#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

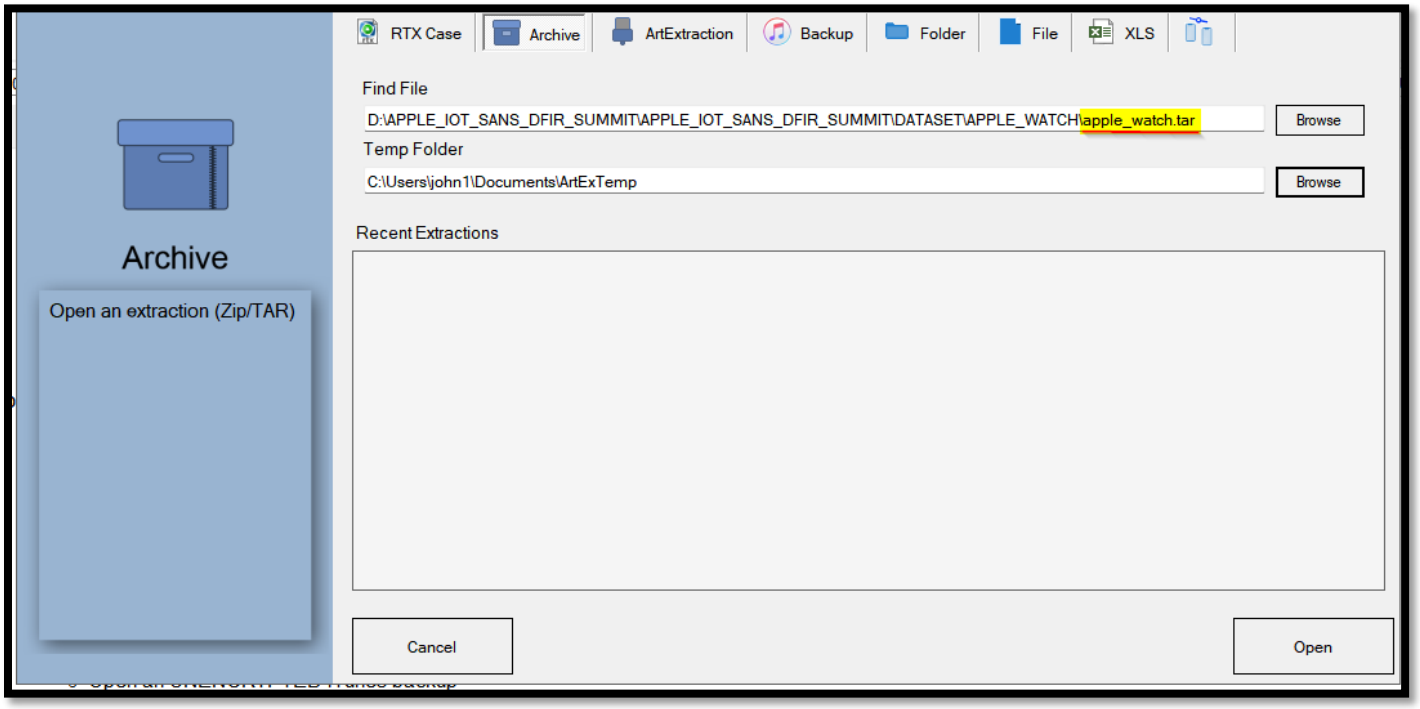
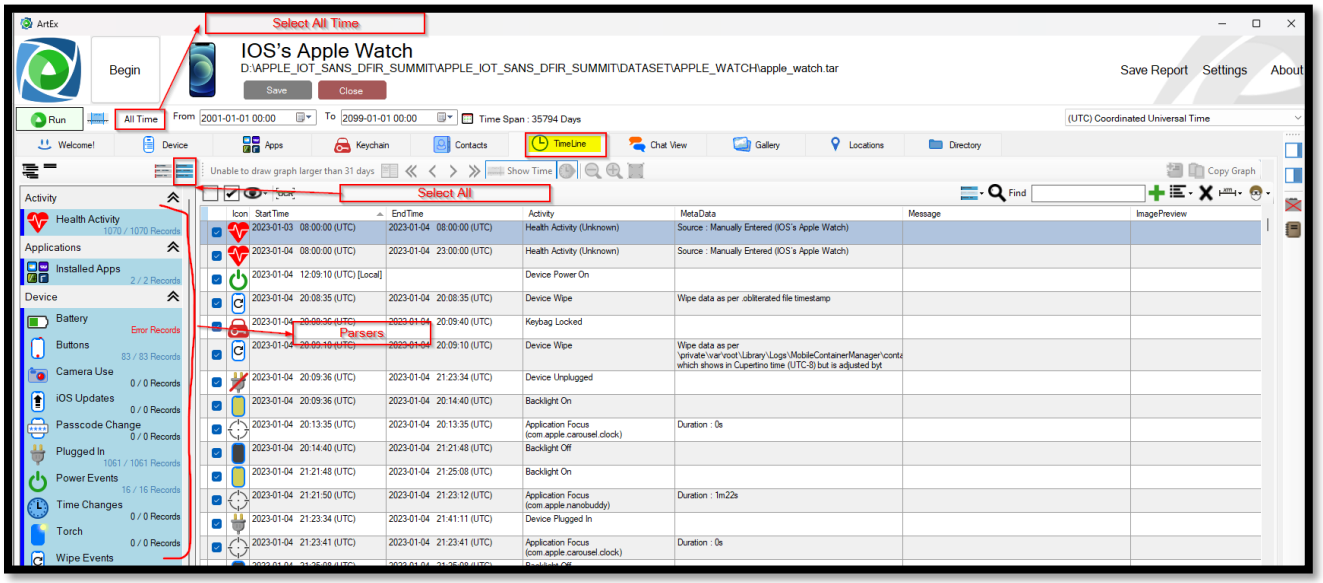


Figure 2 displays the output once the data is loaded.

