Case Report
National Gallery DC

Tracy's iPhone [2012-07-15-National-Gallery]

Table of Contents

Case Report

National Gallery DC

- Tracy's iPhone [2012-07-15-National-Gallery]

Table of Contents

Executive Summary

- Equipment and Tools

Details of Tracy's iPhone

Evidence to Establish Personas

Evidence relating to theft of valuable stamps

Evidence relating to defacement of museum art

Plot Timeline

Conclusion

Appendix A: Correspondence Evidence

Appendix B: WiFi and GPS Location Information

Executive Summary

On January 21, 2016, Digitech Inc. was called in to assist the National Gallery, Washington D.C. (NGDC) case involving the conspiracy associated with the theft of valuable stamps and defacing of museums are at the NGDC.

- Tracy is a suspect in the aforementioned conspiracy.
- As part of the investigation, Tracy's iPhone was taken into custody.
- Digitech, Inc. was tasked with investigating evidence relevant to the aforementioned conspiracy.

As described fully in the report, Digitech, Inc. made the following findings.

Equipment and Tools

We used the Autopsy tool, along with Kali Linux & Nano for Offline Analysis of e-mails and text files.

Details of Tracy's iPhone

Name	Findings	Location
Model	iPhone 3G	/mobile/Library/Logs/AppleSupport/general.log
Host Name	Tracy Sumtwelve's iPhone	/logs/lockdownd.log.1
OS Version	iPhone OS 4.2.1 (8C148)	/mobile/Library/Logs/AppleSupport/general.log
Install Time	6/6/2012 19:03:28	/mobile/Library/Logs/AppleSupport/general.log
User Email	tracysumtwelve@gmail.com	vol5/mobile/Library/Mail
Phone	703-340-9661	/logs/lockdownd.log.1
Serial #	86004482Y7H	/mobile/Library/Logs/AppleSupport/general.log
ICCID	89014103255195342366	/logs/lockdownd.log.1
IMEI	012021003735398	/root/Library/Lockdown/activation_records/wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	

SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d657 7ccb534ca0d1e83ffd27683e621607	

Evidence to Establish Personas

Tracy:

Phone Number:	(703) 340-9961
Personal Email:	tracysumtwelve@gmail.com
Alias Email:	coralbluetwo@hotmail.com
Relationship:	Accused – Planning to steal rare stamps from the National Gallery with her corrupt Police Officer brother to help with both of their financial issues. Tracy needs tuition money for Terry because Daddy won't help. Also, in cahoots with Carry for information but unaware of the krasnovian plot.

Pat:

Phone Number:	(571) 308-3236
Alias Email:	perrypatsum@yahoo.com
Personal Email:	patsumtwelve@gmail.com
Relationship:	Pat is Tracy's brother ad a corrupt Police Officer who loves his sister Tracy and his niece Terry

Terry:

Phone Number:	
Email:	
Relationship:	Terry is Tracy's Daughter who attends an expensive prep school

Joe:

Phone Number:	
Email:	joe.sum.twelve@gmail.com
Relationship:	Joe is Terry's Father and Tracy's Soon to be Bitter Ex-Husband

