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

ArcherHall
AIM HIGH

TPlunkett@ArcherHall.com
855.839.9084

About the Speaker

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

ARCHERHALL
AIM HIGH

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

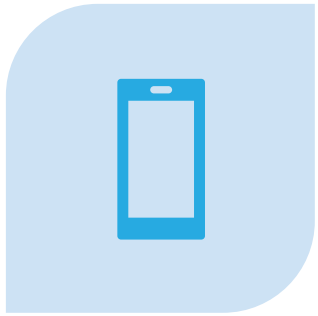
Schools and Higher-Ed

Medical Malpractice

IP Theft

Bankruptcy

Overview



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

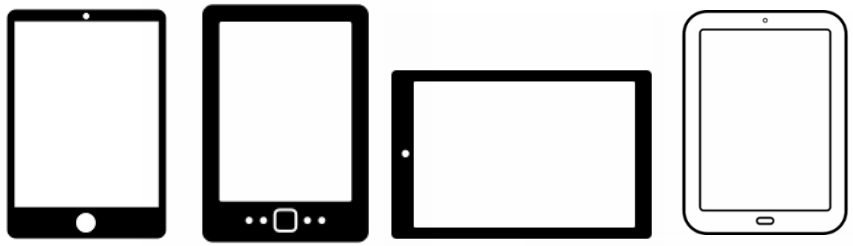
MOBILE TECHNOLOGY

ARCHERHALL
AIM HIGH

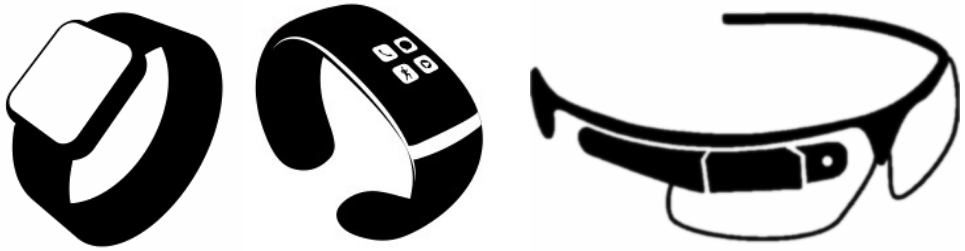
Cellphones and Mobile Devices

Cellphones:

Tablets:



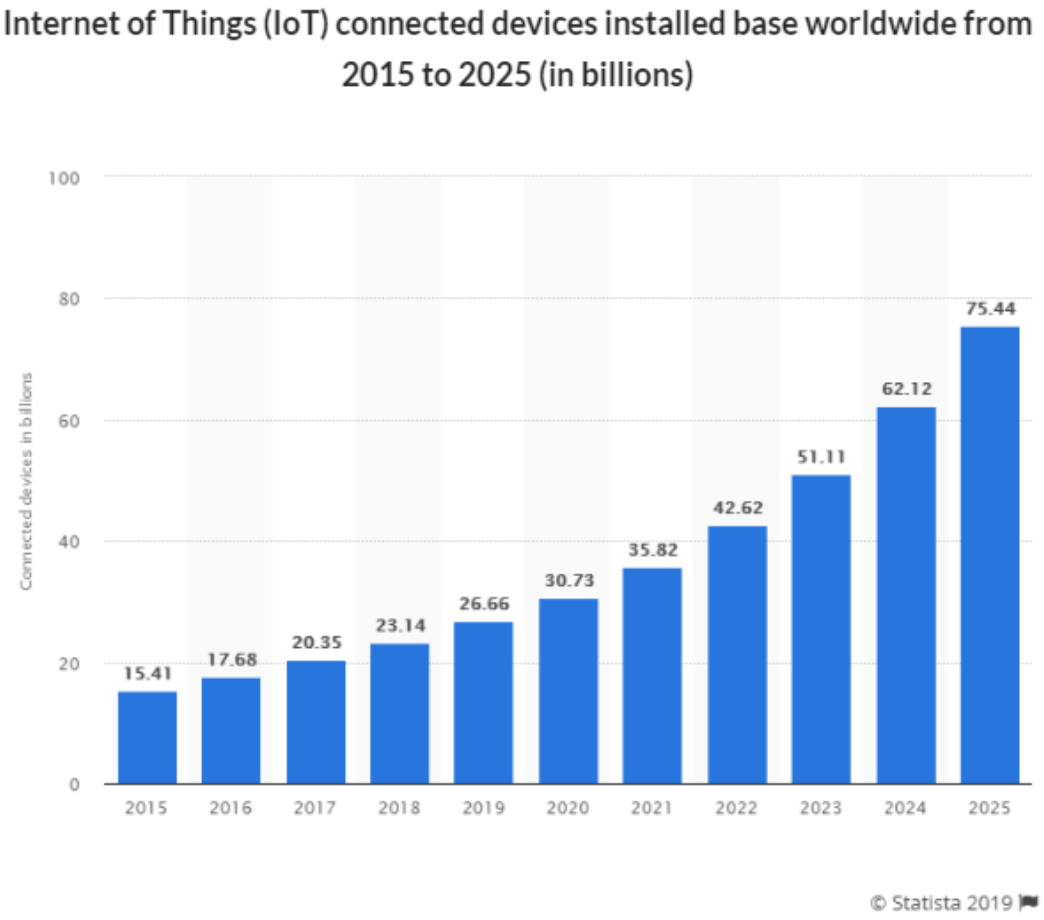
Wearables:



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



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

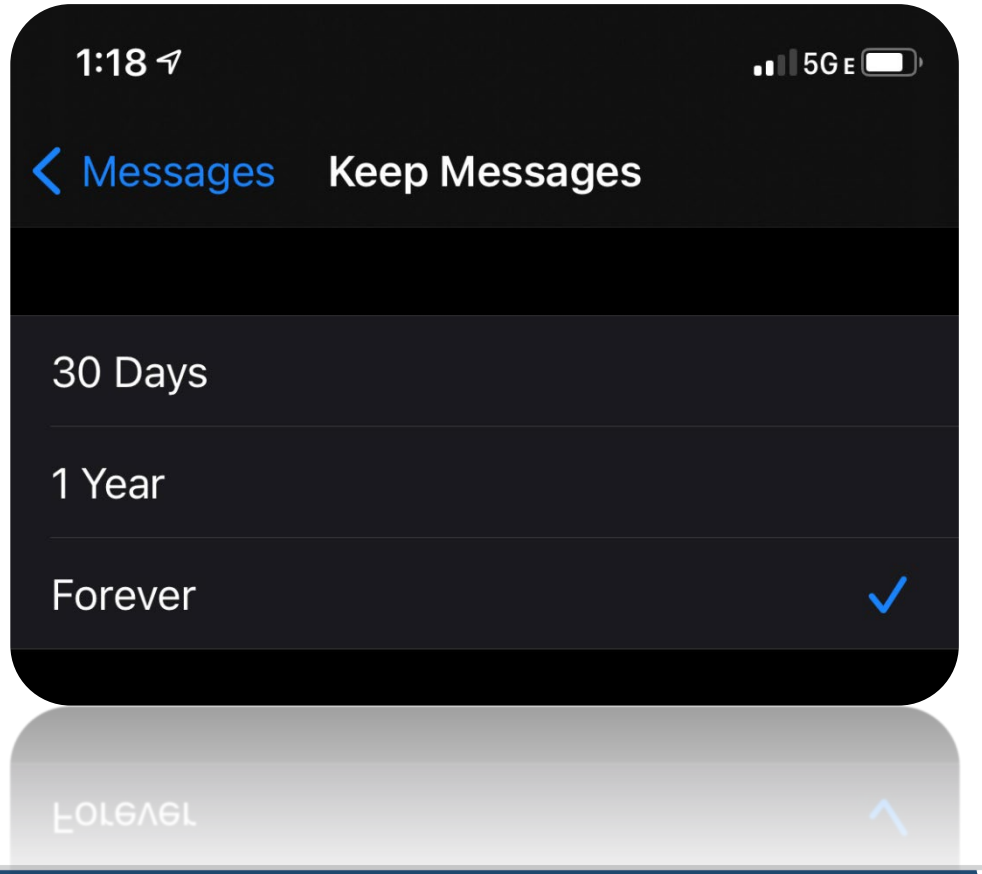
- Move to Trash or Recycle Bin
- Emptied Trash or Recycle bin
- Bypass Trash or Recycle Bin