FIGURE 2: UPLOADED DATA

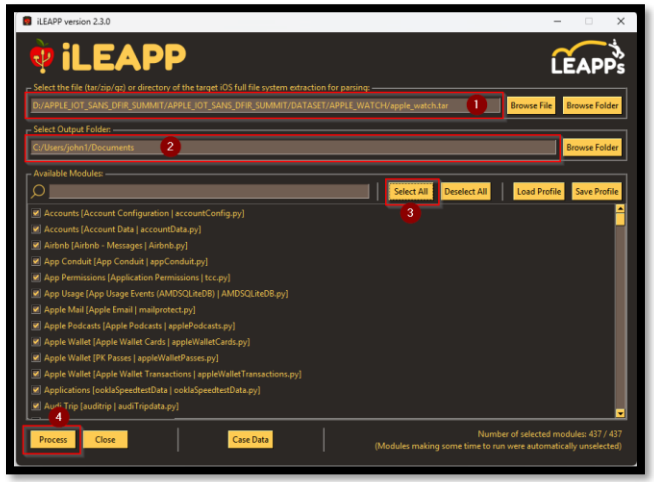
Within the Timeline section of ArtEx, settings were changed to get numerical records of the parsers as seen in Figure 3.

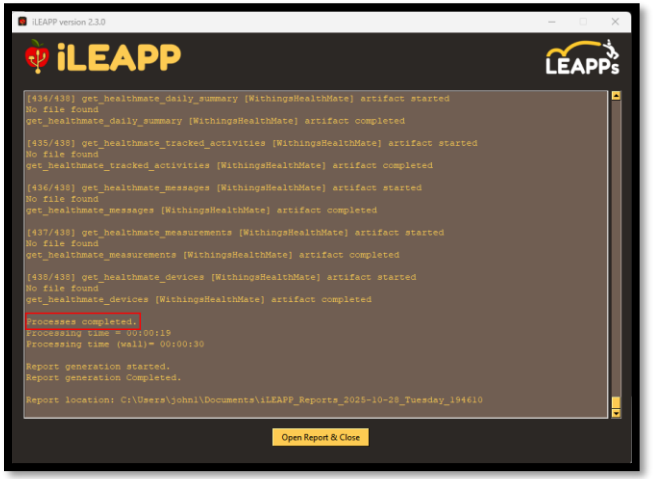
FIGURE 3: SETTINGS



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

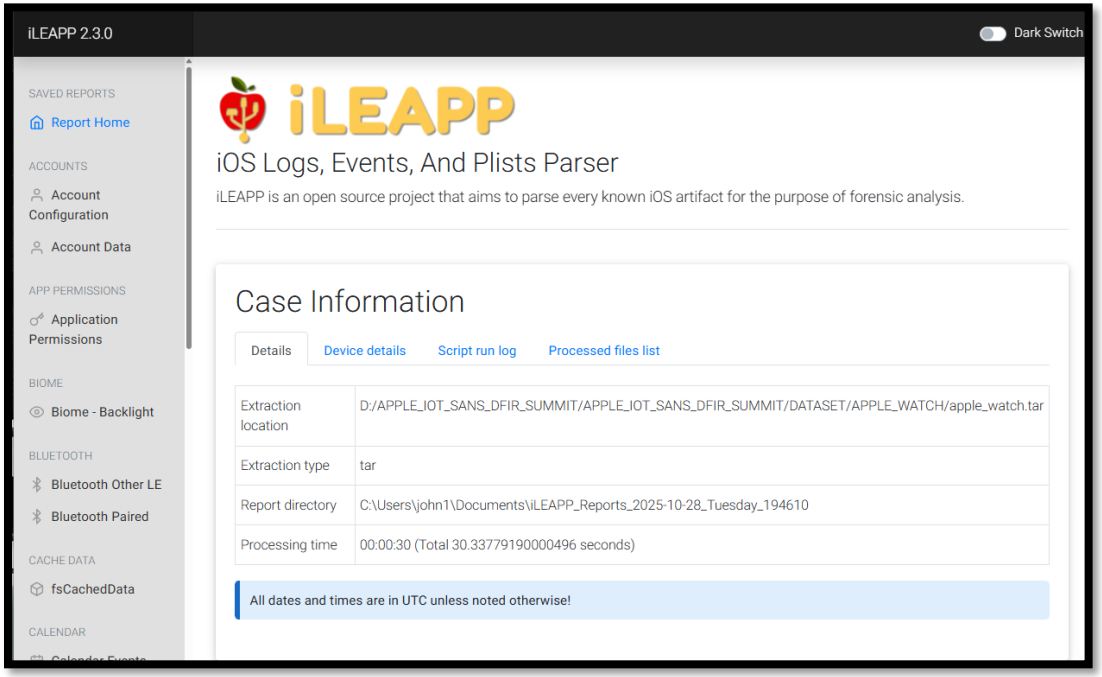
FIGURE 4: iLEAPP DATA UPLOAD





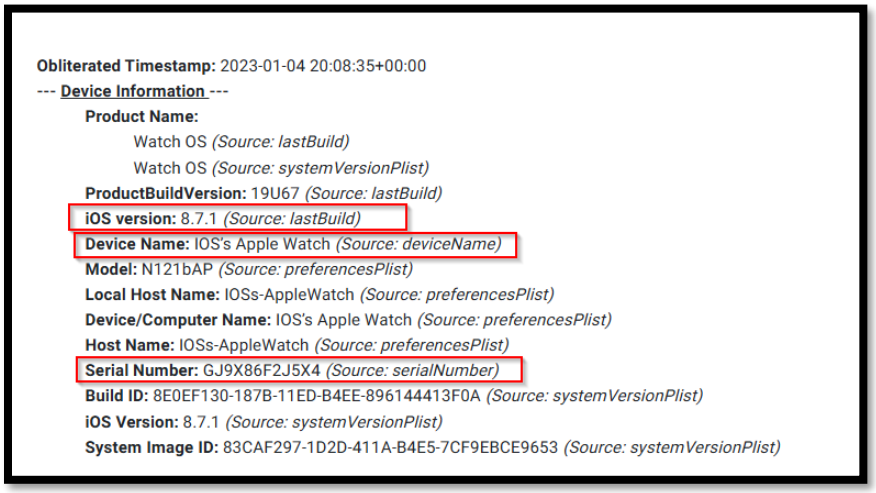
After the data is processed, iLEAPP produces a report which allows you to parse through numerous artifact information such as Account Configuration, Device Details, Calendar Events, etc as seen in Figure 5.

