

Cellphone Forensics: Applications in Discovery and Investigations



ARCHERHALL
AIM HIGH

Stay tuned – the webinar will begin shortly

www.archerhall.com | 855-839-9084



Cellphone Forensics: Applications in Discovery and Investigations

Thomas Plunkett, EnCE, CISSP
Managing Director
Digital Forensics & E-Discovery



TPlunkett@ArcherHall.com
855.839.9084

Tom Plunkett

- MS Information Systems, 2002
- Certified Information Systems Security Professional (CISSP), 2007
- EnCase Certified Forensic Examiner (EnCE), 2008

- Adjunct Professor, MS Cyber Security Leadership, University of San Diego
- Former Information Security Officer, County of Riverside, CA
- Former Cyber Counterintelligence Officer, Los Alamos National Lab
- Former CH46-E Helicopter Crewchief, USMC

- 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



Most cases with Digital Evidence involve Cellphone Data



Cellphones interact with other devices that cannot be overlooked



Cellphones provide Communications, Location, Photos, Health, and other data



How these devices are handled Matters



MOBILE TECHNOLOGY



ARCHERHALL
AIM HIGH

Cellphones and Mobile Devices

Cellphones:

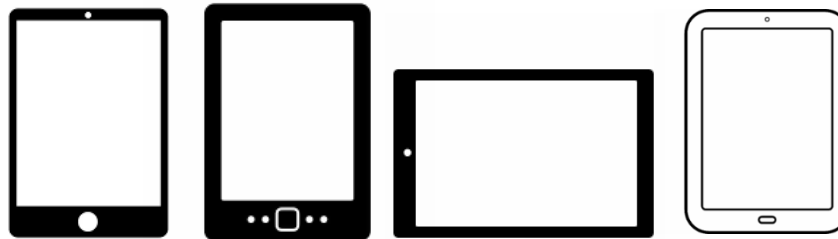
SMART PHONES



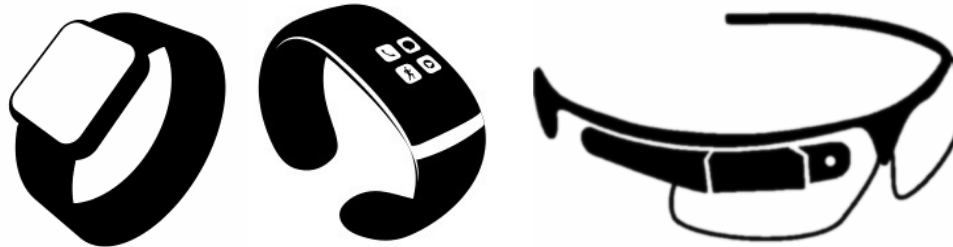
NOT SO SMART PHONES



Tablets:



Wearables:



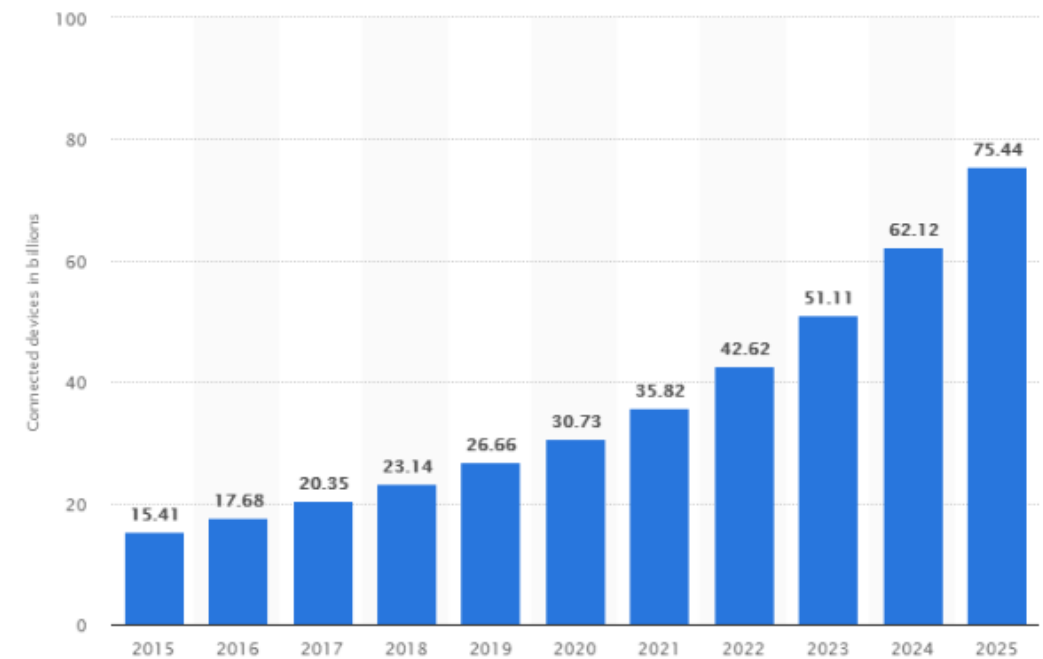
The Internet of Things

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



THE FORENSIC PROCESS



ARCHERHALL
AIM HIGH

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

Proper Handling



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



Life Cycle of Deleted Content

Recoverable

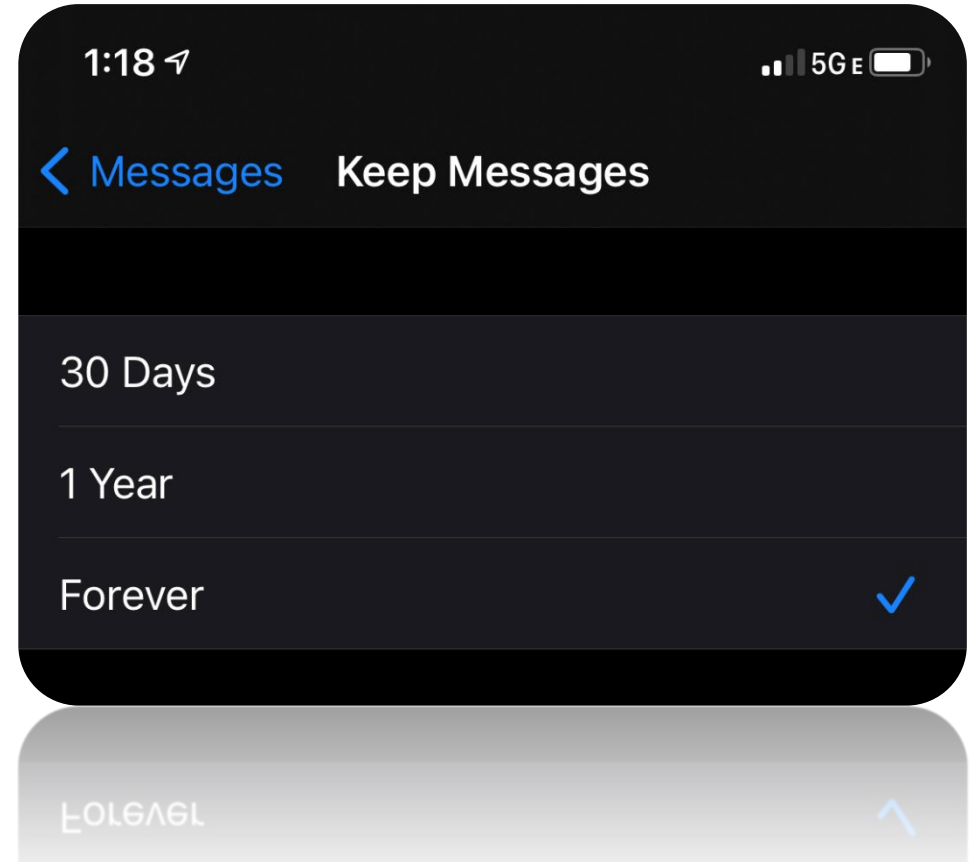
- Move to Trash or Recycle Bin
- Emptied Trash or Recycle bin
- Bypass Trash or Recycle Bin

Partially or Not recoverable

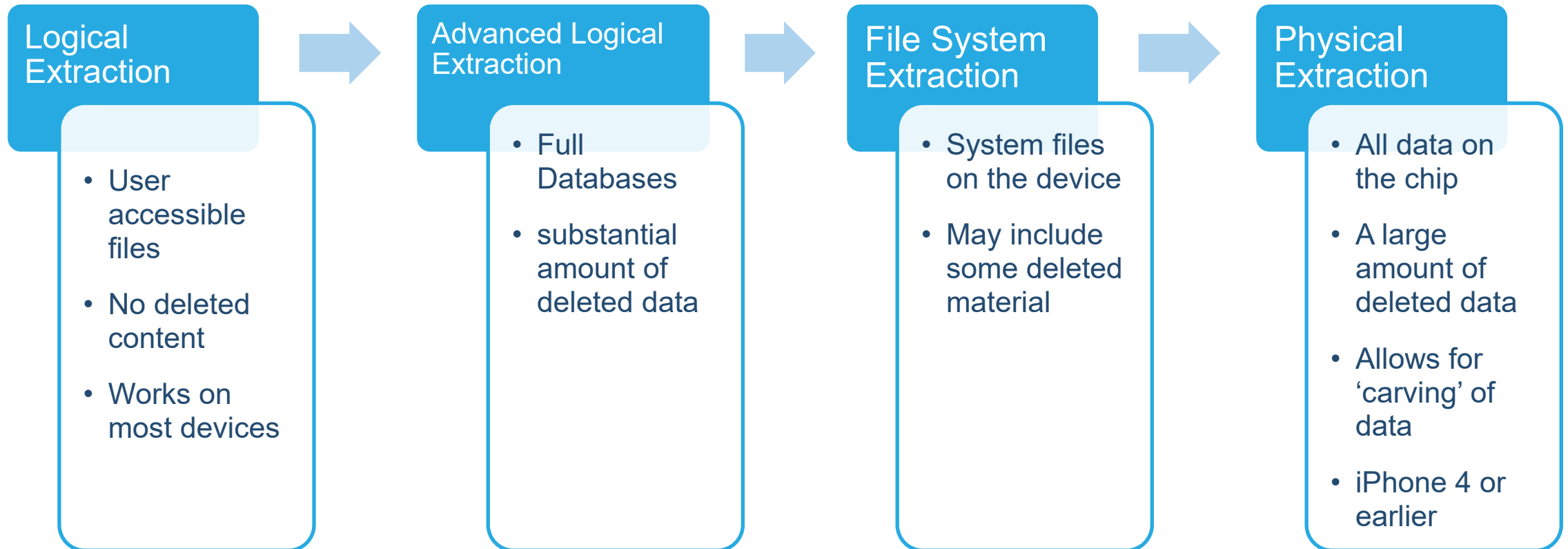
- Partially Overwritten
 - File fragments
- Fully Overwritten
- Wiping