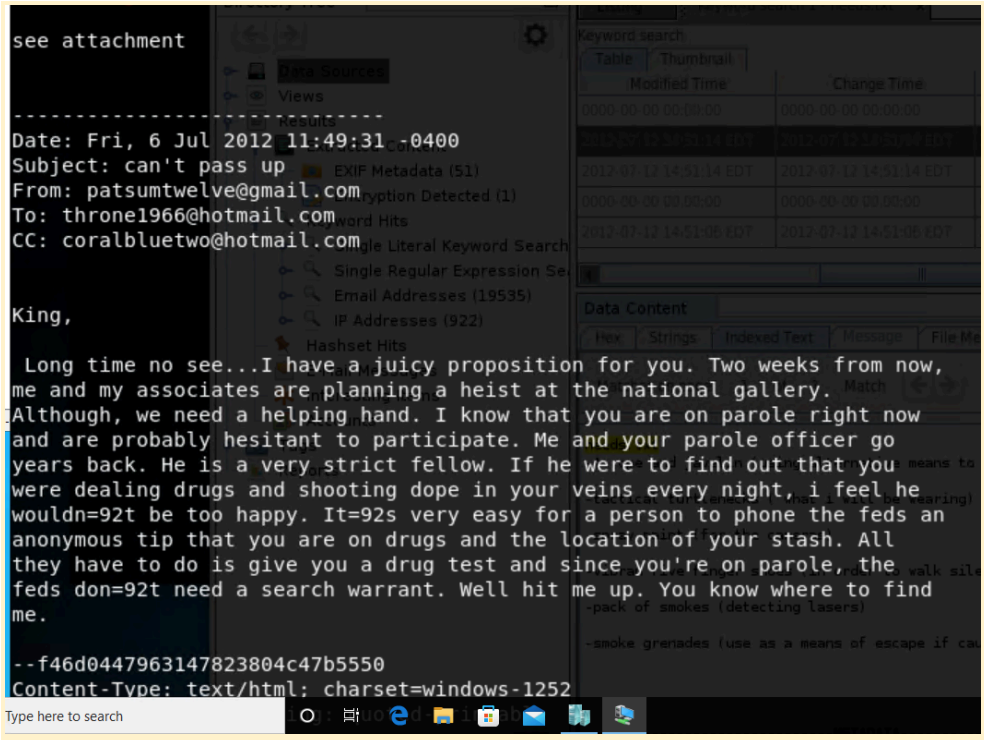
Carry:

Phone Number:	
Email:	carrysum2012@yahoo.com
Relationship:	Carry is a tech savvy criminal and Krasnovian supporter in America that works at the National Gallery. She knows Alex a Krasnovian wealthy businessman. She has been recruited through her father to help this businessman damage US Krasnovian relations.

Evidence relating to theft of valuable stamps

This sub-section provides details regarding the evidence found as it relates to the theft of valuable stamps.

Artifact 13 is referenced from Appendix A below that confirms that the plot was to steal the valuable stamp collection from the museum. In addition there is other email evidence that showed that Pat used his influence to get a parolee that he know to do the job or risk going back to.jail. From Appendix B you can tell that they were at the site of the heist at that time based on GPS data.



Evidence relating to defacement of museum art

This sub-section provides details regarding the evidence found as it relates to the defacement of museum art. In artifact number 23, It shows that Carrey has gotten Tracy to assist her with security shift information and a sneaking in of a tablet to assist in the defacement job in exchange for monies.

Plot Timeline

There are two criminal plots in play here. One is to damage relations between the USA and Krasnovia by having art vandalized, and the other is to steal stamps from an exhibit to pay education costs for a child, and to line people's pockets. Each crime requires help from multiple parties and is what will ultimately get them all caught. The Timeline gleaned for the planning and execution of the stamps job began on June 19th, 2012. The date of the heist is July 20th, 2012. The final date for the defacement of Krasnovian art has not been set but the planning is happening simultaneously. The husband however threw a wrench in everyone's plans because he installed a keylogger on Tracy's computer, caught wingd of everything and turned her into the police. You can refer to Appendix A for the Timeline according to the e-mail communications.

Conclusion

Evidence found on Tracy's iPhone indicated the following:

- The e-mail aliases that were used between Pat and Tracy were Perry and coral.
- The Caper was planned for July 20th 2012 per e-mail between Tracy (Coral) Pat and the hired parolee King (throne1966).
- The parolee who was being blackmailed also sent Pat & Terry a file with what he woud need for the job. No wonder he already got caught once!
- The case information was found in the 9F0508B8 – 04FB -490E – A7F0 – 3E23B0E7C59B.emlx

