <b>\$m%J+63(\$\$</b>
	36	147456		32	17002	2	2	0	0	0	1	709066024.1803	709066023.6523	+O++1:0667(y++
	49	200704		33	17002	2	2	0	0	0	1	709066145.4888	709066144.56588	++I+,aHQ+I+Q+.
•	67	274432		34	17002	2	2	0	0	0	1	709066266.6772	709066265.7423	00300aCy000J
	80	327680		35	17002	2	2	0	0	0	1	709066387.1858	709066386.6743	+++u++Ns+2+
	98	401408		36	17002	2	2	0	0	0	1	709066508.0786	709066507.4977	+p+HO++c+1+S
	111	454656		37	17002	2	2	0	0	0	1	709066629.2956	709066628 5930	++++++++++++++++++++++++++++++++++++++
	129	528384		38	17002	2	2	0	0	0	1	709066749.6549	709066749.1067	00000000000000000000000000000000000000
	131	536576		39	17002	2	2	0	0	0	1	709066870.1014	709066869.5017	Y ++ :K+,+*++,7
	133	544768	111	40	17002	2	2	0	0	0	1	709055990.6184	709066989.9606	*j**@g**Aa*>
	135	552960		41	17002	2	2	0	0	0	1	709067012.1752	709067011.7737	zEeKieJijee%0e
	159	651264		42	17002	2	2	0	0	0	1	709067072.1832	709067071.0402	I++md+CI++2+
	161	659456		43	17002	2	2	0	0	0	1	709067072.2360	709067072.2302	+5+++1C++++++
	164	671744		44	17002	2	0	0	0	0	1	709511018.98377	709511018.8739	Z?#I#p0]#5#/#.
	166	679936		45	17002	2	1	0	0	0	1	709511023.0702	709511020.2380	teeeLeeeqedi
	168	688128		46	17002	2	1	0	0	0	1	709511023.7771	709511023.08017	**:*(K**4**2
	170	696320		47	17002	2	1	0	0	0	1	709511023.9555	709511023.7804	180021M-0002F
	172	704512		48	17002	2	2	0	0	0	1	709511024.4791	709511023.9608	++\$+++Fa+1]+H
	174	712704		49	17002	2	2	0	0	0	1	709511024.4872	709511024.4824	*****01*****
	177	724992		50	17002	2	2	0	0	0	1	709511028.1724	709511027.6367	*****_1****
	179	733184		51	17002	2	2	0	0	0	1	709511058.5751	709511058.04439	100.0000.000
	181	741376		52	17002	2	2	0	0	0	1	709511178.92227	709511178.4405	+++++
	183	749568		53	17002	2	2	0	0	0	1	709511299.5855	709511299.0467	.+(n+Dh)+)+.G

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.

