Cellphone Forensics:

Applications in Discovery and Investigations

Thomas Plunkett, EnCE, CISSP

Director, Digital Forensics

ArcherHall
AIM HIGH

TPlunkett@ArcherHall.com
855.839.9084

Digital Forensics & eDiscovery experts serving attorneys in all 50 states

- Cellphones
- Computers & Tablets
- External Hard Drives
- Smart Devices
- Emails & SMS
- Social Media Accounts
- Cloud Data
- Electronic Medical Records

BUSINESS LITIGATION

EMPLOYMENT LAW

SCHOOLS AND HIGHER-ED

MEDICAL MALPRACTICE

IP THEFT

BANKRUPTCY

Agenda

- **Mobile Technology & Trends**
  - What Do We Mean?
  - Internet of Things
  - Trends and BYOD
- **The Forensic Process**
  - Proper Handling
  - Importance of Preservation
  - Lifecycle of Deleted Content
  - Extraction
  - Data Types
  - Communications
  - Images
  - Location Data
  - Digging Deeper
- **Right to Privacy**
  - SCA Location Data
  - Reasons for Resistance
- **Preservation**
  - Early Preservation
  - FRCP Rule 37(e)
- **The Future**
  - Forensic Footprints
  - The Cloud

MOBILE TECHNOLOGY

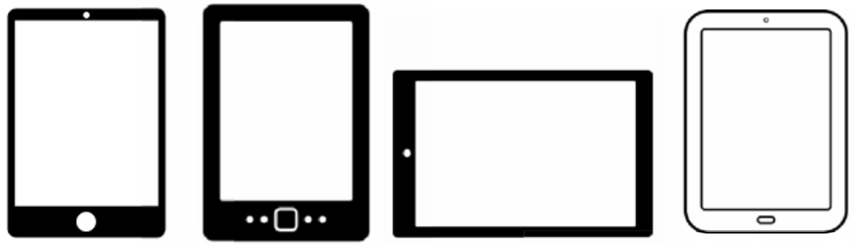
ARCHERHALL
AIM HIGH

What Do We Mean By Mobile Technology?

Cellphones:

SMART PHONES
NOT SO SMART PHONES

Tablets:



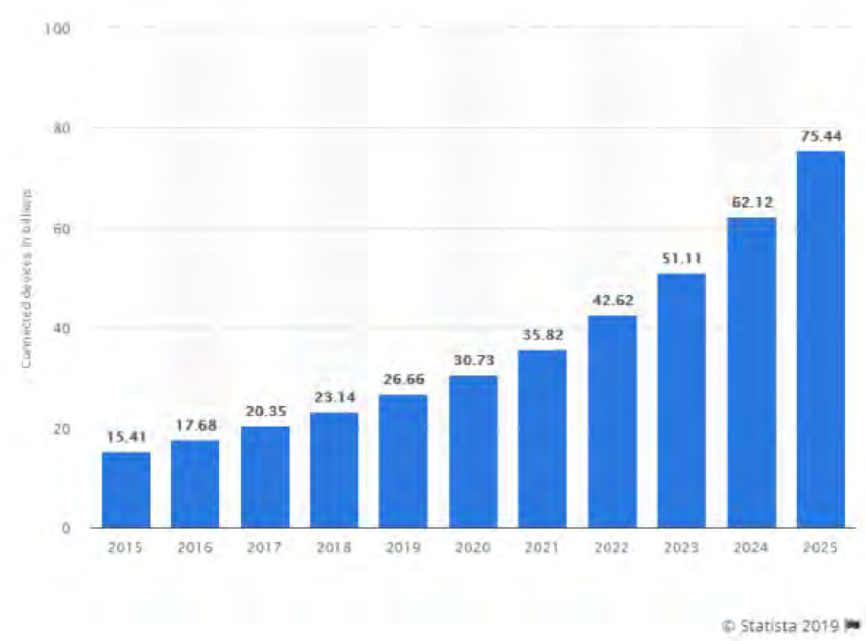
Wearables:

The Internet of Things

Additional devices thanks in part to the rise of the Echo.

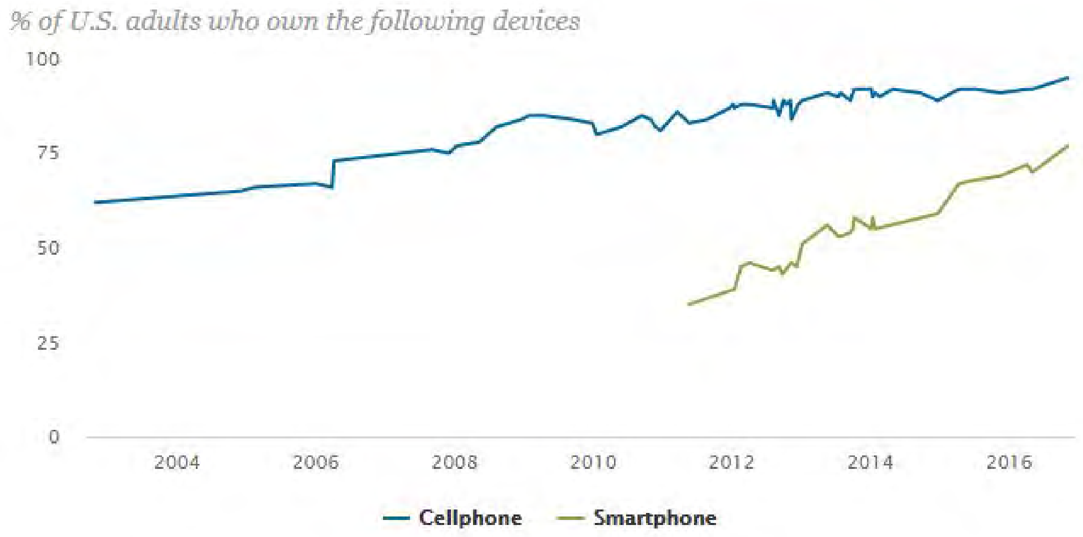
- Thermostats
- Light Bulbs
- Crockpots
- Garage Door Opener
- Door Locks
- Refrigerator
- Camera Systems
- Beds

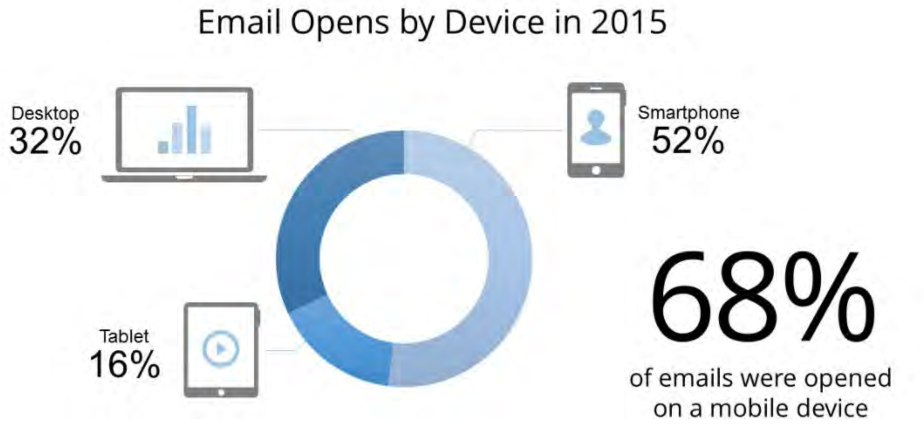
Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)



© Statista 2019

Trend Growth





Data Source: US Consumer Device Preference Report, 2015 Year in Review, Movable Ink
http://go.movableink.com/Device-Report-2015-Review.html

ezoic

Cellphone ownership > 95%

77% own Smart Phones

Increase of work done on Cellphones

Trend Growth

- **According to Stroz Friedberg**
  - The trends of bring-your-own-device (BYOD) and the use of personal online accounts have become prevalent in American businesses, as workers use their personal smartphones, tablets, and preferred cloud providers.
    - 71% of survey respondents admitted to frequently or occasionally sending materials to a personal email account or uploading materials to a personal cloud account.
  - Among the sample:
    - The reason cited most often (37%) is that they have a preference for using their personal computer over their work computers.
    - 14% find that it's too much effort to bring their work laptop home with them.

Trend Growth

- **According to Stroz Friedberg**
  - Corporate managers also put their companies at risk of intellectual property loss if and when they depart the company.
    - 51% of senior management admit to taking job-related emails, files, or materials with them when they have left past employers.
    - 37% of mid-level management
    - 20% of lower ranking employees have done so.

THE FORENSIC PROCESS

ARCHERHALL
AIM HIGH

Proper Handling

What Steps Should You Take Upon Receiving Evidence?