Appendix A: Correspondence Evidence

Correspondence Evidence Worksheet

Group members: Pat, Tracy, & King

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
1.	6/19/2012 20:06:33	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Paris Speak and answer	Pat emails Tracy letting her know that he has accepted her proposal and asks her to email using her alias for further instructions.	Mailbox Data Structure
2.	6/19/2012 20:26:47	F: perrypatsum@yahoo.com T: tracysumtwelve@gmail.com Subject: Look me up sometime	Pat (Perry) emails Tracy to ask her to communicate using her alias.	Mailbox Data Structure
3.	6/19/2012 21:38:59	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Crazydave by the VMs Attachment: Crazydave1.mp3	Pat (Perry) emails Tracy (Coral) with instructions to install a Virtual Machine hidden in an audio file.	Mailbox Data Structure
4.	6/19/2012 21:39:34	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: ???	Pat (Perry) replies to Tracy (Coral) confirming that he was getting her emails.	Mailbox Data Structure
5.	6/21/2012 17:43:15	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Crazydave by the VMs	Pat (Perry) replies to Tracy (Coral) on a email thread about Virtual Machine installation saying that she should listen to	Mailbox Data Structure

			some other songs as well. In the email thread Tracy (Coral) confirms that the instructions sent earlier in the audio file helped her.	
6.	6/28/2012 19:31:33	6/28/2012 19:31:33 F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Whats going on	Pat (Perry) emails Tracy (Coral) asking her to henceforth communicate using the aliases and the Virtual Machine setup to keep them safer. He also indicates that they might have to get into riskier/illegal business since both of them were facing financial hardships. He tells her that few of his workplace friends were good at these businesses and that he will inform her should something pop-up; in the meantime they should keep discussing some ideas for the same.	Mailbox Data Structure
7.	6/29/2012 14:21:56	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Whats going on	This is an email thread between Pat (Perry) and Tracy (Coral) discussing ideas for making some money. To Pat's suggestion that they use the Virtual Machines and aliases to communicate and keep looking for ways to make money, Tracy replies that she will keep her eyes open for opportunities and	Mailbox Data Structure

			insists that Pat try to get in on some business soon, since her kid didn't want to change schools. She also indicates that she is paying attention to documents especially insurance papers so that she could identify something of potential. Pat assures that he will make something happen although he is nervous because IA has been sniffing around.	
8.	6/29/2012 14:31:36	F: perrypatsum@yahoo.com T: tracysumtwelve@gmail.com Subject: hey sis	Pat (Perry) emails Tracy addressing her as 'sister' and enquires about Terry. Asks her to check in with Coral with whom he has been planning some things. He also suggests all of them going together for dinner as friends. He asks Tracy to check in with Coral. Possible misdirection attempted by referring to Coral as a third person in the narrative.	Mailbox Data Structure
9.	6/29/2012 15:21:35	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Whats going on	Pat (Perry) replies to the email thread allaying Tracy's (Coral) concern about IA sniffing around him. Tracy in her earlier email in the thread says that although nothing interesting has turned up yet she expects something soon. Pat in his email mentions that they can	Mailbox Data Structure

			certainly get the job done if something like what they had earlier discussed pops up.	
10.	7/2/2012 16:13:18	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Some good news	Email Thread: Some good news Tracy (Coral) emails Pat (Perry) mentioning that some interesting foreign exhibit is going to happen and that from assessing the paperwork she feels that it would be a big deal. Pat (Perry) replies back feeling hopeful about this being the opportunity they were looking for.	Mailbox Data Structure
11.	7/2/2012 20:00:31	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Some good news	Email thread: Some good news Following up on the earlier email about the exhibit, Tracy (Coral) mentions going through documents related to the exhibit from which she found that the exhibit is worth a lot of money but the shipping cost is very low comparatively. Pat (Perry) emails back saying that such a thing may mean that the exhibit is something small which would be a very good thing for them.	Mailbox Data Structure
12.	7/3/2012 13:29:37	F: joe.sum.twelve@gmail.com T: tracysumtwelve@gmail.com	Email Thread: Regarding Terry Tracy emails Joe asking whether he	Mailbox Data Structure

