JUNE 26, 2023



CSOL590 – Final Forensics Report

**FOR: DEWY, CHEETUM & HOWE**

JOSE FLORES

LEAD INVESTOGATOR

JFLORES1@SANDIEGO.EDU

University of San Diego logo**Table Of Contents**

[1 Executive Summary 3](#_Toc138703693)

[2 Evidence and Custodians 3](#_Toc138703694)

[2.1 Evidence 3](#_Toc138703695)

[2.2 Custodians 4](#_Toc138703696)

[3 Methodology 5](#_Toc138703697)

[3.1 Preservation 5](#_Toc138703698)

[3.2 Analysis 5](#_Toc138703699)

[4 Findings 5](#_Toc138703700)

[4.1 Location 5](#_Toc138703701)

[4.2 Communications with Hickman 5](#_Toc138703702)

[5 Conclusion 6](#_Toc138703703)

[6 References 7](#_Toc138703704)

# Executive Summary

Summary of the assignment and your findings

Attorneys from Dewey, Cheattrum, and Howe have asked to give expert findings and opinions from someone known as “THISISDIFIR.” I examined the phone from “THISISDIFIR” to discover they had no plain communication with Josh Hickman on April 5, 2023, with Cellabrite. However, Tutanota and Proton Mail were used on April 5, 2023. Cellebrite is unable to examine the messages because they are encrypted email applications. Additional information provided by Magnet Acquire confirms that messages were sent using both applications as a “test message.” The client may have communicated with Josh Hickman using encrypted emails or messages due to the activity on the days. The client could have sent attachments as a form of communication, so the software we use only recognizes it as an attachment or picture. The client's location shows they were in North Carolina the whole day and received an email with an address to California.

# Evidence and Custodians

Information about the evidence and owner of the evidence (the Custodian).

## Evidence

Type of Device: iPhone SE. OS version 13.3.1

Serial Number: DX3T126VH2XV

Date it was acquired: 04/12/2020 Imaged created.

Hash Values:

13-3-3.tar

MD5 0806f1105231f12108838de2c3142600  
SHA1 250b38b5293ea40421b416f69c8ec7c4791f1489  
SHA256 14852c9b0bda8f1a1efdb014a10aab0266cfdac2deec2629b2faa88154e3a6f5

c623fbd7e91b041e07a68f8523f53a35973e475d.zip (iTunes Backup – PW: mypassword123)

MD5 8591f294354502f41cca3da23b790081  
SHA1 f1eb18acc6a9321945d976645bb643f275a61350  
SHA256 9022c2e890ce18117bc566ed919dd0ead487dcd61ead00f8458f1b5808bf8c65

sysdiagnose\_2020.04.12\_11-39-31-0400\_iPhone-OS\_iPhone\_17D50.tar.gz (Sysdiagnose Logs)

MD5 32429f7bf3e58dd5eb22b7b539669d65  
SHA1 71959708a5c550aa76cc326034b8c98e4520355d  
SHA256 c3e09c9a06badd8933fae266f8b30460ea3b76f958e9e0b0727d1a047d2cb0b6

## Custodians

First Name: Jose

Last Name: Flores

Address: 5998 Alcala Park Way, San Diego, CA 92110

# Methodology

## Preservation

The tool used to preserve the evidence was an application called Cellebrite. The version is 7.60.0.27, and it was created on 6/25/2023 at 1724. The additional application used was Magnet Acquire, and it was collected on 04/12/20 at 1542 hours.

## Analysis

The tool used to process the evidence was an application called Cellebrite Reader. The tool helps me analyze the description of the phone and other applications it has been using. The additional application used was Magnet Acquire, and it was able to extract additional information about application communication.

# Findings

## Location

On April 5, 2020, at 1636 (UTC), a drive was started at 130 W Holly Springs Rd to 508 Ancient Oaks Dr, indicating they were in North Carolina.

## Communications with Hickman

The Cellibrite application shows there was only communication between the client and Joshua Hickman if it was encrypted. Using Magnet Acquired, we determined that Tutanota and Proton Mail encrypted emails were” test messages.” Applications such as Instagram, MeWe, Signal, and Snapchat were using pictures that were not described. Typing up what needs to be said in a text message and taking a screenshot would be sent as a picture/attachment in these applications. This form of communication can be hidden, and we cannot determine if the client and Joshua communicated in such a manner.

# Conclusion

The client and Joshua weren’t communicating in plain text, but there is a possibility they may have communicated via images/attachments. This type of communication is unnoticed because no one considers taking extra steps to send a message. This is often seen on airplanes without wifi or cellular signal. One user will type up the message on the application notes or text and screenshot it. The user would send it to the other via Bluetooth or airdrop as an image/attachment. Then the other user could edit the picture, save it, and resend it to the sender (Halter, 2019). The same concept is done with applications that can send images and attachments. Due to either software being unable to describe the picture/attachment, we could not determine if they had contact in that communication. Lastly, Cellibrite could not detect Tutanota and Proton Mail due to being encrypted. Magnet Acquired was able to capture the encrypted messages. However, the client may have used another encrypted application that was not captured on either software. We can confirm that the client was not in California due to the locations and journeys he took while in North Carolina. The client could not be in California any time of the day, even with gaps due to impossible travel time (Yatziv, 2022).

# References

Halter, H. (2019). The fastest way to share a screenshot from your iphone. [www.iphonelife.com](http://www.iphonelife.com). https://www.iphonelife.com/content/how-to-quickly-share-screenshot#:~:text=When%20you%20tap%20and%20hold,you%20can%20share%20it%20directly.

Yatziv, A. (2022). *Detecting and remediating impossible travel*. TECHCOMMUNITY.MICROSOFT.COM. https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/detecting-and-remediating-impossible-travel/ba-p/3366017