FIGURE 5: iLEAPP REPORT



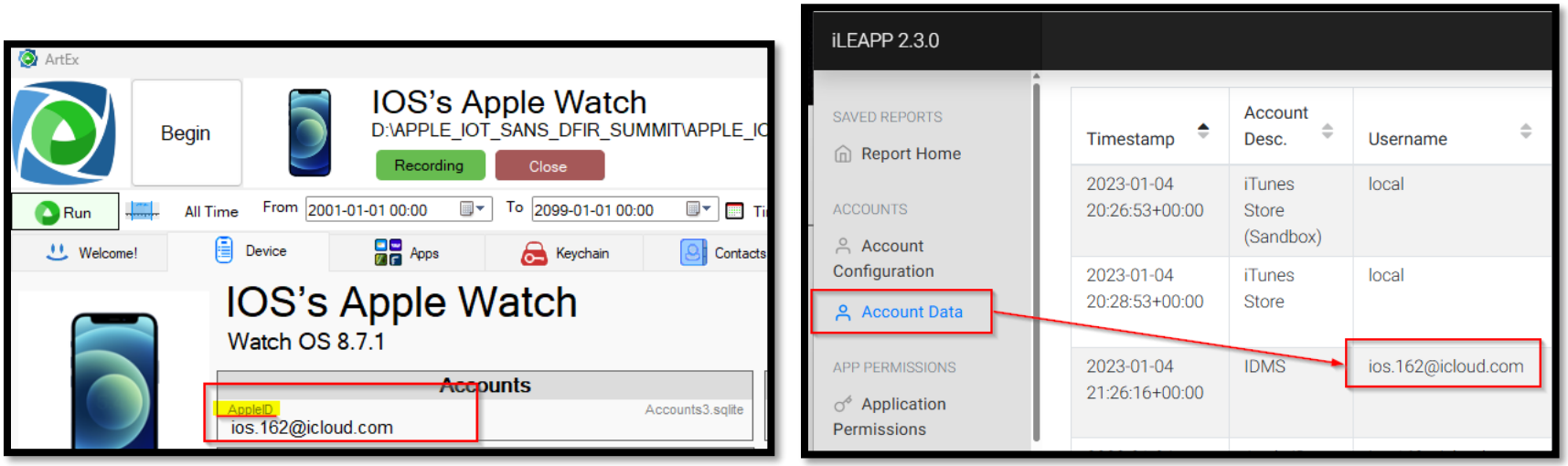
Using both software's allowed me to analysis the artifacts obtained from both ArtEx and iLEAPP to answer the lab questions. The serial number, device name, and WatchOS version of the Apple Watch (GJ9X86F2J5X4) was obtained from the iLEAPP report as displayed in FIGURE 6.

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



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

FIGURE 7: USERS ICLOUD ACCOUNT



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.

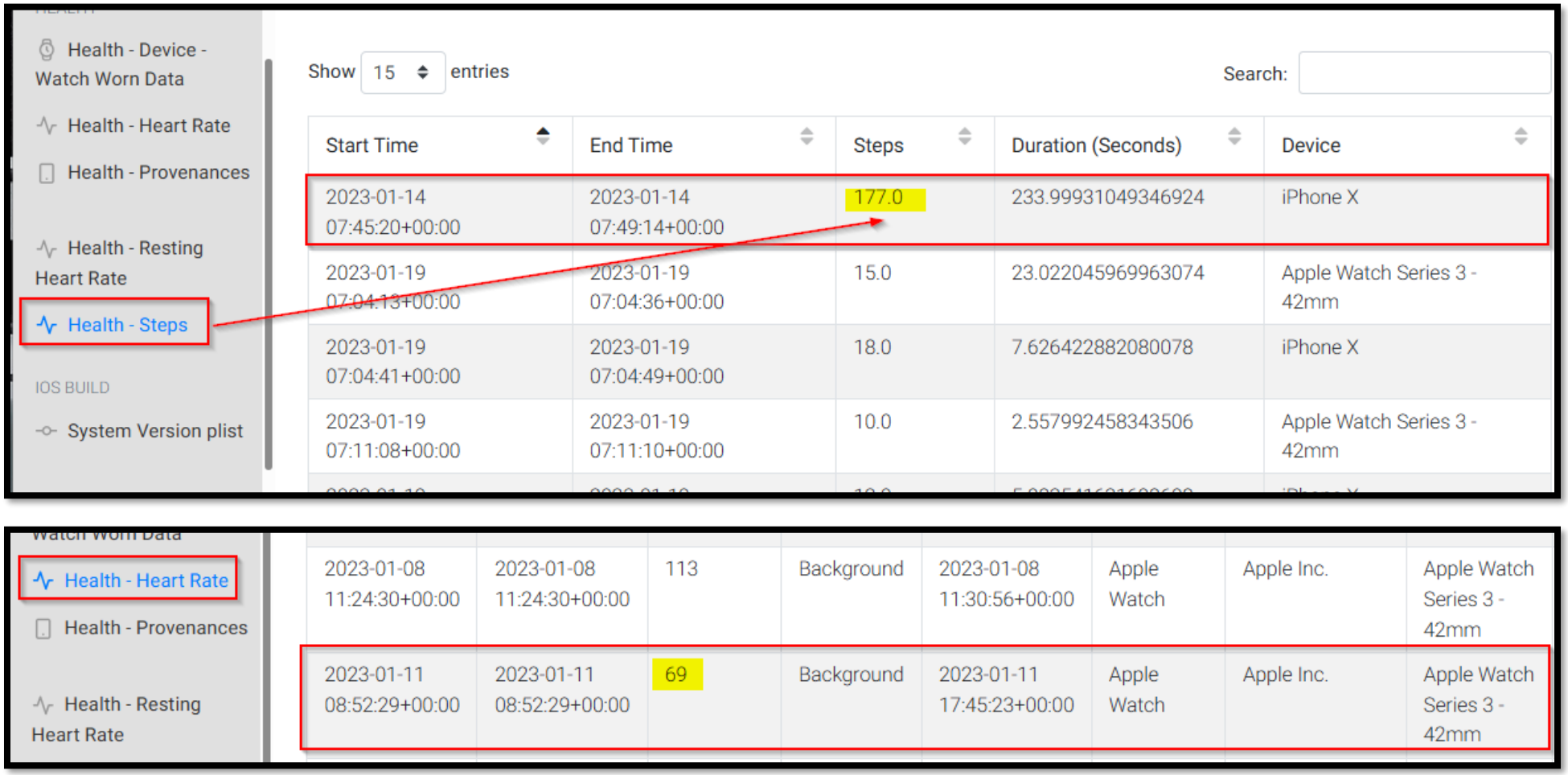
FIGURE 9: USER INSTANT MESSAGING APPS

Icon	Start Time	End Time	Activity	Meta Data
	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 Versio
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