		Subject: Re: Regarding Terry	could help her with Terry's tuition this year since it is becoming too expensive for her. Joe replies back saying that he won't be paying Terry's tuition if she is not living with him.	
13.	7/3/2012 14:53:04	F: perrypatsum@yahoo.com T :coralbluetwo@hotmail.com Subject: Re: Some good news	Email Thread: Some good news Tracy (Coral) emails Pat (Perry) saying that the exhibit is rare and highly valuable stamp collection and that may be this is their opportunity. Pat (Perry) replies to Tracy (Coral) asking her to collect as much information as possible about the stamp exhibit and that in the meantime he would look into options for pulling off the heist.	Mailbox Data Structure
14.	7/5/2012 15:51:31	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Long time no see...	Carry reaches out to Tracy asking her if they could meet-up for lunch and suggests this Friday. She also mentions that through Facebook she realized that Tracy was having a hard time recently.	Mailbox Data Structure
15.	7/6/2012 15:27:51	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Re: Good News	Email Thread: Good News Tracy emailed Pat saying that she spoke with Coral and that Coral got some great news about her job and suggested that Pat catch up with Coral.	Mailbox Data Structure

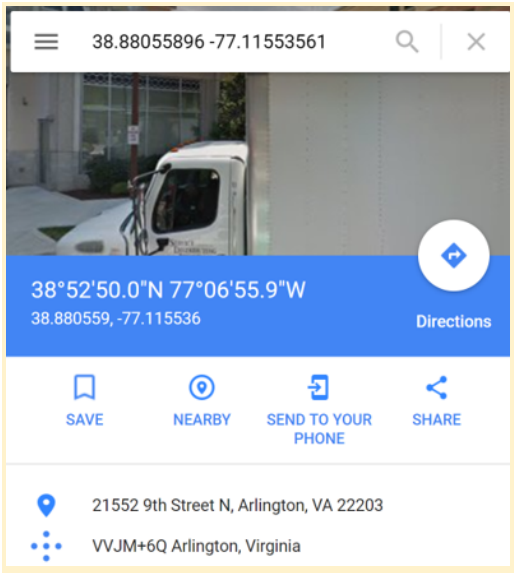
			Pat replied back saying that he knows a guy called King.	
16.	7/6/2012 15:49:31	F: patsumtwelve@gmail.com T: throne1966@hotmail.com Cc:coralbluetwo@hotmail.com Subject: can't pass up	Pat emails King with Tracy (Coral) in cc, saying that he has a lucrative proposition, a heist at national gallery. He also threatens King to comply or else he would put King's parole in jeopardy.	Mailbox Data Structure
17.	7/6/2012 17:59:24	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Re: Good News	Email Thread: Good News Tracy suggests they (meaning King, Tracy and Pat) should hang out sometime. Pat emails Tracy with account login information for: coralblue@hotmail.com Password: legalBee	Mailbox Data Structure
18.	7/9/2012 14:44:11	F: tracysumtwelve@gmail.com T: coralbluetwo@hotmail.com Subject: things	documents.zip is a compressed ZIP folder containing 3 insurance documents related to stamps. docs.zip is an encrypted ZIP folder containing 3 insurance documents related to stamps.	/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messages/8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx
19.	7/9/2012 18:18:47	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see..	Email Thread: Long time no see... Tracy thanked Carry for the lunch.	Mailbox Data Structure