Step 1. If the device is off, leave it off - If the device is on, leave it on.

Step 2. If it's on: Place into 'Airplane Mode'.

Step 3. Make sure to gather all passcode / password information.

Step 4. Hand to a Digital Forensic Specialist.

Next Steps Will Be:

- Photograph the device
- Use of a Faraday Device
- Start of a Chain of Custody
- Documented Imaging Form

FOLD TOP OF FARADAY BAG OVER TWICE FOR PROPER SIGNAL SHIELDING
1
2
EDEC

Importance of Preservation

Mobile Technology Data is Volatile:

- **Crucial data can be lost by:**
  - User selective deletion
  - App updates
  - Constant OS updates
  - ‘Factory Reset’: simple and effective
  - Remote wipe capability

- **Deleted data may not be recoverable because:**
  - Security on the device
  - Wear Levelling of NAND technology

Life Cycle of Deleted Content

- **Recoverable**
  - Move to Trash or Recycle Bin
  - Emptied Trash or Recycle bin
  - Bypass Trash or Recycle Bin

- **Databases**
  - Have their own file system
  - Do not shrink unless purged
  - Backups typically on retain “Active” content – No deleted
    - New iPhone restored from iCloud backup does not have deleted data

- **Partially or Not recoverable**
  - Partially Overwritten
    - File fragments
  - Fully Overwritten
  - Wiping

Extraction

1. **Logical Extraction**
   - Just the active files of the device – within the operating system.
   - Deleted space, deleted files and fragments will NOT be captured.
   - Essentially everything visible to the user on the cellphone.

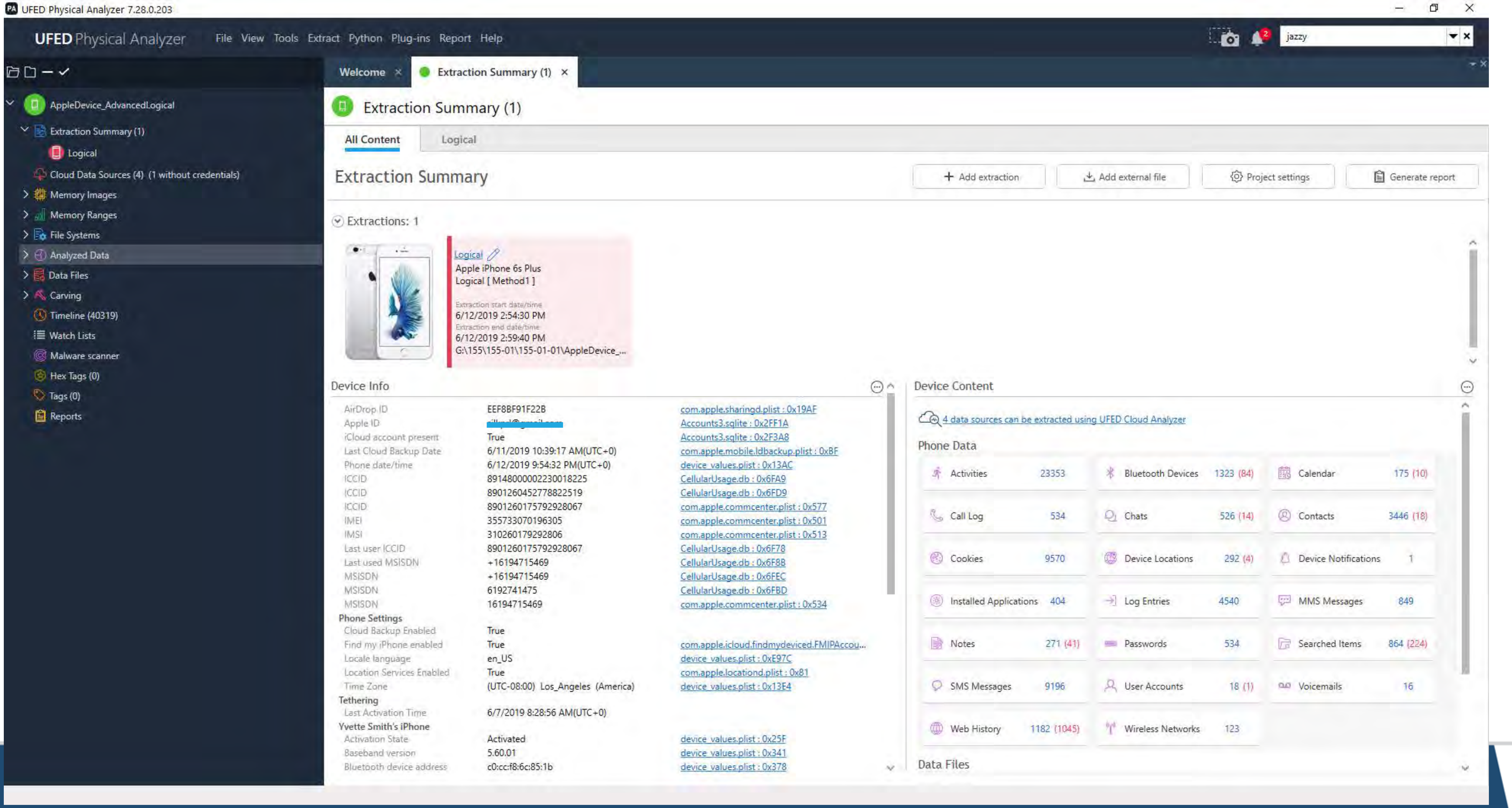
2. **File System Extraction**
   - System files on the device – within the operating system
   - May include some deleted material

3. **Advanced Logical Extraction**
   - iPhone specific extraction
   - Asking OS for files – very helpful OS
   - Databases provided produce a substantial amount of deleted data

Extraction

4. **Physical Extraction**
   - All data on the chip
   - A large amount of deleted data
   - Allows for ‘carving’ of data
   - More likely on an Android
   - iPhone 4 or earlier

Device Summary



Extraction Summary (1)

Extraction Summary

Extractions: 1

Logical
Apple iPhone 6s Plus
Logical [Method1]
Extraction start date/time
6/12/2019 2:54:30 PM
Extraction end date/time
6/12/2019 2:59:40 PM
G:\155\155-01\155-01-01\AppleDevice_...

Device Info

AirDrop ID	EEF8BF91F22B	com.apple.sharingd.plist : 0x19AF
Apple ID	[redacted]	Accounts3.sqlite : 0x2FF1A
iCloud account present	True	Accounts3.sqlite : 0x2F3A8
Last Cloud Backup Date	6/11/2019 10:39:17 AM(UTC+0)	com.apple.mobile.ldbackup.plist : 0xBF
Phone date/time	6/12/2019 9:54:32 PM(UTC+0)	device_values.plist : 0x13AC
ICCID	89148000002230018225	CellularUsage.db : 0x6FA9
ICCID	8901260452778822519	CellularUsage.db : 0x6FD9
ICCID	8901260175792928067	com.apple.commcenter.plist : 0x577
IMEI	355733070196305	com.apple.commcenter.plist : 0x501
IMSI	310260179292806	com.apple.commcenter.plist : 0x513
Last user ICCID	8901260175792928067	CellularUsage.db : 0x6F78
Last used MSISDN	+16194715469	CellularUsage.db : 0x6F8B
MSISDN	+16194715469	CellularUsage.db : 0x6FEC
MSISDN	6192741475	CellularUsage.db : 0x6FBD
MSISDN	16194715469	com.apple.commcenter.plist : 0x534
Phone Settings		
Cloud Backup Enabled	True	
Find my iPhone enabled	True	com.apple.icloud.findmydeviced.FMIPAccou...
Locale language	en_US	device_values.plist : 0xE97C
Location Services Enabled	True	com.apple.locationd.plist : 0x81
Time Zone	(UTC-08:00) Los_Angeles (America)	device_values.plist : 0x13E4
Tethering		
Last Activation Time	6/7/2019 8:28:56 AM(UTC+0)	
Yvette Smith's iPhone		
Activation State	Activated	device_values.plist : 0x25F
Baseband version	5.60.01	device_values.plist : 0x341
Bluetooth device address	c0:cc:f8:6c:85:1b	device_values.plist : 0x378