00012D00 2F 2F 77 77 77 2E 67 6F 6F 67 67 6C 65 2E 63 6C 65 01 00012D00 72 28 70 65 71 76 57 22 87 70 6C 71 65 F2 84 24 82 65 r+power+plant+ren 0012200 26 65 65 30 55 54 46 20 38 26 67 74 6F 62 84 24 30 6C 65 61 00012220 28 74 30 73 61 66 61 72 69 23 67 73 63 CC 65 61 72 65 74 46 55 nt=safarifistate 00012220 20 77 02 C7 26 37 65 77 23 87 73 34 02 67 74 61 74 65 nt=safarifistate 00012220 02 77 02 C7 26 57 71 65 77 23 87 73 36 05 65 12 22 32 33 23 00 62 32 35 32 30 70 6F 77 65 72 23 32 35 26 51 72 28 32 35 22 35 23 23 52 30 70 62 32 35 32 30 70 6F 77 65 72 28 32 65 61 72 25 32 55 97 73 34 00 62 61 72 65 21 22 52 00000000000000000000000000000																						
000122D0 2F 73 65 61 72 28 70 67 61 72 27 70 62 70 67 77 63 72 28 70 67 71 30 62 71 72 87 66 72 72 72 87 70 67 72 72 72 73 72 63 62 65 61 72 72 87 70 67 71 72 72 72 70 71 72 72 72 70 71 71 71 71 71 71 71 71 71 71 71 71 71	00012DC0 2F	2F	77 7	77	77	2E	67	6F	6F	67	6C	65	2E	63	6F	6D	//www.google.com	Lilet1	2 (1 E)			26000
000122P0 02 2B 70 6F 77 65 72 2B 70 6C 61 6E 74 2B 62 85 44 000122P0 02 65 65 3D 55 54 64 2D 38 26 6F 75 3D 55 54 46 00012220 02 65 66 3D 55 54 64 2D 38 26 6F 65 3D 55 54 46 00012220 02 74 3D 73 61 66 61 72 69 23 67 73 32 65 61 72 25 00012220 02 74 3D 73 61 66 61 72 69 23 69 73 74 61 74 65 nt=safarifitatat 00012220 02 74 3D 73 61 66 61 72 69 23 69 73 74 61 74 65 nt=safarifitatat 00012220 02 74 3D 73 61 66 61 72 69 23 69 73 74 61 74 65 nt=safarifitatat 00012220 02 74 70 2C 72 63 77 33 72 65 74 73 26 55 12 72 53 00012220 07 70 2C 72 63 77 35 72 23 32 23 52 30 70 62 00012220 07 70 2C 72 65 77 65 72 23 32 23 52 30 70 62 00012220 07 70 2C 72 65 77 65 72 23 32 23 52 30 70 62 00012270 07 82 72 65 77 65 72 23 32 23 52 30 70 62 00012220 07 8 74 62 66 61 72 25 32 23 52 32 35 23 00 0012220 07 8 74 62 66 61 72 25 32 23 52 32 35 23 00 0012220 07 8 74 62 67 74 65 62 61 72 25 32 23 52 32 35 23 00 0012220 07 8 74 62 62 67 74 67 65 72 23 32 23 52 30 00 0012220 07 8 60 61 69 62 67 74 67 65 72 73 58 77 73 0012220 07 8 30 75 67 67 72 67 22 73 58 77 73 0012220 07 8 30 25 32 33 23 0 72 65 67 67 67 72 67 22 73 58 77 73 0012220 07 8 30 25 32 33 23 0 43 36 22 72 73 58 77 73 0012220 07 8 30 25 32 33 23 0 43 36 22 72 73 58 77 73 0012220 07 8 30 25 32 33 0 43 36 22 72 73 58 77 73 0012220 07 8 30 25 32 33 0 43 36 22 72 75 78 77 69 0012220 07 8 30 25 32 33 0 43 36 27 72 65 67 67 67 67 67 67 67 67 74 66 62 74 48 75 74 67 67 67 67 76 77 72 72 78 78 71 74 72 87 71 72 77 72 87 71 72 87	00012DD0 2F	73	65 6	51	72	63	68	3F	71	ЗD	6E	75	63	6C	65	61	/search?q=nuclea	Unit	D(LE)			20999
000122P0 61 72 28 77 69 76 60 69 62 67 74 67 62 28 42 43       ar **silmingtom*NC       001116 (BE)       30660         000122P1 02 38 26 66 65 35 35 55 44 62 38 26 67 65 35 55 44 64       as 26 56 53 35 55 44 62 38 32 66 76 53 35 55 44 64       Masser 10011221 02 38 26 68 65 38 35 65 44 60       Masser 10011221 02 38 26 68 65 38 55 54 46 29 38 67 37 46 17 4 65 65       Masser 10011221 02 18 22 67 43 27 36 16 66 17 26 77 4 26 77 43 26 78 32 65 77 43 86 75 74 38 67 57 77 70 22 72 63 58 71 38 62 75 63 60 65 61 72 25 32 30 70 66 75 61 72 25 32 32 32 32 30 70 66 65 66 17 22 52 32 32 32 30 70 66 66 66 77 4 25 32 23 52 32 30 70 66 67 77 10 32 67 27 55 76 77 70 0012280 77 65 66 66 67 74 67 66 22 53 22 35 22 30 70 66 77 65 77 13 8, 62 77 55 77 71 38, 62 77 55 77 71 38, 62 77 55 77 71 38, 62 77 55 77 71 38, 62 77 55 77 71 38, 62 77 55 77 71 38, 62 77 55 77 71 38, 62 77 55 77 71 38, 62 72 75 58 77 71 77 72 51 72 52 32 35 22 30 70 66 77 65 72 100112280 75 63 66 56 61 72 25 32 35 22 30 70 67 67 65 77 57 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 38, 62 77 75 75 71 77 77 25 72 75 78 57 65 72 10012280 75 63 66 56 17 72 25 32 35 22 30 70 67 67 67 67 67 76 75 72 10012280 75 63 67 67 67 67 67 67 67 65 78 57 69 77 68 67 60 0012280 75 63 67 74 67 62 22 73 78 57 67 77 77 77 77 77 77 77 77 77 77 77 77	00012DE0 72	2B	70 🤅	δF	77	65	72	2в	70	6C	61	6E	74	2B	6E	65	r+power+plant+ne	Int16	(BE)			30569
00012220 02 6 69 65 30 55 54 46 20 38 2 6 67 65 30 55 54 46 20 38 2 6 67 65 30 55 44 6 20 38 2 6 68 67 30 55 55 44 62 20 38 2 6 68 67 30 56 56 20 20 57 57 3 2 6 5 6 77 20 57 2 6 3 6 5 6 2 9 73 74 61 74 65 70 20 12 20 60 27 47 20 55 77 3 3 4 51 74 61 74 65 71 24 58 74 30 50 55 74 38 47 20 55 77 4 30 75 57 20 27 2 6 7 2 6 5 7 74 30 73 51 2 25 32 35 32 30 70 67 77 65 72 25 32 55 32 35 32 30 70 67 77 65 72 25 32 55 32 35 32 30 70 67 77 65 72 25 32 55 32 35 32 30 70 67 77 65 72 25 32 55 32 35 32 30 70 67 77 65 72 25 32 55 32 35 32 30 70 67 77 65 72 25 32 55 32 35 32 30 70 67 77 65 72 25 32 55 32 35 32 30 70 67 77 65 72 25 32 55 32 35 32 30 70 67 77 65 72 25 32 55 32 35 32 30 70 67 77 65 72 25 32 55 32 35 32 30 70 67 77 65 72 25 32 55 32 35 32 30 70 67 77 65 72 25 32 55 32 35 32 30 70 67 77 65 72 25 32 55 32 35 32 30 70 67 77 65 72 25 32 55 32 30 70 67 71 3 77 25 72 73 26 72 65 61 72 25 32 35 32 30 70 67 71 3 77 65 72 25 32 35 32 30 70 67 71 3 77 65 72 25 32 35 32 30 70 67 71 5 72 25 32 35 32 30 70 67 71 5 75 72 25 32 35 32 30 70 67 71 5 75 71 3 77 75 72 27 73 77 75 72 27 72 25 32 35 32 30 70 67 77 65 72 25 32 32 30 70 67 77 65 72 25 32 32 30 70 67 77 65 72 25 32 32 30 70 67 77 65 72 25 32 32 30 70 67 77 65 72 25 32 32 30 70 67 77 65 72 25 32 32 30 70 67 77 65 72 25 32 32 30 70 67 77 65 72 25 32 32 30 70 67 77 65 72 25 32 32 30 70 67 77 65 72 65 78 57 69 71 3 70 72 25 70 012220 07 56 17 22 58 30 53 34 30 70 47 77 77 72 27 77 77 72 72 77 77 77 77 77	00012DF0 61	72	2в	77	69	6C	6D	69	6E	67	74	6F	6E	2в	4E	43	ar+wilmington+NC	UInt1	6 (BE)			30569
000122210 20 80 26 60 6C 30 65 62 20 75 73 26 63 6C 96 65       -9sh1#enruskc1tel       100022         00012220 67 43 D7 36 16 66 17 26 27 46 74 72 65 78 30 60 57       -9sh1#enruskc1tel       101320(E)       1033621         00012220 67 70 70 2C 72 63 5F 71 3A 62 75 63 6C 56 17 22 53 20 70 6C 52       05 74 3A 67 76       07 77 70 2C 72 63 5F 71 3A 62 75 63 6C 56 17 22 53 20 70 6C 52       101224(BC)       2003397         0012220 67 76 50 27 23 23 23 32 30 76 67 76 57 77 70 2C 72 53 5F 77 3A 62 77 75 5F 77 71 75 5F 77 71 75 72       uclear%2520near%252       10164 (LE)       83387794         0012280 75 63 6C 56 17 22 53 23 53 23 07 0 6C 76 77 65 77 13 A 62 77 75 5F 77 71 5F 67 77 80 cr 12 57 23 23 53 23 07 0 cc 16 67 74 67 72 53 22 53 22 30 70 cc 16 77 45 77 13 A 62 77 75 57 71 3A 62 77 75 57 71 3A 62 77 75 57 71 3A 62 77 75 72       uclear%2520near%252       Int64 (LE)       83387794         0012280 75 63 6C 56 17 22 53 23 53 23 07 0 cc 76 76 57 75 75 75 70 10 2002280 75 63 6C 56 17 22 53 23 30 70 cc 76 16 77 85 78 57 69 77 4       uclear%2520near%252       Int64 (BE)       B6004527         0012280 75 63 6C 56 17 22 53 23 30 70 cc 76 16 67 67 67 67 67 67 67 67 67 76 00 012280 00 00 00 cc 81 68 19 00 14 00 00 00 00 00 00 00 81 68 19 01 14 00 00 00 00 00 81 68 19 50 10 14 00 00 00 00 00 26 81 69 58 00 00 01 14 00 00 00 00 00 00 00 81 68 19 50 17 22 87 77 76 56 C 60 77 4 67 77 65 72 72 76 77 65 72 72 76 77 65 72 72 76 26 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 76 56 77 77 77 77 77 77 77 77 77 77 77 77 77	00012E00 26	69	65 3	3D	55	54	46	2D	38	26	6F	65	3D	55	54	46	&ie=UTF-8&oe=UTF	10122				1025021
0012220 06 7 3 60 7 3 60 60 7 4 60 7 2 60 7 2 60 2 7 3 60 7 9 60 7 9 60 7 9 60 7 9 60 7 9 60 7 7 60 7 2 60 7 7 60 7 2 60 7 7 60 7 2 60 7 7 6 7 2 60 7 7 8 60 7 7 6 60 7 7 6 60 7 7 6 7 2 8 2 3 2 3 2 3 2 3 7 6 8 6 7 7 8 6 7 7 8 7 1 3 8 6 2 7 2 7 5 5 7 7 7 8 7 1 3 8 6 2 7 2 7 5 5 7 7 1 3 8 6 2 7 2 7 5 5 7 7 1 3 8 6 2 7 2 7 5 5 7 7 1 3 8 6 2 7 2 7 5 5 7 7 1 3 8 6 2 7 2 7 5 5 7 7 1 3 8 6 2 7 2 7 5 5 7 7 1 3 8 6 2 7 2 7 5 5 7 7 1 3 8 6 2 7 2 7 5 5 7 7 1 3 8 6 2 7 2 7 5 3 2 3 3 2 3 0 7 6 5 7 7 8 7 1 3 8 6 2 7 2 7 5 5 7 7 1 3 8 6 2 7 2 7 5 5 7 7 1 3 8 6 2 7 2 7 5 5 7 7 1 3 8 6 2 7 2 7 5 5 7 7 1 3 8 6 2 7 2 7 5 5 7 7 1 3 8 6 2 7 2 7 5 7 5 7 1 3 8 6 2 7 2 7 5 7 5 7 1 3 8 6 2 7 2 7 5 7 5 7 1 3 8 6 2 7 2 7 5 7 5 7 1 3 8 6 2 7 2 7 5 7 5 7 1 3 8 6 2 7 2 7 5 7 5 7 1 3 8 6 2 7 2 7 5 7 1 3 8 6 2 7 2 7 5 7 7 1 7 7 7 2 2 5 2 3 2 3 2 3 2 3 0 7 6 6 7 6 6 7 6 7 7 6 6 7 6 7 7 6 6 7 7 4 6 6 2 5 2 3 2 3 7 2 3 2 3 7 2 6 7 7 6 5 7 7 7 7 7 7 2 2 7 2 5 7 8 5 6 7 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 7 2 2 3 2 3 2 3 2 3 2 3 0 7 6 6 7 6 7 6 7 6 7 5 7 5 7 2 7 2 2 3 2 3 2 3 2 3 0 7 6 6 7 6 7 6 7 6 7 5 7 5 7 2 7 2 5 7 8 5 6 9 1 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 6 1 6 1	00012E10 2D	38	26 6	58	6C	3D	65	6E	2D	75	73	26	63	6C	69	65	-8&hl=en-us&clie	intoz	(LL)			1033021
00012240 d6 C7 32 01 26 05 5c 71 23 03 12 00 27 03 03 70       111111111111111111111111111111111111	00012220 82	60	3D 1 72 4	13	27	60	60	74	26	23	72	65	70	20	60	55	-lalani#istate	UInt3	2 (LE)			1835821
00012250 77 70 20 20 72 63 5F 71 3A €2 75 63 6C 56 61 72 25       "pr. c_grnnclarf       Ulti32 (LE)       2003397         000122F0 61 6F 74 25 32 35 23 07 66 76 61 72 25 32 35 32 07 66       Signey strategy       antb2520neart2520       Ulti32 (LE)       8337794         000122F0 61 6F 74 25 32 35 23 07 66 66       Signey strategy       antb2520neart2520       Ulti32 (LE)       8337794         000122F0 76 65 66 77 67 67 67 67 75 77 75 77 77 75 77 77 75 77 77 77 77	00012E30 5D	67	3A 3	31	2C	6D	5F	72	3A	31	2C	6D	5F	74	3A	67	dg:1.m r:1.m t:g	Int32	(BE)			2003397
000122E0 03 28 32 32 30 70 6F 77 65 72 25 32 35 22 30 70 6C <sup>2</sup> 230powe+2522001 <sup>1005</sup> (LC) <sup>1005</sup> (LC)          000122E0 01 77 65 72 05 33 52 30 6E <sup>6</sup> 5 74 65 72 55 75 75 77 75 75 75 77 76 <sup>1005</sup> (LC)	00012E50 77	70	2C 1	72	63	5F	71	3A	6E	75	63	6C	65	61	72	25	wp,rc q:nuclear%	Ullnt3	2 (I E)			2003307
00012220 061 6E 74 25 32 35 23 30 6E 65 61 72 25 32 35 22 0       ant+52520meart2525       UH164 (LE)       8337794         00012280 07 65 65 60 77 65 75 63 3A 32 2c 72 75 5F 67 77       NC,rc_ui:2,ru_gri       UH164 (LE)       8804527         00012280 75 63 6c 75 63 1A 32 2c 72 75 5F 77 1A 36 6F       P:0425260,ru_gri       IH164 (LE)       8804527         00012280 75 63 6c 75 61 72 25 32 35 23 30 70 6F 77 65 72       ucleart2520power       UH164 (LE)       8804527         00012280 75 63 6c 75 61 72 25 32 35 23 30 70 6F 77 65 72       ucleart2520power       UH164 (LE)       8804527         00012280 76 62 51 72 25 32 35 23 30 70 6F 67 65 78 5F 65 0n 001       mc0art2520power       Un164 (LE)       8804527         00012280 6F 61 72 25 32 35 23 00 81 68 19 01 14 00 00 nt 2520 (NFA)       noh2520NC+trext       Single (E)       4.57287         00012280 0F 67 67 65 62 25 23 65 25 23 65 61 72 28 70 77 77 72 65 72       rgmucleartpower	00012E60 32	35	32 3	30	70	6F	77	65	72	25	32	35	32	30	70	6C	2520power%2520p1	Unito	2 (LL)			2003337
