



Digital Evidence Ventures

CELL PHONE FORENSICS

DATA SOURCES, METHODOLOGY, & RESULTS

CELLPHONE FORENSICS

DATA SOURCES, METHODOLOGY, & RESULTS

Don Vilfer JD, MCFE

President, DIGITAL EVIDENCE VENTURES



CELLPHONE FORENSICS

DATA SOURCES, METHODOLOGY, & RESULTS

DIGITAL EVIDENCE VENTURES

Who we are:

Reformed lawyers, former FBI Agents, assisted
by young Brainiacs

What we do:

Computer Forensics, Cell Phone Forensics, Workplace
Misconduct Investigations, Fraud Investigations

CELLPHONE FORENSICS

DATA SOURCES, METHODOLOGY, & RESULTS

WHAT IS DIGITAL FORENSICS?

Digital forensics is a branch of forensic science focused on recovery and investigation of artifacts found on digital devices. Any devices that store data (e.g. computers, laptops, smartphones, thumb drives, memory cards or external hard drives) are within the ambit of digital forensics

-Lawtechnologytoday.org

CELLPHONE FORENSICS

DATA SOURCES, METHODOLOGY, & RESULTS

WHY CELLPHONES ARE IMPORTANT

- Collection of mobile data in eDiscovery
- Can contain irrefutable evidence
- Often evidence available that cannot be had elsewhere
- No longer “he said/she said”

CELLPHONE FORENSICS

DATA SOURCES, METHODOLOGY, & RESULTS

BENEFITS OF CELL DATA

- Establish communication between subjects/witnesses
- Provide location during key times
- Corroborate statements
- Prove misconduct (harassment, relationships, use of time, theft)
- Develop leads (location, banking, contacts)

CELLPHONE FORENSICS

DATA SOURCES, METHODOLOGY, & RESULTS

WHAT WE CAN GET

- Communications
 - Messages, calls
- App interaction
 - messages, pictures, music
- Location data
 - (with location services enabled)
- By the second
 - Speed of phone (vehicle phone is in)

CELLPHONE FORENSICS

DATA SOURCES, METHODOLOGY, & RESULTS

HOW DO WE GET THE DATA

- Forensic software for phones:
 - Cellebrite
 - Magnet Axion
 - Oxygen
- Often, more than one tool is used to extract as much data as possible

CELLPHONE FORENSICS

DATA SOURCES, METHODOLOGY, & RESULTS

SOURCES OF CELL PHONE DATA

- Phone itself
- Local backups
- Not just backing up iTunes
- The cloud
- Service Provider

Protecting the data

Protecting the data

DEVICE DAMAGE

Loss or destruction of cellphones is commonplace to thwart analysis



“I accidentally reversed over my cellphone 3 times”

Protecting the data

DEVICE DAMAGE

Loss or destruction of cellphones is commonplace to prevent analysis

Small v. Univ. Med. Center of S. Nevada

Failure to preserve text messages or other mobile data could result in “death penalty sanctions.”

City of San Jose v. Superior Court, *CA Supreme Court decided March 2, 2017*

Texts and emails sent by public employees on their personal devices or accounts are a matter of public record if they deal with official business.

Protecting the data

DEVICE DAMAGE

Loss or destruction of cellphones is commonplace to prevent analysis

Federal Rule of Civil Procedure 37(e)

Rule 37(e) authorizes courts to issue sanctions where four conditions are met:

- (1) the ESI at issue should have been preserved in the anticipation or conduct of litigation;*
- (2) the ESI is lost;*
- (3) the loss is due to a party's failure to take reasonable steps to preserve it; and*
- (4) the ESI cannot be restored or replaced through additional discovery.*

Once those four conditions are satisfied, the next step in the inquiry is to determine whether

- (1) the non-offending party has been prejudiced from the loss of ESI and/or*
- (2) the offending party acted with the intent to deprive another party of the information's use in the litigation.*

Protecting the data

EXAMPLE CASE

Loss or destruction of cellphones is commonplace to prevent analysis

Shaffer v. Gaither, No. 14-00106 (W.D. N.C., Sept. 1, 2016)

The plaintiff contended that she was constructively discharged due to sexual harassment by defendant. Plaintiff dropped the cellphone in a bathroom.

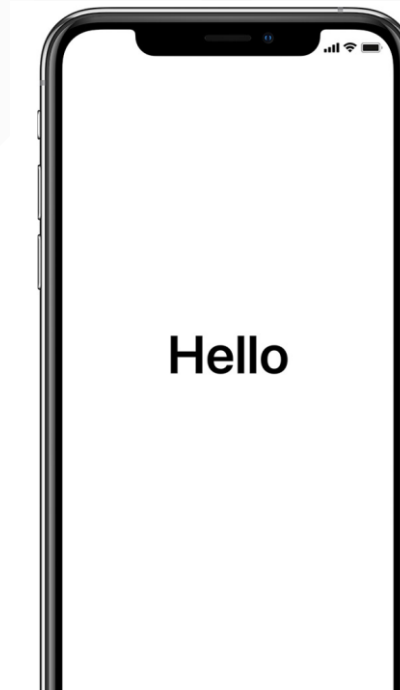
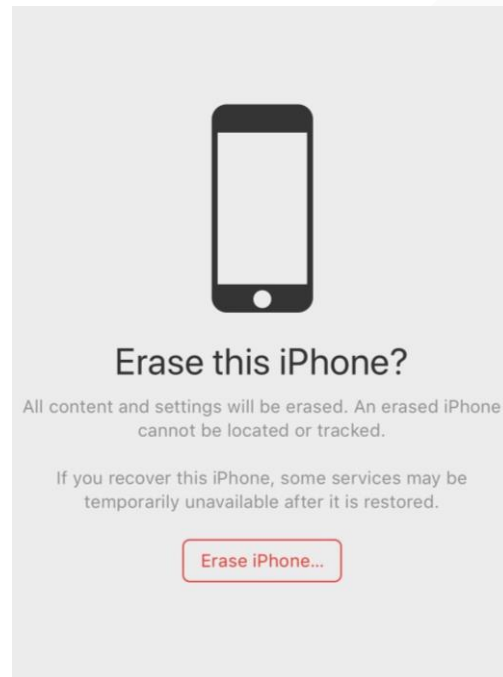
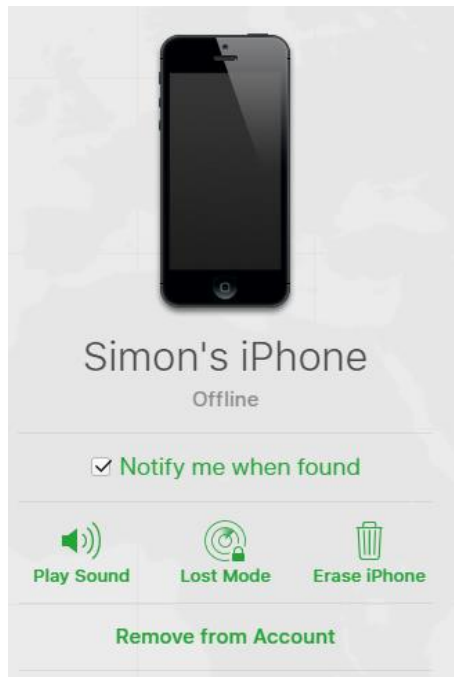
“plaintiff and her counsel failed to take reasonable steps to preserve those texts as they apparently resided only on plaintiff’s phone”

“cannot conclude that plaintiff acted with an intent to deprive defendant of the ESI under Rule 37(e)(2); thus, spoliation does not yet come into play.”

Protecting the data

DEVICE WIPE

iPhone data can easily be wiped without any means of recovery*



❖ Wiped iPhone data cannot be retrieved from that device – Data is Encrypted and encryption keys destroyed

Protecting the data

EXAMPLE CASE

The case of Gerald F. Donovan vs. Kevin S. Fowler (Kevin Spacey)



5/31/2019

- ❖ It appeared the accuser had deleted certain messages
- ❖ Messages were between accuser and his then girlfriend
- ❖ Messages were deleted prior to sending screenshots to an investigating officer

6/19/2019

- ❖ Accuser ordered to hand over the cellphone
- ❖ Accuser cannot find the cellphone

7/17/2019

- ❖ Accuser pleads 5th when questioned about lost cellphone
- ❖ Case dropped, “due to the unavailability of the complaining witness.”

