

**Assignment 4.1: Analyze a Cell Phone Image**

**Joshua A. Wortz**

**University of San Diego**

**CSOL-590**

**Prof. Fulton**

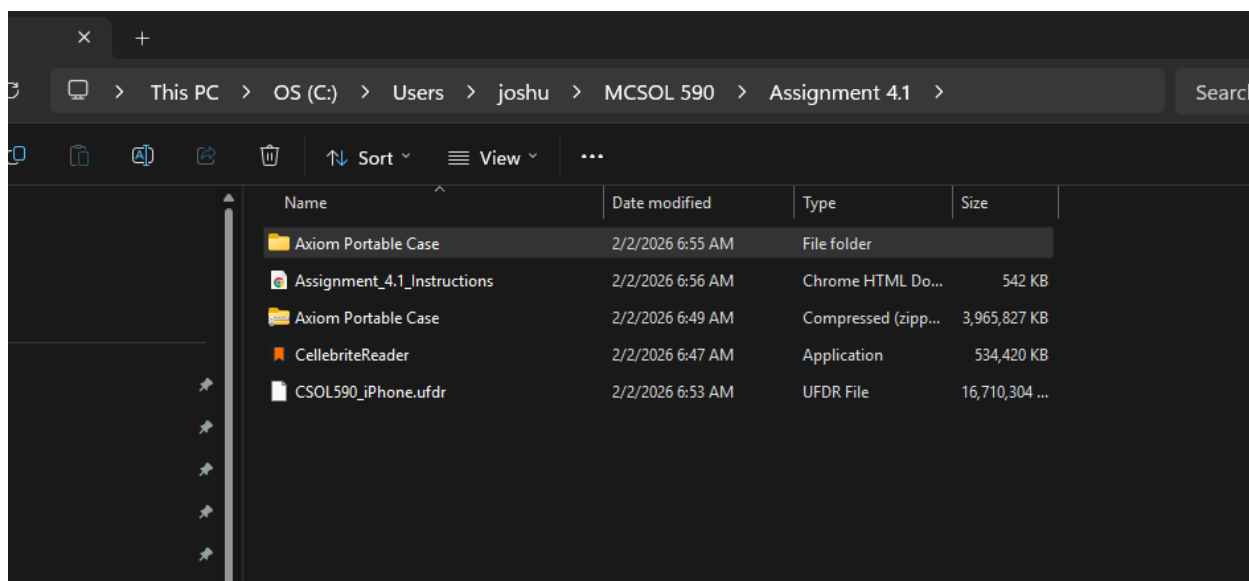
**02/02/2026**



## Part I - Cellebrite reports and questions

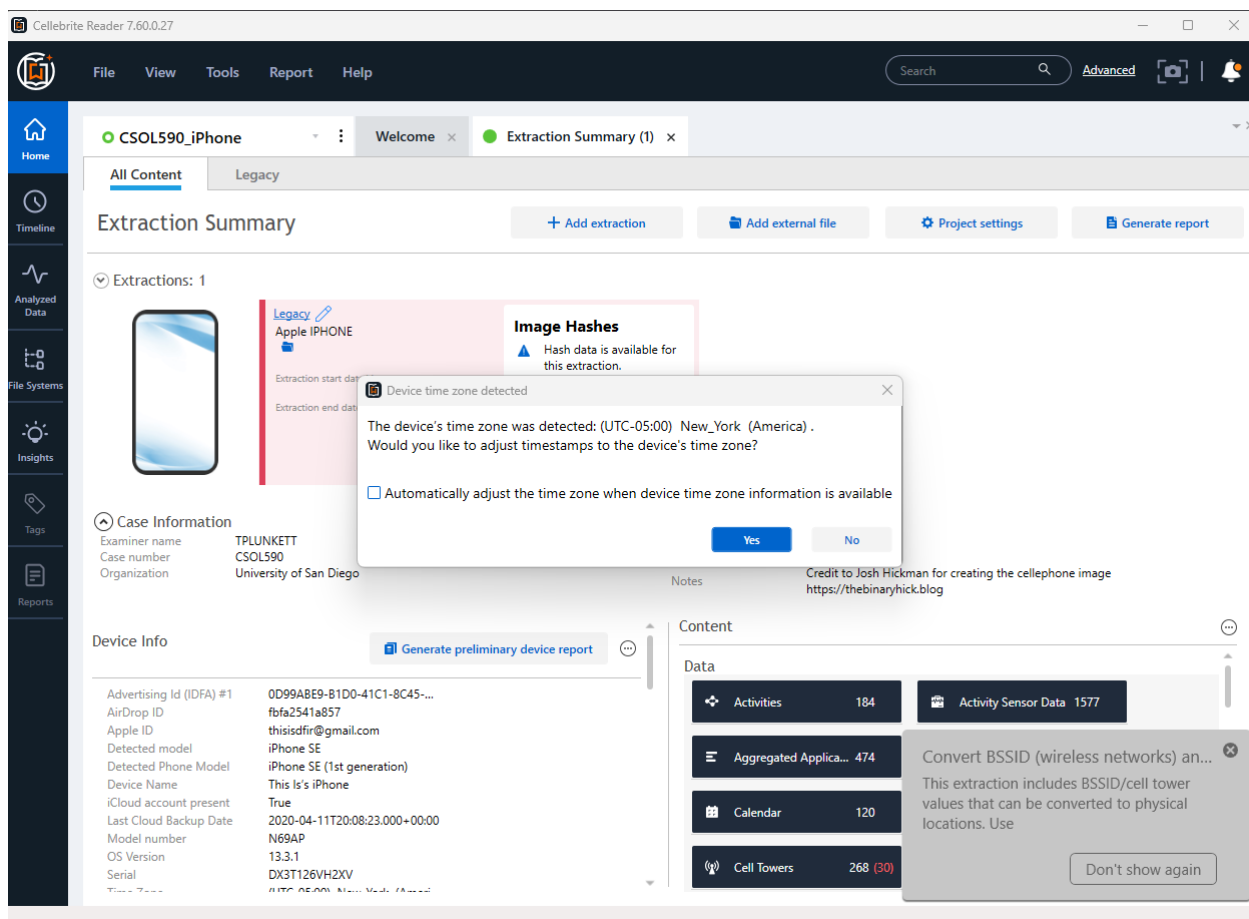
### Review in Cellebrite Reader

*Figure 1*



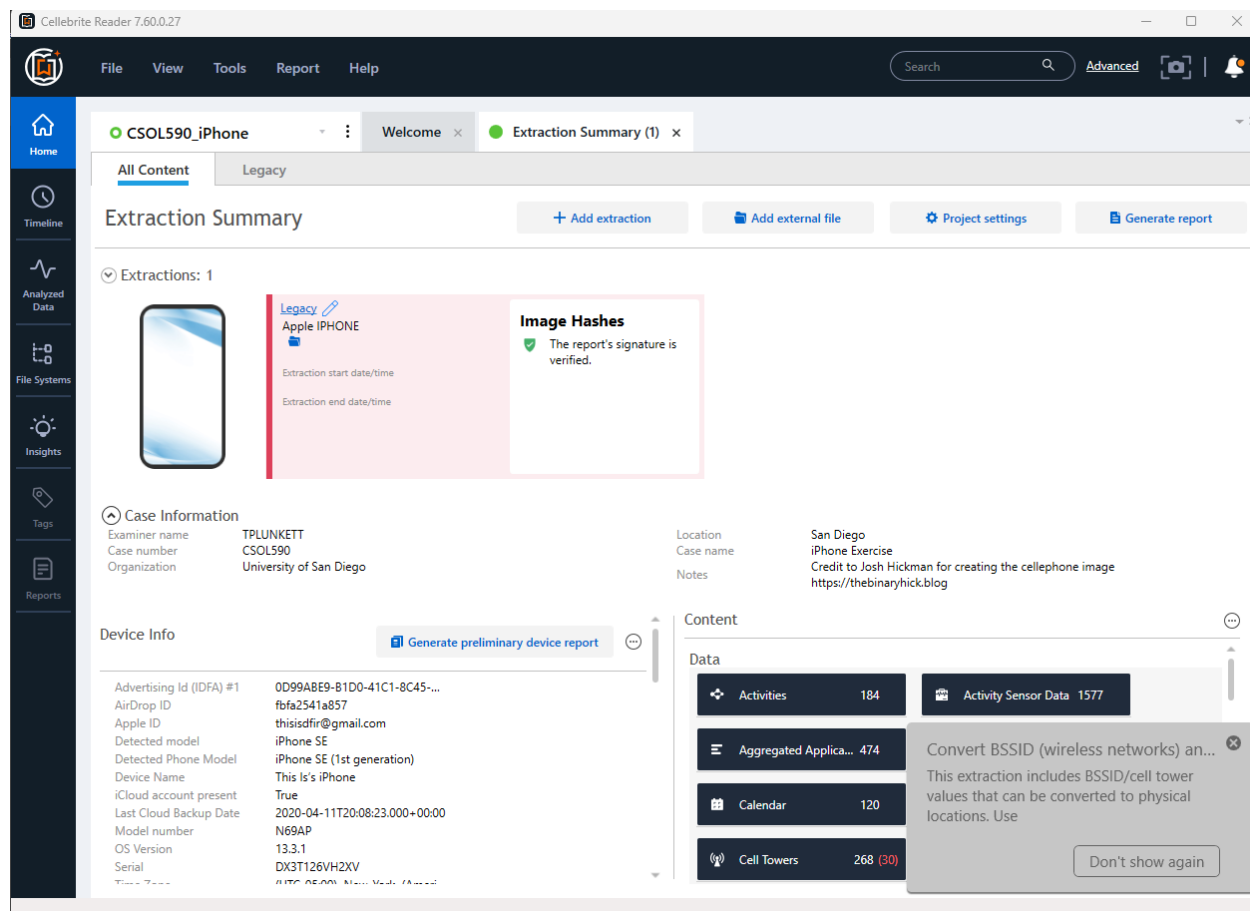
Downloaded and extracted the lab files locally.

Figure 2



After opening CSOL590\_iPhone.ufdr, adjust the time zone to match the device.

Figure 3



Verified image Hash to ensure that the image is still unmodified.

### ***Preliminary Device Report***

Report generated, see the separate attached documentation.

1. What is the Message Retention Duration for this phone?

Forever

2. What is the AppleID used on this phone?

thisisdfr[.]gmail[.]com

3. What is the phone number of this phone? The phone number is the same as the Mobile Subscriber Integrated Services Digital Network (MSISDN) number for the SIM card.