00012280 30 77 69 Cc 0D 69 Cc 17 4 6F 6E 25 22 35 23 30 Willington*2520       0001250 46 20 72 65 5F 75 67 75 5F 77 75 77 NC, rc ui:2ru174 MiR4 (E)       MIR4 (E)       8387794         00012280 47 3 A3 02 53 22 35 32 43 36 2c 72 75 5F 77 15 A CE       p:04523c6, ru, qin       MIR4 (E)       8604527         00012280 47 5 65 Cc 56 17 22 53 23 53 23 07 0 Cc 16 EC 74 45 32 53 23 37 02 65 EC 74 47 12 55 78 5F 77 55 77 15 77 15 77 15 77 15 77 15 77 15 77 15 75 65 10 50 56 EC 74 45 25 20 11 11525200, rtrsx i       MIR4 (E)       8604527         00012280 6F 6E 25 32 35 23 07 0 Cc 16 EC 74 47 25 78 5F 75 67 10 11 40 00       mclartx25201 mtx25200, rtrsx i       Single (E)       4.724339         00012280 6F 6E 25 32 35 10 7 0 Cc 16 ES 19 01 14 00 00       mclartx2520 mcr, rtrsx i       mclartx2520 mcr, rtrsx i       Single (E)       4.73439         00012280 6F 6F 75 C6 55 2E 63 7F 8F 67 77 77 77 77 77 77 77 77 77 77 77 77	00012E70 61	6E	74 2	25	32	35	32	30	6E	65	61	72	25	32	35	32	ant%2520near%252	Int64	(LE)			8387794
00012280 0/28 0/3 2 (2 7 2 6 3 5F 75 69 3A 32 2 (7 2 7 5 5F 67 77 7)       NC r ⊂ ui:2 ru_grt       Int64 (BE)       Int64 (BE)       8604527         00012280 0/5 63 (C 5 61 72 25 32 35 24 30 70 (C 6 7 76 5 72 u)       uclear%2520power       Uclear%2520power       Int64 (BE)       8604527         00012280 0/5 63 (C 7 2 53 23 52 32 30 70 (C 6 1 6 67 76 57 2       uclear%2520power       Uclear%2520power       Int64 (BE)       8604527         00012280 0/5 61 72 25 32 35 23 30 2 30 70 (C 6 1 6 6 9 6E 67 74       ear%2520ullmingt       Single (LE)       4.57287         00012280 0/5 61 72 25 32 35 23 30 42 77 75 6 C 6 0 59 6E 67 74       ear%2520willmingt       int64 (BE)       Int64 (BE)       Single (LE)       4.57287         00012280 0/5 61 72 25 32 30 10 95 05 00 00 31 68 19 0 114 00 00       onx825 200xillmingt       int0x200xereat       Int64 (BE)       Int64 (BE)       Doubte (I E)       E.28032         00012280 0/5 F 67 67 65 22 83 2 6 6 17 22 28 70 17 77 72 8 67       Orde 7 76 5 72       Gogle - cont/search       Interplatermed	00012E80 30	77	69 6	SC	6D	69	6E	67	74	6F	6E	25	32	35	32	30	Owilmington%2520	UInt6	4 (LE)			8387794
00012220 07 8A 30 25 32 35 32 43 36 2c 72 75 5F 71 5A 6E 00012220 05 32 35 32 30 70 6c 6i 6E 74 25 32 35 32 07 6F 77 65 72 00012220 05 6i 72 c5 32 35 32 30 70 6c 6i 6E 74 25 32 53 32 07 66 cc 76 56 70 cc 75 00012220 05 6i 72 c5 32 35 52 30 72 6c 6i 6E 74 74 72 65 76 5F 76 00012220 06 76 62 25 22 35 52 30 4E 43 2c 74 72 65 76 5F 67 00012220 06 00 00 00 0c 8i 19 55 80 cc 00 8i 6E 19 01 14 00 00 00012220 06 F 6F 6C 65 2E 6i 72 2B 73 65 6i 72 2B 77 65 77 65 77 65 77 65 72 00012220 06 10 2c 6i 74 77 70 73 2c 77 77 72 2c 78 5F 69 00012220 06 10 2c 6i 74 77 70 73 2c 78 5F 69 00012220 07 F 6F 67 6c 65 2E 6i 72 2B 70 11 42 00 00 0012220 06 F 6F 76 65 72 6i 72 2B 70 65 6i 72 2B 77 65 6c 62 00012220 07 F 6F 67 76 57 66 6c 65 17 22 B 70 65 6c 77 4 00012220 08 10 2c 6i 74 6F 62 2B 4E 43 26 66 5i 172 2B 77 65 6c 62 00012220 02 26 6F 76 67 74 6F 62 62 82 66 6i 172 2B 77 65 6c 62 00012270 02 80 30 6c 6i 6E 74 2B 6c 65 6i 72 2B 77 65 76 6c 61 00012270 22 6i 77 6F 76 6f 76 6 77 65 77 65 77 65 72 - store st	00012E90 4E	43	2C 7	72	63	5F	75	69	ЗA	32	2C	72	75	5F	67	77	NC,rc_ui:2,ru_gw	Int64	(RE)			8604527
0012E20 75 63 6C 75 61 72 25 32 35 32 30 70 6C 71 62 74 25 32 35 32 30 70 62 77 65 72 4252021mintpt  0012E20 65 61 72 25 32 35 22 30 70 6C 61 65 74 55 32 30 6C 45 74 55 32 30 6C 45 74 55 72 54 56 77 4  0012E20 67 62 52 32 35 23 30 71 65 6C 60 56 6E 77 4  0012E20 64 3A 51 65 5A 56 7A 65 67 67 67 67 67 65 75 57 65 76  0012E20 64 3A 51 65 5A 56 7A 65 67 67 67 67 67 65 65 00 01  0012E20 00 00 00 00 81 68 19 01 14 00 00  0012E20 37 71 30 EE 75 63 EC 74 25 72 57 67 65 72  0012E20 65 E7 77 65 72 25 32 55 54 46 17 22 28 70 67 77 65 72  10012E20 65 E7 67 65 77 65 65 61 72 28 70 65 77 65 72  10012E20 65 E7 67 65 53 55 54 46 23 38 26 66 23 86 51  10012E250 69 EE 77 76 77 73 22 67 66 66 10  10012E20 69 28 26 77 74 67 67 28 55 85 44 62 13 32 66 66 23 86 51  10012E250 20 32 62 67 74 67 65 28 55 54 46 23 30 36 66 62 30 65  0012E270 62 20 77 73 26 63 65 65 67 74 30 73 61 66 61  10012E250 26 77 76 76 76 76 66 20 80 26 10 21  10012E270 26 77 76 76 76 76 66 20 80 23 10 51  10012E270 26 77 76 76 76 76 72 810  10012E20 20 32 62 67 67 67 65 65 67 74 30 73 61 66 61  10012E250 26 77 77 77 72 22 67 67 67 67 66 61  10012E250 24 77 73 26 63 65 95 81 90 11 40 00 00 40 00 28  10012E20 12 64 77 47 07 33 A2 22 87 77 77 77 72 22 67 66 76 76 67 67 67  10012E20 12 64 77 74 70 77 33 22 67 67 66 66 70  10012E20 12 64 74 77 77 72 77 77 72 72 67 67 67 67 67  10012E20 12 64 74 74 70 73 73 24 27 77 77 77 72 25 77  10014  10012E20 14 74 70 73 73 24 72 77 77 77 72 25 77  10014  10012E20 14 74 70 77 73 24 27 77 77 77 72 25 77  10014  10012E20 14 74 70 77 73 25 77  1000 14 10 10 10 10 10 10 10 10 10 10 10 10 10	00012EA0 70	3A	30 2	25	32	35	32	43	36	2C	72	75	5F	71	3A	6E	p:0%252C6,ru_q:n	11104	(02)			0004527
0012220 02 12 20 3 2 3 3 2 30 70 6 6 1 72 5 3 2 3 3 3 2 3 3 2 3 3 2 3 3 2 3 3 2 3 3 3 2 3 3 2 3 3 2 3	00012EB0 75	63	6C 6	55	61	72	25	32	35	32	30	70	6F	77	65	72	uclear%2520power	UInt6	4 (LE)			8604527
00012220 (6 f c 25 22 32 5 3 23 4 7 / 6 5 (6 c 6 5 6 5 7 7 6 5 f c 6 (5 7 8 5 f 6 5 (6 1 4 00 00 1 2 2 0 0 1 2 2 0 0 0 1 0 0 0 0 0	00012200 25	32	30 3	52	30	25	60	61	6E	/4	25	32	30	32	30	6E	\$2520plant\$2520n	Single	) (LE)			4.572872
000122F0 (64 38 51 66 58, 56 78 65 67 67 67 67 67 67 67 67 60 00 000122F0 (00 00 00 00 61 68 19 05 80 00 81 66 19 01 14 00 00 000122F0 (00 01 00 00 00 62 67 74 67 67 28 77 77 77 77 77 77 77 77 77 75 67 72 000122F0 (25 77 76 77 76 56 65 17 22 37 76 77 65 72 00012F0 (25 77 76 77 76 75 65 66 77 16 77 76 56 72 00012F0 (25 77 76 77 76 75 72 72 77 77 75 75 72 00012F0 (25 77 76 77 76 75 72 72 77 77 75 75 72 00012F0 (25 77 76 77 76 75 72 72 76 76 75 72 00012F0 (25 77 76 77 77 77 77 77 77 77 75 67 72 76 86 76 76 86 76 77 68 10 100 100 100 100 100 100 100 100 100	00012ED0 65	62	25 1	20	32	30	32	45	43	20	74	72	65	79	517	69	on%2520Wilmingt	Single				4 724201
00012220000000000000000000000000000000	00012EE0 64	3A	51 6	58	5A	56	7A	65	67	65	6F	67	6C	65	00	00	d:OhZVzegoogle	Single	, (DC)			4.73433
00012220 08 01 02 68 74 74 70 73 3A 22 27 77 77 27 26 77 00012220 05 F6 F6 76 C6 55 22 63 65 F0 27 33 65 17 26 36 00 00012290 37 71 3D 62 75 63 6C 65 61 72 28 70 67 77 65 72 72mucleartyDower 000122F0 65 76 67 74 67 72 88 70 67 77 65 72 72mucleartyDower 000122F0 65 76 77 74 67 72 88 72 63 75 55 44 6 ington+NC6ie=UTP 000122F0 20 38 26 67 65 31 55 54 46 20 38 26 66 23 86 51 000122F0 62 20 77 73 26 63 6C 56 67 74 3D 73 61 66 61 n=us6client=saft 000122F0 25 67 77 67 67 67 66 20 64 00 00 06 40 00 68 00122F0 02 56 77 77 77 72 26 76 76 67 67 66 67 70 71 72 67 67 67 67 75 00122F0 02 10 53 00 81 55 10 11 40 00 08 01 02 68 2() 00122F0 07 47 70 73 3.2 77 77 77 77 72 26 76 67 67 67 67 67 67 67 67 75 00122F0 07 47 47 07 33 0.2 77 77 77 72 26 76 67 67 67 67 67 67 67 67 67 67 67 67	00012F00 00	00	00 0	28	81	09	5B	0C	00	81	6в	19	01	14	00	00		طبيمها				E 260275
00012220 (2F CF G7 CC 65 2E 63 GF CD 2F 73 G5 G1 72 63 G6         00012 - 000/search         Tem         Offset         Before And After           00012240 (2E 70 G5 G6 C7 G5 G6 C6 G5 17 22 B7 05 F6 C7 G5 77 G5 72 G7 G7	00012F10 08	01	02 6	68	74	74	70	73	3A	2F	2F	77	77	77	2E	67	https://www.q		+	Terms (1) 👻		
000122#03         27         13         6E         7         6E         12         28         70         6E         17         28         70         FC         70         70         FC         70         70         70         70         70         70         70         70         70         70         <	00012F20 6F	6F	67 6	SC	65	2E	63	6F	6D	2F	73	65	61	72	63	68	oogle.com/search	-	-			_
000122#0 28 70 6c 61 6E 74 28 6E 65 61 72 28 77 69 6C 6D         +plant+meat+wilm         > wimgdm         x12D5         wimidudidational wingle         wimidudidational wingle         wimidudidational wingle         x2D5         wimidudidational wingle         x2D6	00012F30 3F	71	3D 6	SΕ	75	63	6C	65	61	72	2в	70	6F	77	65	72	?q=nuclear+power	-	lem	Offset	Before And Atter	10.0
000122#50.69 6E 67 74 67 74 67 6E 2B 4E 43 26 69 65 3D 55 54 46 ington+NC6is=UTF wimigdon 412E31 t1:2520mer/125X immergan2:2520 000122#20 6E 2D 75 73 26 63 6C 69 65 6E 74 3D 73 6E 66 12 n=us6client=safa wimigdon 412E31 t1:2520mer/125X immergan2:2520 000122#20 72 69 67 6F 67 6C 65 02 64 00 00 00 64 00 C8 t1 rigogla.d.d. wimigdon 412E36 transmissioner/NC6 wereplantmass/immergan2:2520 000122#30 72 69 77 6F 67 6C 65 02 64 00 00 00 64 00 C8 t1 rigogla.d.d. wimigdon 412E36 transmissioner/NC6 wereplantmass/immergan2:2520 000122#30 71 74 70 70 33 A2 F2 F7 77 77 72 E2 67 6F 6F 67 6C 65 00 68 10 14 00 00 80 10 26 8	00012F40 2B	70	6C (	51	6E	74	2в	6E	65	61	72	2B	77	69	6C	6D	+plant+near+wilm	•	wilmington	x12DF3	wei +plant+neal + wiiningtot+n	
000122F0 (2D 38 26 FF 65 3D 55 54 46 2D 38 26 68 6C 3D 65         -86.0=UTF=06.h1=e         wimington         v12E08         tv2520near/v2520           00012F0 (2E 20 75 73 26 66 2C 65 05 6E 74 3D 73 61 66 61 n=usscellameT=safa         wimington         v12E08         tv2520near/v2520           00012F0 (72 65 67 FF 6F 67 6C 65 02 64 00 00 00 64 00 02         rigocgle.dd         wimington         v12E08         tv2520near/v2520           00012F0 (72 65 67 FF 6F 67 6C 65 02 64 00 00 00 64 00 02         rigocgle.dd         wimington         v12F0           00012F0 (72 65 67 74 76 77 77 77 2E 67 6F 6F 67 67 C         ctoss//www.goodl         wimington         v13ED6         wer-plant-mack-wimington-VC&	00012F50 69	6E	67 7	74	6F	6E	2B	4E	43	26	69	65	ЗD	55	54	46	ington+NC&ie=UTF		wilmington	x12E81	t%2520near%252(wilmington	%2520
0001228/062 2D /3 /3 26 53 65 65 65 74 3D /3 61 66 61 n=us6clent=sata 0001228/072 65 67 67 67 67 67 62 64 00 00 06 40 00 69 rigoogle.d.d. 0001228/081 01 53 0C 00 81 5B 19 01 14 00 00 68 01 02 682	00012F60 2D	38	26 6	SF	65	3D	55	54	46	2D	38	26	68	6C	3D	65	-8&ce=UTF-8&h1=e			-12509	t%2520near%2520wilmingtor	42520
00012250/2 50 51 55 0 C0 61 55 15 0 10 40 00 00 81 02 63 00 10 40 00 00 10 25 00 12 50 10 14 00 00 80 10 2 63 00 12 50 10 14 00 00 81 02 10 14 00 00 81 02 10 14 00 00 10 14 00 14 00	00012570 65	20	15 1	/3 	26	63	60	69	65	65	/4	30	/3	61	66	61	n-us&client=safa		winnington	XIZEDO		Ces 11
00012F20 74 74 70 73 3A 2F 2F 77 77 77 2E 67 6F 6F 67 60 tttps://www.googl whington x13ED6 wer-plant-near-willowgod-NC&i	00012F90 81	01	5 A (	DC.	00	81	5B	19	01	14	00	00	00	01	02	68	z í b		wilmington	×12F4C	wei +piant+neal+Wimington+h	
	00012FA0 74	74	70 7	73	3A	2F	2F	77	77	77	2E	67	6F	6F	67	6C	ttps://www.googl		wilmington	×13ED6	wer+plant+near+ <mark>wilmington</mark> +N	IC8i