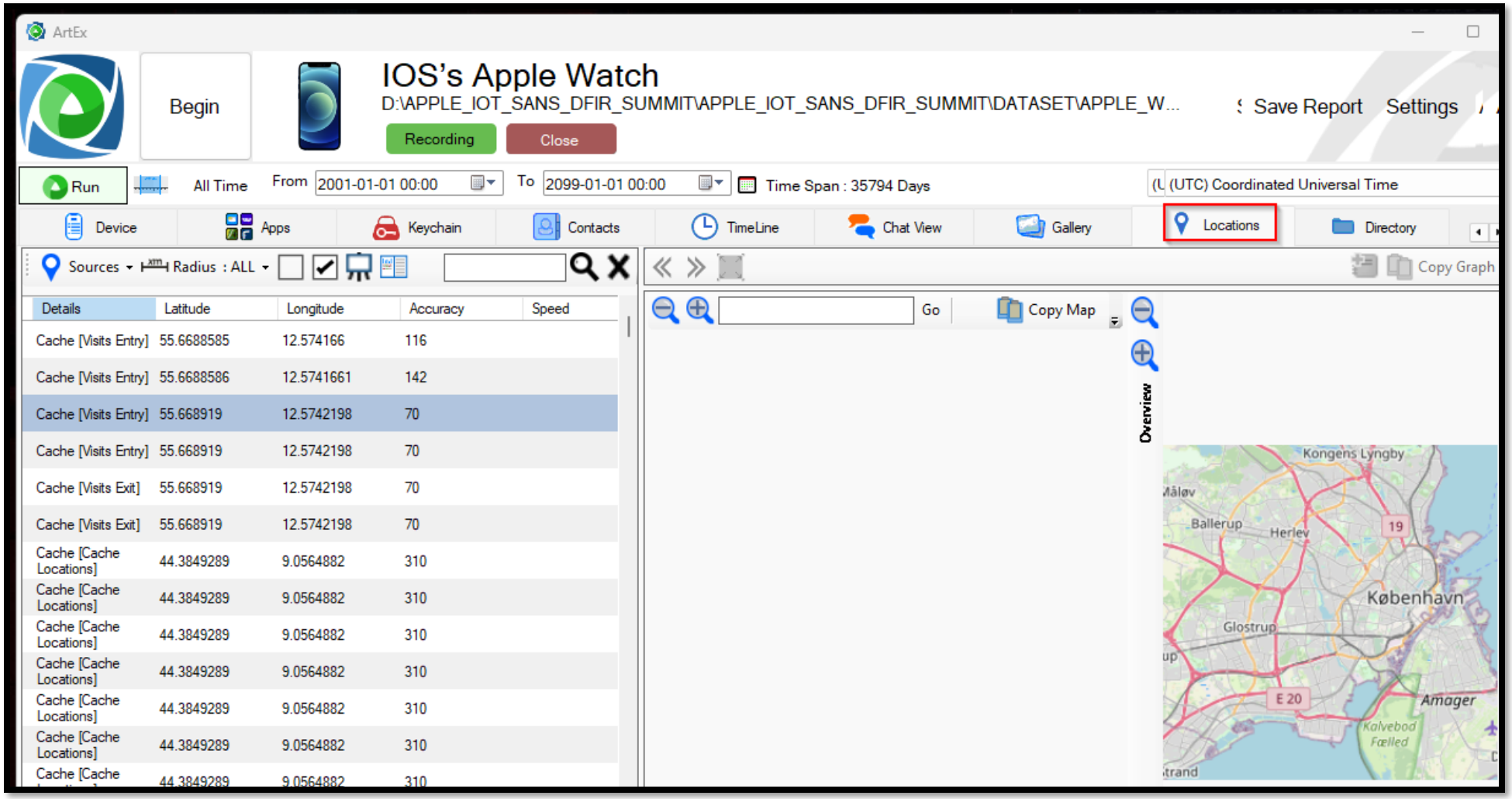
Health information such as how many steps the user took on January 14th, 2023, between 7:45:20 AM and 7:49:14 AM UTC (177 steps) and the users heart rate on January 11th at 8:52:29 AM UTC (69bpm) was obtained from iLEAPP as seen in Figure 10.