+19195794674

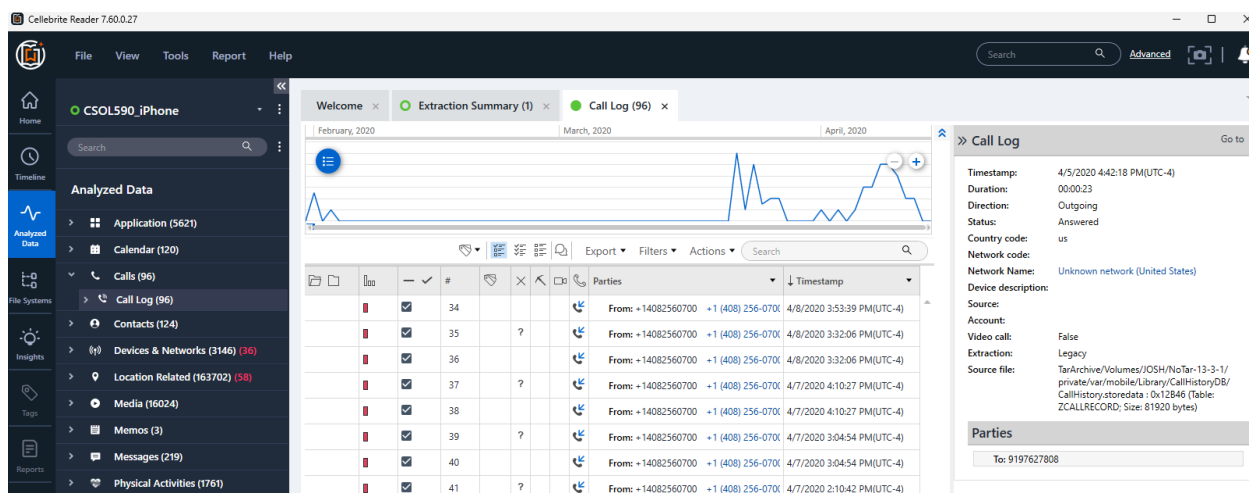
4. What is the name of the computer last used to back up this phone?

Joshua's Mac mini

## Analyzed Data

### Call Logs

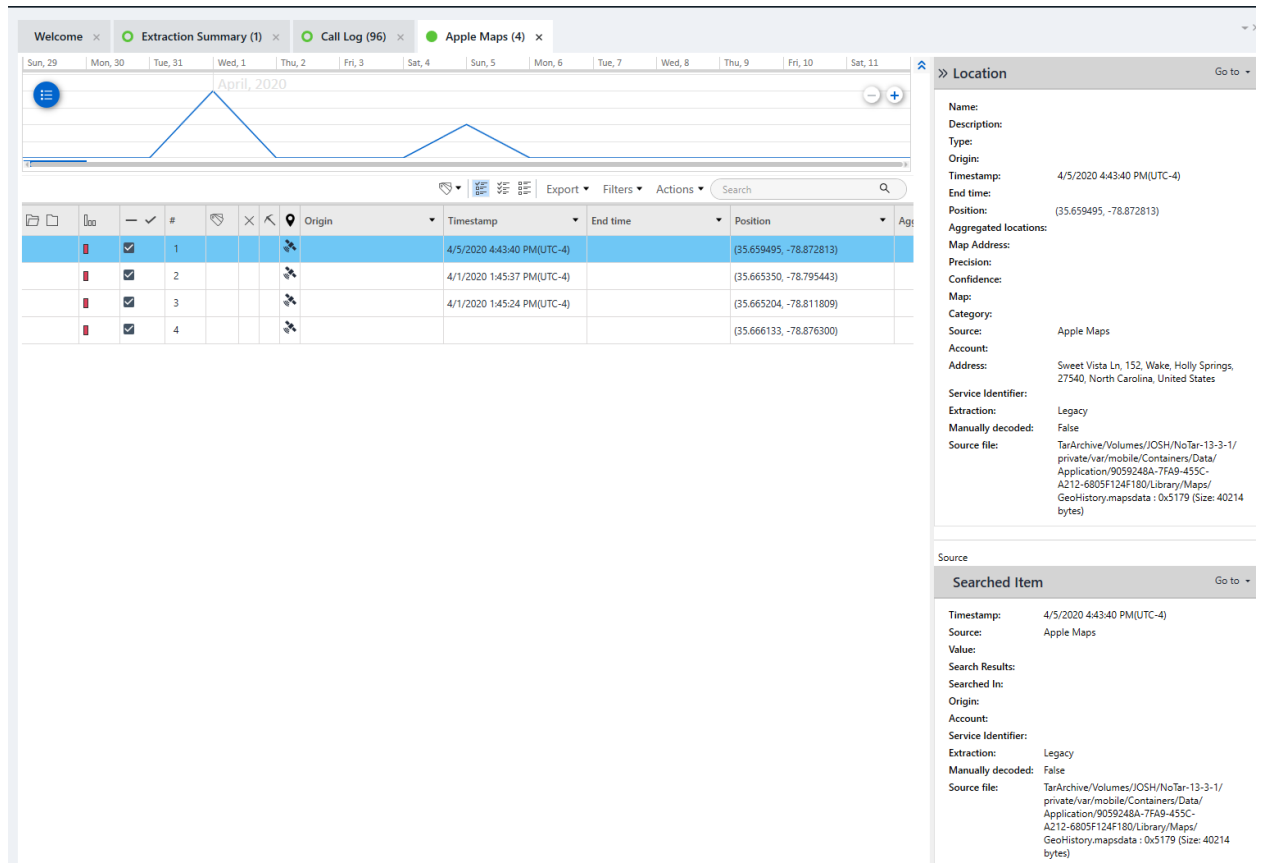
Figure 4



Outgoing phone call at 4/5/2020 4:42:18 PM(UTC-4) that was 23 seconds long.

## Maps

Figure 5



Apple Maps entry on 4/5/2020 4:43:40 PM(UTC-4) at address Sweet Vista Ln, 152, Wake, Holly Springs, 27540, North Carolina, United States.

## Chats/Photos

Figure 6

The screenshot displays the Cellebrite Reader 7.600.27 interface. The left sidebar shows the 'Analyzed Data' section for 'CSOL590\_iPhone'. The main window is divided into three panes: a top pane showing 'No event with timestamp to present', a middle pane displaying a table of participants, and a right pane showing a chat conversation.

