

#JONSECOPS

Forensic Analysis of Apple IoT Devices

TABLE OF CONTENTS

APPLE WATCH ANALYSIS	3
APPLE TV ANALYSIS	12
APPLE HOMEPOD ANALYSIS	16
APPLE HOMEKIT ANALYSIS	18

APPLE WATCH ANALYSIS

To start analysis, ArtExaminer was used for data processing and analysis regarding the Apple Watch as seen in Figure 1.

FIGURE 1: APPLE WATCH DATA ANALYSIS SETUP

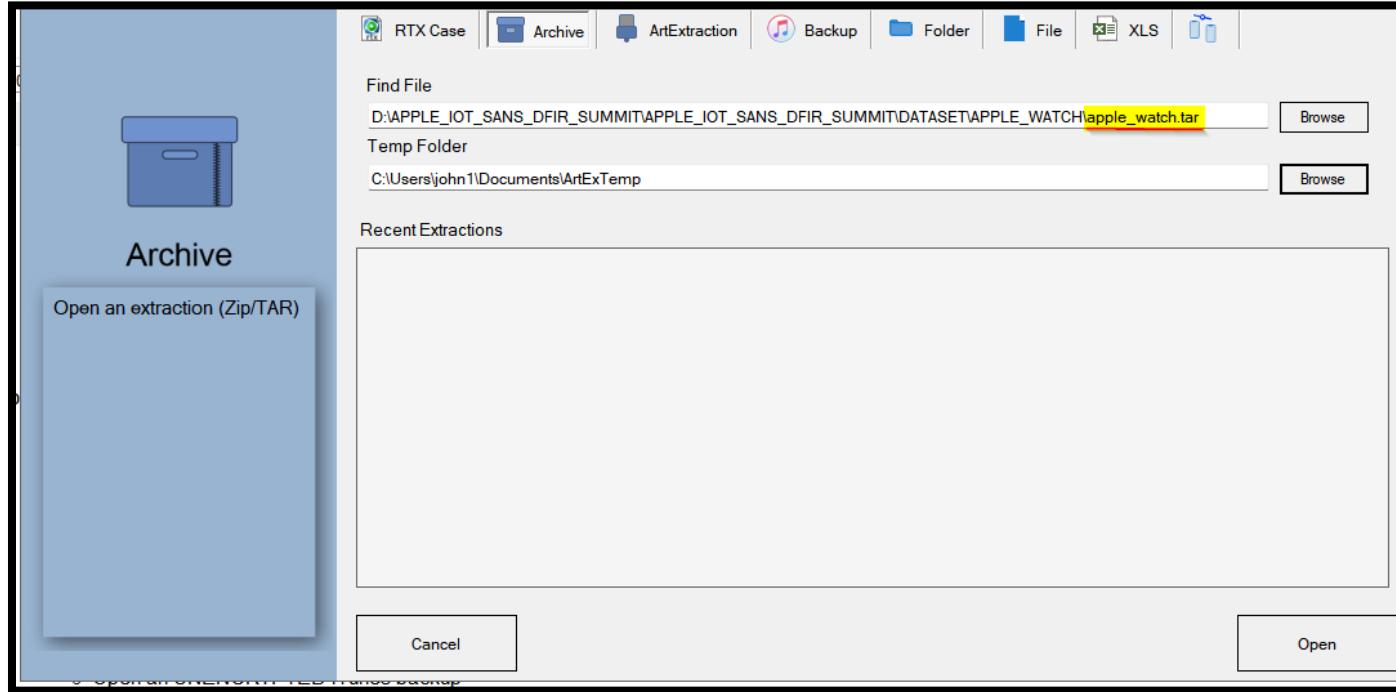


Figure 2 displays the output once the data is loaded.

FIGURE 2: UPLOADED DATA

The screenshot shows the ArtEx software interface with the following details:

Top Bar:
Begin | iOS's Apple Watch | D:\APPLE_IOT_SANS_DFIR_SUMMIT\APPLE_IOT_SANS_DFIR_SUMMIT\DATASET\APPLE_WATCH\apple_watch.tar | Save | Close

Time Filter:
All Time | From: 2001-01-01 00:00 | To: 2099-01-01 00:00 | Time Span: 35794 Days

Navigation:
Device | Apps | Keychain | Contacts | Timeline | Chat View | Gallery | Locations

Main Content Area:

IOS's Apple Watch
Watch OS 8.7.1

Accounts:
AppleID: ios.162@icloud.com | Accounts3.sqlite

Numbers:
SerialNumber: GJ9X86F2J5X4 | mobileactivationd.log.1
UniqueDeviceID: 2a9fbea1643728ce72f820abd21cf5e854242341 | mobileactivationd.log.1
SerialNumber: GJ9X86F2J5X4 | activation_record.plist
UniqueDeviceID: 2a9fbea1643728ce72f820abd21cf5e854242341 | activation_record.plist

Settings:
TimeZone: Europe/Rome | localtime

Interfaces:
Wi-Fi: B8:41:A4:14:37:DF | NetworkInterfaces.plist
Ethernet Adapter (en1) AE:46:A4:9A:E4:08 | NetworkInterfaces.plist