Device Content

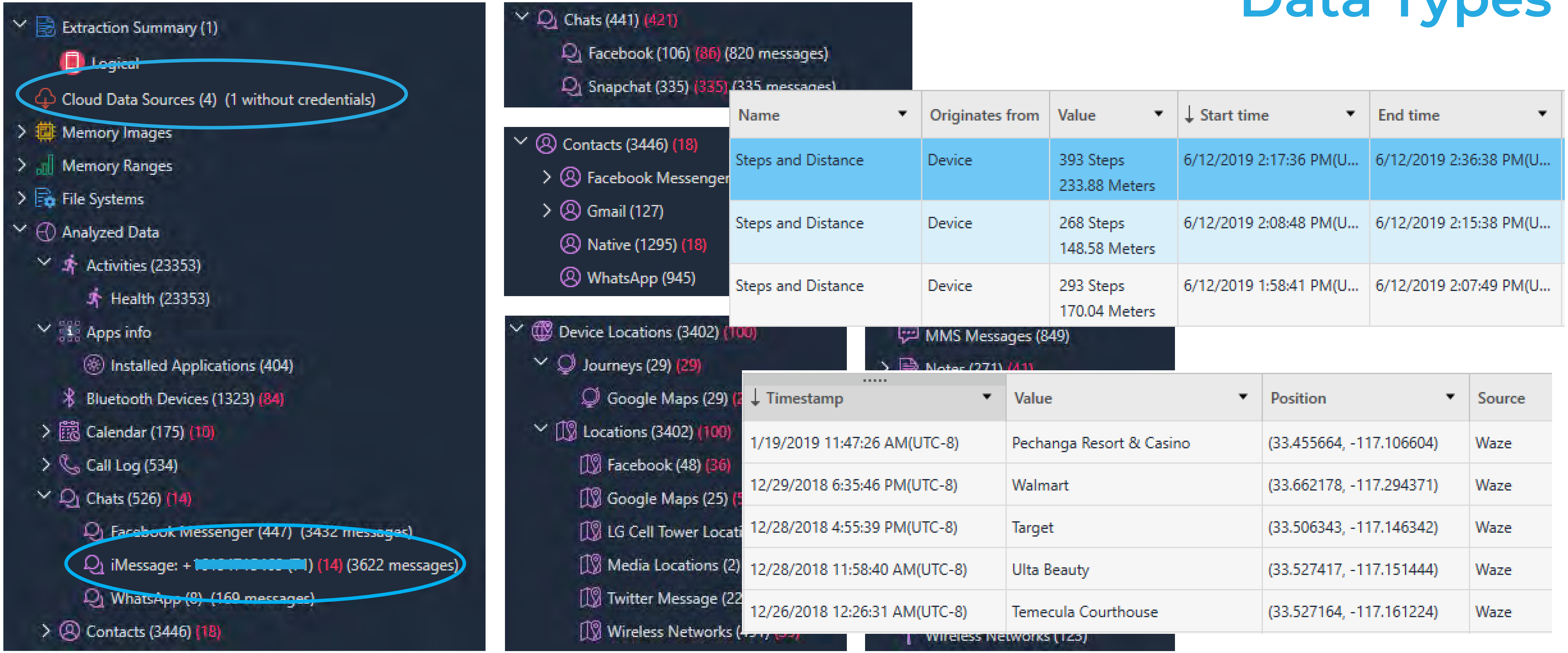
4 data sources can be extracted using UFED Cloud Analyzer

Phone Data

Activities	23353	Bluetooth Devices	1323 (84)	Calendar	175 (10)
Call Log	534	Chats	526 (14)	Contacts	3446 (18)
Cookies	9570	Device Locations	292 (4)	Device Notifications	1
Installed Applications	404	Log Entries	4540	MMS Messages	849
Notes	271 (41)	Passwords	534	Searched Items	864 (224)
SMS Messages	9196	User Accounts	18 (1)	Voicemails	16
Web History	1182 (1045)	Wireless Networks	123		

Data Files

Data Types



- Extraction Summary (1)
  - Logical
  - Cloud Data Sources (4) (1 without credentials)
- Memory Images
- Memory Ranges
- File Systems
- Analyzed Data
  - Activities (23353)
    - Health (23353)
  - Apps info
    - Installed Applications (404)
  - Bluetooth Devices (1323) (84)
  - Calendar (175) (10)
  - Call Log (534)
  - Chats (526) (14)
    - Facebook Messenger (447) (3432 messages)
    - iMessage: +[redacted]) (14) (3622 messages)
    - WhatsApp (8) (169 messages)
  - Contacts (3446) (18)

- Chats (441) (421)
  - Facebook (106) (86) (820 messages)
  - Snapchat (335) (335) (335 messages)

- Contacts (3446) (18)
  - Facebook Messenger
  - Gmail (127)
  - Native (1295) (18)
  - WhatsApp (945)

- Device Locations (3402) (100)
  - Journeys (29) (29)
    - Google Maps (29) (2
  - Locations (3402) (100)
    - Facebook (48) (36)
    - Google Maps (25) (5
    - LG Cell Tower Locati
    - Media Locations (2)
    - Twitter Message (22
    - Wireless Networks (

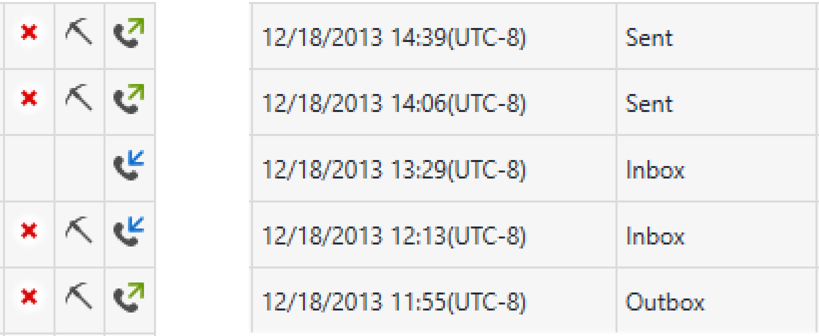
- MMS Messages (849)
- Notes (271) (41)
- Wireless Networks (123)

Name	Originates from	Value	Start time	End time
Steps and Distance	Device	393 Steps 233.88 Meters	6/12/2019 2:17:36 PM(U...	6/12/2019 2:36:38 PM(U...
Steps and Distance	Device	268 Steps 148.58 Meters	6/12/2019 2:08:48 PM(U...	6/12/2019 2:15:38 PM(U...
Steps and Distance	Device	293 Steps 170.04 Meters	6/12/2019 1:58:41 PM(U...	6/12/2019 2:07:49 PM(U...

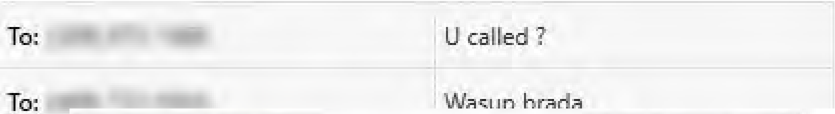
Timestamp	Value	Position	Source
1/19/2019 11:47:26 AM(UTC-8)	Pechanga Resort & Casino	(33.455664, -117.106604)	Waze
12/29/2018 6:35:46 PM(UTC-8)	Walmart	(33.662178, -117.294371)	Waze
12/28/2018 4:55:39 PM(UTC-8)	Target	(33.506343, -117.146342)	Waze
12/28/2018 11:58:40 AM(UTC-8)	Ulta Beauty	(33.527417, -117.151444)	Waze
12/26/2018 12:26:31 AM(UTC-8)	Temecula Courthouse	(33.527164, -117.161224)	Waze

Communications

SMS / MMS

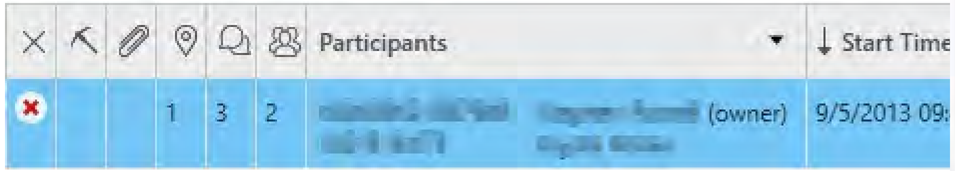


✗	⛏	☎	12/18/2013 14:39(UTC-8)	Sent
✗	⛏	☎	12/18/2013 14:06(UTC-8)	Sent
		☎	12/18/2013 13:29(UTC-8)	Inbox
✗	⛏	☎	12/18/2013 12:13(UTC-8)	Inbox
✗	⛏	☎	12/18/2013 11:55(UTC-8)	Outbox