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.

SQL Explorer WA	L Explorer																						
B	le Header	Frame 19	Offset : 0x	121D	0 (74	192)																	
Key	Value	HEX   DE	ia (	0 01	02	03	04 0	5 06	07	08	09	<b>A</b> 0	08 0	c 0.	D OE	OF							
Magic	931071618	00001000	-	0.00	0.0	02	0.0	0.00	0.0	64	BD.		ND C			05	==		4				
Format Version	3007000	00101001	6 8	EF ES	75	DB	CF D	1 CF	D2	OD	04	4E	00 0	2 0	3 E2	00	- 13	u	N				
PanaSire	4095	00201003	2 0	3 E2	0F	D2 (	F A	5 OE	BE	0E	2C	0D .	A8 01	D 1	C 0B	C3							
	0	00301004	8 0	B 63	08	38	9 3	D 08	F7	03	E2	00	00 0	0 0	0 00	00	. c	.8					
Uneckpoint Seq		00401006	10 0		00	00 0	0 0		00	00	00	00	00 0	00	0 00	00							
Salt1	1690164653	00601009	6 0	0 00	00	00 0	00 0	0 00	00	00	00	00	00 0	ŏŏ	0 00	00							
Salt2	-876958715	0070 011	.2 (	00 00	00	00 (	0 0	0 00	00	00	00	00	00 0	0 0	0 00	00							
< 1	irame 19 🔷 🔿	0080 012	8 0	00 00	00	00	0 0	0 00	00	00	00	00	00 0	0 0	0 00	00							
Key	Value	00a01016	in (		00	00 0			00	00	00	00	00 0		0 00	00							
PageN other	2	00b0 017	6 0	0 00	00	00	0 0	0 00	00	00	00	00	00 0	0 0	0 00	00							
in the second		00c0 019	2 0	0 00	00	00 (	0 0	0 00	00	00	00	00	00 00	0 0	0 00	00							
szeor DEvelerCo	0	00d01020	08 0	00 00	00	00	0 0	0 00	00	00	00	00	00 0	0 0	0 00	00							
Salt1	1690164653	00601022	0 0		00	00 0			00	00	00	00	00 0	00	0 00	00							
Salt2	-876958715	0100 025	6 0	0 00	00	00	00 0	0 00	00	00	00	00	00 0	0 0	0 00	00	- 11						
Checksum1	-269912613	0110 027	2 0	0 00	00	00	0 0	0 00	00	00	00	00	00 0	0 0	0 00	00							
		01201028	18 0	00 00	00	00	0 0	0 00	00	00	00	00	00 0	00	0 00	00							
	Page 2	. 01401032	10 0		00	00			00	00	00	00	00 0		0 00	00							
Кау	Value	0150 033	6 0	0 00	00	00	0 0	0 00	00	00	00	00	00 0	0 0	0 00	00							
PageType	LeafTable	0160 035	2 (	0 00	00	00	0 0	0 00	00	00	00	00	00 0	0 0	0 00	00							
First Freeblock	1102	0170 036	8 0	00 00	00	00 0	0 0	0 00	00	00	00	00	00 0	00	0 00	00							
CellCount	12	01901040	0 0	0.00	00	00 0	0 0	0.00	00	00	00	00	00 0	0 0	0 00	00							
StatOfCelContent	994		Field 0	1	Field 1														Field 2	Field 3	Field 4	Reld 5	Field 6
FreeBytes	0	<b>•</b>	85	h	ttps://w	тити <u>9</u> 0	ogle co	m/sea	ch?q-	chatg	pt&ie-l	UTF-8	loe-UT	F-88h	l-en us	lclert-safa	fari		google	2	d		
Pointer 0	994		86	h	ttps://o	penai.o	om/												openal	4	d		
Pointer 1	4050		87	h	ttps://w	ww.bir	g.com												bing	1	d		
Pointer 2	4005		88	h	ttps://w	ww.bir	g.com	search	?q=ho	w+cor	ne+sar	ne+fig	ht+numi	ber+m	ultiple+	destination	w/+sp8ar	XF	bing	1	d		
Pointer 2	2774		89	h	ttps://tr	avel.st	ickexd	hange	com/q	vestion	ns/163	3124/v	why-do-fi	ights-	tometim	es-share-th	he same fig	htn	travel.stackexch	1	đ		
Reinter 4	3638		90	h	ttps://w	WW 00	ode co	m/sear	ch?a=	unted	+fichte	s+from	+sea+to	+sfo8	ie=UTF	-8&ce=UTF	F-88hl=en-s	sād	ocode	2	d		
Pointer 4	3400		91	h	ttps://w	ww.go	ogle.co	m/sear	ch?q=	nuclea	sr+pox	ier+pla	ant+near	+wilm	ington+	NC&e=UTF	F-Sãoe=U1	F-8	google	2	d		
Pointer 5	3425		92	h	ttps://w	ww.go	ogle.co	m/sear	ch?q=	nuclea	ar+pow	er+pla	ant+near	+wilm	ington+	NC&e=UTR	F-88ce=U1	F-8	google	1			
Pointer 6	3356	L 1	93	h	ttps://w	ww.mi	trrobie	.com/	nelp/h	owło-	config.	.re-iph	one-sett	ings/	-				mintmobile	1	d		-
Pointer /	3011		94	н	ttps://n	vti.ms/	1190													1	d		
Ponter a	2915		95	h	ttps://w	ww.n/	imes o	m/200	3/04/	04/wo	nd/eu	rope/fi	inland n	storu	ssia-ukr	aine html?u	unlocked_a	ntd	nytimes	2	•		
Pointer 9	2872		96	h	ttps://w	WW 30	tube o	om/wa	tch?v	-z8gH	elYM6	aY							youtube	1	d		
Pointer 10	2395																						
Pointer 11	2295																						