Protecting the data

EXAMPLE CASE

State v. Kolanowski, (Wash: Court of Appeals, January 30, 2017).



In a case involving the failure to authenticate social media evidence,

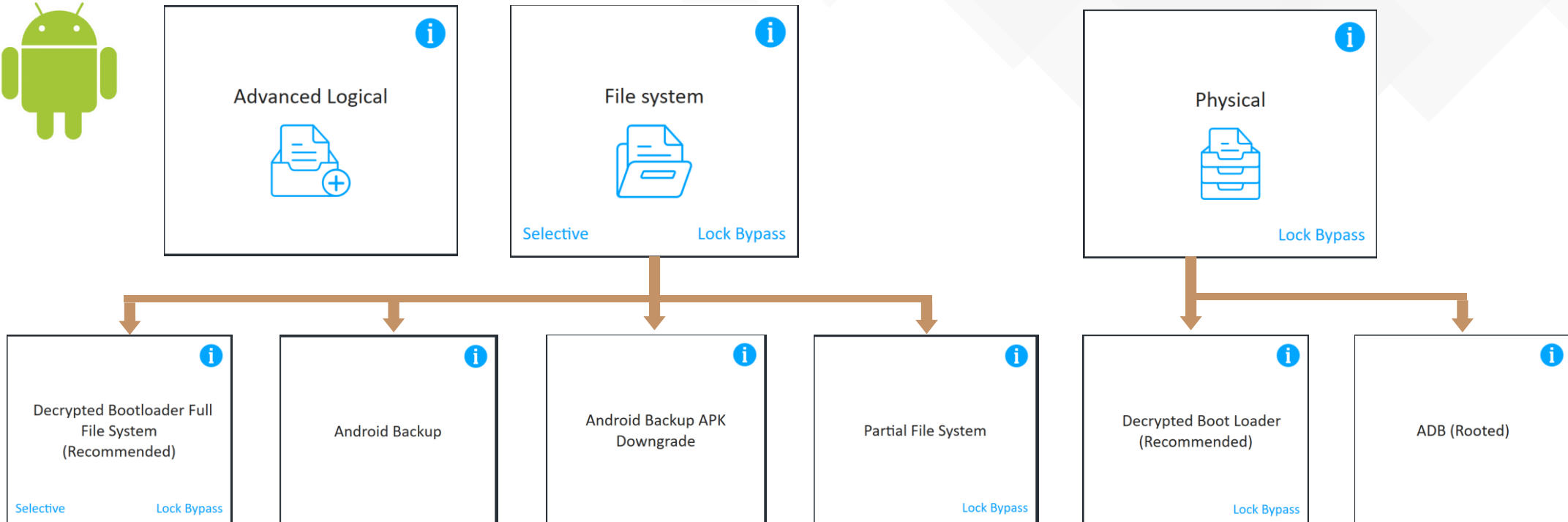
- ❖ a criminal defendant unsuccessfully sought to admit a screenshot of Facebook evidence that he maintained would have served as critical impeachment of the prosecutions' main witness.
- ❖ The State successfully argued the screenshot lacked foundation. Metadata that could have been obtained during the collection was not obtained
- ❖ A simple screenshot did not suffice.
- ❖ INEFFECTIVE ASSISTANCE OF COUNSEL claim
- ❖ His counsel failed to authenticate extrinsic impeachment evidence

Collecting and Reviewing the data

Collecting and Reviewing the data

ANDROID COLLECTION METHODS

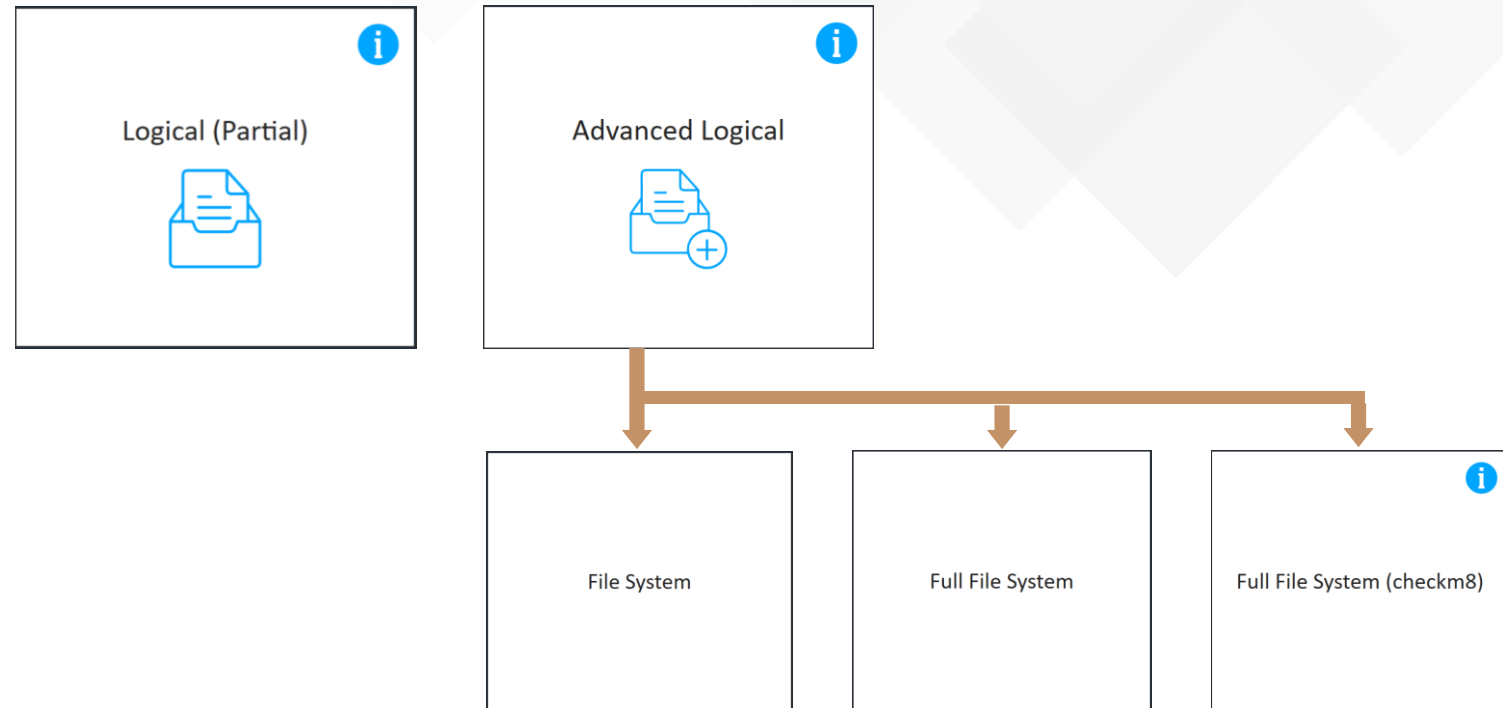
Different methods utilize different weaknesses in device security



Collecting and Reviewing the data

IOS COLLECTION METHODS

Different methods utilize different weaknesses in device security



Collecting and Reviewing the data

CheckM8 Vulnerability – Full Physical Extraction from IOS devices



- ❖ BootRom chip vulnerability
- ❖ Cannot be fixed with a patch
- ❖ Minimum IOS version 12.3
- ❖ Works with these devices:
 - ✓ iPhones from the 4s through the iPhone X
 - ✓ iPads from the 2 up to the 7th generation
 - ✓ iPad Mini 2 and 3
 - ✓ iPad Air 1st and 2nd generation
 - ✓ iPad Pro 10.5-inch and 12.9-inch 2nd generation
 - ✓ Apple Watch Series 1, Series 2, and Series 3
 - ✓ Apple TV 3rd generation and 4k
 - ✓ iPod Touch 5th generation to 7th generation

Collecting and Reviewing the data

GrayKey – Full Physical Extraction from LOCKED devices



- ❖ Attacks vulnerabilities
- ❖ Brute Force
- ❖ Proprietary methods
- ❖ Law Enforcement only
- 2 hours to 3 days to unlock