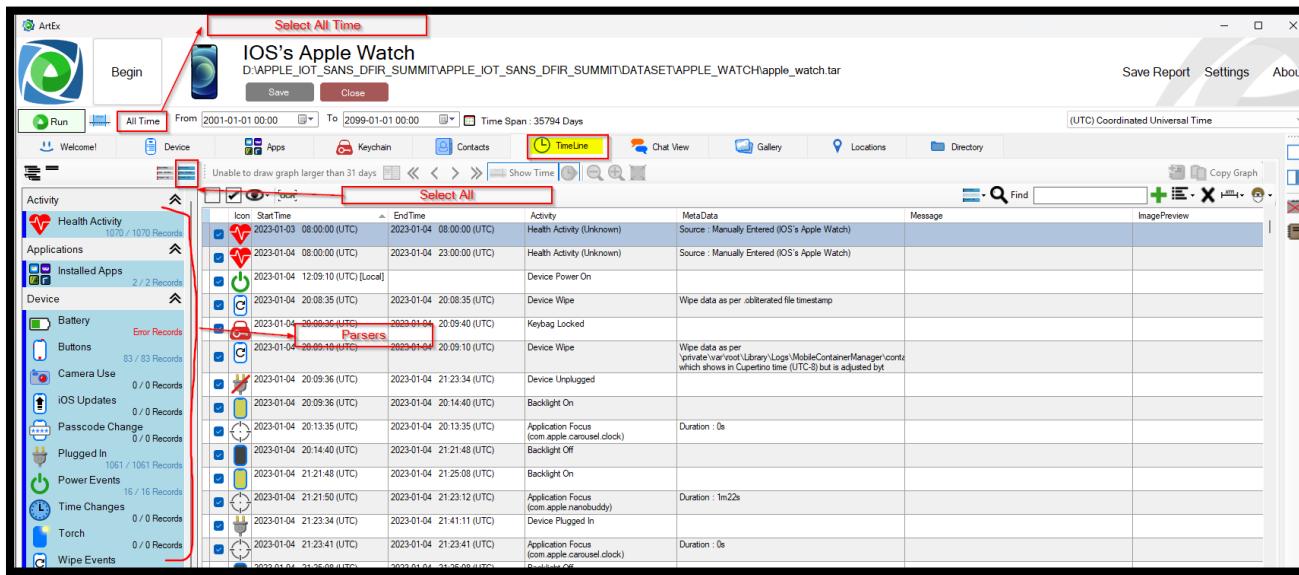
iCloud Photos:

Important Dates:
Device Wipe: 1/4/2023 8:09:10 PM | containermanagerd.log.0
Last KnowledgeC Entry: 1/22/2023 6:51:38 AM | knowledgeC.db
Obliterated: 1/4/2023 8:08:35 PM | .obliterated

File List:
data_ark.plist | SystemVersion.plist

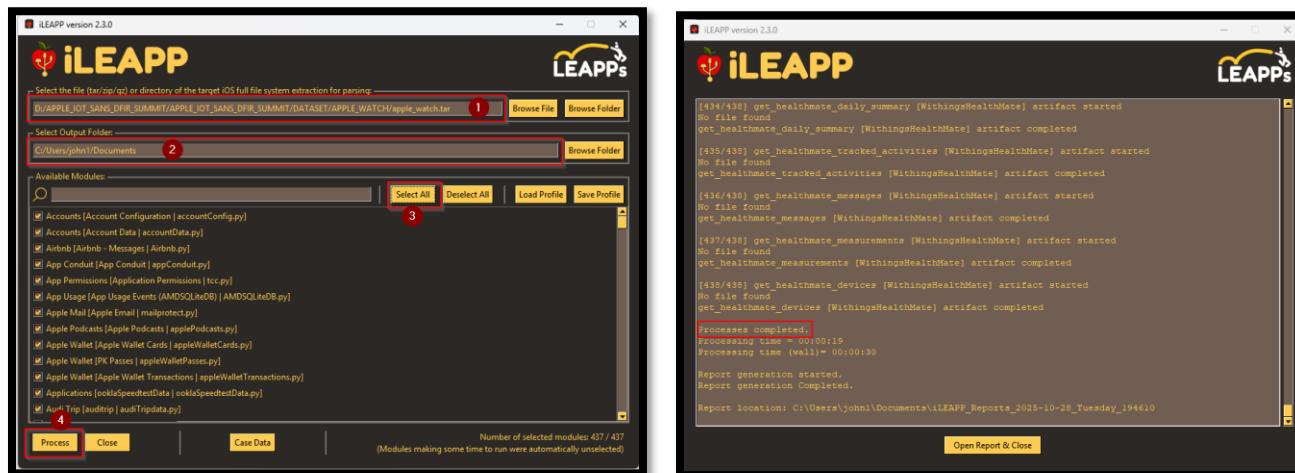
Within the Timeline section of ArtEx, settings were changed to get numerical records of the parsers as seen in Figure 3.

FIGURE 3: SETTINGS



iLEAPP was used to obtain further data artifacts and information from the Apple Watch as seen in Figure 4.

FIGURE 4: iLEAPP DATA UPLOAD



After the data is processed, iLEAPP produces a report which allows you to parse through numerous artifact information such as Account Configuration, Device Details, Calendar Events, etc as seen in Figure 5.