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

### Expand / Collapse All nodes

Expand or collapse all nodes within the serialized data tree.

# **Show Alternate Values**

Since ArtEx is working without a protobul 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.

9 - Save File

11 - Search Options

13 - Main Window

14 - Current Node

12 - View Tabs

15 - Legend

10 - Save HTML Representation

### 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.

<pre>0 PBDisgnosticsPresented (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PBDisgnosticsPresented//key&gt; (disp)PEDDISDPFersented//key&gt; (disp)PEDDISDPFersented//key&gt; (disp)PEDDISDPFersented//key&gt; (disp)PEDDISDPFersented//key&gt; (disp)PEDDISDPFersented//key&gt; (disp)PEDDISDPFersented//key&gt; (disp)PEDDISDPFersented//key&gt; (disp)PEDDISDFERSENTED</pre>	62 70 62 69 73 74 80 30 00 F10 23 01 20 03 46 05       ppliet00.4         64 70 62 69 73 74 80 30 00 F10 23 01 20 20 44 65       ppliet00.4         76 70 62 69 73 74 80 30 00 F10 23 01 20 20 44 65       ppliet00.4         76 70 76 70 76 70 76 70 76 70 70 76 70 70 76 70 77 76 56 65       std224 40 22 43 44 24 44 64 64 64 77 82 74 65 44 24 44 24 44 64 65 10 70 74 65 66 70 77 74 65 66 70 77 74 65 66 70 77 74 65 66 70 77 74 65 66 70 77 74 65 66 70 77 74 65 66 70 77 74 65 66 70 70 74 65 67 70 74 65 66 70 70 74 65 66 70 70 74 67 72 86 67 72 74 67 66 76 74 74 70 72 86 77 72 86 77 72 86 77 74 76 75 74 75 7