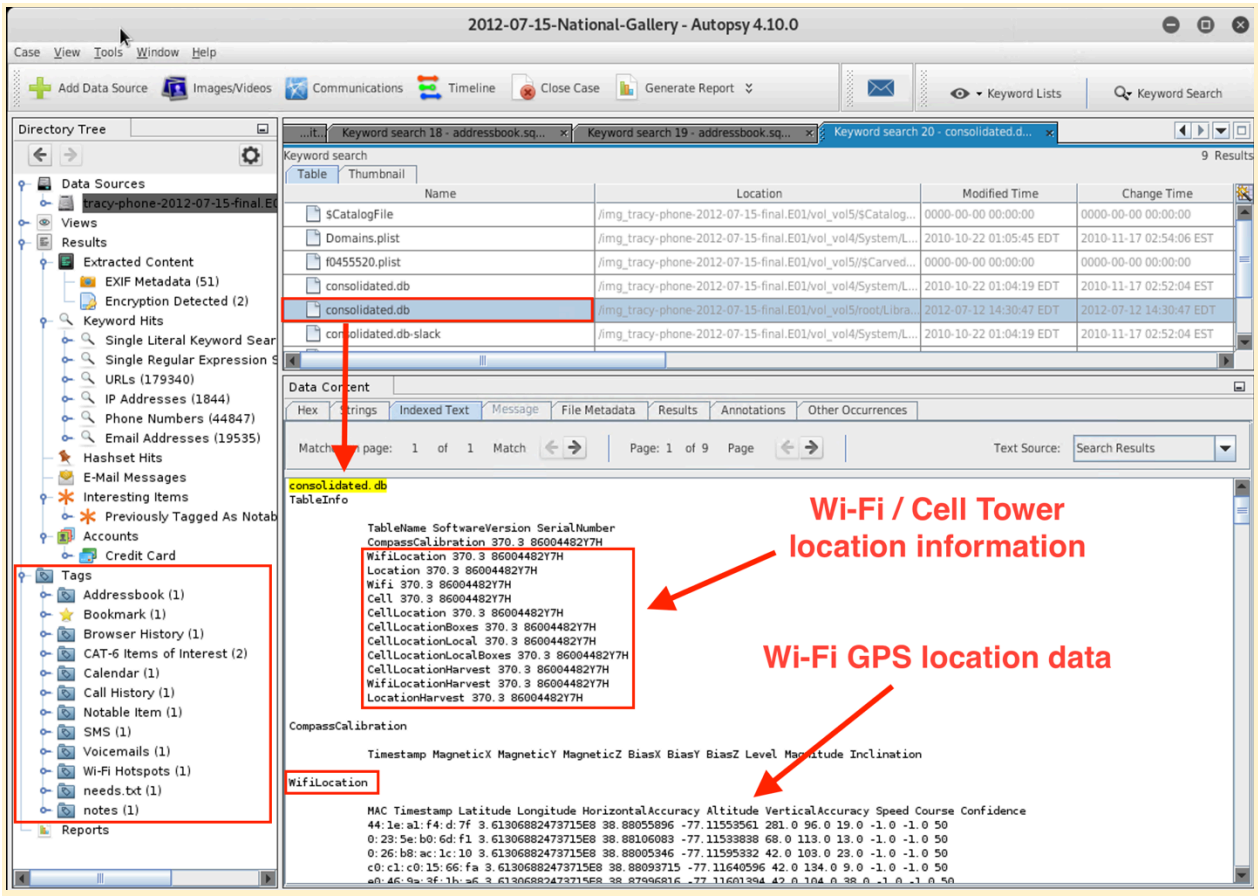
			Carry emails Tracy asking for help sneaking in a tablet for a flash mob event they had spoken earlier about. Carry suggests that Tracy would be compensated in some way for the help.	
20.	7/10/2012 13:48:40	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see...	Email Thread: Long time no see… Tracy agrees to help Carry sneak in the tablet and asks when Carry would like to get in to take a look around the gallery. Carry replies saying that this would be a big help and asks if she could come around 9 tomorrow.	Mailbox Data Structure
21	7/10/2012 15:24:57	F: patsumtwelve@gmail.com T: coralbluetwo@hotmail.com Subject: Fwd: can't pass up Attachment: needs.txt	Email Thread: cant' pass up King agrees to help with the heist and sends in a document with equipment required for it. The attached document is saved as a 'txt' file. Pat forwards that email to Tracy (Coral) *needs.txt is a pdf file which was saved with a wrong extension.	/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messages/9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx
22.	7/11/2012 17:06:19	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see...	Email Thread: Long time no see Tracy confirms the meet at 9 tomorrow. Carry wants Tracy to pass her information regarding shift changes of security. She suggests that Tracy	Mailbox Data Structure