FIGURE 5: iLEAPP REPORT

The screenshot shows the iLEAPP 2.3.0 software interface. On the left is a sidebar with the following categories and sub-items:

- SAVED REPORTS: Report Home
- ACCOUNTS: Account Configuration, Account Data
- APP PERMISSIONS: Application Permissions
- BIOME: Biome - Backlight
- BLUETOOTH: Bluetooth Other LE, Bluetooth Paired
- CACHE DATA: fsCachedData
- CALENDAR: Calendar Events

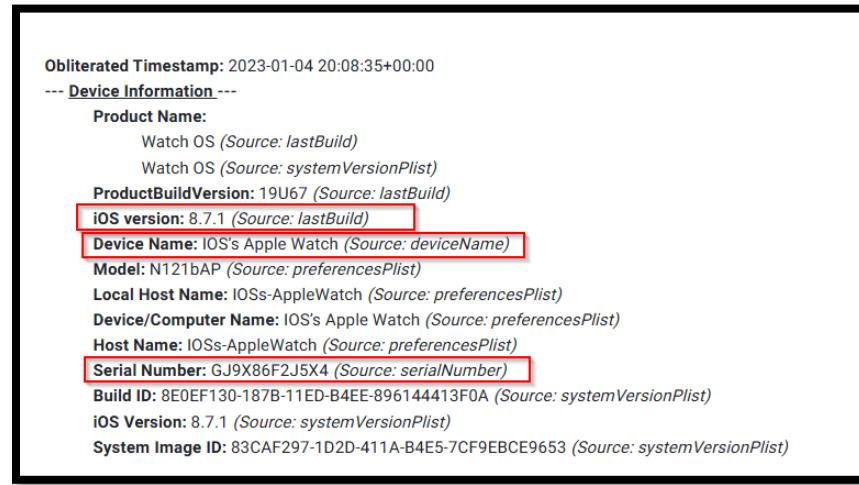
The main content area features the iLEAPP logo and the text "iOS Logs, Events, And Plists Parser". Below this is a sub-header: "iLEAPP is an open source project that aims to parse every known iOS artifact for the purpose of forensic analysis." The main section is titled "Case Information" and contains a table with the following data:

	Details
Extraction location	D:/APPLE_IOT_SANS_DFIR_SUMMIT/APPLE_IOT_SANS_DFIR_SUMMIT/DATASET/APPLE_WATCH/apple_watch.tar
Extraction type	tar
Report directory	C:\Users\john1\Documents\iLEAPP_Reports_2025-10-28_Tuesday_194610
Processing time	00:00:30 (Total 30.33779190000496 seconds)

A note at the bottom states: "All dates and times are in UTC unless noted otherwise!"

Using both software's allowed me to analysis the artifacts obtained from both ArtEx and iLEAPP to answer the lab questions. The serial number, device name, and WatchOS version of the Apple Watch (GJ9X86F2J5X4) was obtained from the iLEAPP report as displayed in FIGURE 6.

FIGURE 6: PRODUCT SERIAL NUMBER, DEVICE NAME, AND OS VERSION



The user's iCloud account (ios.162@icloud.com) was obtained from both ArtEX and iLEAPP as seen in Figure 7.

FIGURE 7: USERS ICLOUD ACCOUNT

The figure shows two screenshots side-by-side. On the left is the ArtEX interface, which has a main window titled "IOS's Apple Watch" showing "Watch OS 8.7.1". Below it, a sub-menu titled "Accounts" lists an entry for "AppleID: ios.162@icloud.com". This entry is highlighted with a red box. On the right is the iLEAPP 2.3.0 interface, which has a sidebar with "ACCOUNTS" selected. Under "ACCOUNTS", there is a sub-menu titled "Account Data". A red box highlights this menu item. To the right is a table titled "ACCOUNTS" with three rows of data. The first row shows a timestamp of 2023-01-04 20:26:53+00:00, an account description of "iTunes Store (Sandbox)", and a username of "local". The second row shows a timestamp of 2023-01-04 20:28:53+00:00, an account description of "iTunes Store", and a username of "local". The third row shows a timestamp of 2023-01-04 21:26:16+00:00, an account description of "IDMS", and a username of "ios.162@icloud.com". A red box highlights the "ios.162@icloud.com" entry in the table.

Timestamp	Account Desc.	Username
2023-01-04 20:26:53+00:00	iTunes Store (Sandbox)	local
2023-01-04 20:28:53+00:00	iTunes Store	local
2023-01-04 21:26:16+00:00	IDMS	ios.162@icloud.com

The only contact available (Mattia Epifani) in the address book was obtained from iLEAPP as seen in Figure 8.

FIGURE 8: CONTACT INFORMATION

Creation Date	Thumbnail	First Name	Last Name	Phone Numbers	Storage Place	Modification Date
2023-01-04 21:31:53+00:00		IOS	16		Card	2023-01-04 21:31:57+00:00
2023-01-20 16:48:22+00:00		Mattia	Epifani	Mobile: +39 334 2340899	Card	2023-01-20 16:48:22+00:00
Creation Date	Thumbnail	First Name	Last Name	Phone Numbers	Storage Place	Modification Date

The instant messaging apps installed on the watch are WhatsApp and Facebook Messenger. This information was obtained from both ArtEx and iLEAPP as seen in Figure 9.

