#JonSecOps

Forensic Analysis of a Suspect’s iPhone for Criminal Evidence Recovery

Background

Mr. McBride is the senior forensic examiner at the Syracuse Police Department. Mr. McBride is ordered by his sergeant to perform an examination of a mobile device that was found on a sidewalk in downtown Syracuse, NY. The device was turned in to the police department by two civilians. The officer on duty previewed the phone in order to identify the owner. During the preview, the officer noted evidence of criminal activity and created a logical image of the device using the Cellebrite Physical Analyzer program. Sgt. Jeffrey Morgan has ordered Mr. McBride to examine the logical image for evidence of criminal activity and identifying information related to the owner.

Request

Mr. McBride's supervisor, Sgt. Morgan, needs Mr. McBride to examine the cell phone image for the following information using the Cellebrite UFED Reader software: • Make and model of the device • ICCID of the device (explain what an ICCID is) • Last activation of the device • The phone number assigned to the device • The device name • Current Time Zone • MAC address of the WiFi antenna • Device encryption status • Contacts or phonebook entries • Recent incoming, outgoing and missed calls (any numbers of interest?) • SMS/MMS messages (including transcripts) • Calendar entries (any of interest?) • Bookmarks/Web activity related to the suspected illegal activity or possible movements of the suspect • Wireless networks the device connected to (any of interest?) • Identifying attributes associated with the owner (ie. user accounts, email addresses, names, associates, etc.) • Installed applications (any of importance?) • General direction the owner was driving based on location data • Highways the owner used What is the illegal activity the device owner is involved with? • Who is the device owner's supplier? • Where does the supplier work? • Who is the device owner's buyer? • Time and location of the meeting with the supplier • Time and location of the meeting with the buyer • Location of the exchange with the buyer • Who is the device owner?

Summary of Findings

During the investigation, pertinent information regarding the findings within the device was found which should lead to a successful conviction for the potential suspect. This type of information is more elaborate in the analysis section of this report.

Evidence

Table 1 outlines the evidence items of this case.

Description	Designation	Filename	MD5 Hash
Evidence Provided	Preservation Copy	AppleDevice_AdvancedLogical	N/A
Evidence Provided	Working Copy	AppleDevice_AdvancedLogical	N/A

Table 1: Case evidence items

Collection and Analysis

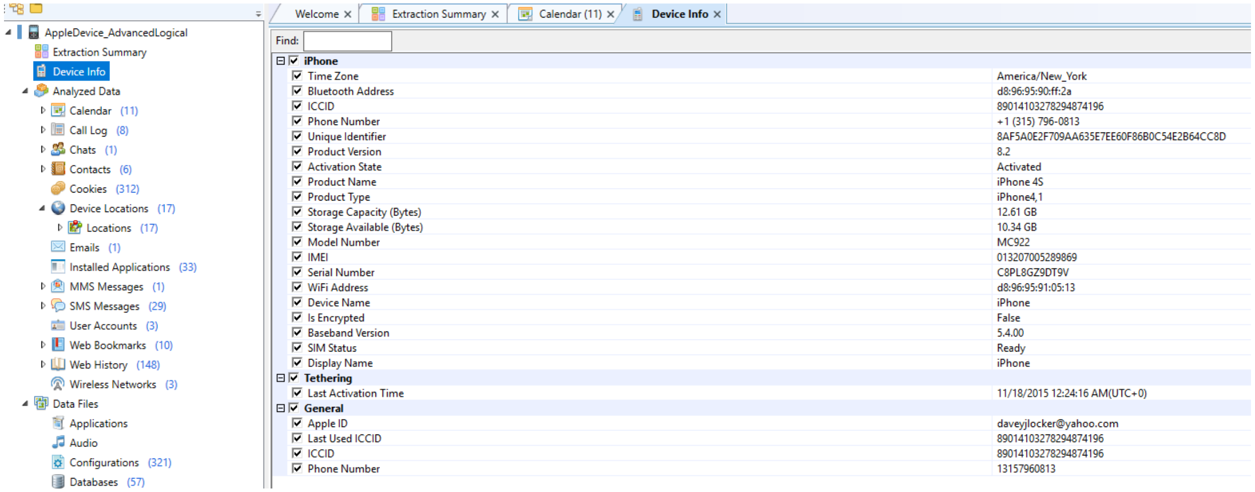
Collection

The phone that was found on a sidewalk in downtown Syracuse, NY was investigated using the Cellebrite UFED Reader software. The information requested was obtained during investigation and answered in the analysis section below

Analysis

During the examination of information such as the make and model of the device, the ICCID of the device, the phones phone number, the device name, current time zone, WIFI address and encryption status was found in the Device info folder as displayed in Figure 1.

FIGURE 1: MAKE AND MODEL OF THE DEVICE, THE ICCID OF THE DEVICE, THE LAST ACTIVATION OF THE DEVICE, THE PHONES PHONE NUMBER, THE DEVICE NAME, CURRENT TIME ZONE, WIFI ADDRESS AND ENCRYPTION STATUS



⊟ ☑ **iPhone**	
☑ Time Zone	America/New_York
☑ Bluetooth Address	d8:96:95:90:ff:2a
☑ ICCID	89014103278294874196
☑ Phone Number	+1 (315) 796-0813
☑ Unique Identifier	8AF5A0E2F709AA635E7EE60F86B0C54E2B64CC8D
☑ Product Version	8.2
☑ Activation State	Activated
☑ Product Name	iPhone 4S
☑ Product Type	iPhone4,1
☑ Storage Capacity (Bytes)	12.61 GB
☑ Storage Available (Bytes)	10.34 GB
☑ Model Number	MC922
☑ IMEI	013207005289869
☑ Serial Number	C8PL8GZ9DT9V
☑ WiFi Address	d8:96:95:91:05:13
☑ Device Name	iPhone
☑ Is Encrypted	False
☑ Baseband Version	5.4.00
☑ SIM Status	Ready
☑ Display Name	iPhone
⊟ ☑ **Tethering**	
☑ Last Activation Time	11/18/2015 12:24:16 AM(UTC+0)
⊟ ☑ **General**	
☑ Apple ID	daveyjlocker@yahoo.com
☑ Last Used ICCID	89014103278294874196
☑ ICCID	89014103278294874196
☑ Phone Number	13157960813