FIGURE 10: USER HEALTH STEPS AND HEART RATE



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

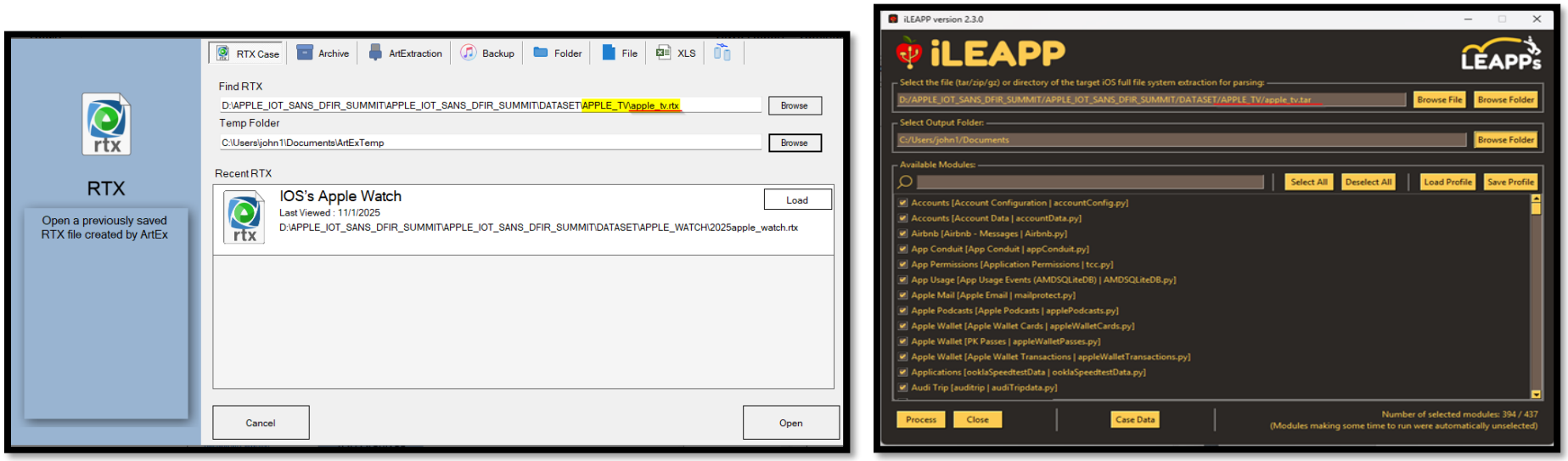
FIGURE 11: USER TRAVELS



APPLE TV ANALYSIS

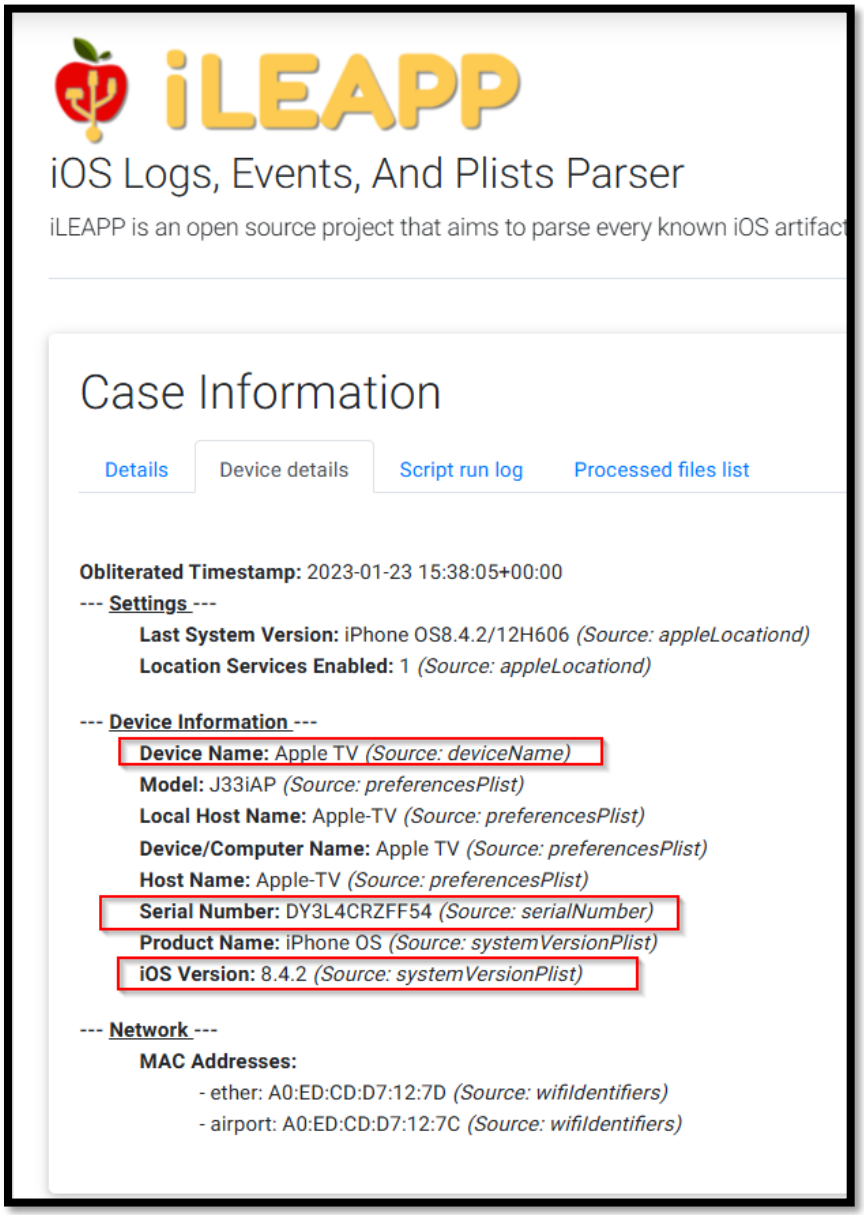
To start analysis, ArtExaminer and iLEAPP was used to upload the data for processing and analysis regarding the Apple TV as seen in Figure 1.

FIGURE 1: APPLE TV ANALYSIS SETUP



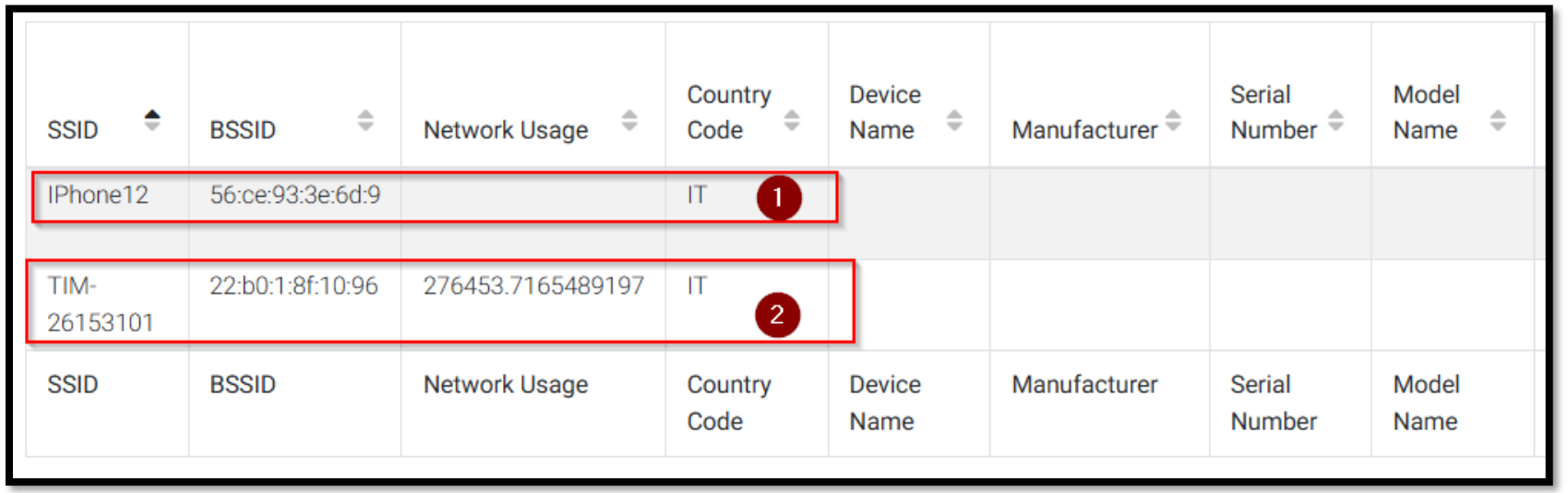
Analyzing the report output from iLEAPP displayed the Apple TV serial number (DY3L4CRZFF54), device name (Apple TV) and OS version (8.4.2) as seen in Figure 2.