**Participants Table:**

| Participant ID            | Participant Name | Start Time                 | Last Activity               |
|---------------------------|------------------|----------------------------|-----------------------------|
| live.cid.6cd30ff00343405b | Josh Hickman     | 2/1/2020 4:18:32 PM(UTC-5) | 4/11/2020 2:07:47 PM(UTC-5) |
| live.cid.832804f1252ed962 | Thisis DFIR      | 2/1/2020 4:09:56 PM(UTC-5) | 2/1/2020 4:11:02 PM(UTC-5)  |

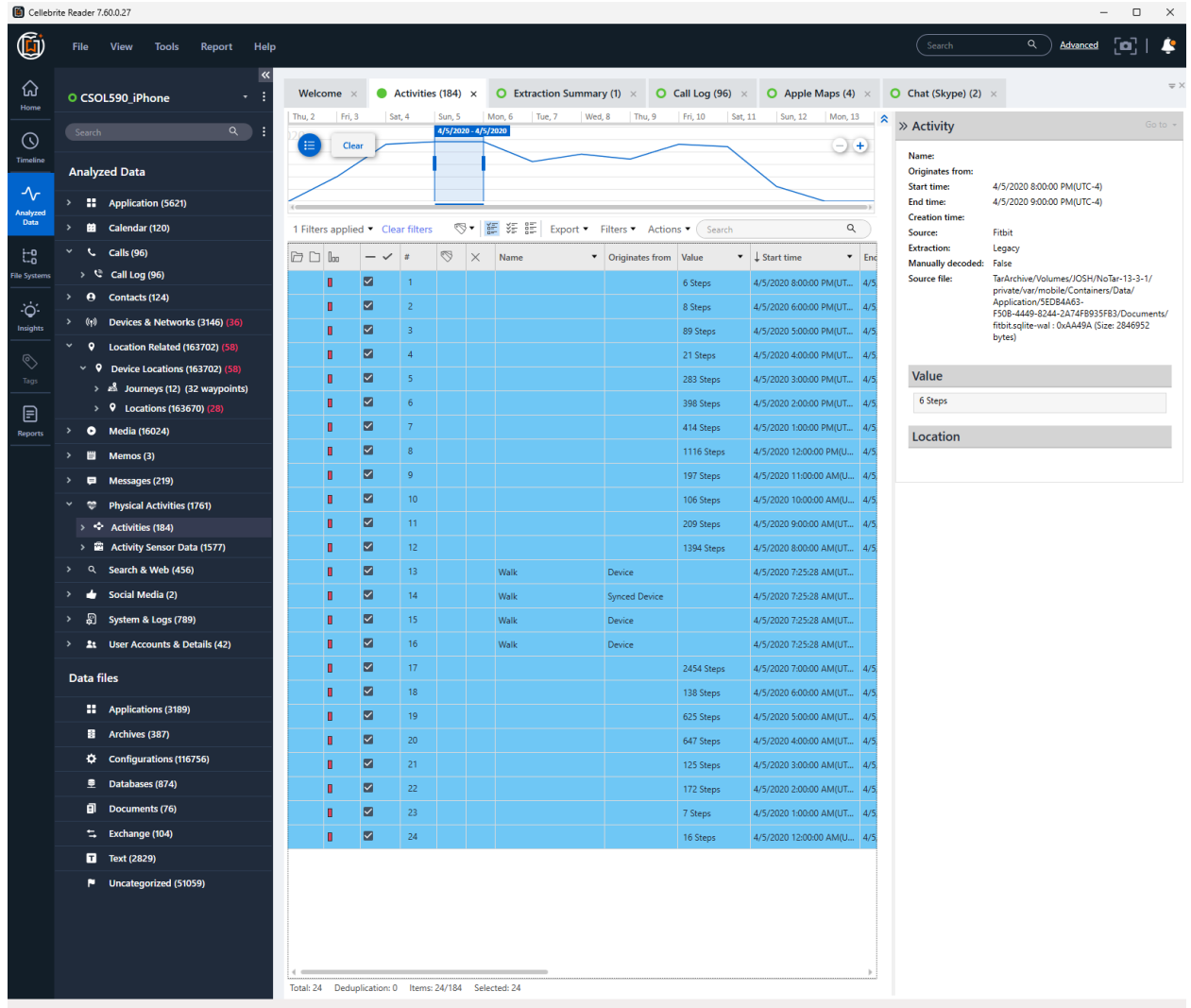
**Chat Conversation:**

- Josh Hickman:** "Ok. No rush. I know there were a few things to document." (3/24/2020 9:12:33 AM(UTC-4))
- Thisis DFIR:** [Image of a man holding a sign] (3/24/2020 9:13:24 AM(UTC-4))
- Josh Hickman:** [Image of a man holding a sign] (3/24/2020 9:16:14 AM(UTC-4))
- Thisis DFIR:** "That is the truth!" (3/24/2020 9:17:12 AM(UTC-4))
- Thisis DFIR:** [Image of a man holding a sign] (4/11/2020 2:07:47 PM(UTC-4))

Skype message sent from Josh Hickman on 3/24/2020 9:16:14 AM(UTC-4) with a photo of a man wearing glasses holding a sign that says “Stop asking me to try YouTube Premium”.