Make and Model of Device: Apple, MC922
ICCID of the Device: 89014103278294874196
Last Activation of the device: 11/18/2015 12:24:16AM (UTC + 0)
Device Phone Number: 1-315-796-0813
Device Name: IPhone 4S
Current Time Zone: America / New York
MAC adress of the Wifi Antenna : d8:96:95:91:05:13
Device Encryption Status: False (Unencrypted)

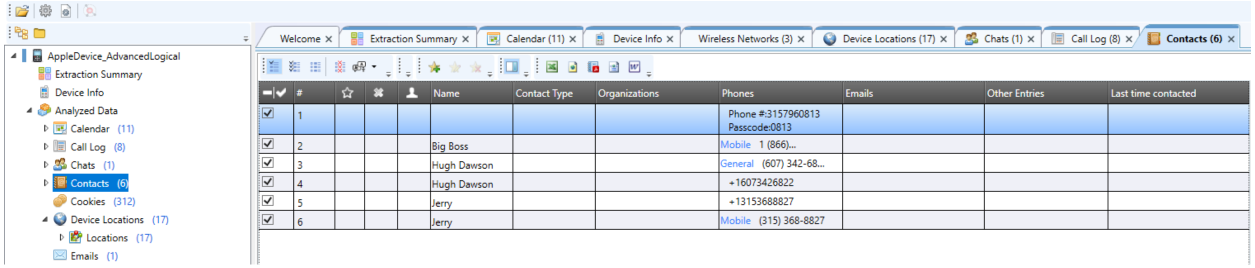
The physical image of the device is displayed in Figure 2.

FIGURE 2: PHYSICAL IMAGE OF DEVICE

For readers reviewing this report, a devices ICCID will be explained. A devices ICCID (Integrated Circuit Card Identifier) is the serial number that consists of either 19 or 20 characters and can be used if the phone owner loses their phone by notifying their network operator (Myphonelocator, 2013).

The device contacts entries were found in the contacts folder displayed in Figure 3.

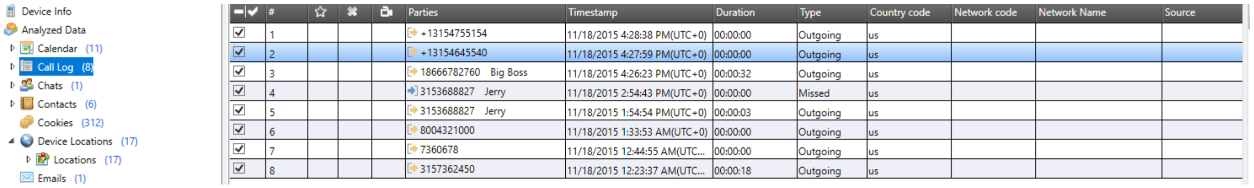
FIGURE 3: CONTACT ENTRIES



✓	#	☆	✖	👤	Name	Contact Type	Organizations	Phones	Emails	Other Entries	Last time contacted
☑	1							Phone #:3157960813 Passcode:0813			
☑	2				Big Boss			Mobile 1 (866)...			
☑	3				Hugh Dawson			General (607) 342-68...			
☑	4				Hugh Dawson			+16073426822			
☑	5				Jerry			+13153688827			
☑	6				Jerry			Mobile (315) 368-8827			

The devices incoming, outgoing and missed calls was displayed in the call log folder displayed in Figure 4.