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



Extraction



Device Summary

UFED Physical Analyzer 7.28.0.203

File View Tools Extract Python Plug-ins Report Help

Welcome Extraction Summary (1)

Extraction Summary (1)

All Content Logical

Extraction Summary

+ Add extraction Add external file Project settings Generate report

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	appleid@icloud.com	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.idbackup.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 : 0x6F88
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.findmydevice.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	c0ccc8-f86c-851b	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: +1-415-415-415 (1) (14) (3622 messages)
 - WhatsApp (8) (160 messages)
 - Contacts (3446) (18)

- Chats (441) (421)
 - Facebook (106) (86) (820 messages)
 - Snapshot (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) (29)
 - Locations (3402) (100)
 - Facebook (48) (36)
 - Google Maps (25) (5)
 - LG Cell Tower Location
 - Media Locations (2)
 - Twitter Message (22)
 - Wireless Networks (123) (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

CHATS

						Participants	↓ Start Time
			1	3	2	Microsoft Lync (owner)	9/5/2013 09:43(UTC-7)

To: Conversation

To:

Select/Deselect all...

Enter text to filter ...

From:

☒

From: hey :) 9/5/2013 09:43(UTC-7) Sources (1)

To:

☒

 Hi 9/5/2013 09:54(UTC-7) Sources (1)

To:

☒

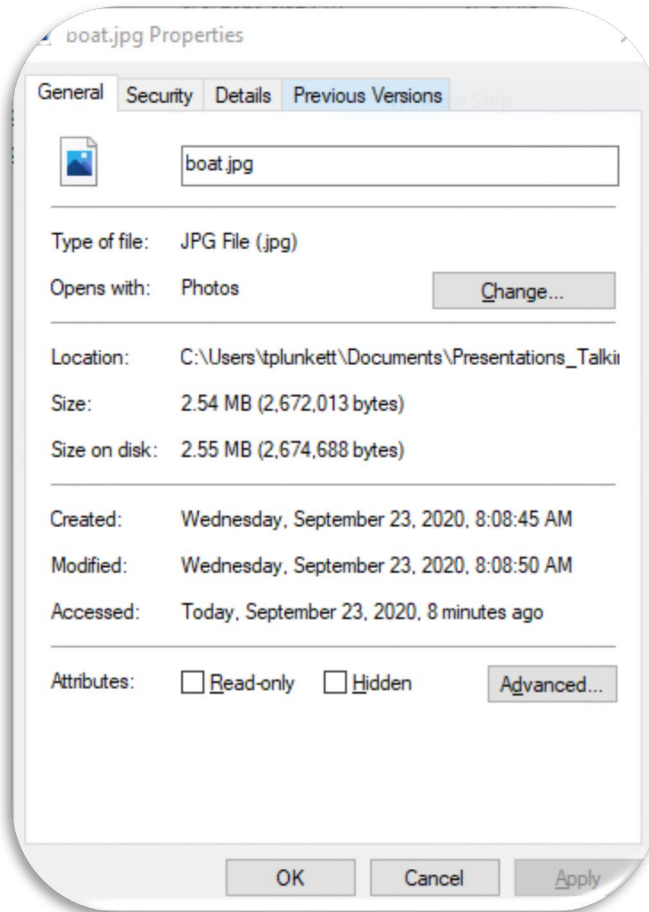
 how u doing ? 9/6/2013 11:24(UTC-7) Sources (1)

- Information about Data
- External
 - Stored in the file system
 - Summary
- Internal
 - Stored within the file itself
 - Comprehensive
 - EXIF in Photos and Multimedia