FIGURE 9: USER INSTANT MESSAGING APPS

	Icon	StartTime	EndTime	Activity	MetaData
		2023-01-20 16:49:02 (UTC)		Message Intent (WhatsApp)	Direction : Outgoing Message From : Owner To : +39 334 2340899 (Mattia Epifani)
		2023-01-20 16:49:21 (UTC)		Message Intent (WhatsApp)	Direction : Outgoing Message From : Owner To : +39 334 2340899 (Mattia Epifani)
		2023-01-20 16:49:38 (UTC)		Message Intent (WhatsApp)	Direction : Outgoing Message From : Owner To : +39 334 2340899 (Mattia Epifani)

Install Timestamp	Bundle ID	App Name	Developer Name	App Version	App Bundle Version
2023-01-20 07:46:15	com.facebook.Messenger.watchkitapp	Messenger	Meta Platforms, Inc.	392.0	43883
2023-01-20 07:46:15	com.facebook.Messenger.watchkitapp	Messenger	Meta Platforms, Inc.	392.0	43883

Health information such as how many steps the user took on January 14th, 2023, between 7:45:20 AM and 7:49:14 AM UTC (177 steps) and the users heart rate on January 11th at 8:52:29 AM UTC (69bpm) was obtained from iLEAPP as seen in Figure 10.

FIGURE 10: USER HEALTH STEPS AND HEART RATE

Health - Device - Watch Worn Data
Show 15 entries
Search:

Start Time	End Time	Steps	Duration (Seconds)	Device
2023-01-14 07:45:20+00:00	2023-01-14 07:49:14+00:00	177.0	233.99931049346924	iPhone X
2023-01-19 07:04:13+00:00	2023-01-19 07:04:36+00:00	15.0	23.022045969963074	Apple Watch Series 3 - 42mm
2023-01-19 07:04:41+00:00	2023-01-19 07:04:49+00:00	18.0	7.626422882080078	iPhone X
2023-01-19 07:11:08+00:00	2023-01-19 07:11:10+00:00	10.0	2.557992458343506	Apple Watch Series 3 - 42mm
2023-01-19 07:11:10+00:00	2023-01-19 07:11:10+00:00	10.0	5.000541691690600	iPhone X

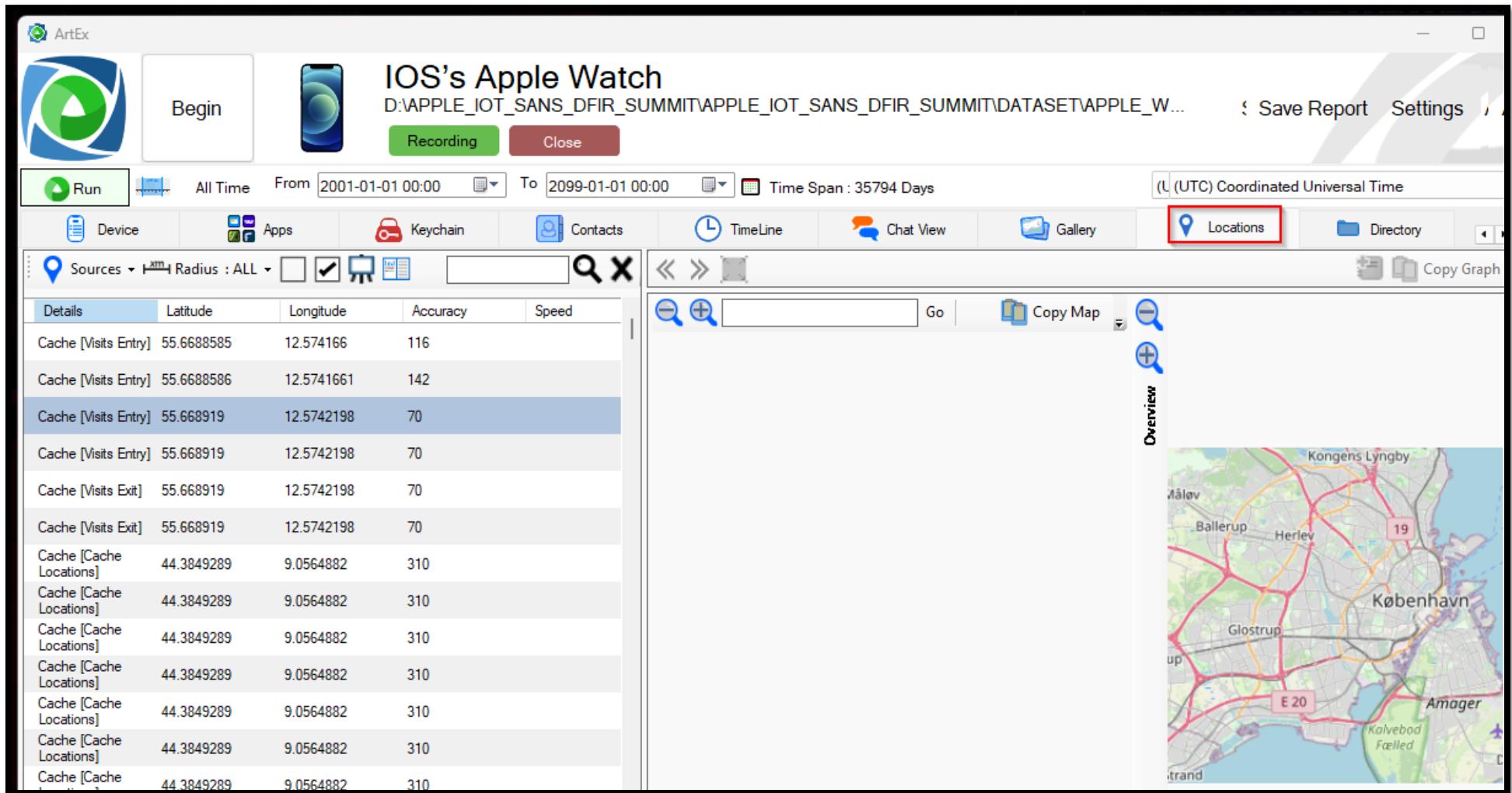
Watch Worn Data
Health - Heart Rate
Health - Provenances
Health - Resting Heart Rate