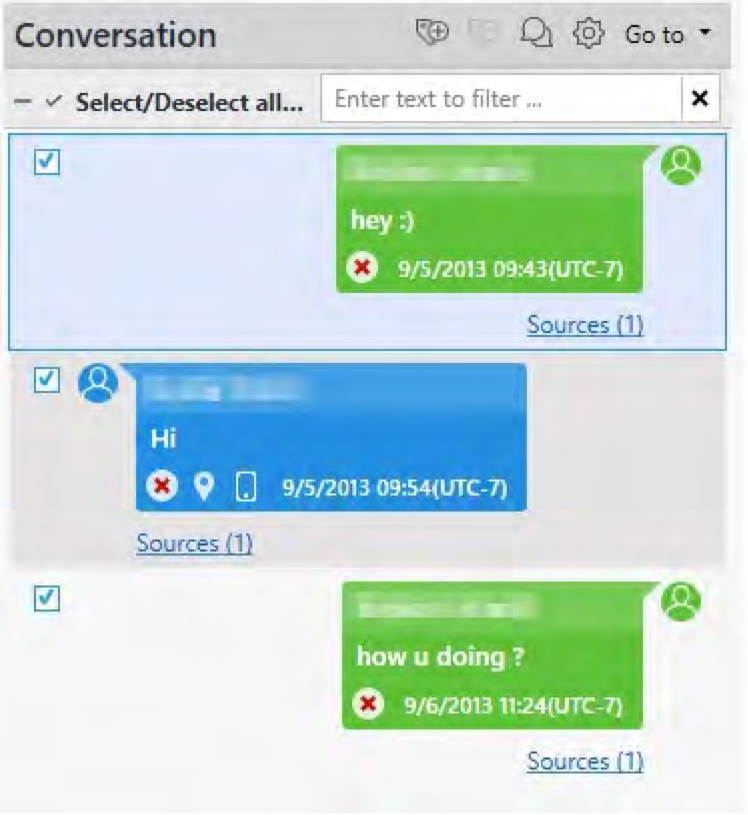


To: [redacted]	U called ?
To: [redacted]	Wasup brada
From:	
From:	
To: [redacted]	

CHATS



✗	⛏	📎	📍	💬	👥	Participants ▾	↓ Start Time
☒			1	3	2	[redacted] [redacted] (owner)	9/5/2013 09:

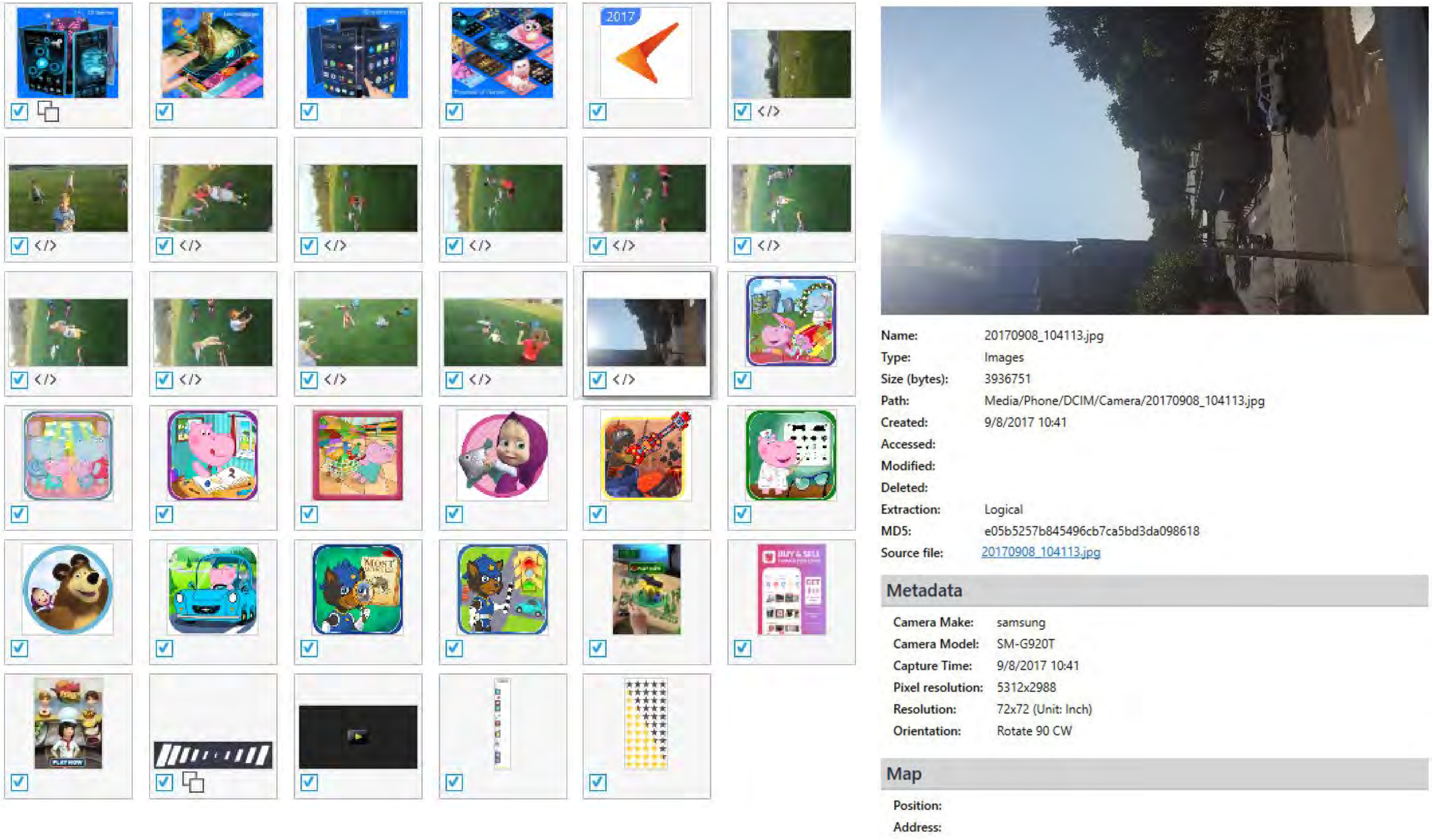


☑ [redacted]
hey :)
☒ 9/5/2013 09:43(UTC-7)
Sources (1)

☑ [redacted]
Hi
☒ 📍 9/5/2013 09:54(UTC-7)
Sources (1)

☑ [redacted]
how u doing ?
☒ 9/6/2013 11:24(UTC-7)
Sources (1)

Images



Name: 20170908_104113.jpg
Type: Images
Size (bytes): 3936751
Path: Media/Phone/DCIM/Camera/20170908_104113.jpg
Created: 9/8/2017 10:41
Accessed:
Modified:
Deleted:
Extraction: Logical
MD5: e05b5257b845496cb7ca5bd3da098618
Source file: 20170908_104113.jpg

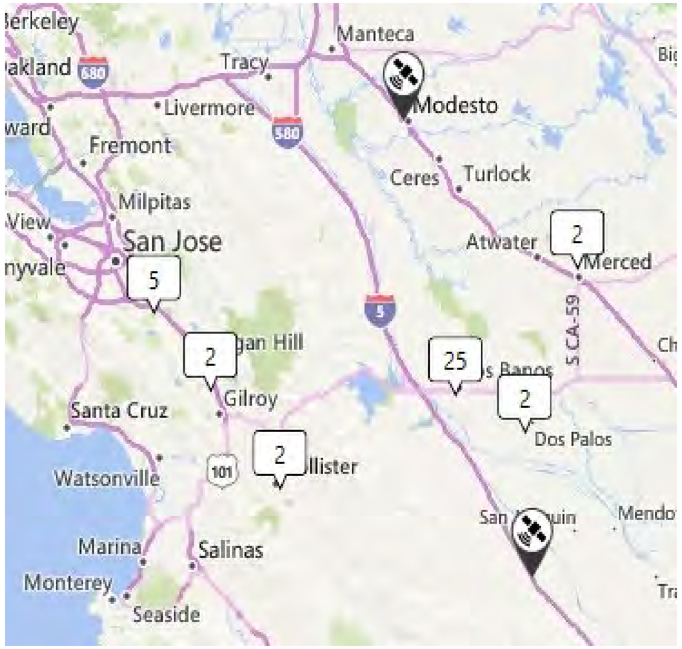
Metadata

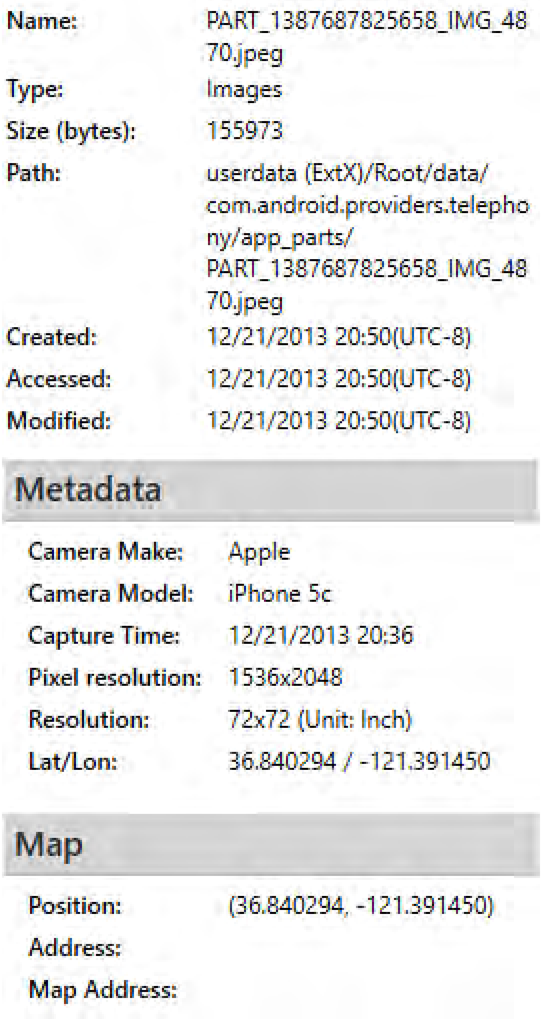
Camera Make: samsung
Camera Model: SM-G920T
Capture Time: 9/8/2017 10:41
Pixel resolution: 5312x2988
Resolution: 72x72 (Unit: Inch)
Orientation: Rotate 90 CW