Collecting and Reviewing the data

CLOUD COLLECTIONS

Key points of note with Cloud sources

- The same data as on phone in many cases
- iCloud, Google, backup services
- Sync across devices
- Often forgotten by those destroying evidence
- Opportunity for multiple snapshots

Collecting and Reviewing the data

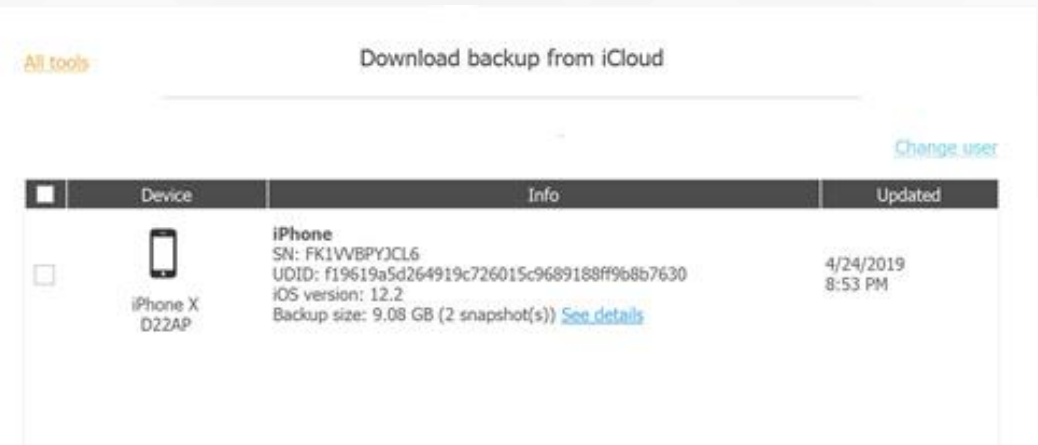
CLOUD COLLECTIONS

Different devices use different cloud backup solutions



```
com.apple.mobile.backup : dict = {  
    CloudBackupEnabled : true = True  
    LastCloudBackupDate : integer = 577746402  
    LastCloudBackupTZ : string = PDT
```

Cellphone can tell us if a backup is in the iCloud



❖ Software based cloud storage

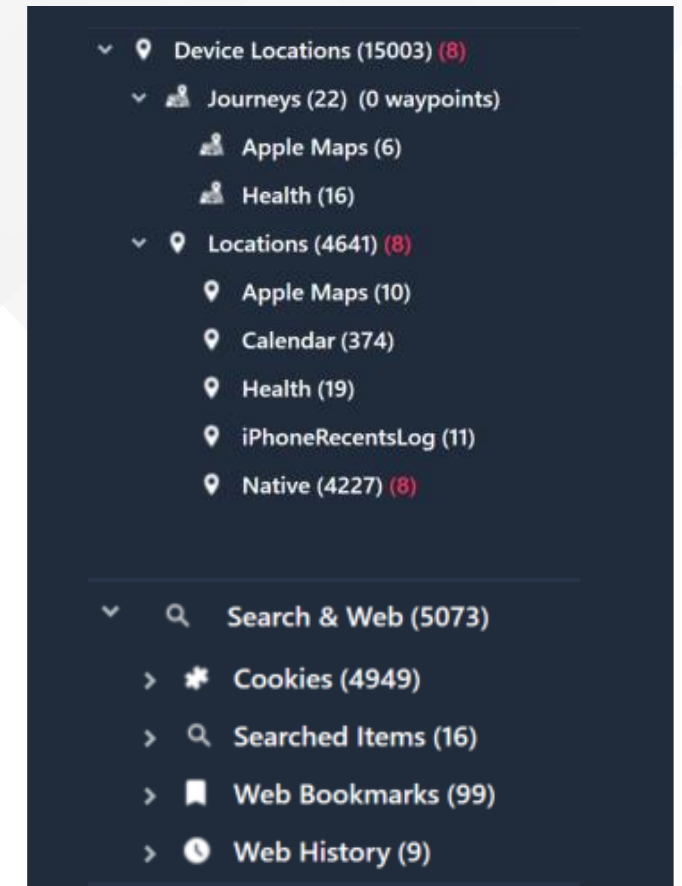
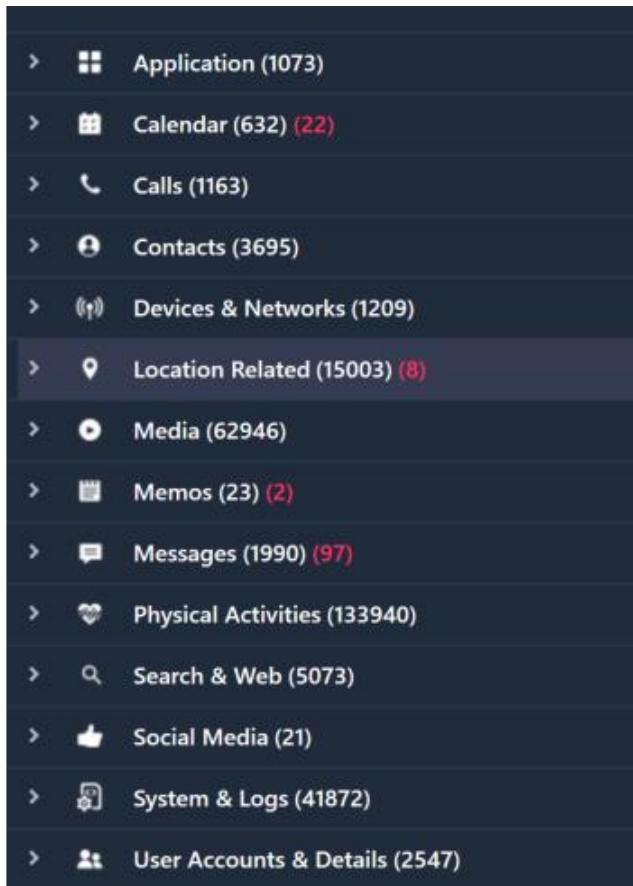
❖ Device based cloud storage

❖ Network based cloud storage

Collecting and Reviewing the data

TYPES OF DATA COLLECTED

General example of data types

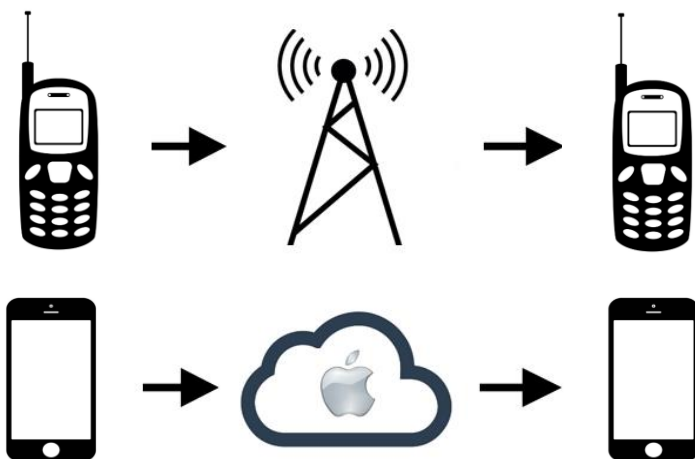


Deeper Analysis - Messages

Deeper Analysis - Messages

TEXT MESSAGING

Analysis of communications and recovery of deleted messages



- ❖ SMS/ MMS will appear on phone bill, iMessages will not
- ❖ iMessages encrypted when broadcast but not on device