Health - Heart Rate
2023-01-08
11:24:30+00:00
2023-01-08
11:24:30+00:00
113
Background
2023-01-08
11:30:56+00:00
Apple Watch
Apple Inc.
Apple Watch Series 3 - 42mm

Health - Heart Rate
2023-01-11
08:52:29+00:00
2023-01-11
08:52:29+00:00
69
Background
2023-01-11
17:45:23+00:00
Apple Watch
Apple Inc.
Apple Watch Series 3 - 42mm

ArtEX was used to discover where the user has been in the world as seen in Figure 11.

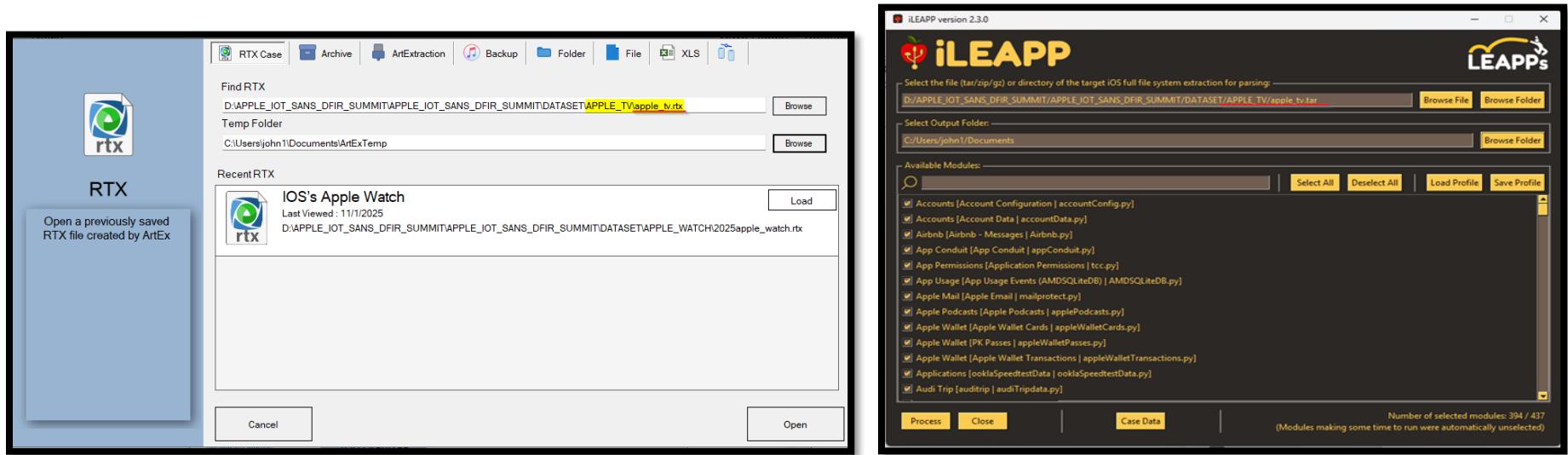
FIGURE 11: USER TRAVELS



APPLE TV ANALYSIS

To start analysis, ArtExaminer and iLEAPP was used to upload the data for processing and analysis regarding the Apple TV as seen in Figure 1.

FIGURE 1: APPLE TV ANALYSIS SETUP



Analyzing the report output from iLEAPP displayed the Apple TV serial number (DY3L4CRZFF54), device name (Apple TV) and OS version (8.4.2) as seen in Figure 2.

FIGURE 2: PRODUCT SERIAL NUMBER, DEVICE NAME, AND OS VERSION

The screenshot shows the iLEAPP interface with the title "iLEAPP" and subtitle "iOS Logs, Events, And Plists Parser". Below the title is a description: "iLEAPP is an open source project that aims to parse every known iOS artifact from logs, events, and plists." The main section is titled "Case Information". It includes tabs for "Details", "Device details" (which is selected), "Script run log", and "Processed files list".