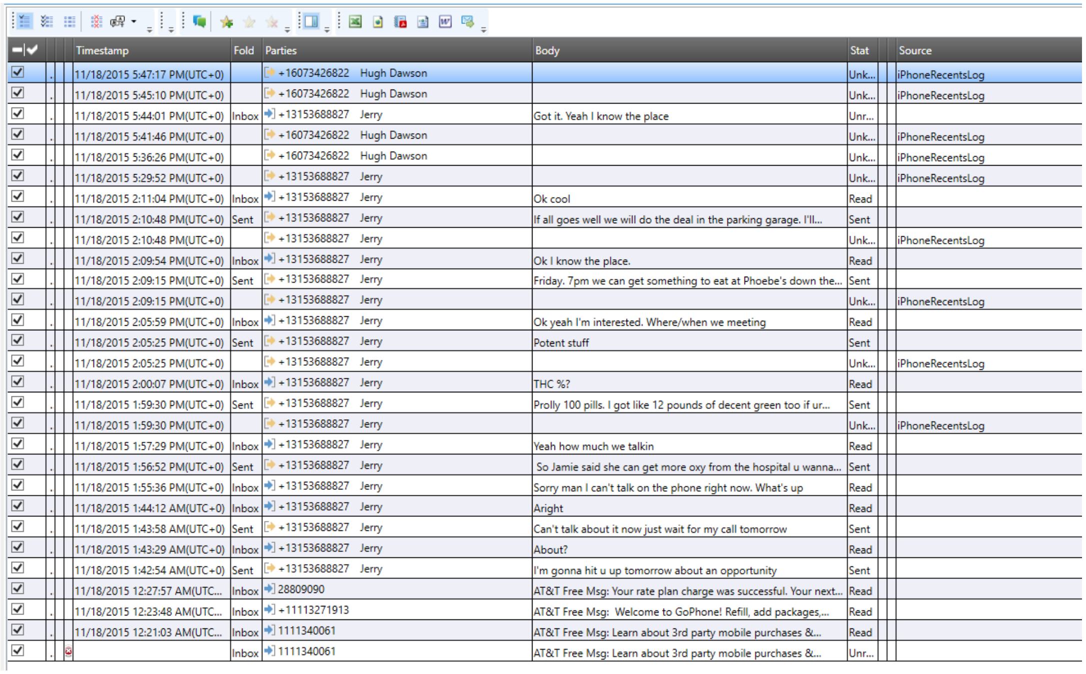
FIGURE 4: CALL LOG INFORMATION



☑	#	☆	✖		Parties	Timestamp	Duration	Type	Country code	Network code	Network Name	Source
☑	1				+13154755154	11/18/2015 4:28:38 PM(UTC+0)	00:00:00	Outgoing	us			
☑	2				+13154645540	11/18/2015 4:27:59 PM(UTC+0)	00:00:00	Outgoing	us			
☑	3				18666782760 Big Boss	11/18/2015 4:26:23 PM(UTC+0)	00:00:32	Outgoing	us			
☑	4				3153688827 Jerry	11/18/2015 2:54:43 PM(UTC+0)	00:00:00	Missed	us			
☑	5				3153688827 Jerry	11/18/2015 1:54:54 PM(UTC+0)	00:00:03	Outgoing	us			
☑	6				8004321000	11/18/2015 1:33:53 AM(UTC+0)	00:00:00	Outgoing	us			
☑	7				7360678	11/18/2015 12:44:55 AM(UTC...	00:00:00	Outgoing	us			
☑	8				3157362450	11/18/2015 12:23:37 AM(UTC...	00:00:18	Outgoing	us			

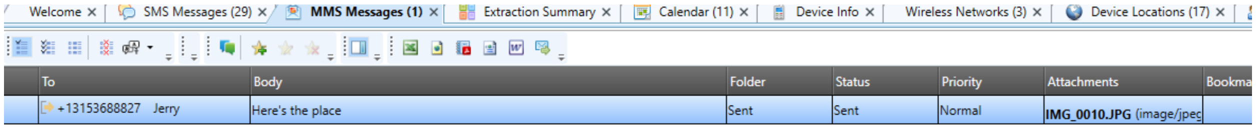
With further investigation there were SMS/MMS messages found in both the SMS and MMS folder as displayed in Figures 5 and 6.