Map

Position:
Address:

Location Data – Media Metadata





Name:	PART_1387687825658_IMG_4870.jpeg
Type:	Images
Size (bytes):	155973
Path:	userdata (ExtX)/Root/data/com.android.providers.telephony/app_parts/PART_1387687825658_IMG_4870.jpeg
Created:	12/21/2013 20:50(UTC-8)
Accessed:	12/21/2013 20:50(UTC-8)
Modified:	12/21/2013 20:50(UTC-8)

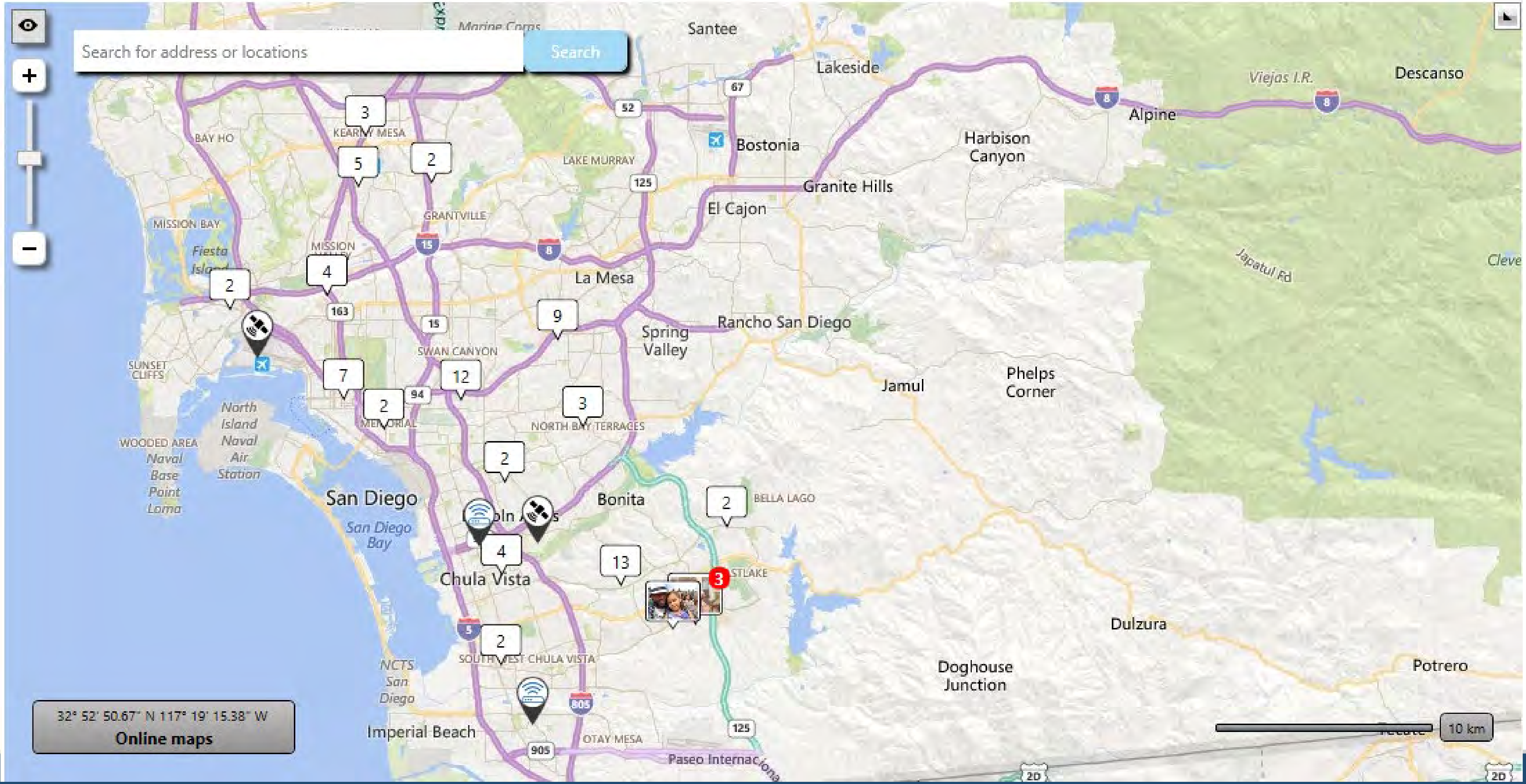
Metadata

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

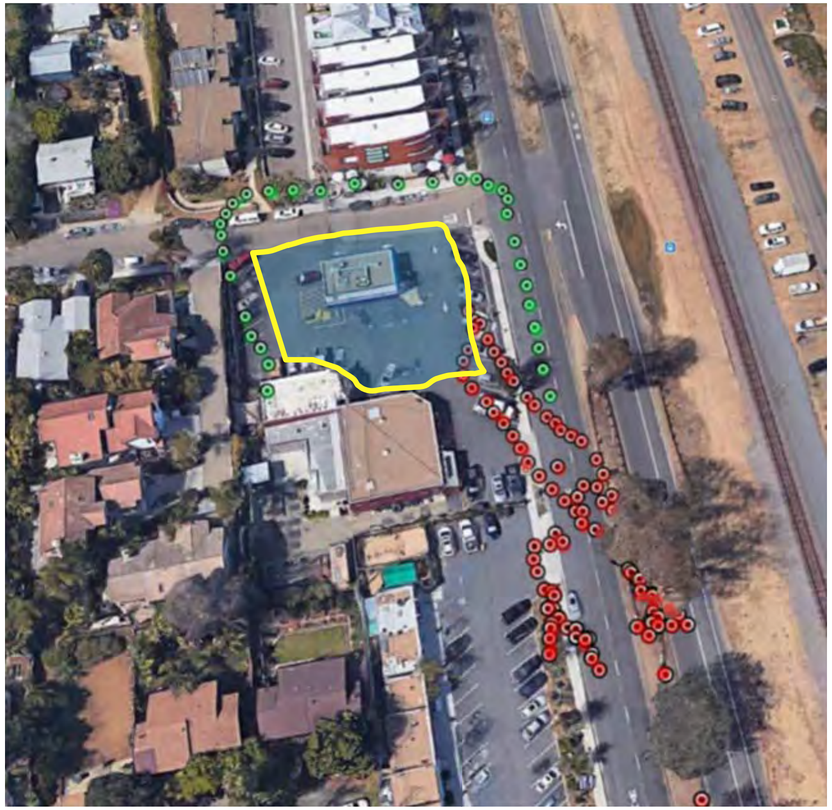
Position:	(36.840294, -121.391450)
Address:	
Map Address:	

Location Data - Automated



Location Data – Manually Extracted

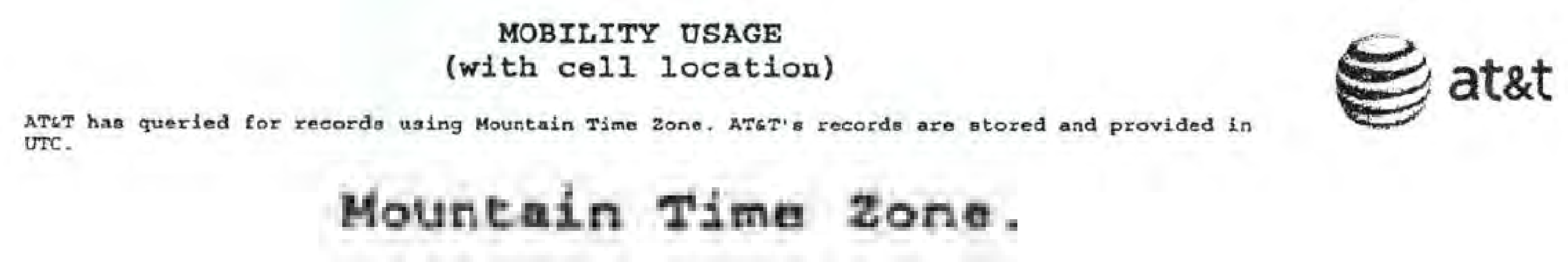
Plot from Wahoo Fitness app



Location Data Animated

Location Data – Cell tower - Network Subpoena

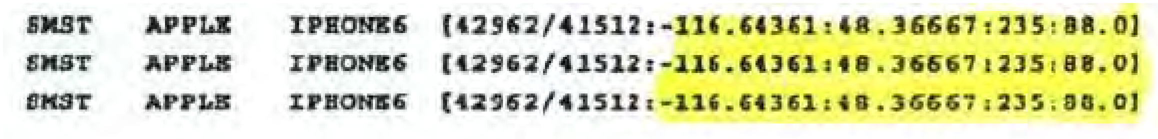
GSM - Global System for Mobile Communications



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.