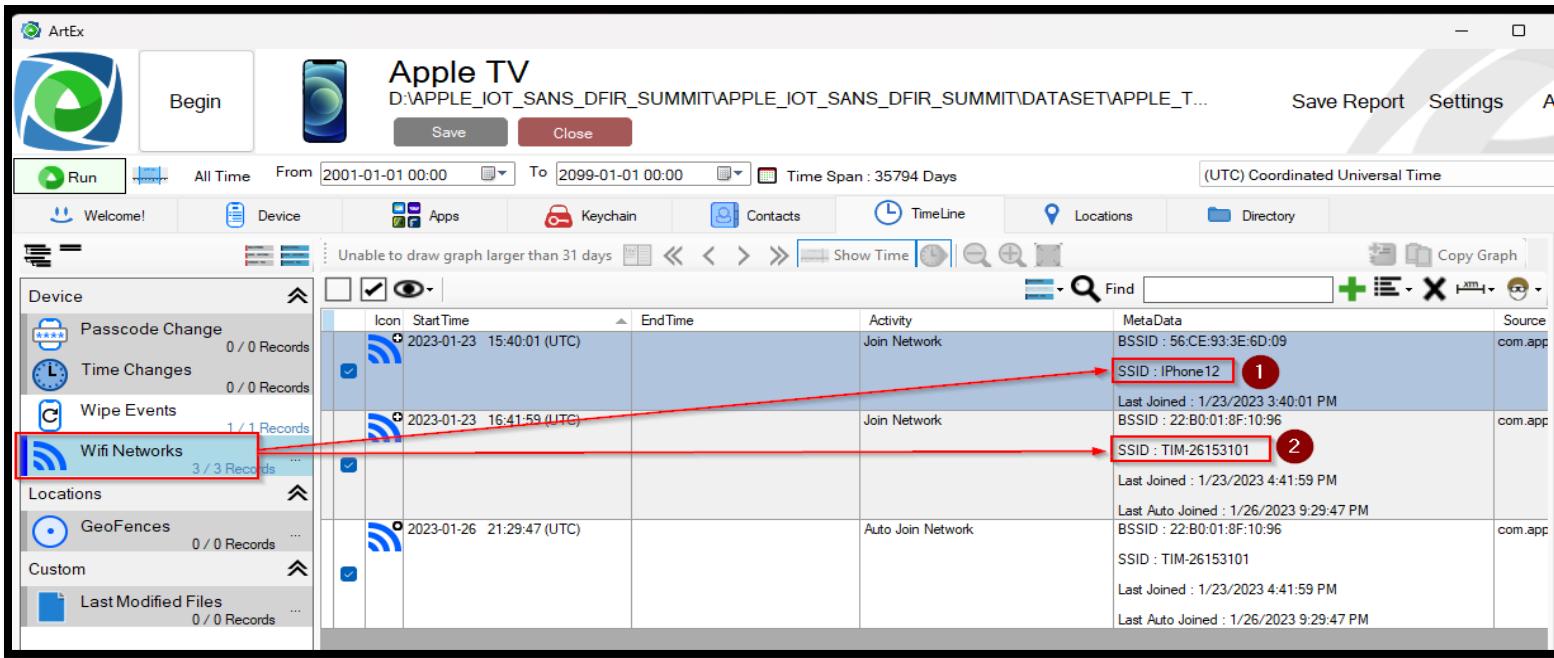
Device details:

- Obliterated Timestamp:** 2023-01-23 15:38:05+00:00
- Settings ---**
 - Last System Version:** iPhone OS8.4.2/12H606 (*Source: appleLocationd*)
 - Location Services Enabled:** 1 (*Source: appleLocationd*)
- Device Information ---**
 - Device Name:** Apple TV (*Source: deviceName*)
 - Model:** J33iAP (*Source: preferencesPlist*)
 - Local Host Name:** Apple-TV (*Source: preferencesPlist*)
 - Device/Computer Name:** Apple TV (*Source: preferencesPlist*)
 - Host Name:** Apple-TV (*Source: preferencesPlist*)
 - Serial Number:** DY3L4CRZFF54 (*Source: serialNumber*)
 - Product Name:** iPhone OS (*Source: systemVersionPlist*)
 - iOS Version:** 8.4.2 (*Source: systemVersionPlist*)
- Network ---**
 - MAC Addresses:**
 - ether: A0:ED:CD:D7:12:7D (*Source: wifiIdentifiers*)
 - airport: A0:ED:CD:D7:12:7C (*Source: wifiIdentifiers*)

The given iLEAPP report was used to gain the which Wi-Fi networks was the device connected (iPhone 12, TIM-26153101) as well as the data output from ArtEx as seen in Figure 3.