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

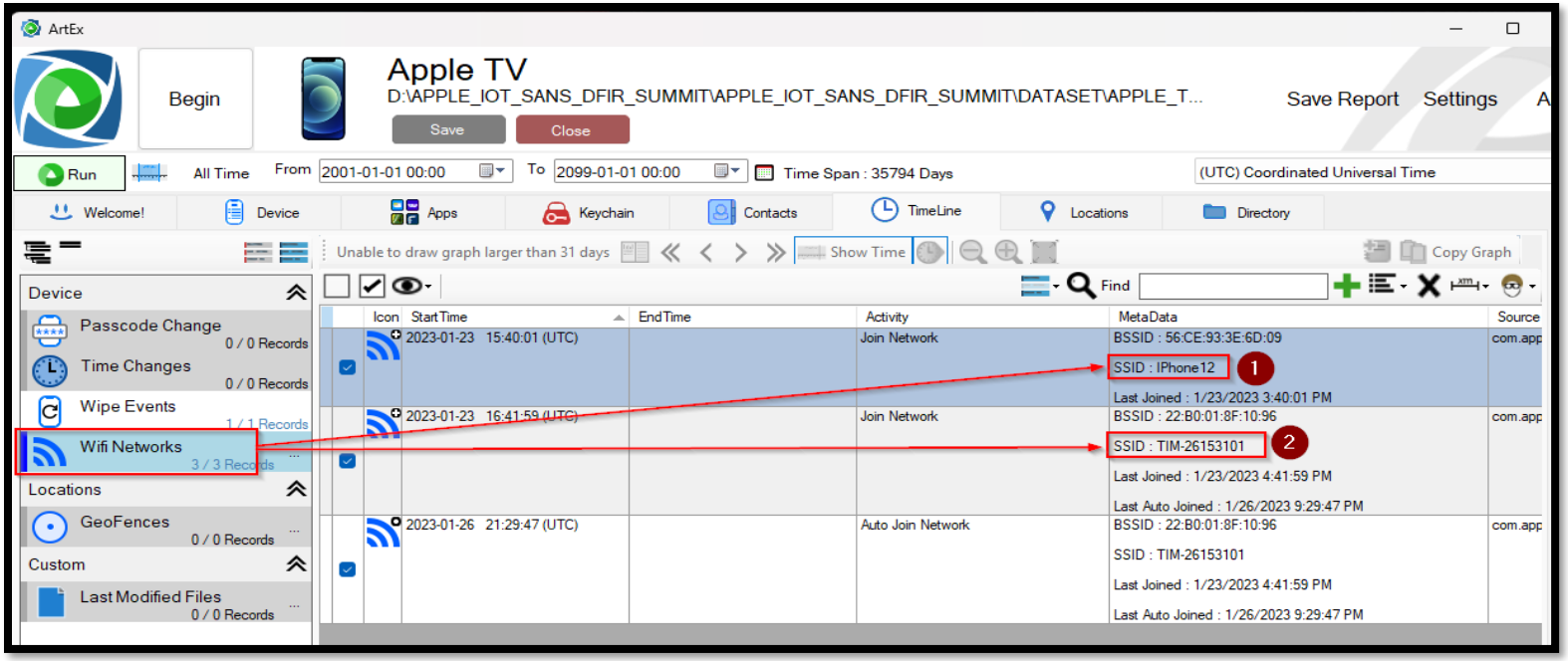


The given iLEAPP report was used to gain the which Wi-Fi networks was the device connected (iPhone 12, TIM-26153101) as well as the data output from ArtEx as seen in Figure 3.

FIGURE 3: DEVICE WIFI CONNECTIONS

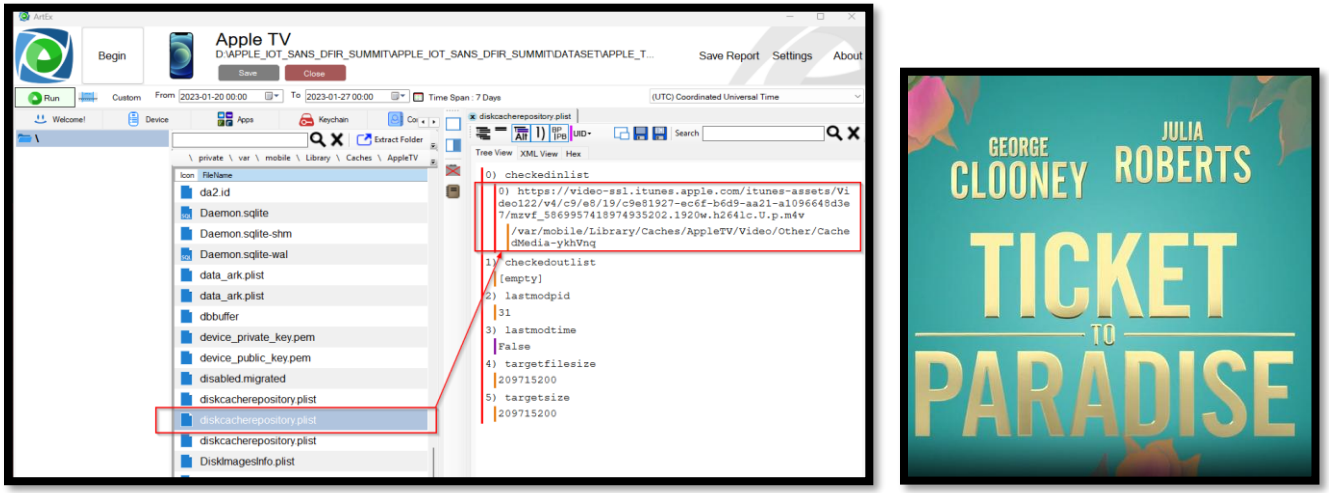


SSID	BSSID	Network Usage	Country Code	Device Name	Manufacturer	Serial Number	Model Name
IPhone12	56:ce:93:3e:6d:9		IT 1				
TIM-26153101	22:b0:1:8f:10:96	276453.7165489197	IT 2				
SSID	BSSID	Network Usage	Country Code	Device Name	Manufacturer	Serial Number	Model Name