## Activities

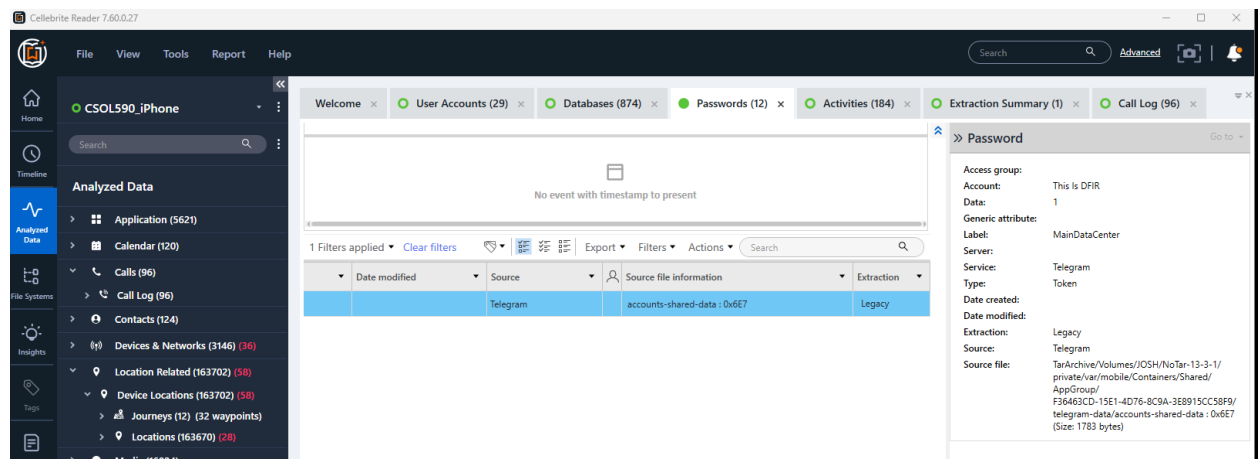
Figure 7



On 4/5/2020, 8,403 steps were recorded via Fitbit.

Passwords

Figure 8



The Telegram user's account name is “This Is DFIR,” and the password is “1”.

Export report

Report generated, see separate attached document.

## Part II - Axiom reports and questions

### Call logs

Figure 9

Magnet AXIOM Examine v5.10.0.30634 - CSOL-590-CellPhone

File Tools Process Help

**FILTERS** Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone

Media categorization Media attributes (VICS)

Type a search term... GO ADV

Column view

**EVIDENCE (81)**

| Type       | Call Status      | Call Date/Time              | Call... | Application...      | Partner Lo...     |
|------------|------------------|-----------------------------|---------|---------------------|-------------------|
| ie         | 49 (not parsed)  | 1/25/2002 7:32:05 PM        | 0       |                     |                   |
| ie         | 48 (not parsed)  | 1/25/2002 7:32:06 PM        | 0       |                     |                   |
| ie         | 49 (not parsed)  | 1/25/2002 7:32:06 PM        | 0       |                     |                   |
| ie         | -35 (not parsed) | 1/25/2002 7:34:08 PM        | 0       |                     |                   |
| ie         | -35 (not parsed) | 1/25/2002 7:34:08 PM        | 0       |                     |                   |
| Time Video | Answered         | 2/9/2002 3:23:50 AM         | 22      |                     |                   |
| Time Video | Answered         | 2/9/2002 3:23:50 AM         | 22      |                     |                   |
| Time Video | Answered         | 7/2/2002 4:41:16 AM         | 15      |                     |                   |
| ie         | Answered         | 8/6/2002 9:00:48 AM         | 1       |                     |                   |
| ie         | Answered         | 8/6/2002 9:01:03 AM         | 1       |                     |                   |
| ie         |                  | 2/16/2003 12:33:52 PM       | 0       |                     |                   |
| Time Video | Unanswered       | 2/17/2003 6:37:39 AM        | 0       |                     |                   |
| ie         |                  | 9/2/2003 12:44:15 PM        | 0       |                     |                   |
| ie         |                  | 3/11/2004 3:18:09 PM        | 255     |                     |                   |
| ie         |                  | 3/11/2004 3:18:09 PM        | 255     |                     |                   |
| Time Video |                  | 3/26/2004 8:44:54 PM        | 51      |                     |                   |
| ie         | Answered         | 9/21/2004 2:26:12 AM        | 1       |                     |                   |
| ie         |                  | 23218964271889 (not parsed) | 3       |                     |                   |
| ie         | Unanswered       | 6/16/2013 1:46:57 AM        | 0       |                     |                   |
| Time Video | Answered         | 8/2/2018 7:22:41 AM         | 3       |                     |                   |
| Time Video | Answered         | 8/2/2018 7:22:41 AM         | 3       |                     |                   |
| ie         | Unanswered       | 3/23/2020 4:02:52 PM        | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 3/24/2020 1:37:18 PM        | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 3/26/2020 1:51:45 PM        | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 3/27/2020 12:25:36 PM       | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 3/27/2020 3:55:03 PM        | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 4/1/2020 4:06:38 PM         | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 4/3/2020 12:10:54 PM        | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Answered         | 4/5/2020 4:42:18 PM         | 23      | com.apple.Telephony | Fuquay-Varina, NC |
| ie         | Unanswered       | 4/6/2020 4:34:33 PM         | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 4/6/2020 5:48:08 PM         | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 4/6/2020 6:43:00 PM         | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 4/7/2020 2:10:42 PM         | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 4/7/2020 3:04:54 PM         | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 4/7/2020 4:10:27 PM         | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 4/8/2020 3:32:06 PM         | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 4/8/2020 3:53:39 PM         | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 4/8/2020 4:21:59 PM         | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 4/8/2020 6:12:22 PM         | 0       | com.apple.Telephony | San Jose, CA      |
| ie         | Unanswered       | 4/8/2020 6:17:45 PM         | 0       | com.apple.Telephony | San Jose, CA      |

**Local User <13-3-1.tar>**

**13-3-1.tar**

**DETAILS**

**ARTIFACT INFORMATION**

Local User: Local User <13-3-1.tar>

Partners: 9197627808

Direction: Outgoing

Call Type: Phone

Call Status: Answered

Call Date/Time: 4/5/2020 4:42:18 PM

Call Duration (Seconds): 23

Application Name: com.apple.Telephony

Partner Location: Fuquay-Varina, NC

Service Provider Country Code: US

Artifact type: iOS Call Logs

Item ID: 6459

**EVIDENCE INFORMATION**

Source: 13-3-1.tar\Volumes\IOSH1NoTar-13-3-1\private\var\mobile\Library\CallHistoryDB\CallHistory.storedata

Recovery method: Parsing

Deleted source: Table: ZCALLRECORD (Z\_PK: 31)

Location: Table: ZREMOVEDPARTICIPANT HANDLES(rowid: 31)

Table: ZHANDLE(Z\_PK: 31)

Evidence number: 13-3-1.tar

Call log on 4/5/2020 4:42:18 PM showing Partner Location is Fuquay-Varina, NC.