Internal vs External

External Metadata



Internal Metadata

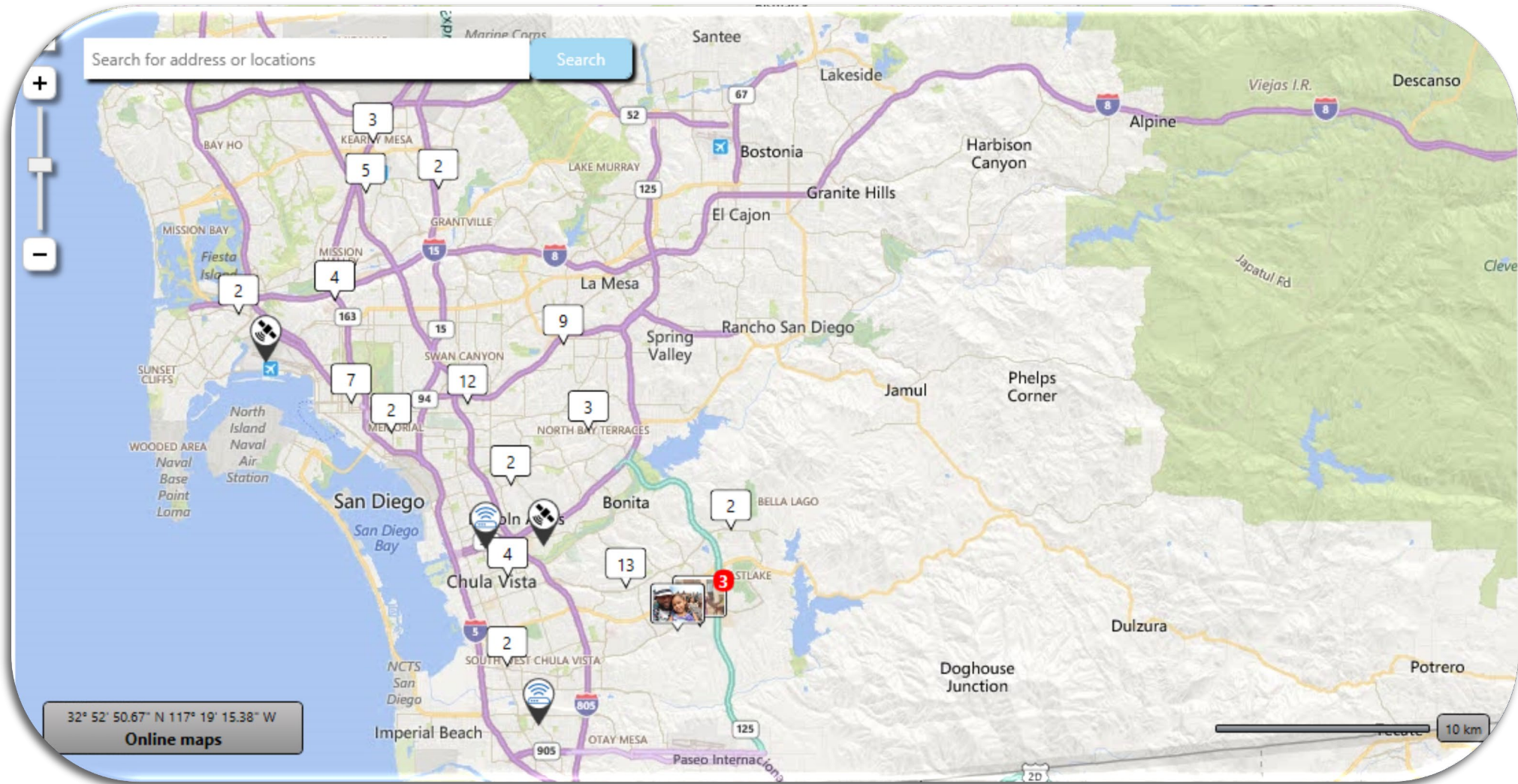
```
lens Make      : Apple
lens Model     : iPhone X back dual camera 6mm f/2.4
GPS Latitude Ref : North
GPS Longitude Ref : West
GPS Altitude Ref : Above Sea Level
GPS Speed Ref   : km/h
GPS Speed       : 4.308832651
GPS Img Direction Ref : Magnetic North
GPS Img Direction : 305.0164948
GPS Dest Bearing Ref : Magnetic North
GPS Dest Bearing  : 305.0164948
GPS Horizontal Positioning Error: 8.001208277 m
```

```
utter Speed    : 17025
Create Date    : 2020:08:09 18:52:51.554-04:00
Date/Time Original : 2020:08:09 18:52:51.554-04:00
Modify Date    : 2020:08:09 18:52:51-04:00
Thumbnail Image : (Binary data 8255 bytes, use -b option to extract)
GPS Altitude    : 234 m Above Sea Level
GPS Latitude    : 42 deg 45' 3.61" N
GPS Longitude   : 85 deg 32' 5.00" W
Circle Of Confusion : 0.003 mm
```