# **SEGB Viewer**

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

		SEGB Viewe	er	= 〒11 11 11 11 11 11 11 11 11 11 11 11 11	>Q 🗙
		711272741011788	1	Tree View XML View Hex	
		2023-12-18 15:04:52 (L	JTC)	0) 1	
	er by Global Dates	Show Hex Offset		0) 1	
	Offset	Date1	Date2	2F 64 65 76 69 63 65 2F 69 73 50 6C 75 67 67 65 /device	/isPlugge
	0x143E0	2023-11-27 12:04:20 (UTC)	2023-11-27 12-04:20 (UTC)	64 49 6E dIn	
	0x14490	2023-11-27 12:04:23 (UTC)	2023-11-27 12:04:23 (UTC)	/device/isPluggedIn	
	0x14550	2023-11-27 12:04:23 (UTC)	2023-11-27 12:04:23 (UTC)	1) 2	
	0x14620	2023-11-27 12:04:24 (UTC)	2023-11-27 12:04:24 (UTC)	0) 1	
	0x146F0	2023-11-27 12:04:24 (UTC)	2023-11-27 12:04:24 (UTC)	0	
	0x147C0	2023-11-27 12:04:25 (UTC)	2023-11-27 12:04:25 (UTC)	1) 2	
	0x14890	2023-11-27 12:04:25 (UTC)	2023-11-27 12:04:25 (UTC)	-2475731913145812025	
	0x14960	2023-11-27 12:04:25 (UTC)	2023-11-27 12:04:25 (UTC)	1) 2	
_	0x14A30	2023-11-27 12:04:26 (UTC)	2023-11-27 12:04:26 (UTC)		
	0x14B00	2023-11-27 12:04:26 (UTC)	2023-11-27 12:04:26 (UTC)		
	0x14BD0	2023-11-27 12:04:26 (UTC)	2023-11-27 12:04:26 (UTC)	Apple Time : 2023-11-27 12:03:00 PM	
	0x14CA0	2023-11-27 12:04:30 (UTC)	2023-11-27 12:04:30 (UTC)	21.3	
	0x14D70	2023-11-27 12:04:30 (UTC)	2023-11-27 12:04:30 (UTC)	00 00 00 32 58 65 65 41	
_	0x14E40	2023-11-27 12:04:31 (UTC)	2023-11-27 12:04:31 (UTC)	100 00 00 X2 52 5X C5 41	
_	0x14F10	2023-11-27 12:04:32 (UTC)	2023-11-27 12:04:32 (UTC)	Budden Trea + 2023-11-27 12:04:20 PM	
	0x14FE0	2023-11-27 12:04:32 (UTC)	2023-11-27 12:04:32 (UTC)	2) 4	
-	0x150B0	2023-11-27 12:04:32 (UTC)	2023-11-27 12:04:32 (UTC)		
	0x15180	2023-11-27 12:04:36 (UTC)	2023-11-27 12:04:36 (UTC)		
_	0x15250	2023-11-27 12:04:37 (UTC)	2023-11-27 12:04-37 (UTC)		
	0x15320	2023-11-27 12:04:38 (UTC)	2023-11-27 12:04:38 (UTC)		
	0x153C0	2023-11-27 12:05:51 (UTC)	2023-11-27 12:05:51 (UTC)	2/2	
	0x15490	2023-11-27 12:05:51 (UTC)	2023-11-27 12:05:51 (UTC)	-64/3/31313143012023	
-	0x15560	2023-11-27 12:05:51 (UTC)	2023-11-27 12:05:51 (UTC)	1) 4	
	0x15630	2023-11-27 12:05:52 (UTC)	2023-11-27 12:05:52 (UTC)		
	0x15700	2023-11-27 12:05:52 (UTC)	2023-11-27 12:05:52 (UTC)	4) 5	
-	0x157D0	2023-11-27 12:05:52 (UTC)	2023-11-27 12:05:52 (UTC)	35 41 46 36 34 43 42 44 2D 36 39 41 36 2D 34 34 5AF64CBD-	69A6-44
-	0x158A0	2023-11-27 12:05:55 (UTC)	2023-11-27 12:05:55 (UTC)	37 44 2D 35 41 33 46 2D 35 37 36 31 39 34 31 42 7D-5A3F-5 30 44 39 31 0091	7619418
	0k15970	2023-11-27 12:05:55 (UTC)	2023-11-27 12:05:55 (0 TC)	SAF64CBD-69A6-447D-8A3F-5761941B0D91	
	0x15A40	2023-11-27 12:05:56 (UTC)	2023-11-2/ 12:05:56 (UTC)	51.8	
	0-16050	2023-11-27 12:05:56 (UTC)	2022-11-27 12:05:56 (UTC)	13 36 40 32 55 93 05 41	
-	UKISBED	2023-11-27 12:06:00 (010)	2023-11-27 12:06:00 (01C)		
	OK15CB0	2023-11-27 12:06:00 (01C)	2023-11-27 12:06:00 (01C)	Limit Harman - 2023-11-27 12:04:20 PM	
	0.150.00	202311/2712:06:01 (01C)	202311/2712:05:01 (01C)	6) 10	
-	OKTOEDU	2023-11-27 12:06:01 (01C)	2023-11-27 12:06:01 (01C)	17200	
-	0-16660	2023-11-27 12:06:02 (UTC)	2023-11-27 12:00:02 (UTC)	11	
	0x16000	2023-11-27 12:06:02 (01C)	2023-11-27 12:06:02 (UTC)		
-	0-16190	2022112712/06:37(010)	2022-11-27 12:06:37 (UTC)		
	0-16260	2023.11.27 12:06:38 (UTC)	2022-11-27 12:00:30 (01C)		
	0-16220	2022 11 27 12 06 28 (UTC)	2022 11 27 12 05 25 (UTC)		
	0x16400	2023.11.27 12:06:58 (170)	2023-11-27 12:06:58 (170)		
-	0x16400	2023.11.27 12:06:59 (UTC)	2023-11-27 12:06:59 (UTC)	1886 Ball	And Market Tes Dates Date Date
L	a 0400	AND 1121 121 121 12 12 12 12 12 12 12 12 12	EVEN THEY TEMPORE (UTG)	Dictio	nary Array Number fort Bootean Data Date

Essentially, the SEGB viewer is a list of frames on the left and the normal protobul viewer on the right. Each frame can be selected to view the protobul 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.

[=]	👰 RTX Case 🚍 Archive 🖟 ArtExtraction 🙃 Backup 🖆 Folder 🖺 File 🛄 XLS	Compare
	IP Address         Port         User         Password           127.0.0.1         22         root         alpine         Reset	t Saved
the state of the s	Is your device checkm8 compatible? Yes No Compatibility Chart	$\sim$
ArtExtraction		_
Connect to a live device via SSH for extraction or Live		
Examination (Device		$\checkmark$
must be jailbroken)	Test Connection	() Backup
5 Sugar	Temp Folder C:\Users\iwhiflOneDrive\Documents\ArtExTemp	Browse
Read T	Cancel	Open

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.

[-]	RTX Case 🛱 Archive 🖟 ArtExtraction 🕖 Backup 🛱 Folder 📗 File 🛄 XLS 🛅 Compare
	IP Address     Port     User     Password       127.0.0.1     22     root     alpine     Reset     Saved
a di <b>T</b> erra di Santa	Is your device checkm8 compatible? Yes No Compatibility Chart
ArtExtraction	
Connect to a live	
extraction or Live	
Examination (Device	$\sim$
must be jailbroken)	
Regence	Connected Live Connection
a state	Temp Folder
a station	C:\Users\iwhiflOneDrive\Documents\ArtExTemp Browse
ACRA T	Cancel

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.

Image: Second	About
U Welconer C Device A Alos Reform Contacts I Timetine Contacts I Timetine Contactions I Devicing A Alos Reformance A Alo	
lan's iPhone des_dripte	
in Home Col (201000) Strender (20	X
Accounts Settings	E11
Apple D Accounts Lugte Carrier Trinizone conception politic proferences destitine pilot	
Coud Accounts auto	<b>.</b>
Subscriters con apple composite data plat     Vessage Relation     Con apple MobileSUS plat	-
anfannos aliel 2024-19-02 1154-56 8930272204/5948441383 Transmission Cambridge Cambri	
IPhone X 2024-10-02 11:55:34 8912230102126586142 Laosten Sante comapte locationd plat	
IPhone IU,6 2024-10-02 11:56.22 89302720533840727948 Site Method con apple pupilitividy plat	
0221AP 202410.02115111 8012230000426447587 SetupUsingAssistant	
Interfaces	
C Numbers Visit Fa 28.24.87.85 EE Networksterfaces plat	
Fullewin         International/loade/pupment/toestry         activation_record pike         Effective         International/loade/pupment/toestry           Fullewin         3sternationality         activation_record pike         Effective data pike (ori )         Networkinterforces pike	
Serialiumber activation_record joint	
Go W 22 GUILLEN Unbander voor de Grant and de	
040c85e4bc1209c90450a993/6a29a57c1b4c1e6 iCloud Photos	
Advertings D con-apple addes/fers pilt Operational and Keep Ortprats con-apple mobiles/deshav pilst Palea Con-apple mobiles/deshav pilst Palea Con-apple mobiles/deshav pilst Palea Con-apple mobiles/deshav pilst Con-apple mobiles/deshav Con-app	
Important Dates Kool Photos Enabled dou/ServiceEnabled.gp.lst	
Last/profile-tobp disk_sets/bit 2004 do 20 29 4 cD Dat Source A hume Pratient doordfarvios/Haddel ao diat	
Zvcevograz z z to o PW Device Wor containemana gerd to 0	
2024-09-23 310.07 PM	
2024-10-06 11:15:52 AM	
Obtained 2024-09-23 3:09:45 PM coherented	
Bootstrapped 2024 06 22 4 06 20 EM	
	1000

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.