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

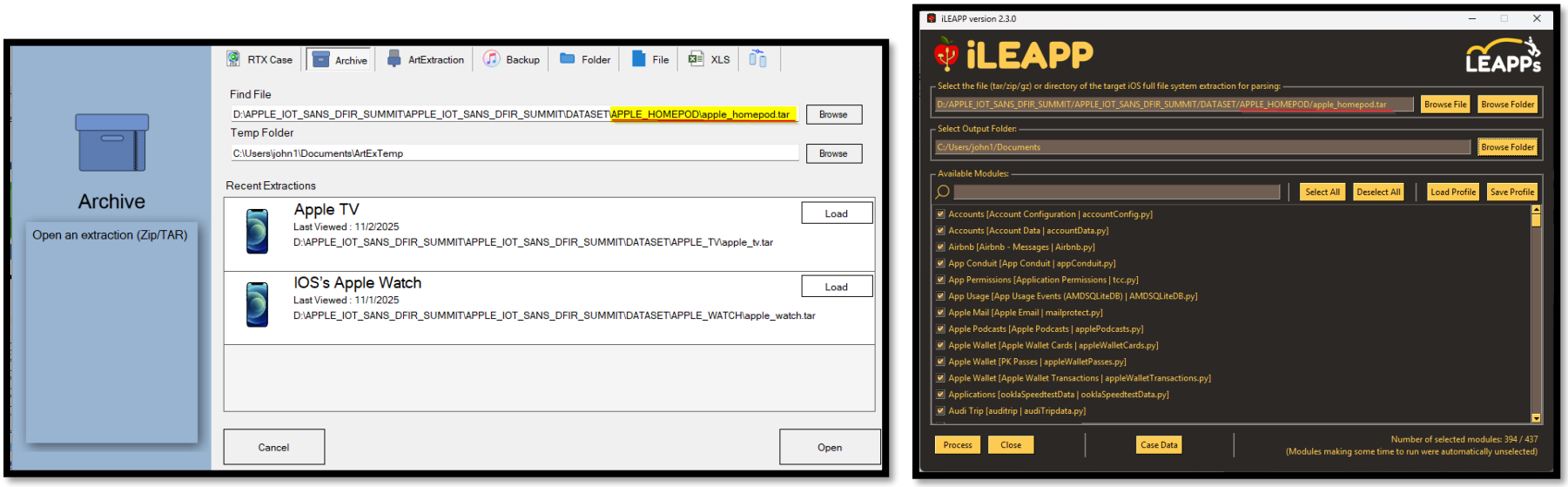
FIGURE 4: LAST MOVIE PREVIEWED ON DEVICE



APPLE HOMEPOD ANALYSIS

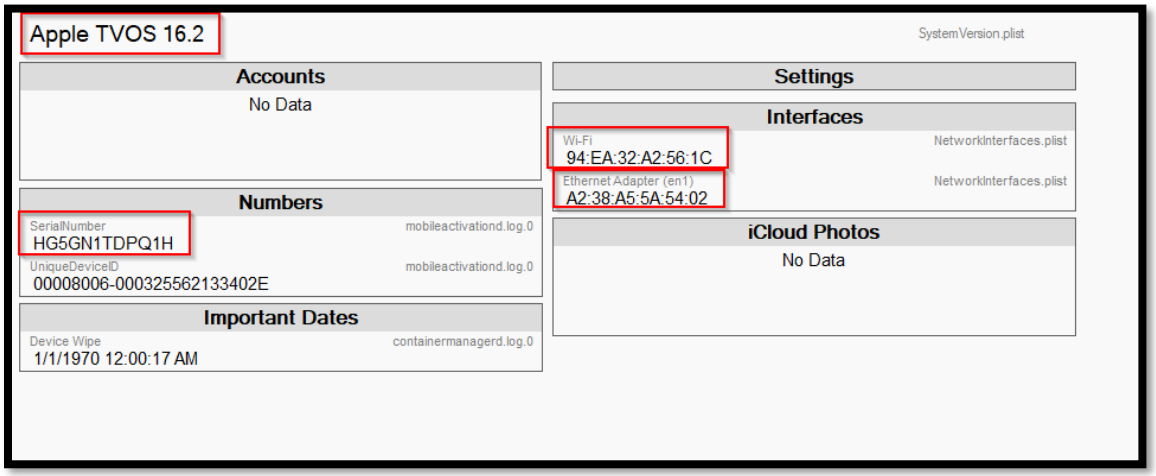
To start analysis, ArtExaminer and iLEAPP was used to upload the data for processing and analysis regarding the Apple HomePod as seen in Figure 1.