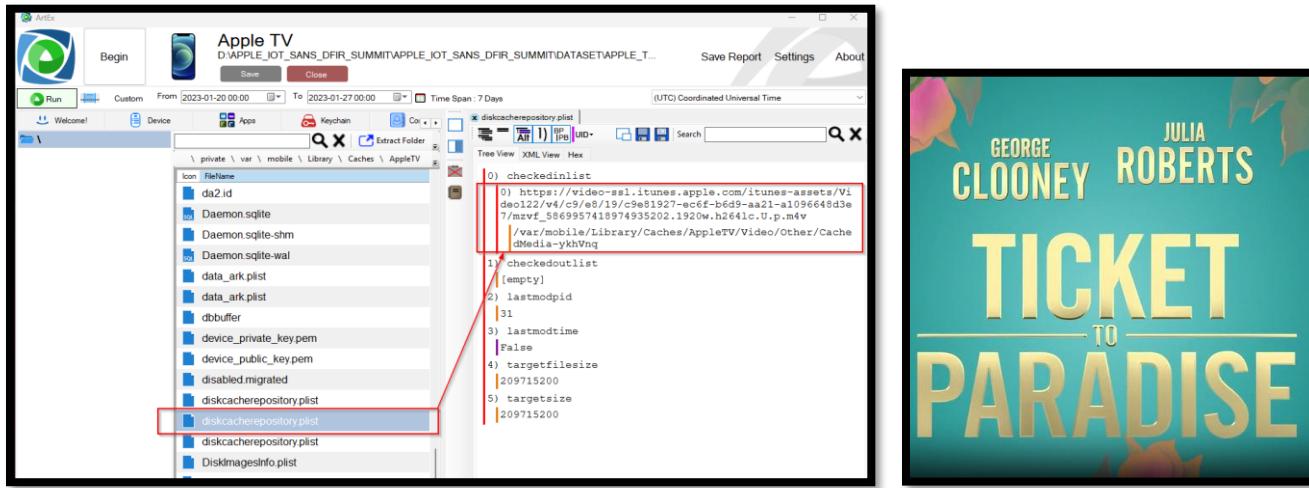
FIGURE 3: DEVICE WIFI CONNECTIONS

SSID	BSSID	Network Usage	Country Code	Device Name	Manufacturer	Serial Number	Model Name
iPhone12	56:ce:93:3e:6d:9		IT	1			
TIM-26153101	22:b0:1:8f:10:96	276453.7165489197	IT	2			
SSID	BSSID	Network Usage	Country Code	Device Name	Manufacturer	Serial Number	Model Name



ArtEx was used to identify the last movie previewed on Apple TV (Ticket to Paradise) as seen in Figure 4.

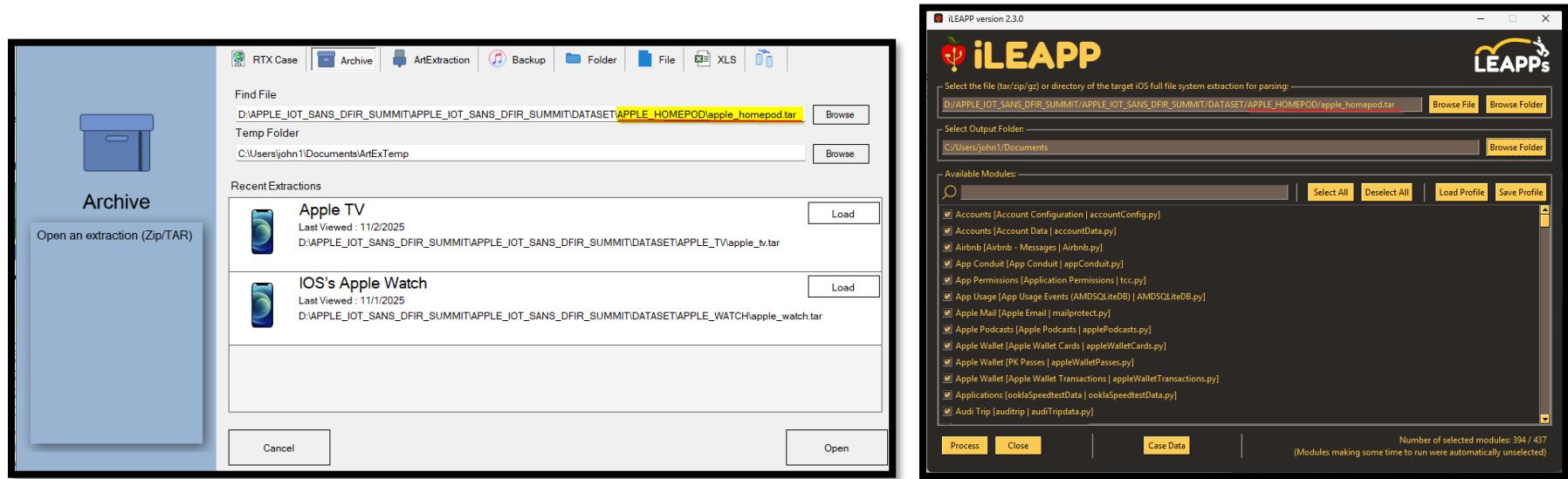
FIGURE 4: LAST MOVIE PREVIEWED ON DEVICE



APPLE HOMEPOD ANALYSIS

To start analysis, ArtExaminer and iLEAPP was used to upload the data for processing and analysis regarding the Apple HomePod as seen in Figure 1.

FIGURE 1: APPLE HOMEPOD ANALYSIS SETUP



Analyzing output from ArtEx displayed the Apple HomePod serial number (HG5GN1TDPQ1H), device name (Apple TVOS), OS version (16.2), Wi-Fi Mac address (94:EA:32:A2:56:1C), and Bluetooth MAC address A2:38:A5:5A:54:02) as seen in Figure 2.