FIGURE 5: SMS MESSAGES

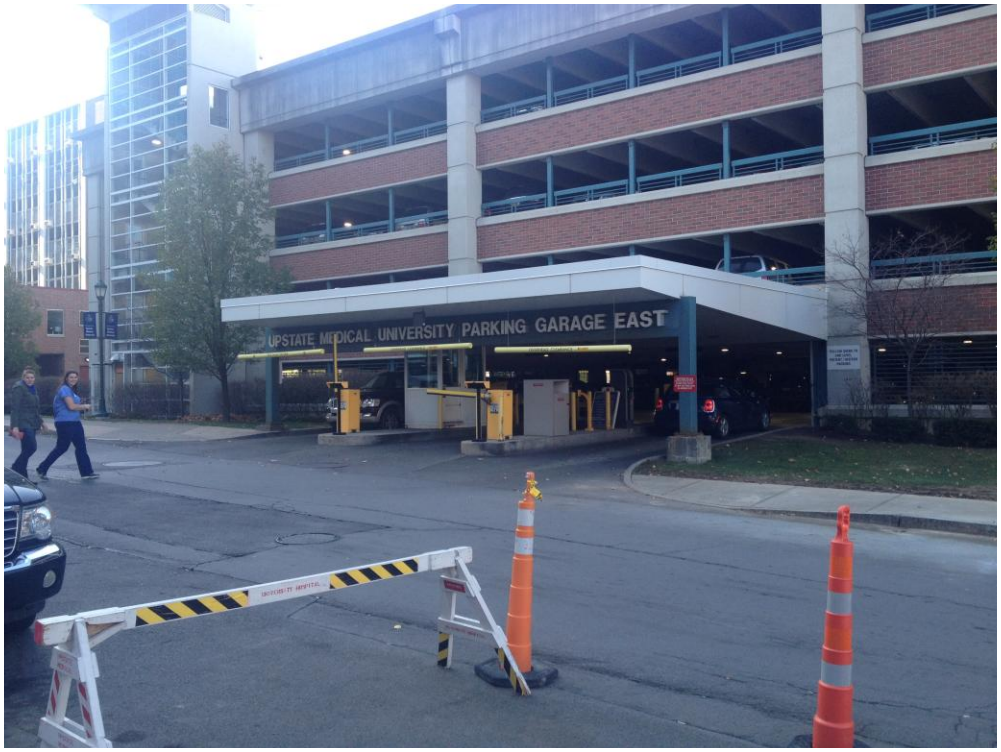


☑		Timestamp	Fold	Parties	Body	Stat	Source
☑	.	11/18/2015 5:47:17 PM(UTC+0)		+16073426822 Hugh Dawson		Unk...	iPhoneRecentsLog
☑	.	11/18/2015 5:45:10 PM(UTC+0)		+16073426822 Hugh Dawson		Unk...	iPhoneRecentsLog
☑	.	11/18/2015 5:44:01 PM(UTC+0)	Inbox	+13153688827 Jerry	Got it. Yeah I know the place	Unr...	
☑	.	11/18/2015 5:41:46 PM(UTC+0)		+16073426822 Hugh Dawson		Unk...	iPhoneRecentsLog
☑	.	11/18/2015 5:36:26 PM(UTC+0)		+16073426822 Hugh Dawson		Unk...	iPhoneRecentsLog
☑	.	11/18/2015 5:29:52 PM(UTC+0)		+13153688827 Jerry		Unk...	iPhoneRecentsLog
☑	.	11/18/2015 2:11:04 PM(UTC+0)	Inbox	+13153688827 Jerry	Ok cool	Read	
☑	.	11/18/2015 2:10:48 PM(UTC+0)	Sent	+13153688827 Jerry	If all goes well we will do the deal in the parking garage. I'll...	Sent	
☑	.	11/18/2015 2:10:48 PM(UTC+0)		+13153688827 Jerry		Unk...	iPhoneRecentsLog
☑	.	11/18/2015 2:09:54 PM(UTC+0)	Inbox	+13153688827 Jerry	Ok I know the place.	Read	
☑	.	11/18/2015 2:09:15 PM(UTC+0)	Sent	+13153688827 Jerry	Friday. 7pm we can get something to eat at Phoebe's down the...	Sent	
☑	.	11/18/2015 2:09:15 PM(UTC+0)		+13153688827 Jerry		Unk...	iPhoneRecentsLog
☑	.	11/18/2015 2:05:59 PM(UTC+0)	Inbox	+13153688827 Jerry	Ok yeah I'm interested. Where/when we meeting	Read	
☑	.	11/18/2015 2:05:25 PM(UTC+0)	Sent	+13153688827 Jerry	Potent stuff	Sent	
☑	.	11/18/2015 2:05:25 PM(UTC+0)		+13153688827 Jerry		Unk...	iPhoneRecentsLog
☑	.	11/18/2015 2:00:07 PM(UTC+0)	Inbox	+13153688827 Jerry	THC %?	Read	
☑	.	11/18/2015 1:59:30 PM(UTC+0)	Sent	+13153688827 Jerry	Prolly 100 pills. I got like 12 pounds of decent green too if ur...	Sent	
☑	.	11/18/2015 1:59:30 PM(UTC+0)		+13153688827 Jerry		Unk...	iPhoneRecentsLog
☑	.	11/18/2015 1:57:29 PM(UTC+0)	Inbox	+13153688827 Jerry	Yeah how much we talkin	Read	
☑	.	11/18/2015 1:56:52 PM(UTC+0)	Sent	+13153688827 Jerry	So Jamie said she can get more oxy from the hospital u wanna...	Sent	
☑	.	11/18/2015 1:55:36 PM(UTC+0)	Inbox	+13153688827 Jerry	Sorry man I can't talk on the phone right now. What's up	Read	
☑	.	11/18/2015 1:44:12 AM(UTC+0)	Inbox	+13153688827 Jerry	Aright	Read	
☑	.	11/18/2015 1:43:58 AM(UTC+0)	Sent	+13153688827 Jerry	Can't talk about it now just wait for my call tomorrow	Sent	
☑	.	11/18/2015 1:43:29 AM(UTC+0)	Inbox	+13153688827 Jerry	About?	Read	
☑	.	11/18/2015 1:42:54 AM(UTC+0)	Sent	+13153688827 Jerry	I'm gonna hit u up tomorrow about an opportunity	Sent	
☑	.	11/18/2015 12:27:57 AM(UTC...	Inbox	28809090	AT&T Free Msg: Your rate plan charge was successful. Your next...	Read	
☑	.	11/18/2015 12:23:48 AM(UTC...	Inbox	+11113271913	AT&T Free Msg: Welcome to GoPhone! Refill, add packages,...	Read	
☑	.	11/18/2015 12:21:03 AM(UTC...	Inbox	1111340061	AT&T Free Msg: Learn about 3rd party mobile purchases &...	Read	
☑	.		Inbox	1111340061	AT&T Free Msg: Learn about 3rd party mobile purchases &...	Unr...	

FIGURE 6: MMS MESSAGES WITH IMAGES

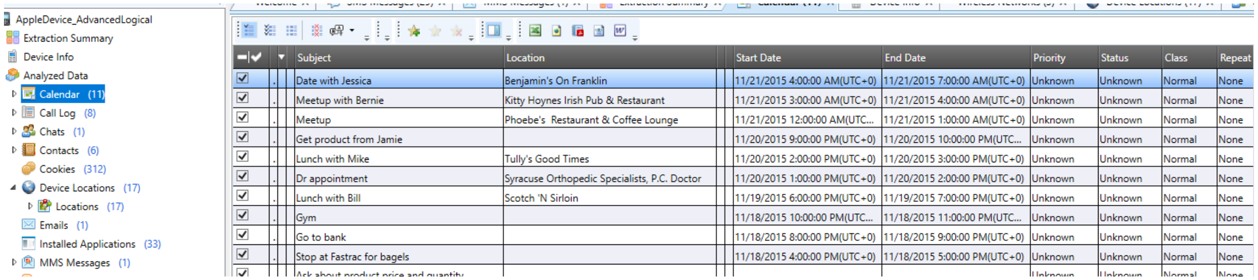


To	Body	Folder	Status	Priority	Attachments	Bookma
+13153688827 Jerry	Here's the place	Sent	Sent	Normal	IMG_0010.JPG (image/jpeg	



The calendar folder was investigated and displayed from key entries as displayed in Figure 7.