Deeper Analysis - Messages

TEXT MESSAGING

Parsing Data and Handle IDs

Hex View	
001A91B2	35 46 35 39 45 1E 77 5A AB 1E 77 5A AB 06 88 02 F6 3E 00 55 33 08
001A91C8	00 01 00 00 83 70 01 08 1D 29 55 08 04 04 08 09 09 08 08 08 08
001A91DE	08 09 08 08 08 08 08 08 08 08 00 09 08 08 08 08 08 00 08 08 08
001A91F4	08 08 08 08 00 08 00 00 00 08 08 08 00 42 39 35 35 33 32 42 45 2D
001A920A	30 41 46 34 2D 34 42 33 38 2D 41 39 35 34 2D 35 38 36 43 39 35 39
001A9220	46 30 34 39 31 41 6E 64 20 61 20 6C 69 63 6B 20 F0 9F 91 85 20 74
001A9236	6F 6F 5C 04 0B 73 74 72 65 61 6D 74 79 70 65 64 81 E8 03 84 01 40
001A924C	84 84 84 19 4E 53 4D 75 74 61 62 6C 65 41 74 74 72 69 62 75 74 65
001A9262	64 53 74 72 69 6E 67 00 84 84 12 4E 53 41 74 74 72 69 62 75 74 65
001A9278	64 53 74 72 69 6E 67 00 84 84 08 4E 53 4F 62 6A 65 63 74 00 85 92
001A928E	84 84 84 83 3F 8E 5E 3E 00 55 31 08 00 01 00 00 83 6E 01 09 1D 29
001A92A4	55 08 04 04 08 09 09 08 08 08 08 08 08 09 08 08 08 08 08 08 08
001A92BA	39 09 08 08 08 08 08 08 00 08 08 08 08 08 08 00 08 00 00 00 08
001A92D0	08 08 00 42 36 43 46 34 39 30 43 2D 46 46 37 43 2D 34 34 44 30 2D
001A92E6	39 42 44 36 2D 44 33 30 32 46 35 36 31 43 35 35 46 4F 6B 20 4A 75
001A92FC	6C 69 65 61 6E 6E 20 74 68 61 6E 6B 73 04 04 0B 73 74 72 65 61 6D
001A9312	74 79 70 65 64 81 E8 03 84 01 40 84 84 84 19 4E 53 4D 75 74 61 62

5F59E.wZ..wZ.....>.U3.
.....p....)U.....
.....
.....B95532BE-
0AF4-4B38-A954-586C959
F0491And a lick t
oo\..streamtyped.....@
....NSMutableAttribute
dString....NSAttribute
dString....NSObject...
....?.^>.U1.....n...)
U.....
9.....
...B6CF490C-FF7C-44D0-
9BD6-D302F561C55F0k Ju
lieann thanks...stream
typed.....@....NSMutab

6F 5C 04 0B

Handle ID – Unique Identifier on iPhone

Collecting and Reviewing the data

ADVANCED DATA CARVING

Physical extractions allow for more deleted data recovery



Carved Image

```
67794400 00 00 CC 99 44 45 41 44 42 45 45 46 01 00 07 91 ....DEADBEEF....
67794404 44 97 32 70 94 99 FF FF FF FF 04 00 0C 91 44 87 D..7p.....D.
67794408 55 43 20 91 FF FF FF FF 00 00 60 90 82 90 05 70 UC .....p
6779440C 40 59 41 79 19 94 7F D7 41 61 37 19 24 7D 0B 41 @Yay....Aq?.$).A
67794410 EF 35 C8 FC 96 83 A6 61 7A 5D 4E 0E E7 41 ED 30 .5.....oz]N..A.0
67794414 80 EC 02 C5 E0 6D 58 98 0E 42 BF DB 65 90 F9 2D .....nP...B...e..
67794418 07 05 41 32 78 1B B4 4E 8F D7 2E 97 0B 44 7C 83 ..A2x...N.....Dl.
6779441C EA 20 77 B9 4C 06 C1 D3 E3 75 DA 7D 06 D5 E1 3F . w.L.....u.)...?
67794420 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
67794424 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
67794428 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
6779443C FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
67794440 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
67794444 FF FF FF FF FF FF FF FF FF FF FF FF 44 45 41 44 42 45 .....DEADBE
67794448 45 46 01 00 07 91 44 97 05 78 09 58 FF FF FF FF EF....D..x.X....
67794454 24 00 0C 91 44 97 74 75 55 46 FF FF FF FF 00 00 $.D.tuUF.....
67794460 60 01 02 22 14 25 40 81 CC BA 1D 94 0F 83 64 20 '..."%9.....d
67794464 F6 9B 00 72 83 DA E9 F9 BC 4C 06 E5 C3 20 F6 9B ...r.....L....
67794468 3E 07 E9 50 A0 74 1B 74 2E D3 E9 69 37 48 1C 1E >..P.t.t....17H..
67794474 83 C2 74 90 F8 4E 07 D1 EF 6F 50 DA 0D A2 A3 CB ..t..N....oP.....
67794478 A0 F6 5B EE 4E B0 41 F3 37 28 0D 32 A7 D0 6B 50 ..[.N.A.7(.2..kP
67794484 5D 0E A2 A3 C8 A0 B7 BB 0C 42 D7 41 E9 39 E8 5C ]......B.A.9.\
67794488 77 87 41 62 50 78 CE 2E 97 E1 20 F6 9B 00 C2 E3 w.AbPx.....
67794494 41 EC BA 1D 94 0F 83 F0 78 FF FF FF FF FF FF FF FF A.....x.....
67794498 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
67794504 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
67794508 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
```

Carved SMS Message

Deeper Analysis - Messages

DELETED MESSAGES

Recovery of deleted communications is a key part of our work



#							Participant
1		✗				1 1	+19519
2		✗				1 1	+19519
3		✗				1 1	+19519
4		✗				1 1	+17163
5		✗				1 1	+17163
6		✗				1 1	+17163
7		✗				1 1	+17163
8		✗				1 1	+17605
9		✗				1 1	+17605
10		✗				1 1	+19519
11		✗				1 1	+19519
12		✗				1 1	+19519
13		✗				1 1	+19519

Factors effecting successful recovery of deleted messages

❖ Time since deletion

Microcontrollers ensure all parts of the memory chip are used, 'vacuuming' of databases by system removes deleted records