		(UTC) Coordinated Universal Time	~
Director	у		
		🚺 🔤 🗮 Flat View 📔 Extra	t Folder
FileSize Rutes	FileSize MegaBytes	LastModified	X
388289	0	2023-11-29 14:10:46 (U	0
11264	0	2023-11-29 13:29:14 (U	<b>1</b>

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".

Q1	Copy Path
671	Jump to \private\var\mobile\Library\Caches\com.apple.routined\
<b>[</b> ]	Open New Tab at \private\var\mobile\Library\Caches\com.apple.routined\
8	View in Hex Viewer
e	Extracted Selected File(s)
G.	Bookmark \private\var\mobile\Library\Caches\com.apple.routined\
6	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.

Timed Extract	tion Queue			×
Target		Browse		~
\private\var	\mobile\Library\Caches\com.apple.routined\Cache.sqlite			
			×	+

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 several button in the top right of the window.

This will launch the Report feature.

		Report	Save	Save	Save
		Creator	Graph	CSV	HTM
Target					_
C:\Users\iwhi	if\Desktop\MyReport				
Report Deta	ils	Tab Options	Grap	hs & Maps	
Case	12345	Include Device Details		Include Graphs/	Maps
Exhibit	IDW1	Include TimeLine			
Examiner	Whiffin	Include Locations			
		Include Contacts			
Cancel					Save

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.

ArtEx	Case : 12345 Exhibit : IDW1 Examiner : Whiffin ArtEx Version : 2.8.0.2 etails Contacts C Timeline	P Locations	
0941	New name iPhone X iPhone10,6 D221AP iPhone OS 16.3 (21D5026f)		
0.4	Accounts	Carrier Terrener	Settings

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.

Back   Next	timeline	1x @ Q	🕈 Data Type	s				
				April 2023 (Hide	)			
			RowID Ico	on StartTime	EndTime	Activity	MetaData	Source
Description (m)			1	D 2023-04-28 10:50:16 (UTC)		Battery Level (69%)		knowledgeC.db [ZOBJECT: 10330]
			2	D 2023-04-28 12:10:16 (UTC)		Battery Level (68%)		knowledgeC.db [ZOBJECT : 10352]
			3	D 2023-04-28 12:41:36 (UTC)		Battery Level (67%)		knowledgeC.db [ZOBJECT: 10380]
			4	D 2023-04-28 12:48:36 (UTC)		Battery Level (66%)		knowledgeC.db [ZOBJECT: 10390]
			5	D 2023-04-28 12:50:56 (UTC)		Battery Level (65%)		knowledgeC.db [ZOBJECT: 10396]
			6	D 2023-04-28 12:52:56 (UTC)		Battery Level (64%)		knowledgeC.db [ZOBJECT: 10413]
			7	D 2023-04-28 12:57:56 (UTC)		Battery Level (63%)		knowledgeC.db [ZOBJECT: 10414]
			8	D 2023-04-28 12:58:16 (UTC)		Battery Level (62%)		knowledgeC.db [ZOBJECT: 10415]
			9	D 2023-04-28 12:58:36 (UTC)		Battery Level (61%)		knowledgeC.db [ZOBJECT: 10416]
			10	D 2023-04-28 12:58:56 (UTC)		Battery Level (60%)		knowledgeC.db [ZOBJECT: 10418]
			11	D 2023-04-28 12:59:16 (UTC)		Battery Level (59%)		knowledgeC.db [ZOBJECT: 10423]
	1 - Reports Tabs 2 - View Options 3 - Graph / Map 4 - Graph / Map Navig	ration						

- 5 Graph / Map Zoom Controls
- 6 Data Type Filter
- 7 Data Type Fi

# **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

Friday 2	8 Apr	il 2023 (show	)			
				$\mathbf{I}$		
Friday 2	8 Apı	ril 2023 (Hide)				j
RowID	Icon	StartTime	EndTime	Activity	MetaData	Source
1		2023-04-28 10:50:16 (UTC)		Battery Level (69%)		knowledgeC.db [ZOBJECT : 10330]
2		2023-04-28 12:10:16 (UTC)		Battery Level (68%)		knowledgeC.db [ZOBJECT : 10352]
3		2023-04-28 12:41:36 (UTC)		Battery Level (67%)		knowledgeC.db [ZOBJECT : 10380]
3		2023-04-28 12:41:36 (UTC)		Battery Level (67%)		knowledgeC.db [ZOBJECT : 10380]

# 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

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 된.

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

X Report Elements	The Report Elements feature lists all images that have been saved.
X       Timeline 1	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.
Locations 1	
E Constanting and	
Locations 2	

# **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.

gin		Abe's iPhone M:\Extractions\CTF2023\CellebriteCTF23_Abe\UFE			
		Save	Close		
ne Frame	From	a oc aa oo.oo 📖	To Doop of ar		

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 Direc	ctory View
-----------------------------------	------------

S Extraction Comparison		- 🗆 X
Create Comparison Database Files based on extension (eg. sqite, db., sqite3)	Run Comparison	
sqite. sqite3, db, dbstore	Re 2 Prid	
Create Database	Compare	
v	Start	
Save Details		

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

Create Comparison Database Files based on extension (eg .sqlite, .db, .sqlite3)	🗌 File 🔽 Extension		
.sqlite, .sqlite3, .db, .dbstore			
	🕑 Hash File		
Create Database			

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.

 Run Comparison

 File 1
 Find

 File 2
 Find

 Compare
 Compare

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.

Straction C	omparison						-	
Create Comparis Files based on en .sqlite, .sqlite3, .	on Database dension (eg. sqite, db., sqite3) db, dbstore	🗌 File 🗹 Extension	Run Comparison File 1 C:\Users\whit\ File 2 C:\Users\whit\	Desktop\Compare\16.sqite Desktop\Compare\17.sqite	Find			
	Run Comparison			Completed				
		~			Start			
5 Records								
	FilePath	FileHash		Result		Details		
	\Mobile Documents\com~apple~CloudDocs\Downloads\Photos.sqli			Only in 16.sqlite			 	
	\Libraries\Syndication.photoslibrary\database\Photos.sqlite	Mismatch		Schema is different in both extractions	c	lick to see details		
	\Libraries\Syndication.photoslibrary\database\Photos.sqlite-shm	Schema Match						
<b>F</b>	\mobile \Media \Photo Data \Photos.sqlite	Mismatch		Schema is different in both extractions	c	lick to see details		
	\mobile\Media\PhotoData\Photos.sqlite-shm	Schema Match						
🗄 🔚 Save Detail	s							
Missing	Table From 16.sqlite							^
Z_3HIGHLI Z_3HIGHLI Z_3HIGHLI Z_3HIGHLI Z_3HIGHLI Z_3HIGHLI	GHTSBEINGADAPTIVEASSETS GHTSBEINGADAPTIVEEXPLICITLYADDEDASS GHTSBEINGADAPTIVEEXPLICITLYREMOVED/ GHTSBEINGADAPTIVEEXTENDEDASSETS GHTSBEINGADAPTIVESUMMARYASSETS	SETS ASSETS						
Missing	Field From 16.sqlite - ZADDITI	ONALASSETATTRIB	UTES					
ZDUPLICA	TEDETECTORPERCEPTUALPROCESSINGST	ATE						~

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.