Mountain Time Zone.

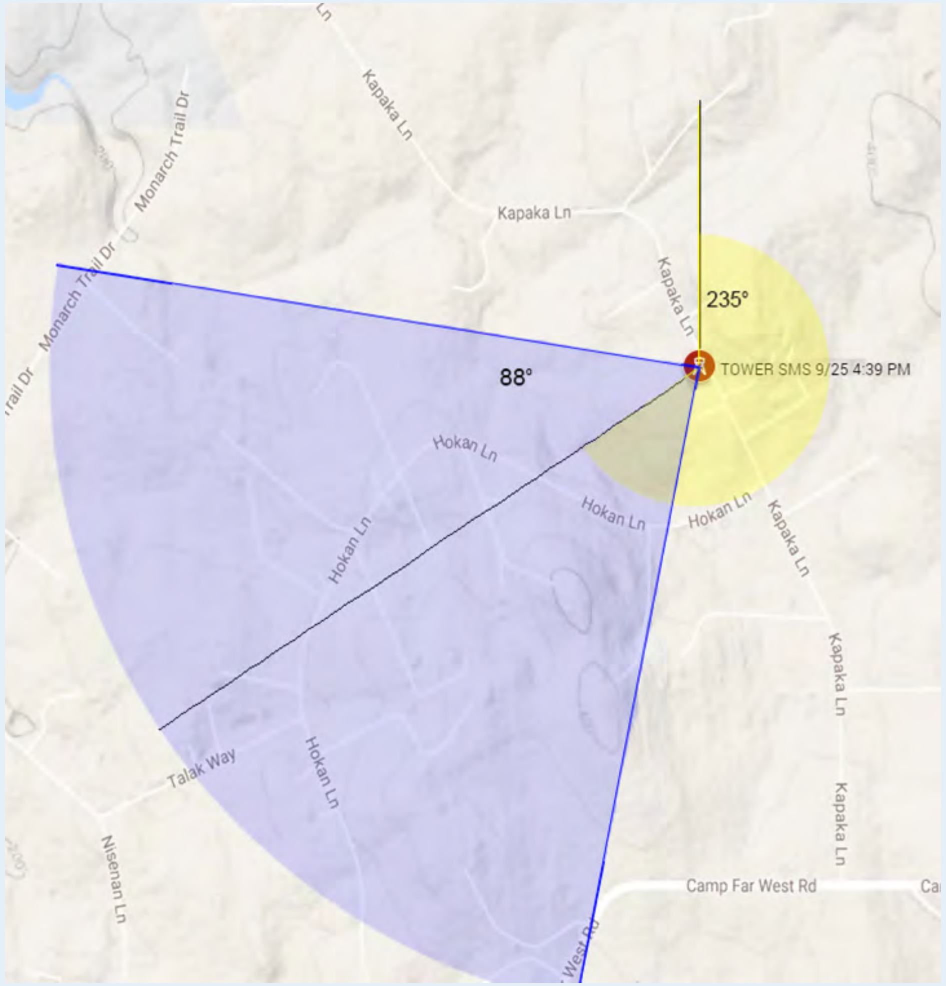


Conn.Date	Conn. Time UTC	Originating #	Terminating #	IMEI	IMSI	Desc	MAKE	MODEL	Cell Location
						SMST	APPLE	IPHONE6	[42962/41512:-116.64361:48.36667:235:88.0]
						SMST	APPLE	IPHONE6	[42962/41512:-116.64361:48.36667:235:88.0]
						SMST	APPLE	IPHONE6	[42962/41512:-116.64361:48.36667:235:88.0]

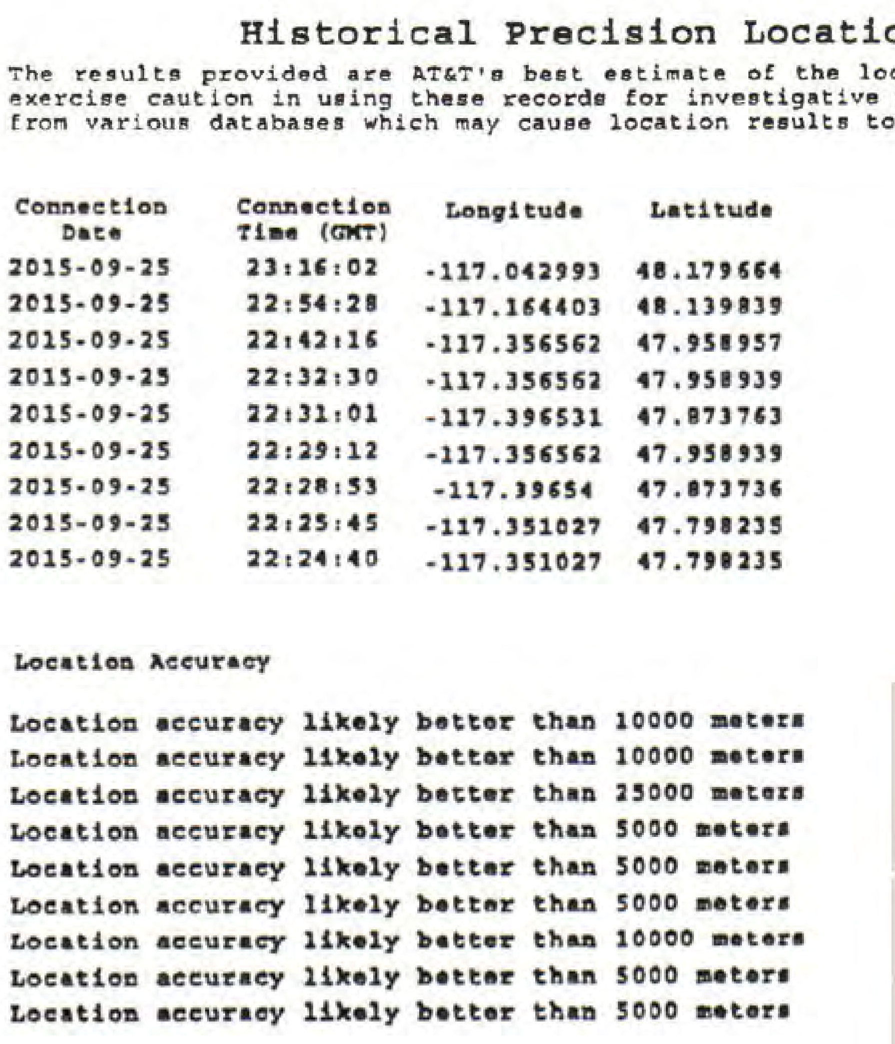
[LAC/CID:Longitude:Latitude:Azimuth:BeamWidth]

Location Data – Mapping Tower Data

- **LAC/CID Longitude, Latitude**
  - Location of the Tower
- **Azimuth**
  - Sector angle from due North
- **Beam Width**
  - Angle of coverage of sector.