❖ Operating System updates

Restructuring of internal architecture can remove deleted data

❖ Amount of device use

Regular use causes deleted items to be overwritten or removed to conserve space

❖ Type of messaging App

Some apps store more data in the cloud or use encryption

❖ Security on the device

Carving for messages may not be possible unless the best extraction is performed

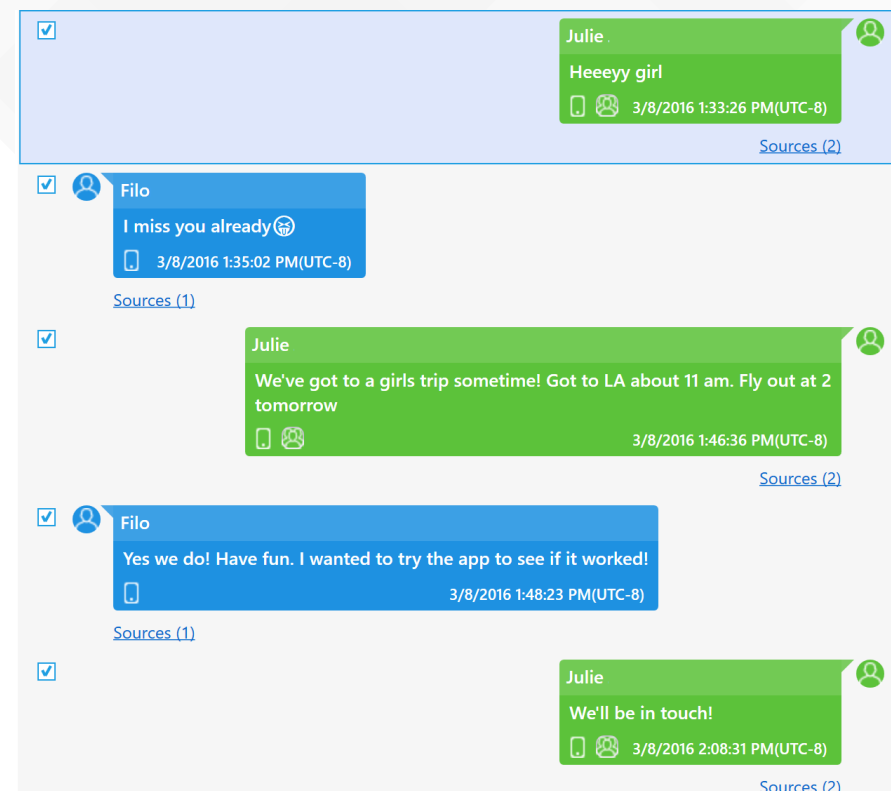
Deeper Analysis - Messages

OTHER APPS

Other chat apps are common and most based on SQL databases



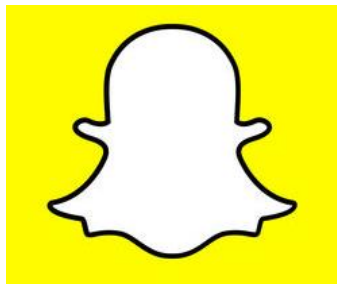
ZWABACKLISTITEM	(3)	AB60F4D24BAD20EBBD	Hello
ZWACHATPROPERTIES	(0)	601D97B3B4529556ED	Are you ok?
ZWACHATPUSHCONFIG	(0)	A914A0D4A16D4D5328	Going on lunch you home?
ZWACHATSESSION	(45)	A08F276618B4013683	Lunch buddy check it
ZWAGROUPINFO	(7)	F0201A3A17667F421B	Oh la la I love
ZWAGROUPMEMBER	(279)	615C8D332663538D96	Hello
ZWAGROUPMEMBERSCHANGE	(12)	43C5A5576D58890798	I am calling
ZWAMEDIAITEM	(475)	9E2DF692BA3797B956	Hello
ZWAMESSAGE	(9065)	068FD58C3CE6DE527F	Answer
ZWAMESSAGEDATAITEM	(6)	BE0813B2958D6A24F6	Hello
ZWAMESSAGEINFO	(3209)	64AECA1E02D0F2990F	Really
ZWAPROFILEPICTUREITEM	(139)	456D2B9C8B762F8B11	Too busy to check on me
ZWAPROFILEPUSHNAME	(70)	2CF262A79E04CCE6EC	How was your coffee date?
ZWAVCARDMENTION	(0)	0E35D0F22DB185C663	Called you
Z_METADATA	(1)	89E2B564743C0D1479	On lunch
Z_MODELCACHE	(1)	049E0CCA79B82721E	Check the other
Z_PRIMARYKEY	(14)	4DE852F3B4012407D1	Ok
		CC38719D2590E069C4	You still on the phone



Deeper Analysis - Messages

SNAPCHAT ISSUES

Snapchat has historically caused investigators problems, but forensic software advances now allow regular recovery of Snapchat text and images.



ID:UNKNOWN_CHAT_NUM_17

Source:Snapchat

Start Time:

Last Activity:

Number of attachments: 1

Extraction:Physical

Source file:

Participants (0)

Conversation

Select/Deselect all...

Enter text to filter ...

Unknown

h1a81hurcs00h139007938907...

Username	lilredmonsta
Username	aj_alvarez008
Username	aydeng7
Username	alssalee
Username	amberhoney22
Username	amber-lee108
Username	murphy321
Username	dmt04
Username	ianjmiller90
Username	that530addict
Username	jessmichellep



Snapchat - CheckM8

ADDED IPHONE DATA

Larger amount of data extracted from iOS devices

Item	Type	Artifact ca...	Date and ti...
+19162079716	iOS iMessage/SMS/MMS	Chat	4/13/2020 4:24:02 PM
Don Vilfer (+19162079716)	iOS iMessage/SMS/MMS	Chat	4/13/2020 4:24:02 PM
Local User <FullFileSystem.1.dar>	iOS Call Logs	Mobile	4/13/2020 4:33:18 PM
Starbucks WiFi	iOS Wi-Fi Profiles	Mobile	4/13/2020 4:40:46 PM
38.911289405386	Cached Locations	Operating System	4/13/2020 4:46:56 PM
Local User <FullFileSystem.1.dar>	iOS iMessage/SMS/MMS	Chat	4/13/2020 4:47:00 PM
Local User <FullFileSystem.1.dar>	iOS iMessage/SMS/MMS	Chat	4/13/2020 4:47:00 PM
38.9078710821536	Cached Locations	Operating System	4/13/2020 4:47:15 PM
+19162079716	iOS iMessage/SMS/MMS	Chat	4/13/2020 4:48:43 PM
Don Vilfer (+19162079716)	iOS iMessage/SMS/MMS	Chat	4/13/2020 4:48:43 PM
Local User <FullFileSystem.1.dar>	iOS iMessage/SMS/MMS	Chat	4/13/2020 4:49:38 PM
Local User <FullFileSystem.1.dar>	iOS iMessage/SMS/MMS	Chat	4/13/2020 4:49:38 PM
Local User <FullFileSystem.1.dar>	iOS iMessage/SMS/MMS	Chat	4/13/2020 4:50:21 PM
Local User <FullFileSystem.1.dar>	iOS iMessage/SMS/MMS	Chat	4/13/2020 4:50:21 PM
jackwalsh1864	Snapchat Chat Messages	Chat	4/13/2020 4:51:39 PM
jackwalsh1864	iOS Snapchat Conversations	Chat	4/13/2020 4:51:39 PM
38.9077210934186	Cached Locations	Operating System	4/13/2020 4:55:16 PM
Unplugged	KnowledgeC Device Plugged-in States	Operating System	4/13/2020 5:08:28 PM
com.spotify.client	KnowledgeC Media History	Operating System	4/13/2020 5:08:31 PM
56	Apple Health Steps	Internet of Things	4/13/2020 5:09:15 PM
Local User <FullFileSystem.1.dar>	iOS Call Logs	Mobile	4/13/2020 5:12:24 PM
Plugged in	KnowledgeC Device Plugged-in States	Operating System	4/13/2020 5:40:04 PM

FullFileSystem.1.dar

PREVIEW

E3C6-470D-A1F6-8D02DA6E6AB3

DONVILSER20

4/13/2020 4:05:55 PM

Sent attachment
324484586819155461r

JACKWALSH1864

4/13/2020 4:09:47 PM

Sent attachment
JACKWALSH1864~016C9EB6-A10A-44D6-8B24-D7D25C0430D8

JACKWALSH1864

4/13/2020 4:51:39 PM

What's up

Time zone UTC-8:00

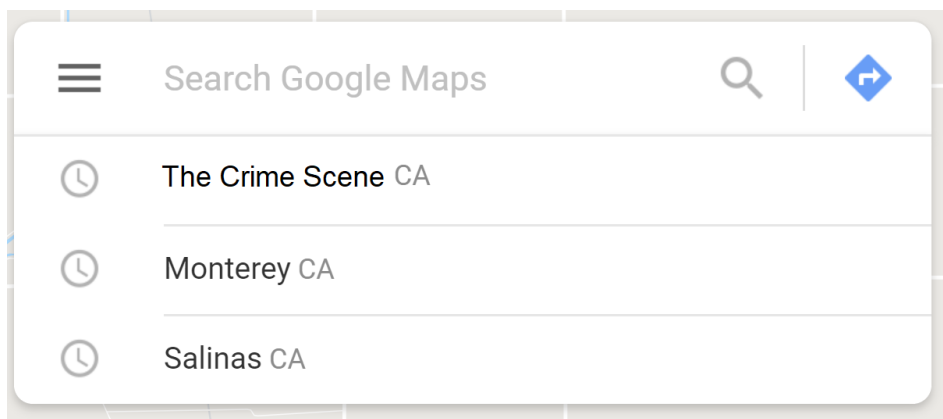
Deeper Analysis - Location

Deeper Analysis - Location

DEVICE LOCATION DATA

Location data from apps and data on the device

Apple Maps (4)	Find My iPhone (1)
iPhoneRecentsLog (289) (182)	Reminder Locations (64) (14)
Media Locations (137) (1)	Wireless Networks (161)
Safari (13)	Twitter Message (22) (22)
Waze Favorites (4) (2)	Facebook (47) (31)
Waze History (92) (1)	Google Maps (25) (5)
Waze Recents (88) (1)	



To point ▼

(42.416867, -70.909918)



Deeper Analysis - Location

LOCATION METADATA

Location data stored in image or video files



Created: 12/21/2013 20:50(UTC-8)
Accessed: 12/21/2013 20:50(UTC-8)
Modified: 12/21/2013 20:50(UTC-8)

Metadata

Camera Make: Apple
Camera Model: iPhone 5c
Capture Time: 12/21/2013 20:36
Pixel resolution: 1536x2048
Resolution: 72x72 (Unit: Inch)
Lat/Lon: 36.840294 / -121.391450

Map

Position: (36.840294, -121.391450)
Address:
Map Address:




Deeper Analysis - Location

WIFI LOCATION DATA

Stored networks can provide location information

Last Connected ▾	Last Auto Connected ▾	↑ BSSID ▾	SSID ▾
3/6/2016 2:49:26 PM(UTC-8)		E0:10:7F:26:DD:C8	Westgate_Las_Vegas
11/6/2016 9:30:03 AM(UTC-8)	11/6/2016 12:42:58 PM(UTC-8)	00:0D:67:36:C7:FB	CableWiFi
12/27/2016 10:19:05 AM(UTC-8)	12/28/2016 9:26:02 AM(UTC-8)	00:0F:CC:6F:89:EC	HI Express Grass Valley
	7/6/2017 9:52:33 AM(UTC-7)	00:23:EB:27:2C:42	Guest
5/2/2017 9:48:47 PM(UTC-7)		04:A1:51:91:1E:70	Pete's Pizza Guest

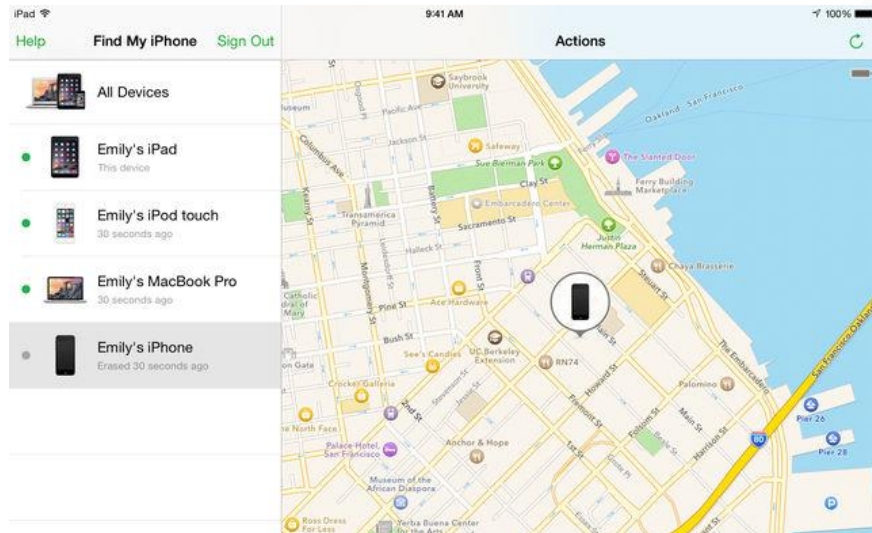
Last Connected ▾	Last Auto Connected ▾	↑ BSSID ▾	SSID ▾
		60:02:92:F5:DB:E8	Carlins-wifi



Deeper Analysis - Location

CLOUD LOCATION DATA

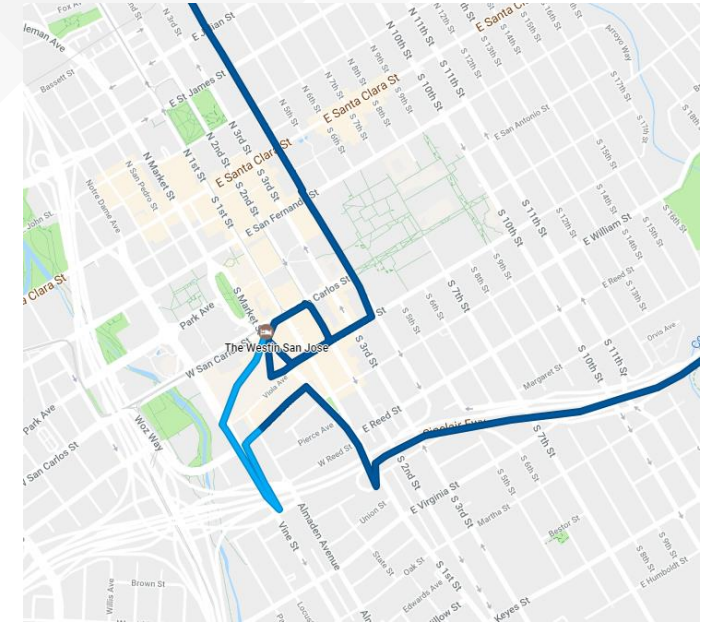
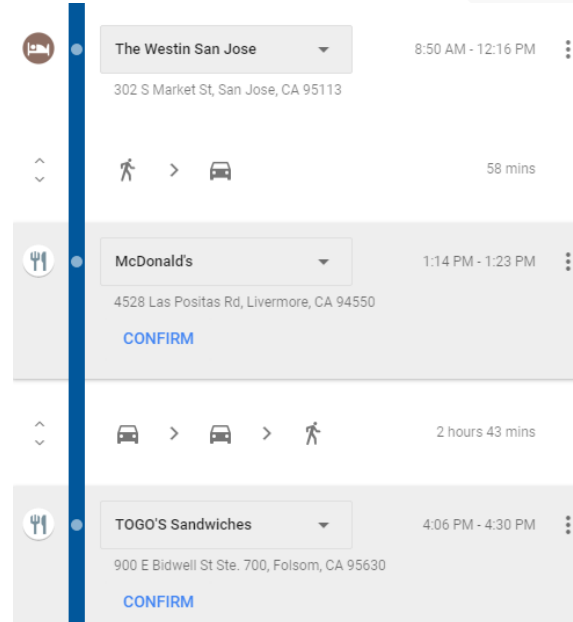
Location data from Social Media and Cloud sites



Find My iPhone



Find My Device
by Google Play Protect



Deeper Analysis - Location

CLOUD LOCATION DATA

Location data from Social Media and Cloud sites

Posted on February 9, 2010
by [don't try this](#)



Now it's off to work in my beast. Wait... How'd that DOG get in there?

- ❖ Metadata from uploaded images since this twitter post by MythBusters actor led hundreds of fans to his house.
- ❖ Social Media sites will store metadata in a separate location on their servers, so may be available via subpoena or court order.

Deeper Analysis - Location

CELL SITE LOCATION DATA

Mapping of cell site data to show path of movement

- Data not had elsewhere
- Ping data and geolocation data
- Transactional records

Deeper Analysis - Location

CELL SITE LOCATION DATA

Mapping of cell site data to show path of movement



Cell Site data retained for 1 year



Cell Site data retained for 23 months



Cell Site data retained for 18 months




Cell Site data retained for 7 years

Deeper Analysis - Location

CELL SITE LOCATION DATA

Mapping of cell site data to show path of movement

MOBILITY USAGE (with cell location)								
AT&T has queried for records using Mountain Time Zone. AT&T's records are stored and provided in UTC.								
								
Conn.Date	Conn. Time UTC	Originating #	Terminating #	IMEI	IMSI	Desc	MAKE	MODEL
Cell Location								

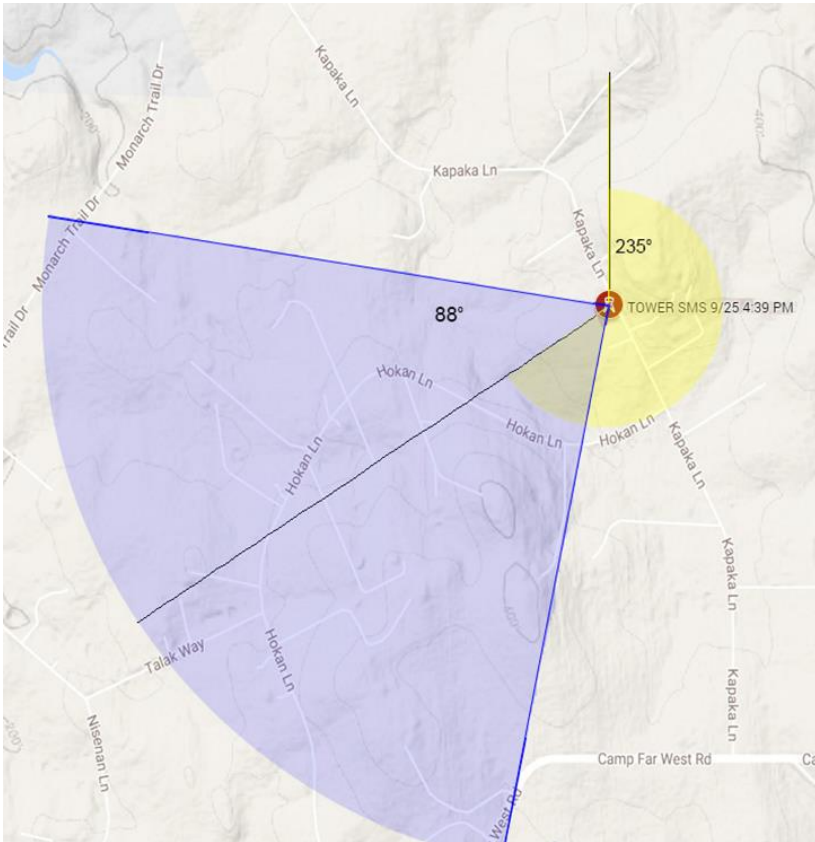
SMST APPLE IPHONE6 [42962/41512:-116.64361:48.36667:235:88.0]
SMST APPLE IPHONE6 [42962/41512:-116.64361:48.36667:235:88.0]
SMST APPLE IPHONE6 [42962/41512:-116.64361:48.36667:235:88.0]