			would be well compensated for the information. Tracy confirms that she will give the security shift information Carry requested in exchange for money but asks Carry to be careful with it. Carry replies asking Tracy not to worry and says “It will be gun”.	
23.	7/11/2012 19:28:53	F: "Google+" <noreply-5dd47ca1@plus.google.com> T: tracysumtwelve@gmail.com Subject: Carry Carsumtwotwelve added you on Google+	Email Thread: Long time no see Previous email from the thread from Carry asking for the security shift details from Tracy.	Mailbox Data Structure
24.	7/11/2012 23:22:03	F: "Carry Carsumtwotwelve (Google+)" <replyto-748d3d22@plus.google.com> T: tracysumtwelve@gmail.com Subject: Carry Carsumtwotwelve is sharing with you on Google+	Notification from Google+ informing Tracy that Carry had shared an album.	Mailbox Data Structure
25.	7/12/2012 16:12:07	F: "Carry Carsumtwotwelve (Google+)" <replyto-748d3d22@plus.google.com> T: tracysumtwelve@gmail.com Subject: Carry Carsumtwotwelve is sharing with you on Google+	Notification from Google+ informing Tracy that Carry had shared an album.	Mailbox Data Structure
26.	7/12/2012 18:03:51	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com	Email Thread: Long time no see... Tracy emailed Carry asking her what she	Mailbox Data Structure

		Subject: Re: Long time no see...	meant by “It will be gun”. Carry replies saying that it was a typographical error and she meant “It will be fun”.	

Appendix B: WiFi and GPS Location Information


38.88055896 -77.11553561
38°52'50.0"N 77°06'55.9"W
38.880559, -77.115536
Directions
SAVE
NEARBY
SEND TO YOUR PHONE
SHARE
21552 9th Street N, Arlington, VA 22203
VVJM+6Q Arlington, Virginia


2012-07-15-National-Gallery - Autopsy 4.10.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
Close Case
Generate Report
Keyword Lists
Keyword Search
Directory Tree
Data Sources
Views
Results
Extracted Content
EXIF Metadata (51)
Encryption Detected (2)
Keyword Hits
URLs (179340)
IP Addresses (1844)
Phone Numbers (44847)
Email Addresses (19535)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Credit Card
Tags
Addressbook (1)
Bookmark (1)
Browser History (1)
CAT-6 Items of Interest (2)
Calendar (1)
Call History (1)
Notable Item (1)
SMS (1)
Voicemails (1)
Wi-Fi Hotspots (1)
needs.txt (1)
notes (1)
Reports
Keyword search 18 - addressbook.sq...
Keyword search 19 - addressbook.sq...
Keyword search 20 - consolidated.d...
Keyword search
9 Results
Table
Thumbnail
Name
Location
Modified Time
Change Time
$CatalogFile
Domains.plist
f0455520.plist
consolidated.db
consolidated.db
consolidated.db-slack
Data Content
Hex
Strings
Indexed Text
Message
File Metadata
Results
Annotations
Other Occurrences
Page: 1 of 9 Page
Text Source:
Search Results
consolidated.db
TableInfo
TableName SoftwareVersion SerialNumber
CompassCalibration 370.3 86004482Y7H
WifiLocation 370.3 86004482Y7H
Location 370.3 86004482Y7H
Wifi 370.3 86004482Y7H
Cell 370.3 86004482Y7H
CellLocation 370.3 86004482Y7H
CellLocationBoxes 370.3 86004482Y7H
CellLocationLocal 370.3 86004482Y7H
CellLocationLocalBoxes 370.3 86004482Y7H
CellLocationHarvest 370.3 86004482Y7H
WifiLocationHarvest 370.3 86004482Y7H
LocationHarvest 370.3 86004482Y7H
CompassCalibration
Timestamp MagneticX MagneticY MagneticZ BiasX BiasY BiasZ Level Magnitude Inclination
WifiLocation
MAC Timestamp Latitude Longitude HorizontalAccuracy Altitude VerticalAccuracy Speed Course Confidence
44:1e:a1:f4:d:7f 3.6130688247371 5E8 38.88055896 -77.11553561 281.0 96.0 19.0 -1.0 -1.0 50
0:23:5e:b0:6d:f1 3.6130688247371 5E8 38.88106083 -77.11533838 68.0 113.0 13.0 -1.0 -1.0 50
0:26:b8:ac:1c:10 3.6130688247371 5E8 38.88005346 -77.11595332 42.0 103.0 23.0 -1.0 -1.0 50
c0:c1:c0:15:66:fa 3.613068824737 1 5E8 38.88093715 -77.11640596 42.0 134.0 9.0 -1.0 -1.0 50
Wi-Fi / Cell Tower location information
Wi-Fi GPS location data