boat.jpg.txt

Location Data - Automated



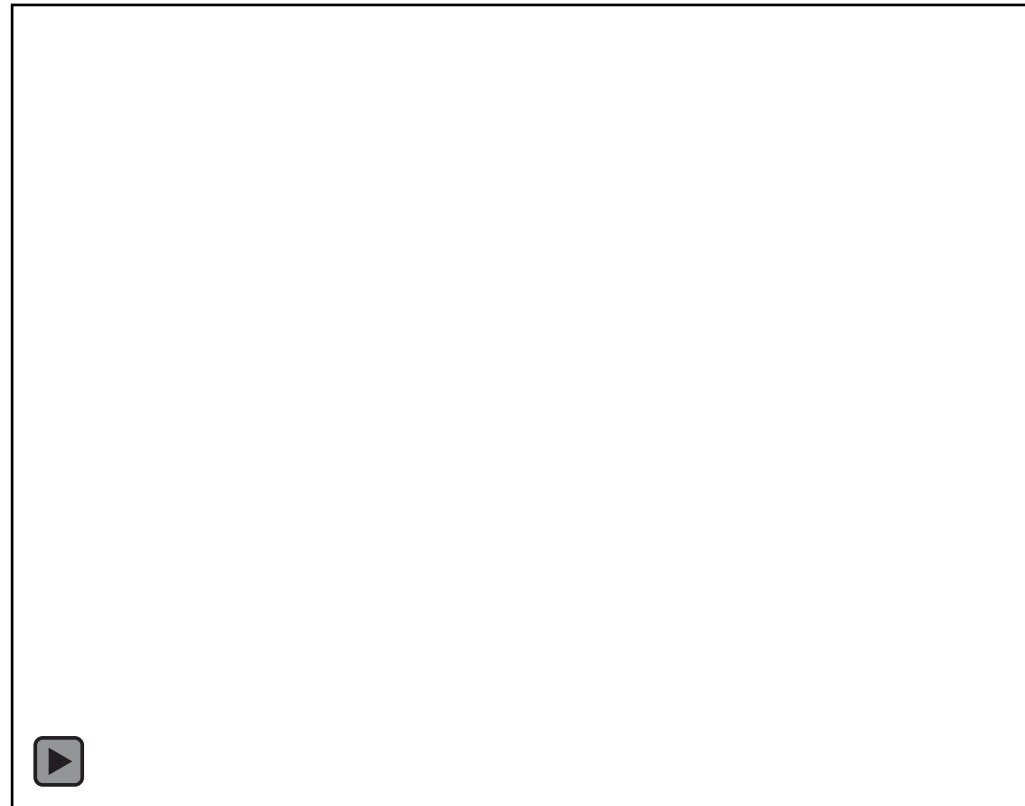


Location Data – Manually Extracted

Plot from Wahoo Fitness app

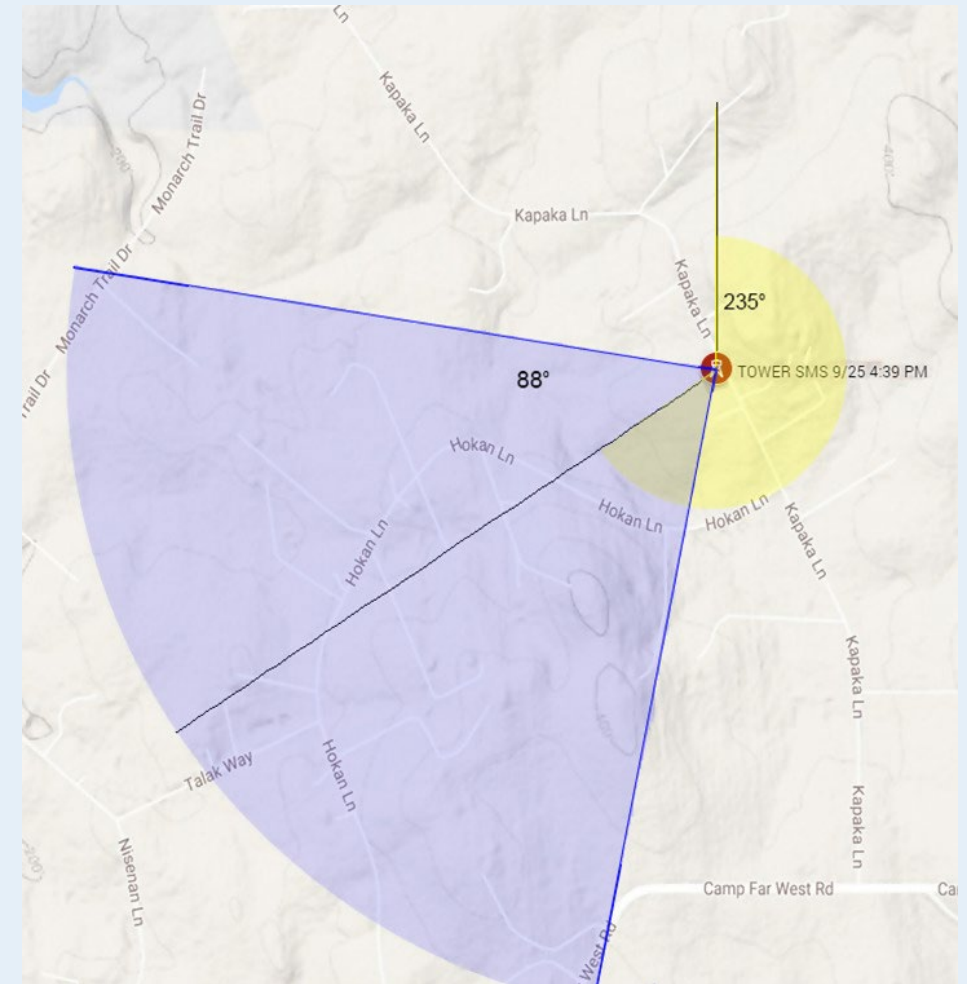


Location Data Animated

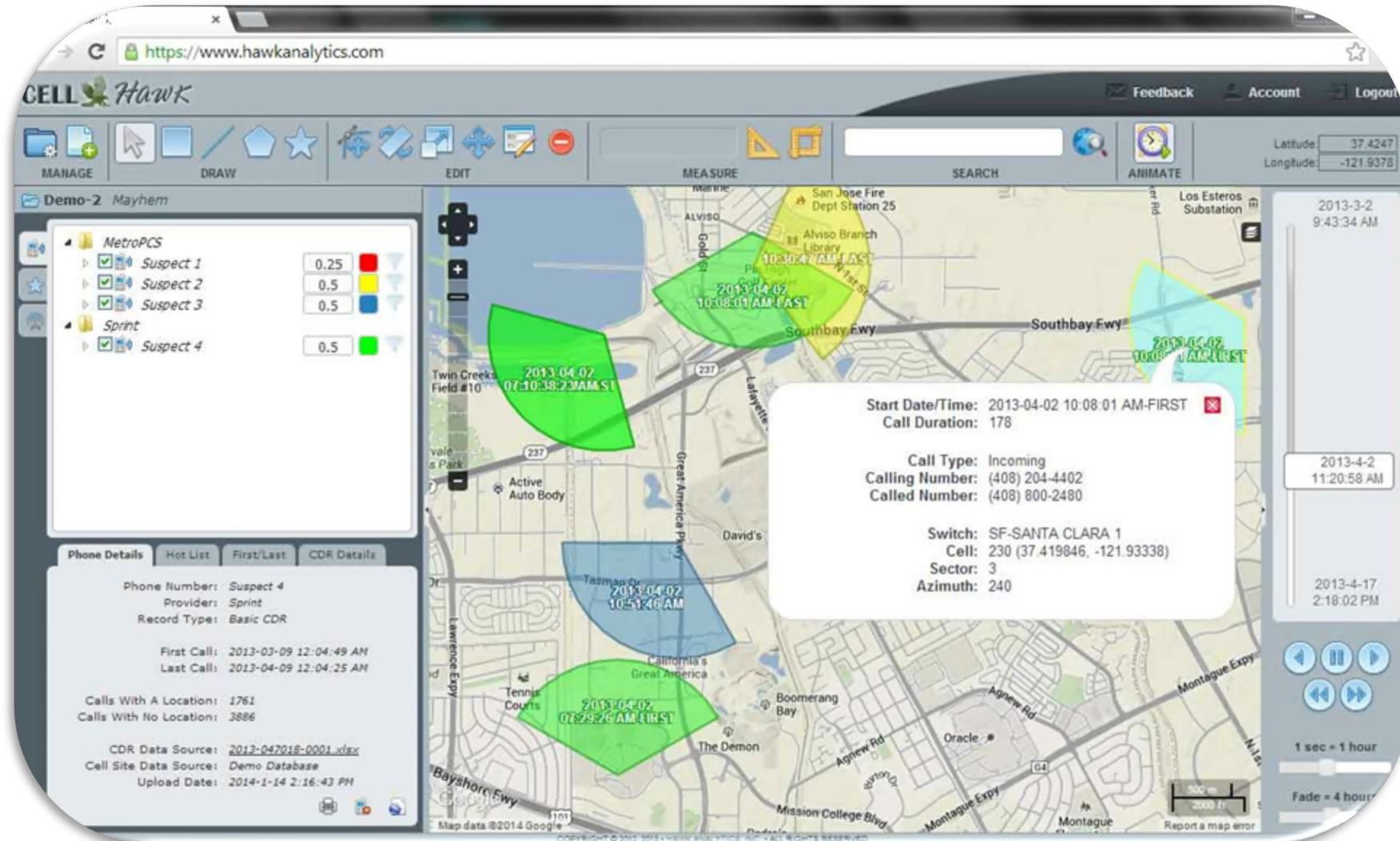


Location Data – Mapping Tower Data