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

Logical Extraction

- User accessible files
- No deleted content
- Works on most devices

Advanced Logical Extraction

- Full Databases
- substantial amount of deleted data

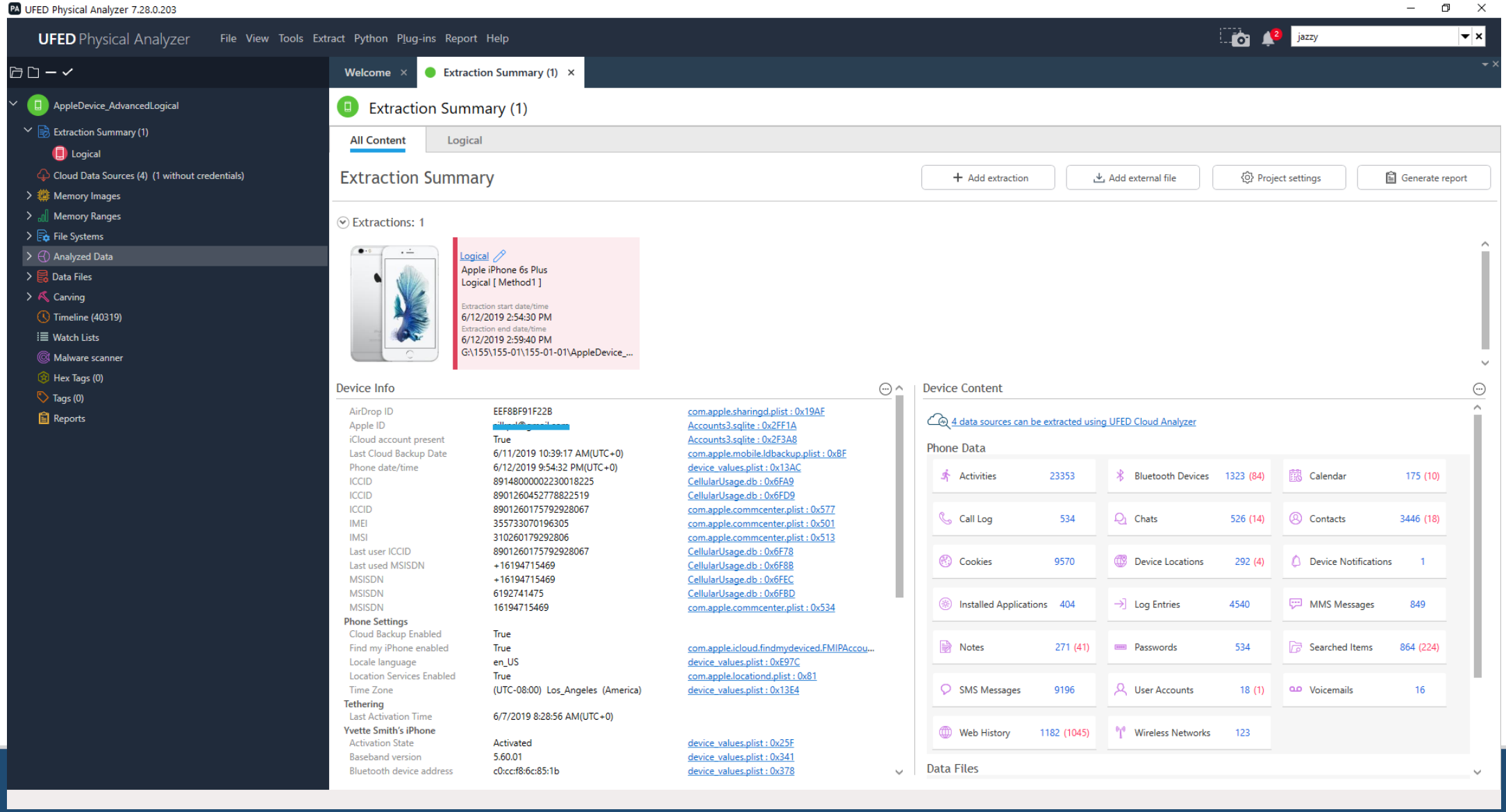
File System Extraction

- System files on the device