Figure 10

Magnet AXIOM Examine v5.10.0.30634 - CSOL-590-CellPhone

File Tools Process Help

FILTERS Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone

Type a search term... GO ADVANCED

Media categorization Media attributes (VICS)

Artifacts

- LINE Messages 30
- LINE Pictures 1
- Skype Activity 27
- Skype Contacts 4
- Snapchat Chat Messages 14
- Snapchat Contacts 2
- Snapchat Memories 11
- Snapchat Stories - iOS 1
- Telegram Chats - iOS 2
- Telegram Messages - iOS 20
- Telegram Users - iOS 4
- Textfree Messages / Calls 4
- TextPlus Messages 1
- Viber Messages 10
- WeChat Friends 1
- Zoom Chat Messages 6
- Zoom Contacts 2

**SOCIAL NETWORKING 1,065**

**MEDIA 28,380**

**EMAIL & CALENDAR 797**

**EVIDENCE (4)**

| Timestamp Date/Time   | Latitude         | Longitude         | Artifact type        | Source                           |
|-----------------------|------------------|-------------------|----------------------|----------------------------------|
| 4/1/2020 2:12:48 PM   | 35.6594619129684 | -78.8726180602014 | Parked Car Locations | 13-3-1.tar\Volumes\UOSH\NoTar... |
| 4/4/2020 6:20:36 PM   | 35.6595250849876 | -78.8727674502324 | Parked Car Locations | 13-3-1.tar\Volumes\UOSH\NoTar... |
| 4/5/2020 4:55:29 PM   | 35.6594874386797 | -78.872669079253  | Parked Car Locations | 13-3-1.tar\Volumes\UOSH\NoTar... |
| 4/12/2020 10:27:43 AM | 35.6594921660079 | -78.8726052862633 | Parked Car Locations | 13-3-1.tar\Volumes\UOSH\NoTar... |

Column view

**4/5/2020 4:55:29 PM**

13-3-1.tar

**WORLD MAP PREVIEW**

**DETAILS**

**ARTIFACT INFORMATION**

Timestamp Date/Time 4/5/2020 4:55:29 PM

Latitude 35.6594874386797

Longitude -78.872669079253

Artifact type **Parked Car Locations**

Item ID 35070

**EVIDENCE INFORMATION**

Source 13-3-1.tar\Volumes\UOSH\NoTar-13-3-1\private\var\mobile\Library\Caches\com.apple.routined\Local.sqlite