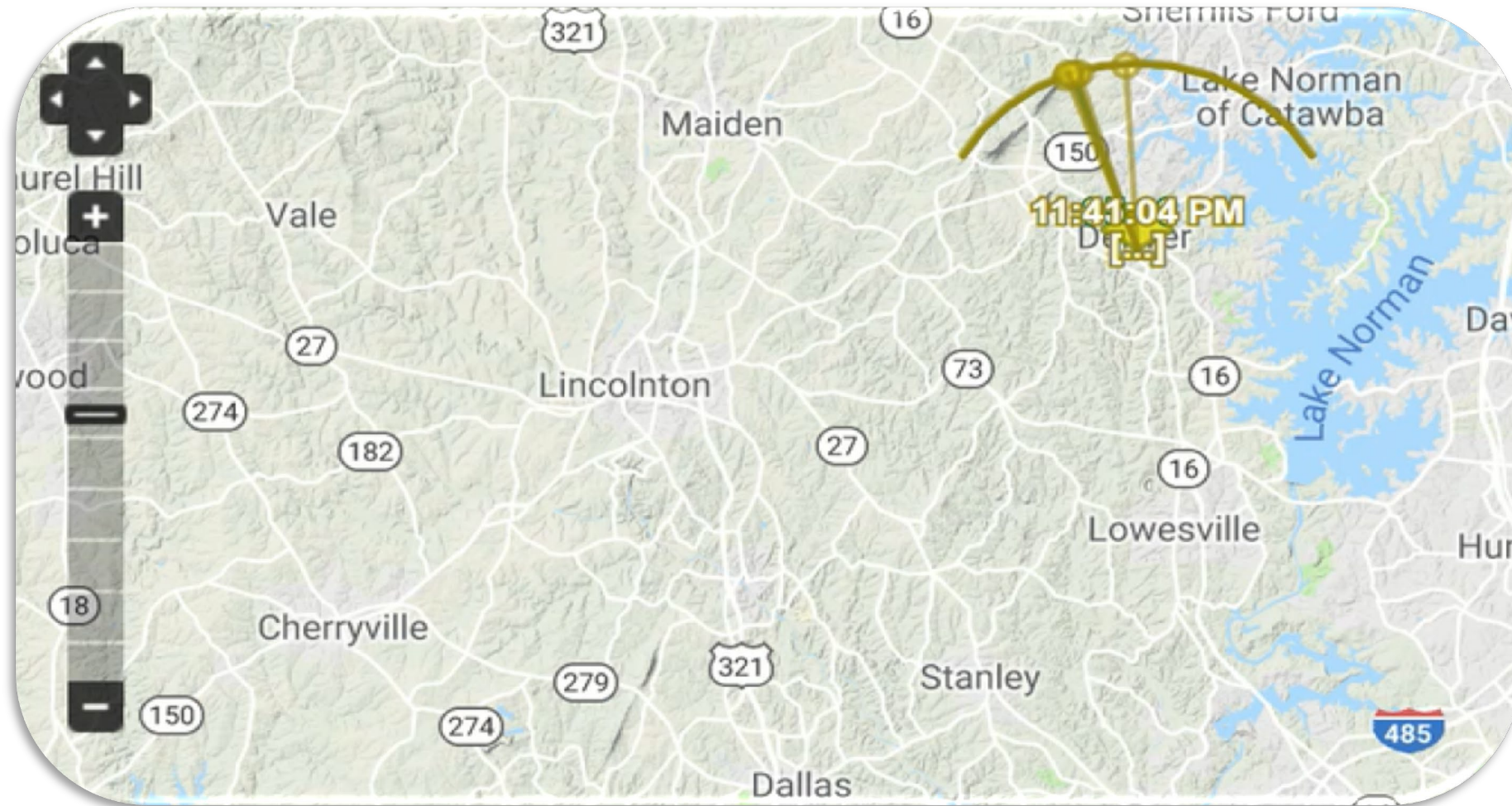
- **LAC/CID Longitude, Latitude**
 - Location of the Tower
- **Azimuth**
 - Sector angle from due North
- **Beam Width**
 - Angle of coverage of sector.



Location Data – Mapping Cell Site Data



Location Data – Mapping Cell Site Data



Triangle Agreement



Instrument to allow supervised preservation and collection



Used in conjunction with the preservation letter



Describes inspection protocol for third party



Allows opposing party to review responsive content for privilege prior to delivery to you