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



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

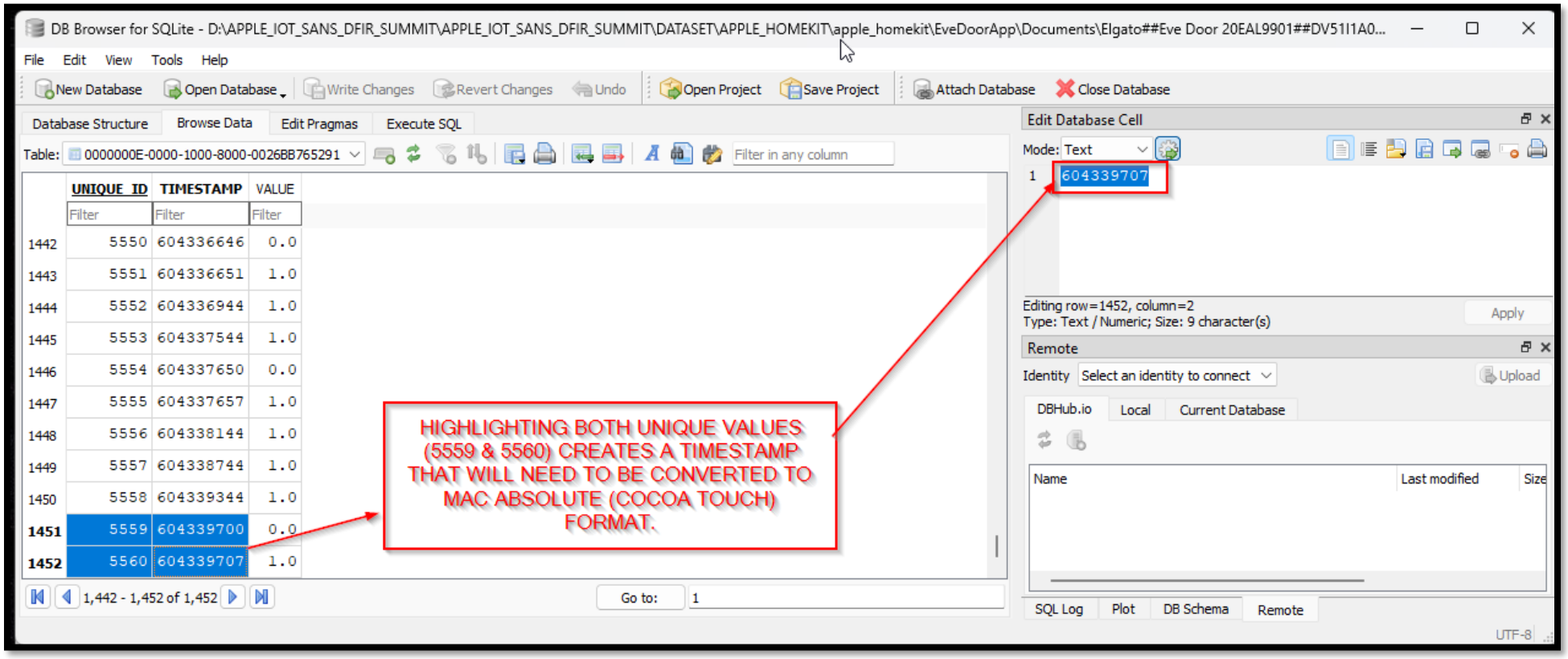
FIGURE 3: DEVICE WIFI NETWOK CONNECTION

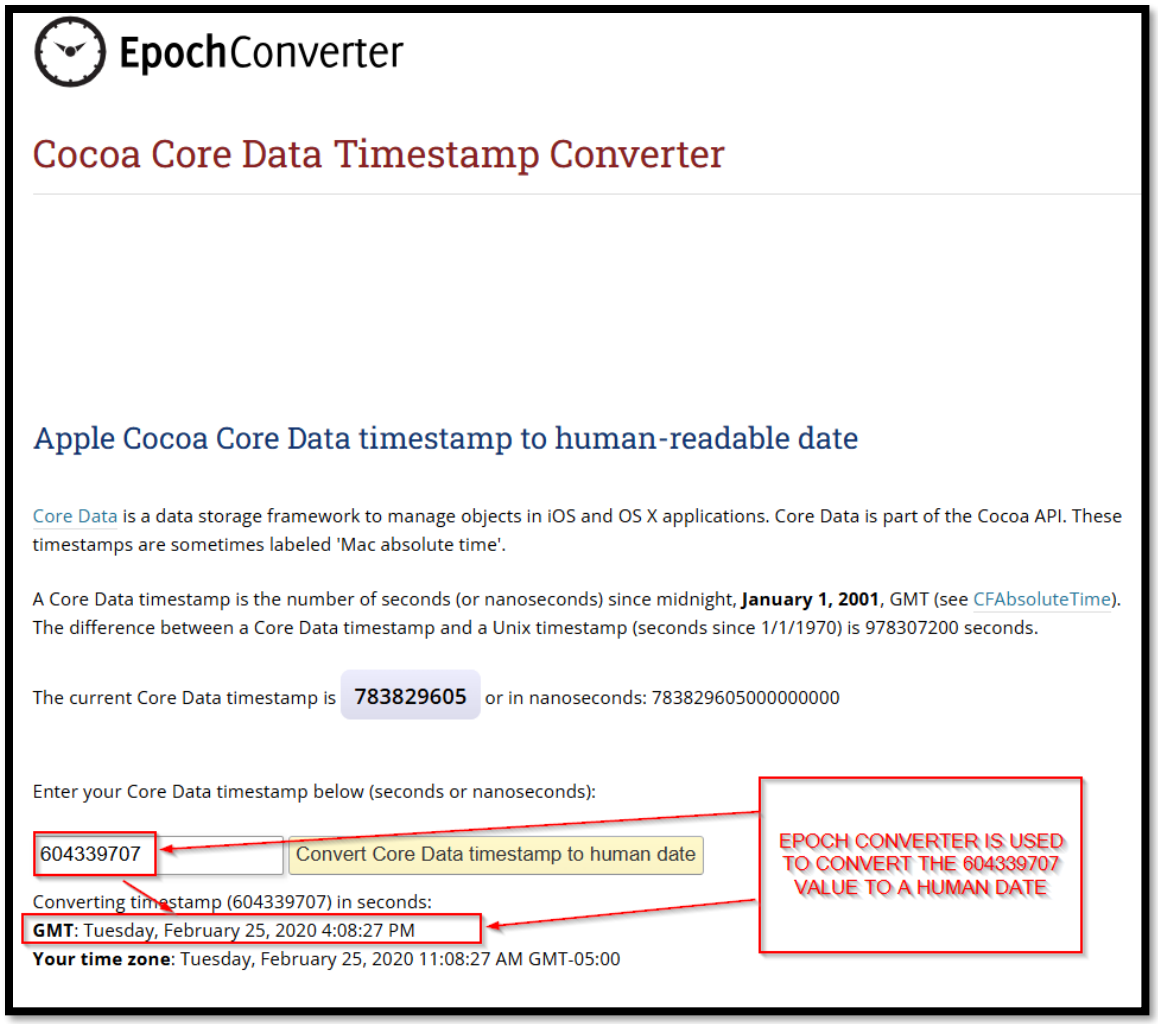
SSID	BSSID	Network Usage	Country Code	Device Name	Manufacturer	Serial Number	Model Name	Enabled
TIM-26153101	22:b0:1:8f:10:96							
SSID	BSSID	Network Usage	Country Code	Device Name	Manufacturer	Serial Number	Model Name	Enabled

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




EpochConverter
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