Call History.storedata SQL Vewer SQL Explorer WAL Explor	rer													
Execute SQL 📋 Canned Q	ueries +	🄊 - 🔁 😠	M Searching SQL	My Parser								Q 4		Reload
SELECT * FROM ZCALL	RECORD											No Sug	gestions	
<											>			
Walter														
۹. ×	14	With WAL (2)	Without WAL (0) C	Combined (2)										.:
ZCALLDBPROPERTIES	B Decords	Conve	rt Dates Show NU	u 🥅 🔜 🖗	) <b>.</b>									CSV
ZCALLRECORD	Theodras		Z_РК	Z_ENT	Z_OPT	ZANSWERED	ZCALL_CATEGO	ZCALLTYPE	ZDISCONNECT	ZFACE_TIME_D	ZFILTERED_OU	ZHANDLE_TY	ZJUNKCONFIDE	11
	2 Records	» 1 2	1	2	1	0	1	1	0		0	2	0	
ZIWWOLL	2 Records	-												5
Z_2REMOTEPARTICIP	2 Records													TAB
Z_METADATA	1 Records													
Z_MODELCACHE														
Z PRIMARYKEY	1 Hecords													
-	3 Records													
							-							
7 Tables		2 Kows (1 Ce	II Selected)											

#### 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
- 4 Parser Preview
- 2 SQL Results
- 3 Parser Mapping

For example, entering the SQL

# SELECT \* FROM ZCALLRECORD WHERE ZORIGINATED = 1

## Will result in a list of all outgoing calls

Rule 1	sule 1 Focus												Focus				
SQL	SQL SELECT * FROM ZCALLRECORD WHERE ZORIGINATED = 1																
G	Convert Dates Show N	ULL 🧮 🔜 🖗	) -												CSV		
	Z_PK	Z_ENT	Z_OPT	ZANSWERED	ZCALL_CATEGO	ZCALLTYPE	ZDISCONNECTI	ZFACE_TIME_D	ZFILTERED_OU	ZHANDLE_TYP	ZJUNKCONFIDE	ZNUMBER_AV	ZORIGINATED	ZRE			
<b>▶ 01</b>	6	2	1	0	1	0	0		0	1	0	0	1	1	<b></b>		
02	8	2	1	0	1	0	0		0	1	0	0	1	1	Nots		
03	10	2	1	0	1	0	6		0	2	0	0	1	1			
04	12	2	1	0	2	0	6		0	2	0	0	1	1	TAB		
05	13	2	1	0	2	0	6		0	2	0	0	1	1			
06	16	2	1	0	1	0	6		0	2	0	0	1	1			
45 Rows	(1 Cell Selected)					Rows (1 Cell Selected)											

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

lcon	Activity	Start Time		End Time	Metadata		Message		Media	
~	Outgoing Call	-		• •						
					¥	· ·	ЧЧ	· ·	<u> </u>	· ·
lcon	StartTime	Activity	MetaData		Source					
2		Outgoing Call		(	CallHistory.storedata [ZCALLRECORD:6]					
<b>1</b>		Outgoing Call		0	CallHistory.storedata [ZCALLRECORD:8]					
2		Outgoing Call		(	CallHistory.storedata [ZCALLRECORD:10]					
2		Outgoing Call		(	CallHistory.storedata [ZCALLRECORD:12]					
2		Outgoing Call		(	CallHistory storedata [ZCALLRECORD:13]					
2		Outgoing Call		0	CallHistory.storedata [ZCALLRECORD:16]					1
2		Outgoing Call		(	CallHistory.storedata [ZCALLRECORD:17]					
		Outgoing Call		(	CallHistory storedata [ZCALLRECORD: 19]					

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.

lcon	Activity			Start Time		E				
27	Outgoing	g Call		ZDATE						
				MAC Absolute	~	🕑 Is UTC 🛛				
				-						
				Parse MAC Absolute						
				MAC (NanoSec	onds)					
				Unix Unix (Millionae						
				Google Chrom	e					
Lean	Ou aT			FireFox						
Icon	Start lime	10.10.01 (UTO)	4	Activity	MetaData					
2	2023-07-27	18:48:24 (UTC)	U	Itgoing Call						
2	2023-07-27	18:57:15 (UTC)	0	utgoing Call						
2	2023-07-27	20:20:13 (UTC)	O	utgoing Call						
2	2023-07-27	20:26:13 (UTC)	O	utgoing Call						
2	2023-07-27	20:47:28 (UTC)	0	utgoing Call						
2	2023-07-27	21:11:07 (UTC)	O	utgoing Call						
2	2023-07-28	16:24:18 (UTC)	0	tgoing Call						
<b>Ф</b> 7	2023-07-28	16:32:04 (UTC)	0	utgoing Call						

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:

Metadata		
Duration: <zdur <br="">Name: <zname></zname></zdur>	ATION>	
Address	ZADDRESS	× +

Press the + button to save the item.

This will be viewable in the Parser Preview.

lcon	StartTime	Activity	MetaData	Source
27	2023-07-27 18:48:24 (UTC)	Outgoing Call	Duration: 105.61427199840546 Name: This Is DFIR Two Address: DX8X8X4S	CallHistory.storedata [ZCALLRECORD:6]

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

∎ My	Parsers [Beta]																	
Parse	My Nev	v Call His	story	Parser	Vers	iion 1.0	]											Save
	Author		Description	Parser Description	1													
Rule	1																	Focus
Rule	2																	Focus
SQL	SELECT * FROM ZCALLRE	CORD WHERE ZORIC	SINATED = 0							Limit Example								
G	Convert Dates Show NUL	L 📰 🔜 🖗																CSV
	Z_PK	Z_ENT	Z_OPT	ZANSWERED	ZCALL_CATEGO	ZCALLTYPE	ZDISCONNECT	ZFACE_TIME_D	ZFILTERED_O	U ZHANDLE_TYP	ZJUNKCONFIDE	ZNUMBER_AVA	ZORIGINATED	ZREAD	ZVERIFICATION	ZDATE	ZDURATIO	· · · · · · · · · · · · · · · · · · ·
<b>▶ 01</b>	1	2 2	2	0	1	1	6		0	2	0	0	0	1	1	2023-07-14 17:	0	
02	2	2 2	2	0	1	1	6		0	2	0	0	0	1	4	2023-07-26 19:	0	
47 Rov	vs (1 Cell Selected) Activity	Start	Time		End Time		Metadata			м	lessage			Medi	a			
2	Incoming Call	ZDAT	Æ			· · · · · · · · · · · · · · · · · · ·	Duration: <zdi< td=""><td>IRATION&gt; E&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>_</td></zdi<>	IRATION> E>										_
	•1	MAC	Absolute	v 🧧 is UTC			Address: <zad< th=""><th>oress&gt;</th><th></th><th>× +</th><th></th><th>]</th><th></th><th>•</th><th>~ _</th><th></th><th></th><th>1.</th></zad<>	oress>		× +		]		•	~ _			1.
lcon	StartTime	Activity	N	AetaData		Source												
Ľ	2023-07-14 17:35:41 (UTC)	) Incoming	Call D. Ne Ac	uration: 0 anne: 3dress: +15828887553		CallHat	ory storedata [2CALI	RECORD:1]										
<b>S</b> <sup>K</sup>	2023-07-26 19:34:42 (UTC)	) Incoming	Call D. Na Ac	uration: 0 anne: ddness: +7196494670		CallHet	ory storedata [ZCALI	RECORD:2]										
6K	2023-07-26 19:35:11 (UTC)	) Incoming	Call D.	uration: 0		CallHist	ory storedata [2CALI	RECORD:3]									Add	New Rule

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.

U Welcome!	Device	A Apps	Keychain 🔘 Cont	tacts 🕑 TimeLine 🛇 Locations	C Directory
<u> </u>		Unable to draw graph larg	erthan 31 days 📃 ≪ < > ≫	📖 Show Time 🕑 🤤 🕀 🧮	
ALL - my new ca	×	🗍 🖉 👁 · 📮 ·			
My Parsers	★ ≫	Icon StartTime	<ul> <li>Activity</li> </ul>	MetaData	Source
My New Ca	II History 80 / 80 Reco	2023-07-14 17:3	55:41 (UTC) Incoming Call	Duration: 0 Name: Address: +15828887553	CallHistory.storedata [ZCALLRECORD : 1]
		2023-07-26 19:3	34:42 (UTC) Incoming Call	Duration: 0 Name: Address: +7196494670	CallHistory.storedata [ZCALLRECORD : 2]
		2023-07-26 19:3	35.11 (UTC) Incoming Call	Duration: 0 Name: Address: +7196494670	CallHistory.storedata [ZCALLRECORD : 3]
		2023-07-26 21:3	11:45 (UTC) Incoming Call	Duration: 0 Name: Address: +15639293174	CalHistory.storedata [ZCALLRECORD : 4]
		2023-07-27 18:4	I5:29 (UTC) Incoming Call	Duration: 95.65569198131561 Name: This Is DFIR Two	CallHistory.storedata [ZCALLRECORD : 5]

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 0 Media FilePath: <ZDIRECTORY> <ZFILENAME> Icon StartTime 2023-07-01 20:23:25 (UTC) Activity Photo MetaData Filename: IMG\_0010.JPG urce tos.sqlite [ZASSET:1] **TEAM OF 1980** THEY WERE UNBEATABLE 0 Add Maps using the Media Block Media Latitude: <ZLATITUDE> Longitude: <ZLONGITUDE> StartTime 2023-12-06 23:50:19 (UTC) MetaData Filename: IMG\_0049.HEIC Activity qite [ZASSET:294]

## Use Deserialized Data



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