Location Data – Mapping Other Data



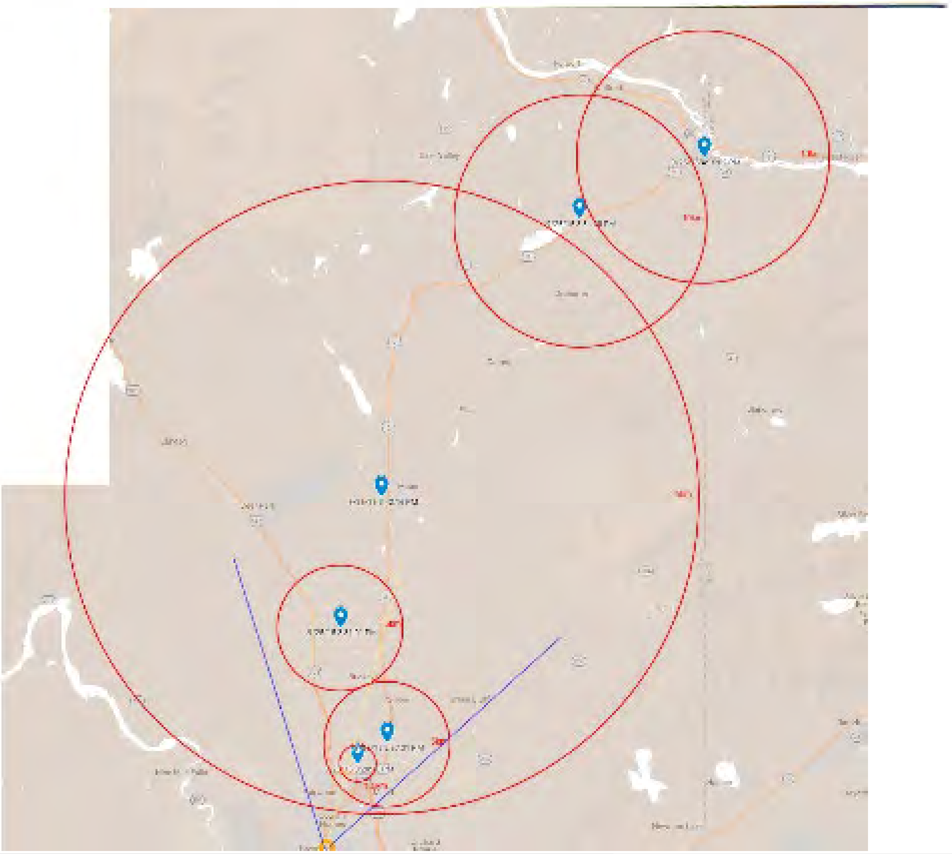
Historical Precision Location Information

The results provided are AT&T's best estimate of the location of the target number. Please exercise caution in using these records for investigative purposes as location data is sourced from various databases which may cause location results to be less than exact.

Connection Date	Connection Time (GMT)	Longitude	Latitude
2015-09-25	23:16:02	-117.042993	48.179664
2015-09-25	22:54:28	-117.164403	48.139839
2015-09-25	22:42:16	-117.356562	47.958957
2015-09-25	22:32:30	-117.356562	47.958939
2015-09-25	22:31:01	-117.396531	47.873763
2015-09-25	22:29:12	-117.356562	47.958939
2015-09-25	22:28:53	-117.39654	47.873736
2015-09-25	22:25:45	-117.351027	47.798235
2015-09-25	22:24:40	-117.351027	47.798235

Location Accuracy

Location accuracy likely better than 10000 meters
Location accuracy likely better than 10000 meters
Location accuracy likely better than 25000 meters
Location accuracy likely better than 5000 meters
Location accuracy likely better than 5000 meters
Location accuracy likely better than 5000 meters
Location accuracy likely better than 10000 meters
Location accuracy likely better than 5000 meters
Location accuracy likely better than 5000 meters



Digging Deeper

- **Malware Scan**
  - Very important in Family Law cases
  - Very common in CP cases that the defendant claims virus

- **Cloud Sharing Analysis**
  - Pull down iPhone or iPad backups
  - Check iCloud Drive and iCloud Photos
  - DropBox etc. key for Theft of IP

RIGHT TO PRIVACY

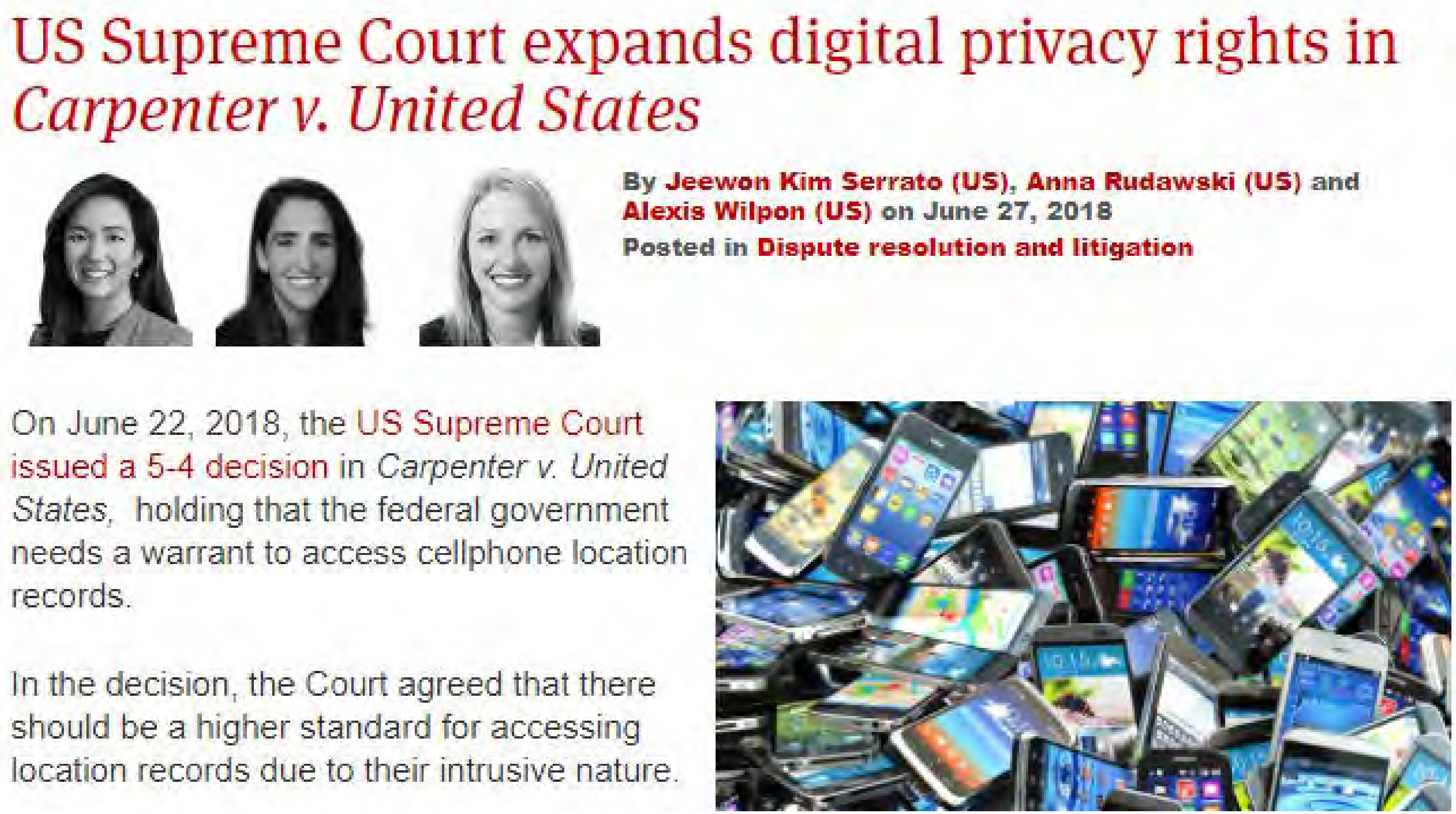
ArcherHall
AIM HIGH

RIGHT TO PRIVACY – SCA Location Data

- U.S. Court of Appeals for the Eleventh Circuit's decision in United States v. Davis.
  - Prosecutors' c ls
  - NOT a violatic able search and seizure.

- A cell phone ver a cell service carrie tions, the opinion held, a crime scene.