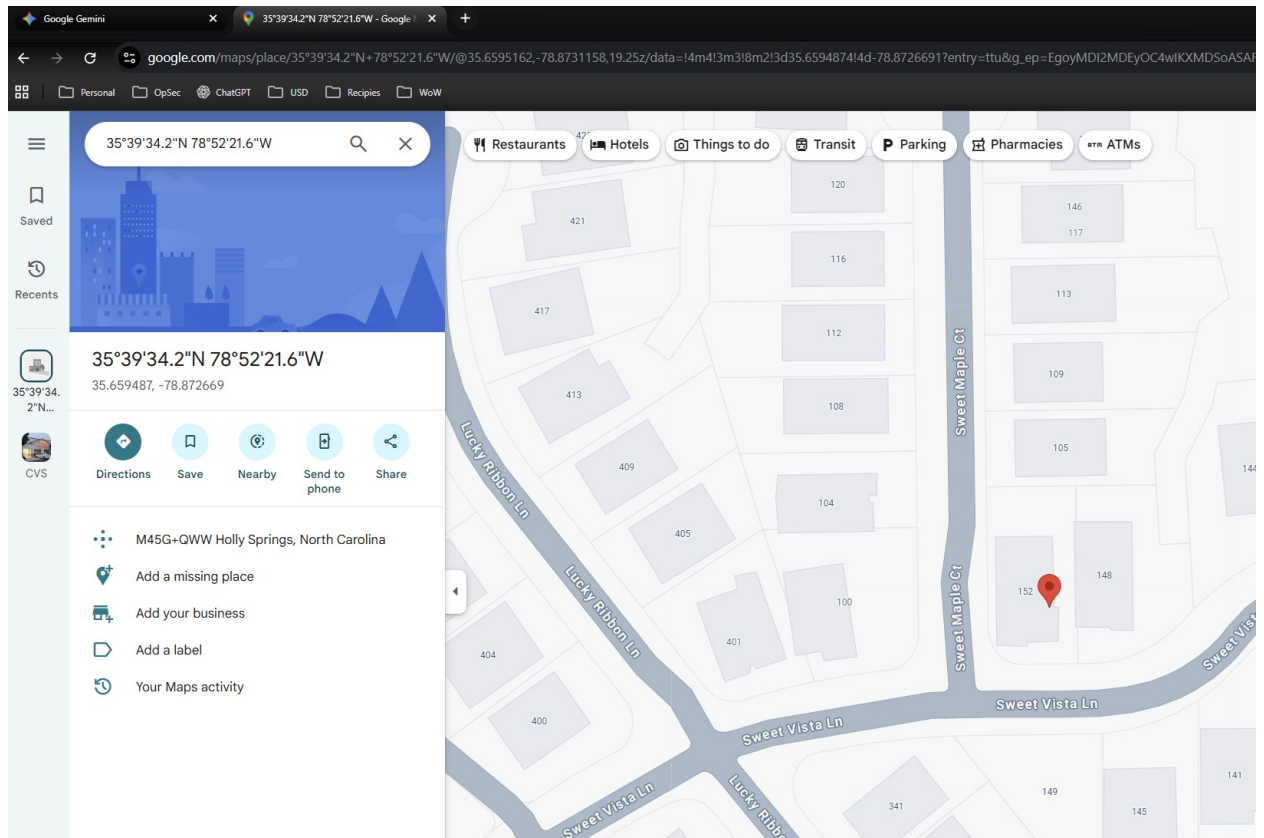
Recovery method **Parsing**

Deleted source

Location Table: ZRTVEHICLEEVENTHISTORYMO (Z\_PK: 19)

Evidence number 13-3-1.tar

Parked Car location on 4/5/2020 at 4:55:29 PM was shown to be at Lat 35.6594874386797 Longitude -78.872669079253.

*Figure 11*

The Latitude and Longitude from the previous search show the car is parked at the corner of Sweet Vista Lane and Sweet Maple Court in Holly Springs, North Carolina.

## Chat Messages

Figure 12

The screenshot displays the Magnet AXIOM Examine v5.10.0.30634 - CSOL-590-CellPhone interface. The left sidebar shows a list of artifacts, with 'Snapchat Chat Messages' selected, showing 14 items. The main pane displays a list of evidence items (14 total) with columns for Sender, Recipient, Message ID, Message Date/Time, and Message. The selected item is a message from 'thisisdfr' to 'hickdawg957' dated 4/11/2020 9:35:07 PM. The right pane shows a preview of the selected message, which reads: 'So I just realized Snapchat has location sharing capabilities.' Below the preview, the details section shows the artifact information, including the sender 'thisisdfr', recipient 'hickdawg957', message ID '85A44C82-8344-4983-AAA4-077C95A31BC3', and message date/time '4/11/2020 9:35:07 PM'.

| Sender      | Recipient   | Message ID                                    | Message Date/Time     | Message                                                  |
|-------------|-------------|-----------------------------------------------|-----------------------|----------------------------------------------------------|
| teamsnachat | thisisdfr   | 251991586702023480r                           | 4/12/2020 10:33:43 AM | https://storage.googleapis.com/broadcasts/Easter_2...    |
| thisisdfr   | hickdawg957 | 81e2a800-fb27-a7e6-5c46-244e39f710e           | 12/1/2018 5:05:16 PM  | I can't get this phone to have any badges over the a...  |
| thisisdfr   | hickdawg957 | 5778923e-05bc-4c2f-2473-fea8351662e6          | 12/1/2018 5:03:42 PM  | My bad.                                                  |
| hickdawg957 | thisisdfr   | 2D79038D-8ED5-4161-8BF1-578345D4D8CE          | 4/11/2020 9:40:02 PM  | Try it tomorrow. Let's just do the calls right now.      |
| hickdawg957 | thisisdfr   | 96FC1ACD-75CD-4357-AB89-964417583678          | 4/11/2020 9:39:06 PM  | Interesting.                                             |
| hickdawg957 | thisisdfr   | 3796CFFA-3E25-4450-A572-870F2C820C46          | 4/11/2020 9:36:04 PM  | It does?                                                 |
| thisisdfr   | hickdawg957 | 28531CFD-C879-4A63-81A3-198A5A297D85          | 4/11/2020 9:38:29 PM  | Yep. I found Snap Map. You can either share your lo...   |
| thisisdfr   | hickdawg957 | 85A44C82-8344-4983-AAA4-077C95A31BC3          | 4/11/2020 9:35:07 PM  | So I just realized Snapchat has location sharing capa... |
| hickdawg957 | thisisdfr   | E0D116F8-6783-4DE1-9A5A-5A67F8129917          | 2/13/2020 7:59:46 PM  | Sent attachment 7484508C-83A9-48DF-B1C7-1213...          |
| thisisdfr   | hickdawg957 | F2C52A1D-0775-4C95-A39F-6A82D6959D04          | 4/12/2020 10:01:01 AM |                                                          |
| thisisdfr   | hickdawg957 | 33A4EEFD-6A3F-4113-8092-0BD140738639          | 4/12/2020 10:15:50 AM |                                                          |
| hickdawg957 | thisisdfr   | 74D0F418-C775-46DA-8C64-8826F38739F7          | 4/12/2020 10:16:30 AM |                                                          |
| hickdawg957 | thisisdfr   | 58940586718403056r                            | 4/12/2020 3:06:43 PM  | Sent attachment 58940586718403056r                       |
| thisisdfr   | hickdawg957 | THISISDFR-951414A5-0503-4024-A024-52E1438C... | 4/12/2020 3:07:32 PM  | Sent attachment THISISDFR-951414A5-0503-4024-...         |

**PREVIEW**

**THISISDFR** 4/11/2020 9:35:07 PM  
Sent  
So I just realized Snapchat has location sharing capabilities.

**HICKDAWG957** 4/11/2020 9:38:04 PM  
Received  
It does?

**THISISDFR** 4/11/2020 9:38:29 PM  
Sent  
Yep. I found Snap Map. You can either share your location or request a location from someone.