FIGURE 2: DEVICE SERIAL NUMBER, DEVICE NAME, OS VERSION, WI-FI MAC ADDRESS, BLUETOOTH MAC ADDRESS

Apple TVOS 16.2		SystemVersion.plist	
Accounts No Data		Settings	
		Interfaces	
Wi-Fi 94:EA:32:A2:56:1C		NetworkInterfaces.plist	
Ethernet Adapter (en1) A2:38:A5:5A:54:02		NetworkInterfaces.plist	
Numbers		iCloud Photos	
SerialNumber HG5GN1TDPQ1H		No Data	
UniqueDeviceID 00008006-000325562133402E			
Important Dates			
Device Wipe 1/1/1970 12:00:17 AM			

The output report from iLEAPP displayed the Wi-Fi network the device was connected to (TIM-26153101) as displayed in Figure 3:

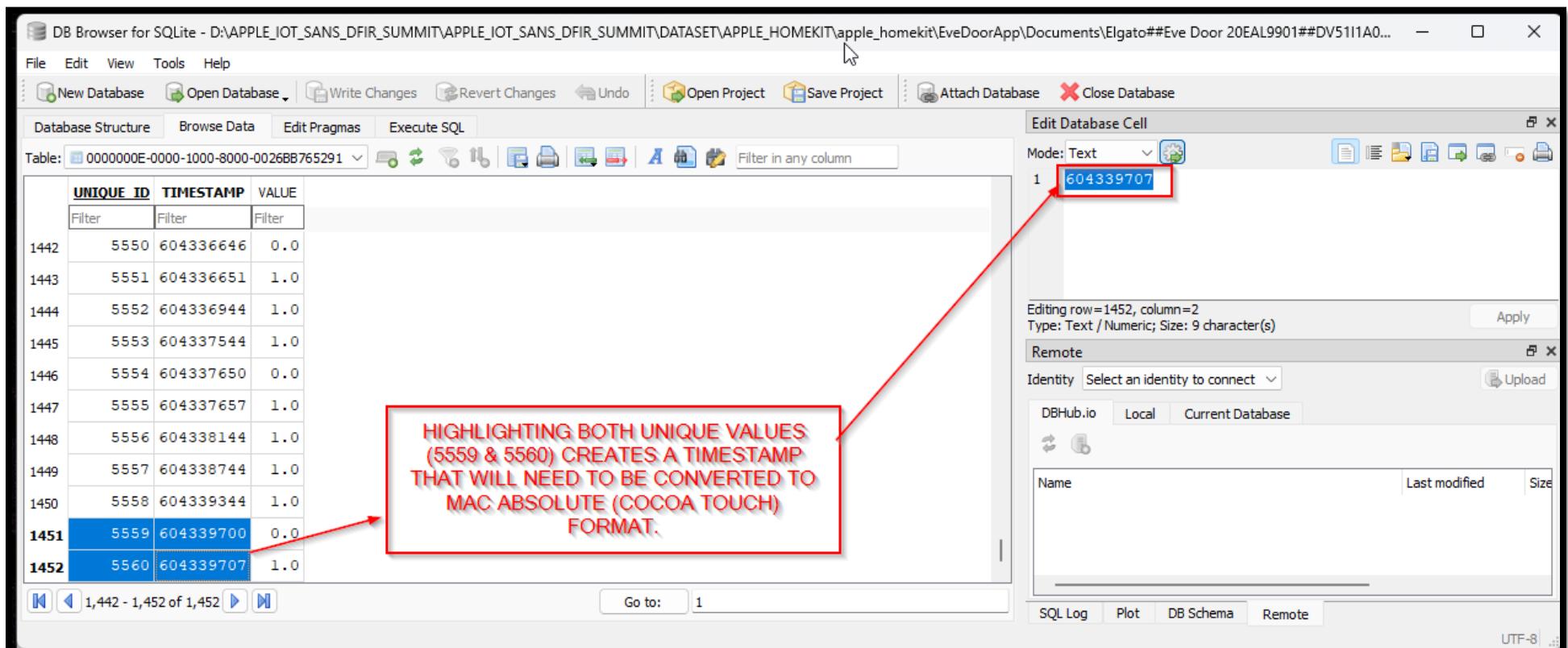
FIGURE 3: DEVICE WIFI NETWOK CONNECTION

SSID	BSSID	Network Usage	Country Code	Device Name	Manufacturer	Serial Number	Model Name	Enabled
TIM-26153101	22:b0:1:8f:10:96							
SSID	BSSID	Network Usage	Country Code	Device Name	Manufacturer	Serial Number	Model Name	Enabled

APPLE HOMEKIT ANALYSIS

The DB Browser for SQLite and Epochconverter was used to locate when the door was opened for the last time (Tuesday, February 25, 2020) as seen in Figure 1.

FIGURE 1: LAST TIME DOOR WAS OPENED





Cocoa Core Data Timestamp Converter

Apple Cocoa Core Data timestamp to human-readable date

Core Data is a data storage framework to manage objects in iOS and OS X applications. Core Data is part of the Cocoa API. These timestamps are sometimes labeled 'Mac absolute time'.

A Core Data timestamp is the number of seconds (or nanoseconds) since midnight, **January 1, 2001**, GMT (see [CFAbsoluteTime](#)). The difference between a Core Data timestamp and a Unix timestamp (seconds since 1/1/1970) is 978307200 seconds.

The current Core Data timestamp is **783829605** or in nanoseconds: 783829605000000000

Enter your Core Data timestamp below (seconds or nanoseconds):

604339707

Convert Core Data timestamp to human date

Converting timestamp (604339707) in seconds:

GMT: Tuesday, February 25, 2020 4:08:27 PM

Your time zone: Tuesday, February 25, 2020 11:08:27 AM GMT-05:00

EPOCH CONVERTER IS USED
TO CONVERT THE 604339707
VALUE TO A HUMAN DATE