- This decision ne metadata privacy more



US Supreme Court expands digital privacy rights in *Carpenter v. United States*

By Jeewon Kim Serrato (US), Anna Rudawski (US) and Alexis Wilpon (US) on June 27, 2018
Posted in Dispute resolution and litigation

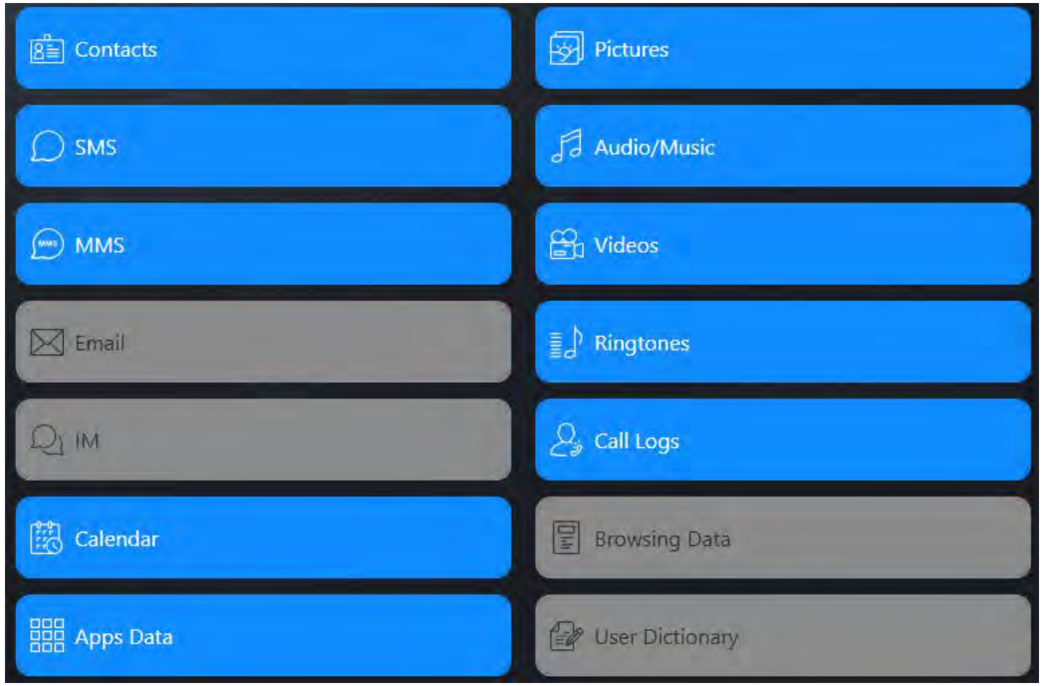
On June 22, 2018, the US Supreme Court issued a 5-4 decision in *Carpenter v. United States*, holding that the federal government needs a warrant to access cellphone location records.

In the decision, the Court agreed that there should be a higher standard for accessing location records due to their intrusive nature.

RIGHT TO PRIVACY – Reasons for Resistance

- **Cellphone resistance to extraction**
  - Adult images
  - Private conversations
  - Mistrust of giving more information than needed

- **Solutions:**
  - Selective extraction
    - Only on Android
    - No deleted data
    - Just SMS
    - Just images
  - **Triangle agreement**



PRESERVATION

ArcherHall
AIM HIGH

Preservation

- Mobile data is Volatile
- Preserve as early and thoroughly as possible
- Advise clients to change settings to keep messages “forever”
- Preserve data from backups and the device itself

Preservation

- FRCP Rule 37(e)

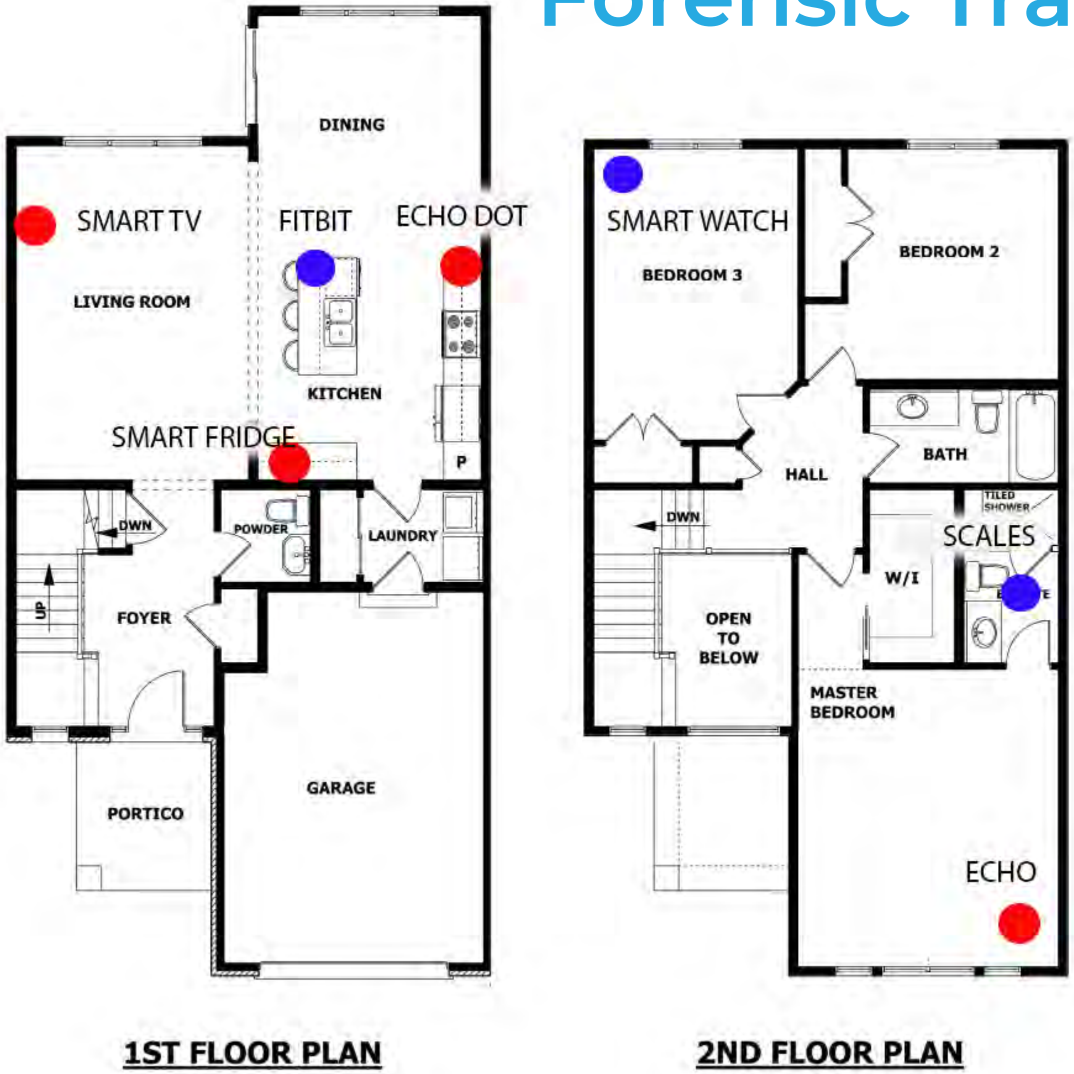
- **Upon a finding of prejudice to another party from the loss of the information, it may order measures no greater than necessary to cure the prejudice, under the terms of Rule 37(e)(1); or**
- **Only upon a finding that the party acted with intent to deprive another party of the information's use in the litigation, it may, under the terms of Rule 37(e)(2):**
  1. Presume that the lost information was unfavorable to the party;
  2. Instruct the jury that it may or must presume the information was unfavorable to the party; or
  3. Dismiss the action or enter a default judgment.

THE FUTURE

ARCHERHALL
AIM HIGH

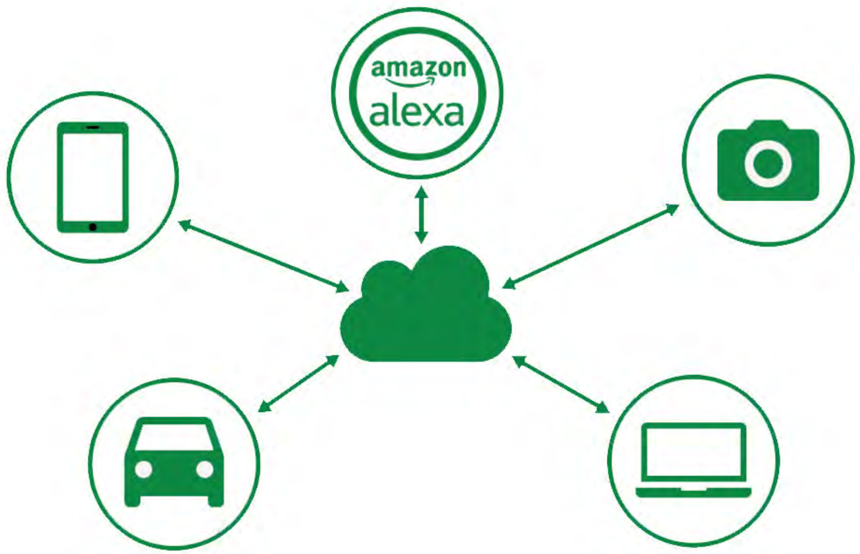
Forensic Trails

- IOT and Smart Homes and wearables provide much more info



The Cloud

Device Independent Cloud Based Identity



More and more data is stored in and accessed from the Cloud

We’d love to hear from you!

Tom Plunkett
Director of Digital Forensics

TPlunkett@ArcherHall.com
855.839.9084

ARCHERHALL
AIM HIGH