LAC/CID:Longitude:Latitude:Azimuth:BeamWidth]

Deeper Analysis - Location

CELL SITE LOCATION DATA

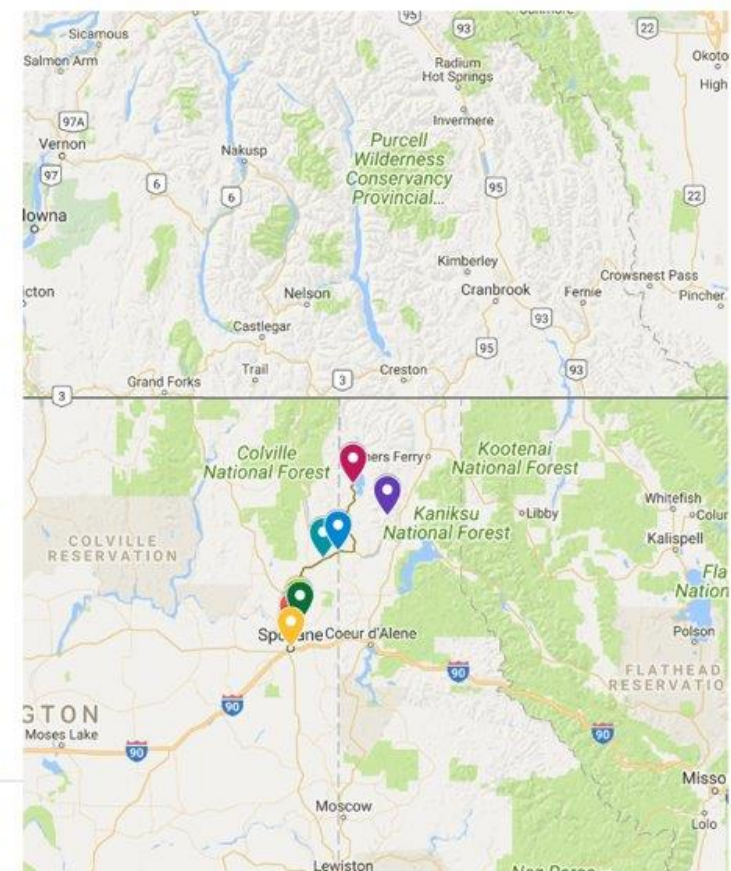
Mapping of cell site data to show path of movement



Track 005

- 2:04PM
- 2:46PM
- 2:54PM
- 3:37 pm
- 47.784771 -117.380151
- AT&T Tower
- AT&T Tower A
- AT&T Tower B2
- AT&T Tower C

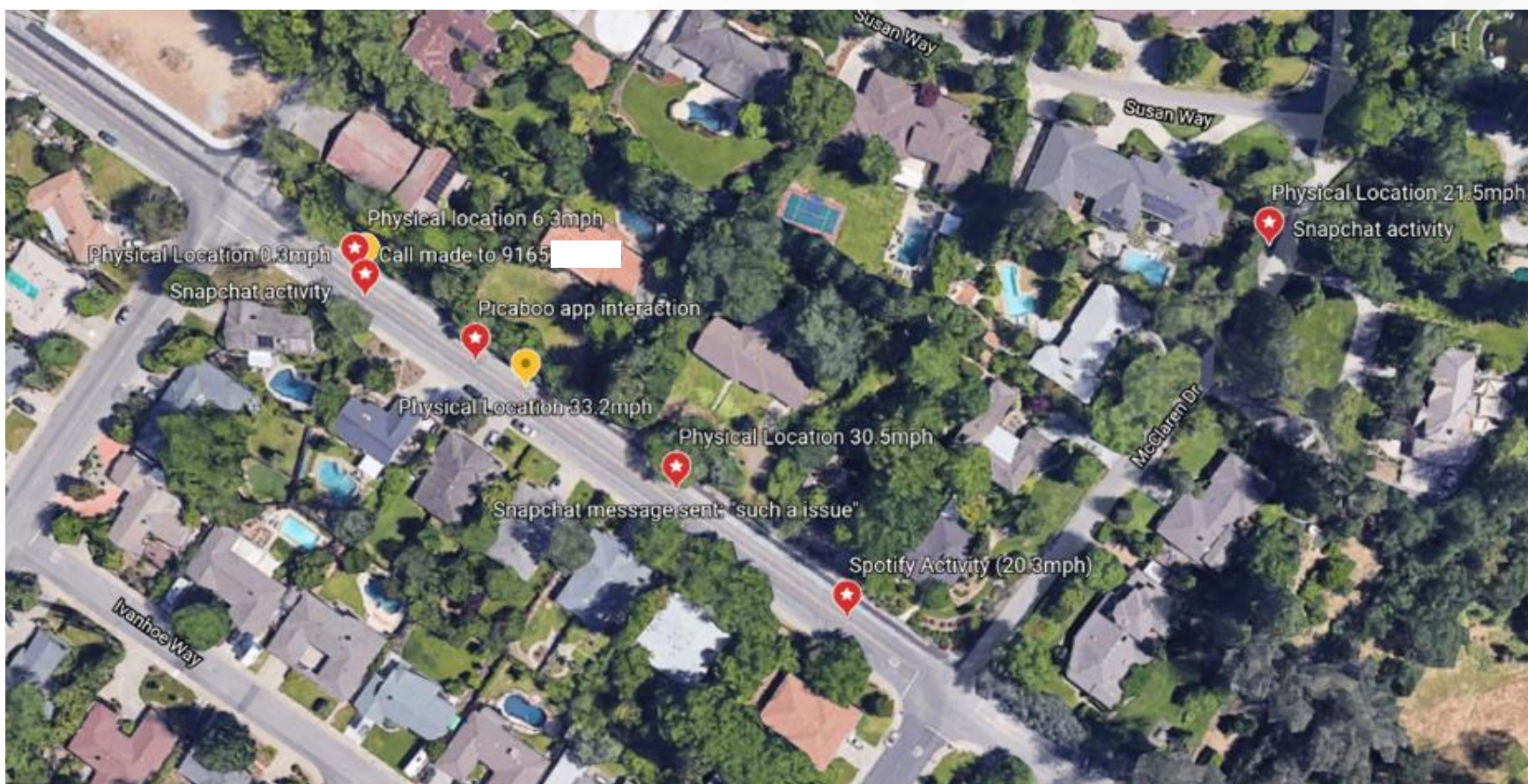
Date: Sep 29, 2017 2:04 pm
Distance: 72.2 miles Elapsed Time: 1:33:34 Avg Speed: 46.3 mph Max Speed: 79.5 mph Avg Pace: 1' 17" per mile Min Altitude: 1,755 ft Max Altitude: 2,606 ft Start Time: 2017-09-29T21:04:05Z Start Location: Latitude: 47° 49' 04" N Longitude: 117° 21' 51" W Finish Time: 2017-09-29T22:37:39Z Finish Location: Latitude: 48° 32' 17" N Longitude: 116° 55' 22" W