**HICKDAWG957** 4/11/2020 9:39:06 PM  
Received  
Interesting.

**DETAILS**

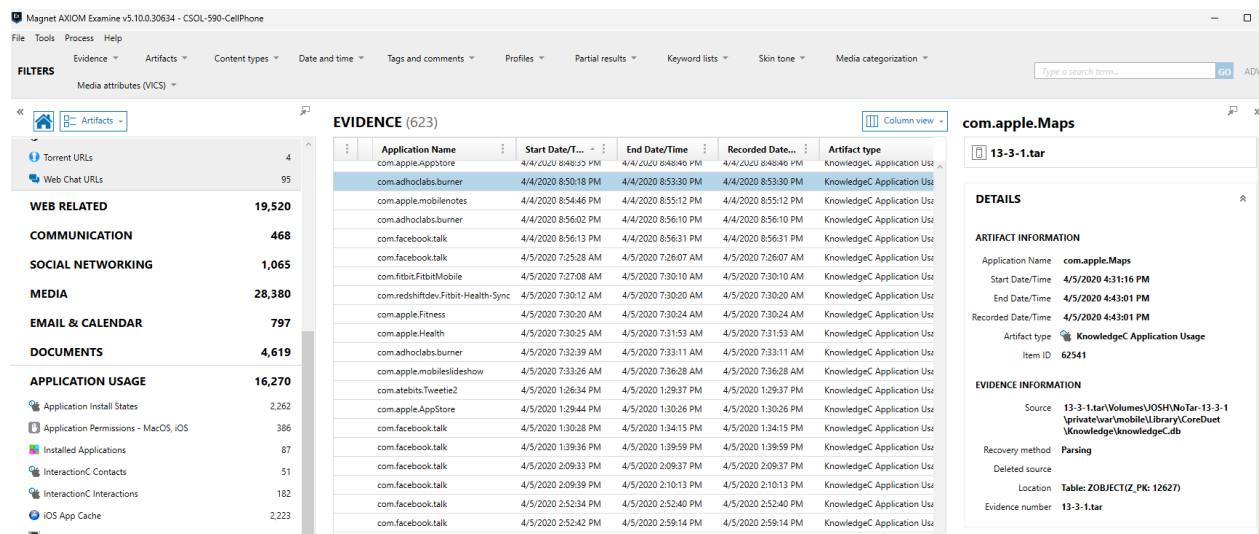
**ARTIFACT INFORMATION**

Sender: thisisdfr  
Recipient(s): hickdawg957  
Message ID: 85A44C82-8344-4983-AAA4-077C95A31BC3  
Message Date/Time: 4/11/2020 9:35:07 PM  
Message: So I just realized Snapchat has location sharing capabilities.  
Saved By Sender: No  
Saved By Recipient: No  
Released By Recipient: Yes  
Artifact type: Snapchat Chat Messages  
Item ID: 162414

On 4/11/2020 at 9:35:07 PM, thisisdfr sent a message to hickdawg957 saying they had just realized Snapchat has location sharing.

App Usage

Figure 13



On 4/5/2020 4:31:16PM, the Apple Maps application was started.

Export Report

The report for all iOS iMessages/SMS/MMS is available in separately attached document.

Part III - Brief analysis of Cellebrite vs. Axion.

In the field of digital forensics, academic literature distinguishes Cellebrite (Physical Analyzer/UFED) and Magnet AXIOM by their operational success rates and underlying investigative philosophies. Peer-reviewed research, such as a 2026 study published via ResearchGate, utilized the NIST Mobile Forensic Criteria to evaluate performance on modern, high-security devices like the Google Pixel 5a. The findings revealed that Cellebrite achieved a 75% success rate in artifact recovery, particularly excelling at extracting internet, geolocation, and social application data. In contrast, Magnet AXIOM recorded a **56% success rate**. While it slightly outperformed Cellebrite in basic SMS recovery, it was notably less effective at decoding complex data from modern third-party applications (ResearchGate, 2026).

Further academic analysis focuses on the "artifact-first" versus "low-level" forensic methodologies. Cellebrite is widely recognized for its technical depth in bypassing hardware-level encryption and performing Full File System (FFS) extractions, making it a critical tool for acquiring data from mobile devices (James, 2024). Conversely, Magnet AXIOM is a unified analysis platform that ingests and correlates data from mobile, computer, and cloud sources (Herald Scholarly Open Access, 2025). This holistic approach allows AXIOM to reconstruct user timelines across multiple platforms. However, researchers emphasize that, because both tools use different scanning algorithms and parsers, a dual-tool approach is essential to ensure evidentiary integrity and maximize artifact retrieval (Atlantis Press, 2025; ResearchGate, 2026).

## References

Herald Scholarly Open Access. (2025). *Digital forensics: Confronting modern cyber crimes, technological advancements, and future challenges*.

<https://www.heraldopenaccess.us/openaccess/digital-forensics-confronting-modern-cyber-crimes-technological-advancements-and-future-challenges>

James, S. (2024). Foundations of mobile forensics: An academic approach. *Issues in Information Systems*, 25(3), 94-108.

[https://www.iacis.org/iis/2024/3\\_iis\\_2024\\_94-108.pdf](https://www.iacis.org/iis/2024/3_iis_2024_94-108.pdf)

Kumar, P., Rashid, E., & Narayan, R. (2025). A comparative study of mobile forensic tools for Android devices. *Proceedings of the Recent Advances in Artificial Intelligence for Sustainable Development (RAISD 2025)*. Atlantis Press.

<https://www.atlantis-press.com/proceedings/raisd-25/126013758>

ResearchGate. (2026, January 31). *Comparative analysis of mobile forensic tools for digital evidence recovery using NIST framework*.

[https://www.researchgate.net/publication/400268268\\_Comparative\\_analysis\\_of\\_mobile\\_forensic\\_tools\\_for\\_digital\\_evidence\\_recovery\\_using\\_NIST\\_framework](https://www.researchgate.net/publication/400268268_Comparative_analysis_of_mobile_forensic_tools_for_digital_evidence_recovery_using_NIST_framework)