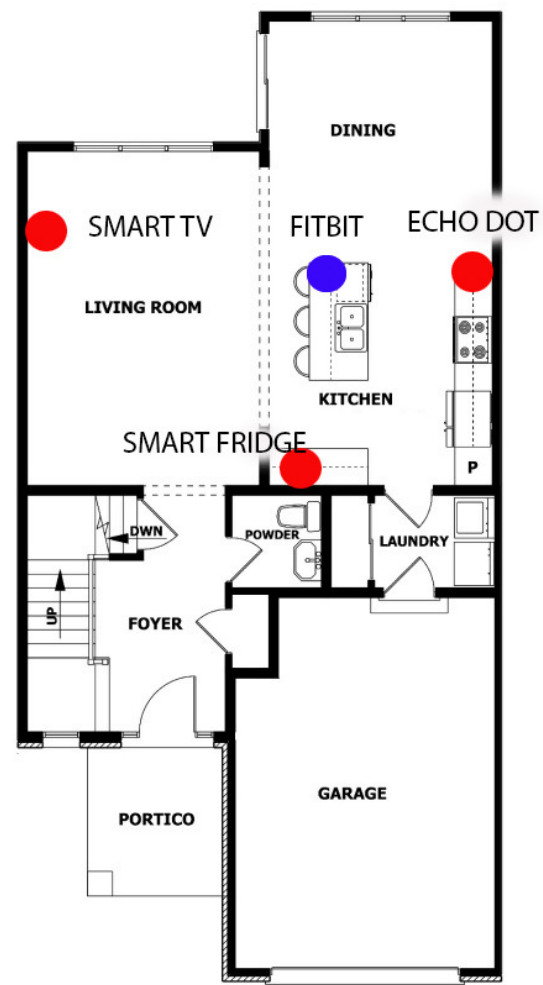


THE FUTURE



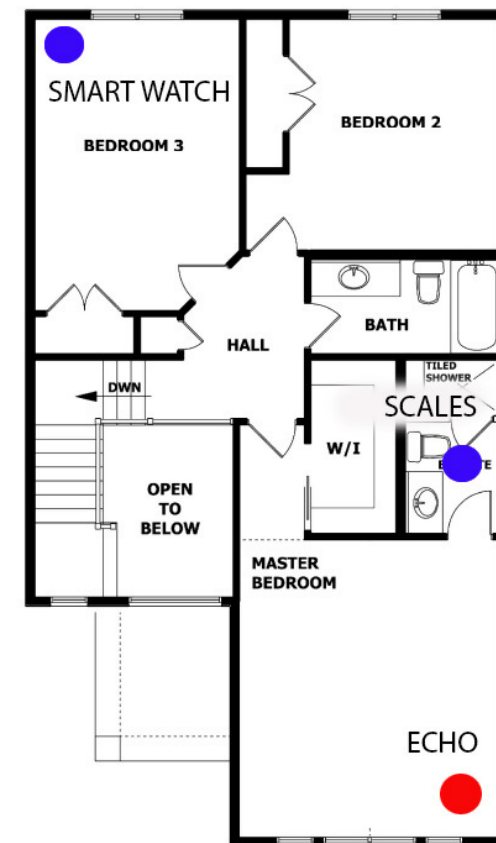
ARCHERHALL
AIM HIGH

- IoT and Smart Homes and wearables provide much more info



1ST FLOOR PLAN

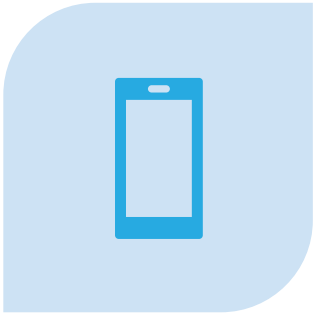
Forensic Trails



2ND FLOOR PLAN



Key Takeaways



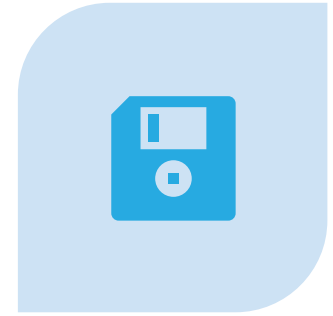
Mobile data is Volatile



Preserve as early and thoroughly as possible



Advise clients to change settings to keep messages “forever”



Preserve data from backups and the device itself

Thank you!

Tom Plunkett

TPlunkett@ArcherHall.com

855.839.9084



ARCHERHALL
AIM HIGH



Preservation – FRCP Rule 37(e)

Failure to Preserve Evidence - Federal Rule of Civil Procedure 37(e).

- The loss or destruction of relevant cell phone texts, intentional or not, can lead to sanctions under Federal Rule of Civil Procedure 37(e).
 - Rule 37(e) authorizes courts to issue sanctions where four conditions are met:
 - the ESI at issue should have been preserved in the anticipation or conduct of litigation;
 - the ESI is lost;
 - the loss is due to a party's failure to take reasonable steps to preserve it;
 - the ESI cannot be restored or replaced through additional discovery.

Preservation – FRCP Rule 37(e) (cont.)

If the court finds that these four conditions are satisfied, then:

- 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):
 - I. Presume that the lost information was unfavorable to the party;
 - II. Instruct the jury that it may or must presume the information was unfavorable to the party; or
 - III. Dismiss the action or enter a default judgment.

Data Retention by Carriers