New Advances – CheckM8 and GrayKey

ADDED IPHONE DATA

Larger amount of data extracted from iOS devices





















Cellphone Activity - Timeline

Cellphone Activity - Timeline

TIMELINE ANALYSIS

Timeline can show all activity around an incident

			Call Log	6/16/2017 10:53(UTC-7)	From: +1916		00:00:00
			Call Log	6/16/2017 10:54(UTC-7)	To: +1916		00:00:19
			Image: Location	6/16/2017 15:05			IMG_2799.JPG
			Video: Location	6/16/2017 15:05(UTC-7)			IMG_2799.MOV
			Video: Location	6/16/2017 15:05(UTC-7)			FullSizeRender.mov
			Image: Location	6/16/2017 15:05			FullSizeRender.jpg
×			Call Log	6/16/2017 15:10(UTC-7)	From: +1916	Dad 	00:01:44
×			Call Log	6/16/2017 16:32(UTC-7)	From: +1916	Dad 	00:00:24
×			Call Log	6/17/2017 18:03(UTC-7)	From: +1408	Mum    	00:00:00
			Call Log	6/17/2017 18:05(UTC-7)	To: +1408	Mum    	00:21:23
			Searched Items	6/17/2017 23:43(UTC-7)			farthers day drawings by kids
×			Web History	6/17/2017 23:44(UTC-7)			father's day drawings by kids - Google Search

Cellphone Activity - Timeline

EXAMPLE CASE

The case of Tony Scott Cercy

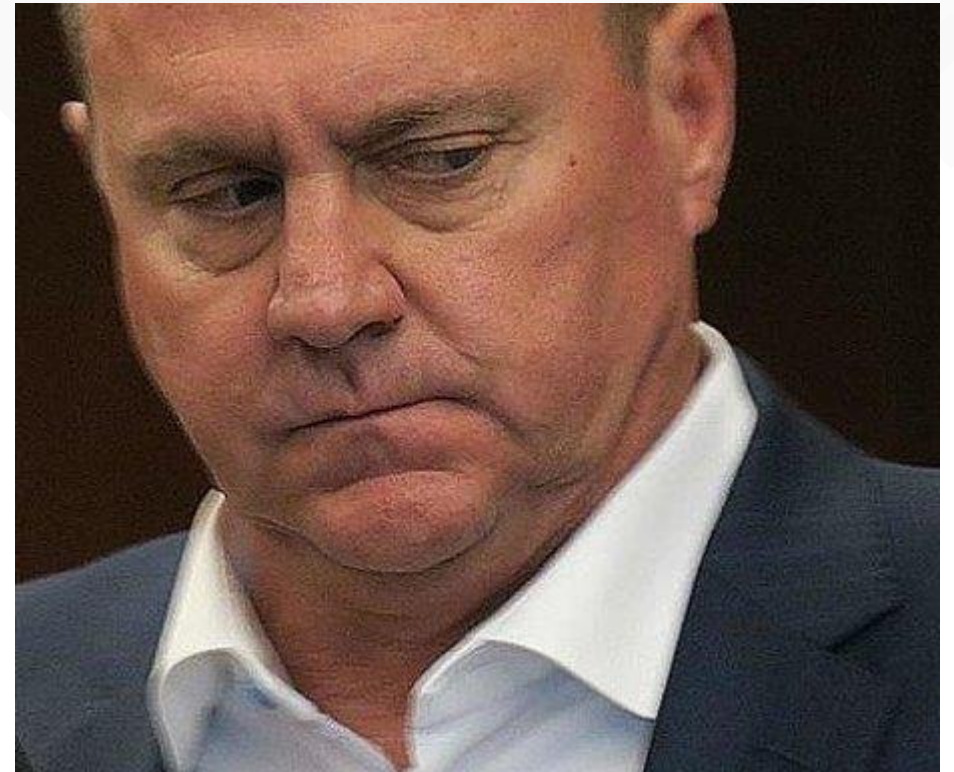
7/28/2017

- ❖ Mr Cercy testified that he was asleep during the time period of a sexual assault

*“The **timeline** created identified several mobile cell phone artifacts that indicated that Tony Cercy's cellular phone ... was accessed and used **during the specified timeframes** including when the victim alleged the sexual assault..”*

Feb 27, 2019

- ❖ Former Casper businessman Tony Scott Cercy sentenced to 6-8 years for Third-Degree Sexual Assault



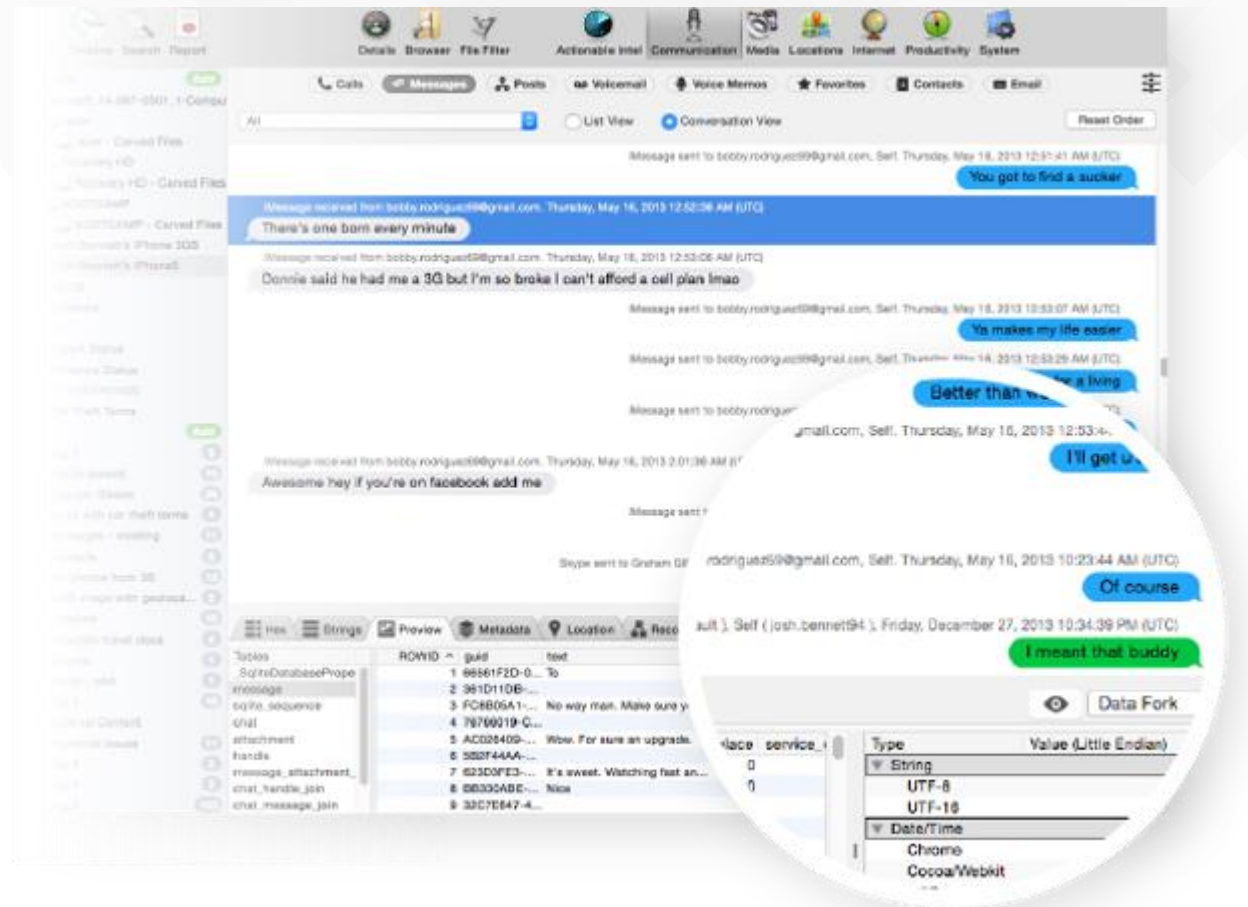
Final Product - Ready for review

THE PRODUCT **YOU WANT**

Results can be in many possible formats to provide clear understanding

Report vs Extraction

Report Formatting





Digital Evidence Ventures



Meridian, ID 208-401-3740
Roseville, CA (916) 883-2020

THANK YOU



PLEASE FOLLOW US FOR ARTICLES AND NEWS

DON@DIGITALEVIDENCEVENTURES.COM

WWW.DIGITALEVIDENCEVENTURES.COM