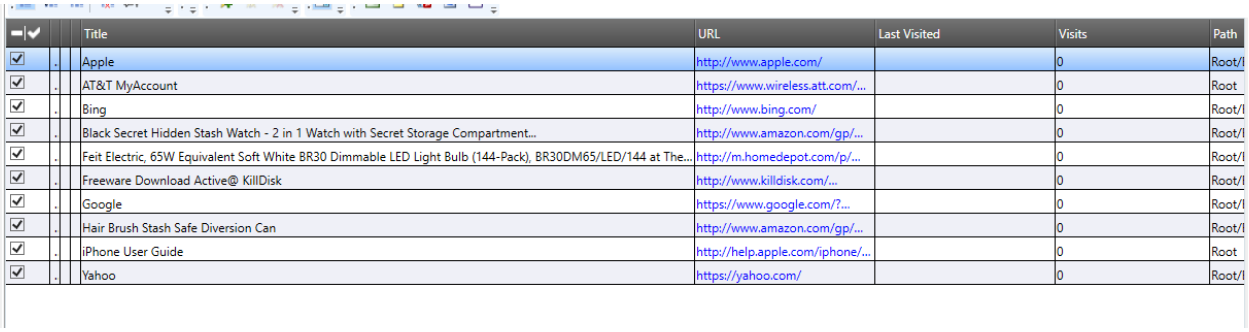
FIGURE 7: CALENDAR ENTRIES



☑	Subject	Location	Start Date	End Date	Priority	Status	Class	Repeat
☑	Date with Jessica	Benjamin's On Franklin	11/21/2015 4:00:00 AM(UTC+0)	11/21/2015 7:00:00 AM(UTC+0)	Unknown	Unknown	Normal	None
☑	Meetup with Bernie	Kitty Hoynes Irish Pub & Restaurant	11/21/2015 3:00:00 AM(UTC+0)	11/21/2015 4:00:00 AM(UTC+0)	Unknown	Unknown	Normal	None
☑	Meetup	Phoebe's Restaurant & Coffee Lounge	11/21/2015 12:00:00 AM(UTC...	11/21/2015 1:00:00 AM(UTC+0)	Unknown	Unknown	Normal	None
☑	Get product from Jamie		11/20/2015 9:00:00 PM(UTC+0)	11/20/2015 10:00:00 PM(UTC...	Unknown	Unknown	Normal	None
☑	Lunch with Mike	Tully's Good Times	11/20/2015 2:00:00 PM(UTC+0)	11/20/2015 3:00:00 PM(UTC+0)	Unknown	Unknown	Normal	None
☑	Dr appointment	Syracuse Orthopedic Specialists, P.C. Doctor	11/20/2015 1:00:00 PM(UTC+0)	11/20/2015 2:00:00 PM(UTC+0)	Unknown	Unknown	Normal	None
☑	Lunch with Bill	Scotch 'N Sirloin	11/19/2015 6:00:00 PM(UTC+0)	11/19/2015 7:00:00 PM(UTC+0)	Unknown	Unknown	Normal	None
☑	Gym		11/18/2015 10:00:00 PM(UTC...	11/18/2015 11:00:00 PM(UTC...	Unknown	Unknown	Normal	None
☑	Go to bank		11/18/2015 8:00:00 PM(UTC+0)	11/18/2015 9:00:00 PM(UTC+0)	Unknown	Unknown	Normal	None
☑	Stop at Fastrac for bagels		11/18/2015 4:00:00 PM(UTC+0)	11/18/2015 5:00:00 PM(UTC+0)	Unknown	Unknown	Normal	None
☑	Ask about product price and quantity				Unknown	Unknown	Normal	None

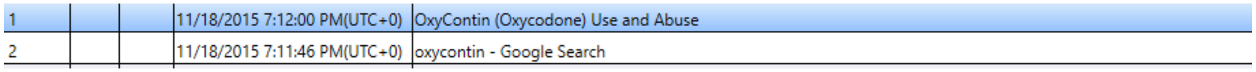
The devices web activity related to suspected illegal activity as well as possible movements was found in the web bookmarks section as well as the web history section as displayed in Figure 8 and 9.

FIGURE 8: WEB BOOKMARKS

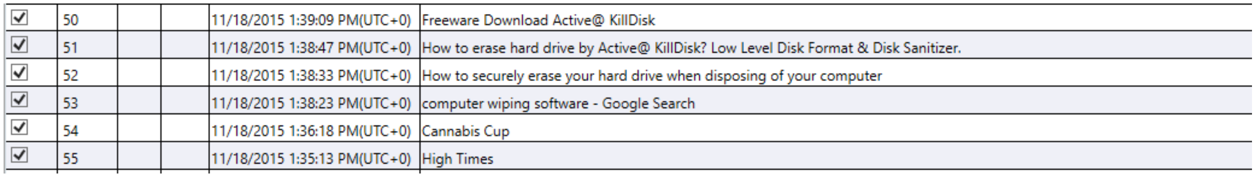


☑	Title	URL	Last Visited	Visits	Path
☑	Apple	http://www.apple.com/		0	Root/I
☑	AT&T MyAccount	https://www.wireless.att.com/...		0	Root
☑	Bing	http://www.bing.com/		0	Root/I
☑	Black Secret Hidden Stash Watch - 2 in 1 Watch with Secret Storage Compartment...	http://www.amazon.com/gp/...		0	Root/I
☑	Feit Electric, 65W Equivalent Soft White BR30 Dimmable LED Light Bulb (144-Pack), BR30DM65/LED/144 at The...	http://m.homedepot.com/p/...		0	Root/I
☑	Freeware Download Active@ KillDisk	http://www.killdisk.com/...		0	Root/I
☑	Google	https://www.google.com/?...		0	Root/I
☑	Hair Brush Stash Safe Diversion Can	http://www.amazon.com/gp/...		0	Root/I
☑	iPhone User Guide	http://help.apple.com/iphone/...		0	Root
☑	Yahoo	https://yahoo.com/		0	Root/I

FIGURE 9: WEB HISTORY COMPILATION



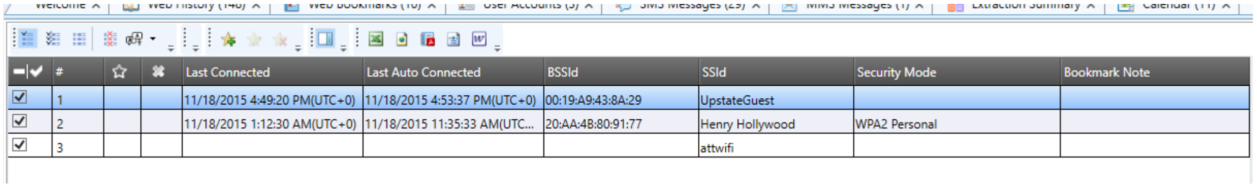
1			11/18/2015 7:12:00 PM(UTC+0)	OxyContin (Oxycodone) Use and Abuse
2			11/18/2015 7:11:46 PM(UTC+0)	oxycontin - Google Search



☑	50			11/18/2015 1:39:09 PM(UTC+0)	Freeware Download Active@ KillDisk
☑	51			11/18/2015 1:38:47 PM(UTC+0)	How to erase hard drive by Active@ KillDisk? Low Level Disk Format & Disk Sanitizer.
☑	52			11/18/2015 1:38:33 PM(UTC+0)	How to securely erase your hard drive when disposing of your computer
☑	53			11/18/2015 1:38:23 PM(UTC+0)	computer wiping software - Google Search
☑	54			11/18/2015 1:36:18 PM(UTC+0)	Cannabis Cup
☑	55			11/18/2015 1:35:13 PM(UTC+0)	High Times

Findings of the devices wireless networks was found in the wireless networks folder displayed in Figure 10.

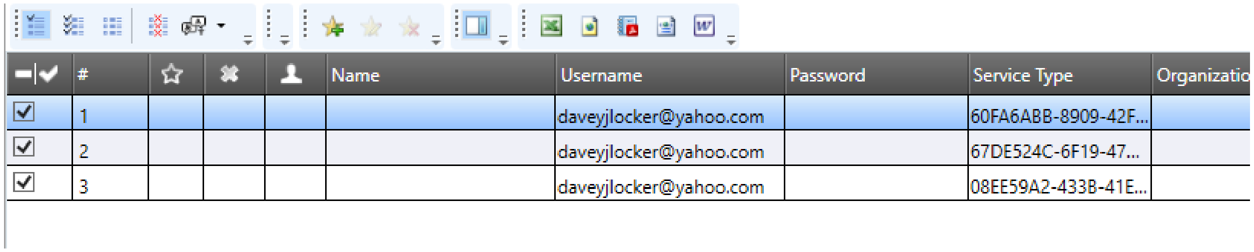
FIGURE 10: WIRELESS NETWORKS



▬✔	#	☆	✖	Last Connected	Last Auto Connected	BSSId	SSId	Security Mode	Bookmark Note
☑	1			11/18/2015 4:49:20 PM(UTC+0)	11/18/2015 4:53:37 PM(UTC+0)	00:19:A9:43:8A:29	UpstateGuest		
☑	2			11/18/2015 1:12:30 AM(UTC+0)	11/18/2015 11:35:33 AM(UTC...	20:AA:4B:80:91:77	Henry Hollywood	WPA2 Personal	
☑	3						attwifi		

The owners identifying attributes such as user accounts, email addresses, names and associates was found in the user account folder

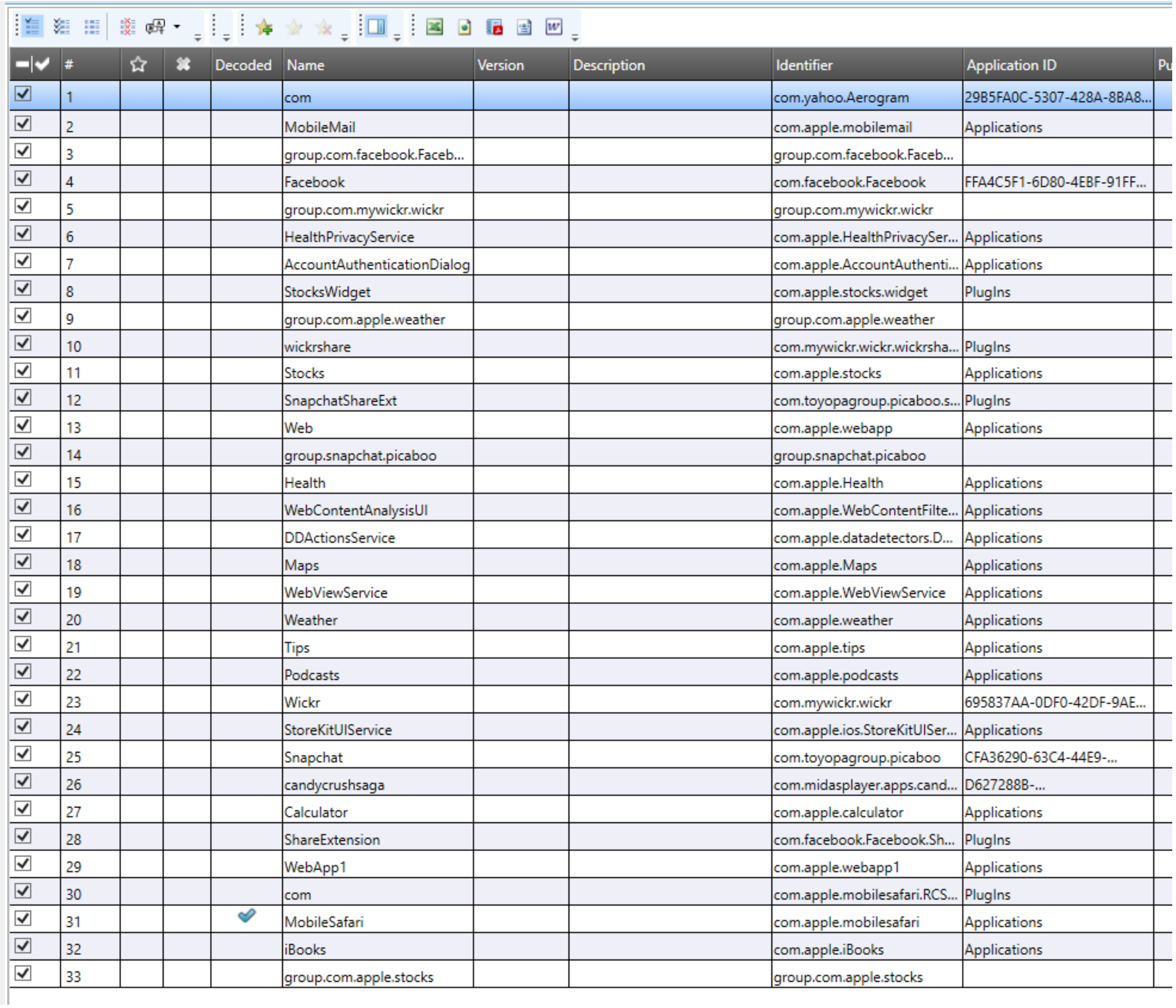
FIGURE 11: IDENTIFYING ATTRIBUTES COMPILATION



▬✔	#	☆	✖	👤	Name	Username	Password	Service Type	Organizatio
☑	1					daveyjlocker@yahoo.com		60FA6ABB-8909-42F...	
☑	2					daveyjlocker@yahoo.com		67DE524C-6F19-47...	
☑	3					daveyjlocker@yahoo.com		08EE59A2-433B-41E...	

Installed applications was discovered in the installed applications folder displayed in Figure 12

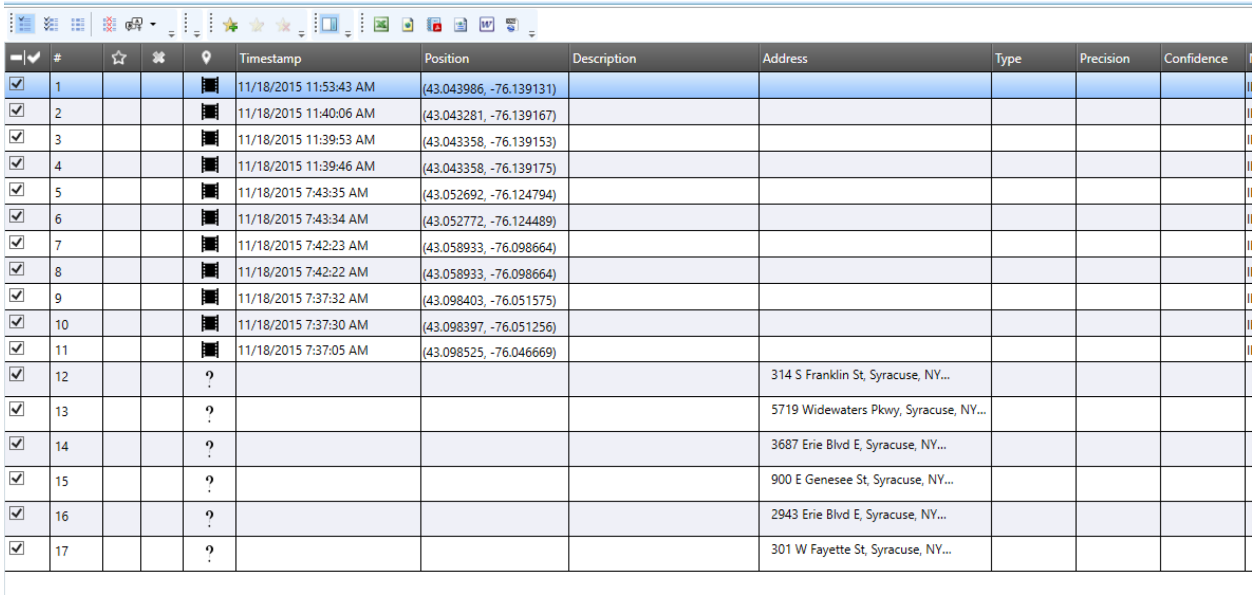
FIGURE 12: INSTALLED APPLICATIONS



▬✓	#	☆	✖	Decoded	Name	Version	Description	Identifier	Application ID	Pu
☑	1				com			com.yahoo.Aerogram	29B5FA0C-5307-428A-8BA8...	
☑	2				MobileMail			com.apple.mobilemail	Applications	
☑	3				group.com.facebook.Faceb...			group.com.facebook.Faceb...		
☑	4				Facebook			com.facebook.Facebook	FFA4C5F1-6D80-4EBF-91FF...	
☑	5				group.com.mywickr.wickr			group.com.mywickr.wickr		
☑	6				HealthPrivacyService			com.apple.HealthPrivacySer...	Applications	
☑	7				AccountAuthenticationDialog			com.apple.AccountAuthenti...	Applications	
☑	8				StocksWidget			com.apple.stocks.widget	PlugIns	
☑	9				group.com.apple.weather			group.com.apple.weather		
☑	10				wickrshare			com.mywickr.wickr.wickrsha...	PlugIns	
☑	11				Stocks			com.apple.stocks	Applications	
☑	12				SnapchatShareExt			com.toyopagroup.picaboo.s...	PlugIns	
☑	13				Web			com.apple.webapp	Applications	
☑	14				group.snapchat.picaboo			group.snapchat.picaboo		
☑	15				Health			com.apple.Health	Applications	
☑	16				WebContentAnalysisUI			com.apple.WebContentFilte...	Applications	
☑	17				DDActionsService			com.apple.datadetectors.D...	Applications	
☑	18				Maps			com.apple.Maps	Applications	
☑	19				WebViewService			com.apple.WebViewService	Applications	
☑	20				Weather			com.apple.weather	Applications	
☑	21				Tips			com.apple.tips	Applications	
☑	22				Podcasts			com.apple.podcasts	Applications	
☑	23				Wickr			com.mywickr.wickr	695837AA-0DF0-42DF-9AE...	
☑	24				StoreKitUIService			com.apple.ios.StoreKitUISer...	Applications	
☑	25				Snapchat			com.toyopagroup.picaboo	CFA36290-63C4-44E9-...	
☑	26				candycrushsaga			com.midasplayer.apps.cand...	D627288B-...	
☑	27				Calculator			com.apple.calculator	Applications	
☑	28				ShareExtension			com.facebook.Facebook.Sh...	PlugIns	
☑	29				WebApp1			com.apple.webapp1	Applications	
☑	30				com			com.apple.mobilesafari.RCS...	PlugIns	
☑	31			✓	MobileSafari			com.apple.mobilesafari	Applications	
☑	32				iBooks			com.apple.iBooks	Applications	
☑	33				group.com.apple.stocks			group.com.apple.stocks		

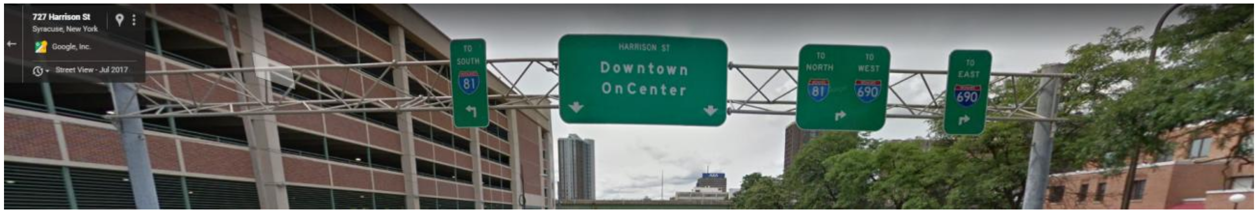
Using the most recent timestamp information in the locations folder as displayed in Figure 13, the owner of the device was driving West using the latitude and longitude of 43.043986, -76.139131. Using the latitude and longitude information provided displayed possible highways the suspect used. This was revealed by inputting the latitude and longitude information into google maps. Possible highways used were Interstate 81 or Interstate 690 as displayed in Figure 14.

FIGURE 13: MOST RECENT LOCATION TIMESTAMP



▬|✓	#	☆	✖	📍	Timestamp	Position	Description	Address	Type	Precision	Confidence
☑	1			🎞	11/18/2015 11:53:43 AM	(43.043986, -76.139131)					
☑	2			🎞	11/18/2015 11:40:06 AM	(43.043281, -76.139167)					
☑	3			🎞	11/18/2015 11:39:53 AM	(43.043358, -76.139153)					
☑	4			🎞	11/18/2015 11:39:46 AM	(43.043358, -76.139175)					
☑	5			🎞	11/18/2015 7:43:35 AM	(43.052692, -76.124794)					
☑	6			🎞	11/18/2015 7:43:34 AM	(43.052772, -76.124489)					
☑	7			🎞	11/18/2015 7:42:23 AM	(43.058933, -76.098664)					
☑	8			🎞	11/18/2015 7:42:22 AM	(43.058933, -76.098664)					
☑	9			🎞	11/18/2015 7:37:32 AM	(43.098403, -76.051575)					
☑	10			🎞	11/18/2015 7:37:30 AM	(43.098397, -76.051256)					
☑	11			🎞	11/18/2015 7:37:05 AM	(43.098525, -76.046669)					
☑	12			?				314 S Franklin St, Syracuse, NY...			
☑	13			?				5719 Widewaters Pkwy, Syracuse, NY...			
☑	14			?				3687 Erie Blvd E, Syracuse, NY...			
☑	15			?				900 E Genesee St, Syracuse, NY...			
☑	16			?				2943 Erie Blvd E, Syracuse, NY...			
☑	17			?				301 W Fayette St, Syracuse, NY...			

FIGURE 14: HIGHWAYS OWNER USED



With the provided information, the examiner was able to answer the following questions:

What is the illegal activity the device owner is involved with?
The owner is into selling Oxy and weed

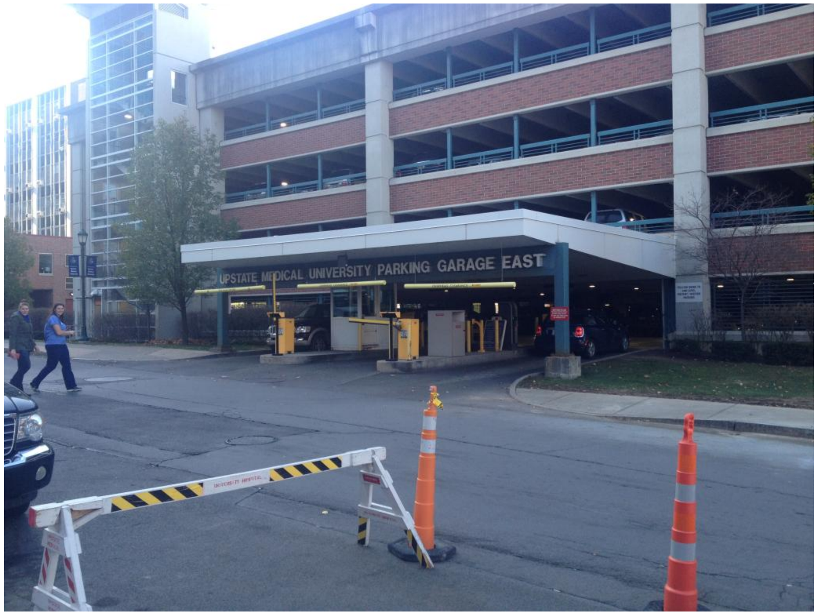
Who is the device owner’s supplier?
The supplier to the owner is Jamie

Where does the supplier work?
The supplier (Jamie) works at a hospital

Who is the device owner’s buyer?
Jerry

Time and location of the meeting with the supplier?
11/20/2015 @ 9PM

Time and location of the meeting with the buyer?
11/21/2015 @ 12AM
Phoebes Restaurant & Coffee Lounge
900 E Genesee St, Syracuse, NY 13210



Who is the device owner?
Dave

CONCLUSION

The Cellebrite UFED software that was provided for the investigation was used successfully to obtain the required information for Sgt. Morgan. All the information obtained should be highly considered in the incriminating of the potential suspect.