- May include some deleted material

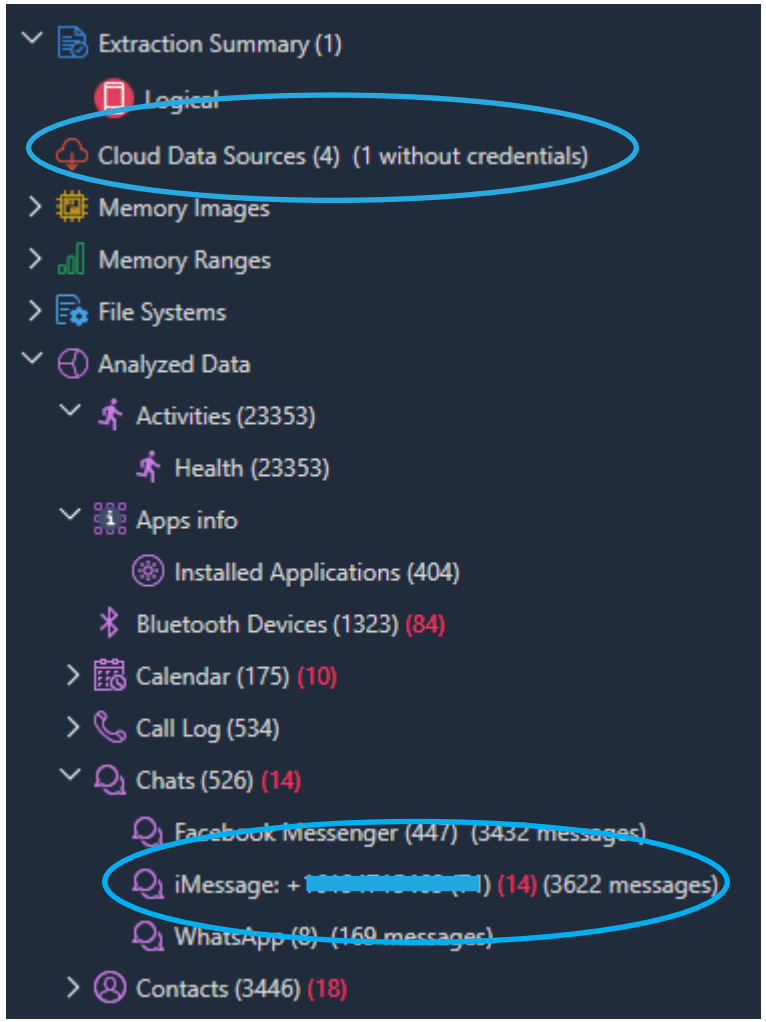
Physical Extraction

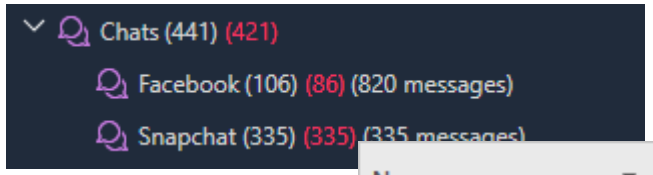
- All data on the chip
- A large amount of deleted data
- Allows for ‘carving’ of data
- iPhone 4 or earlier

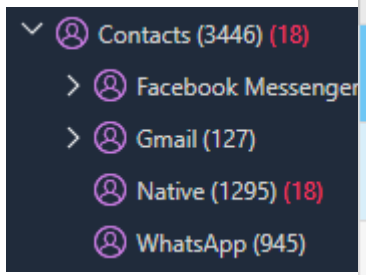
Device Summary

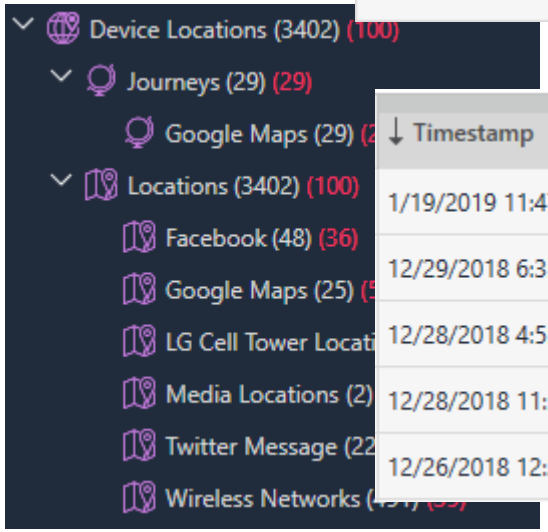


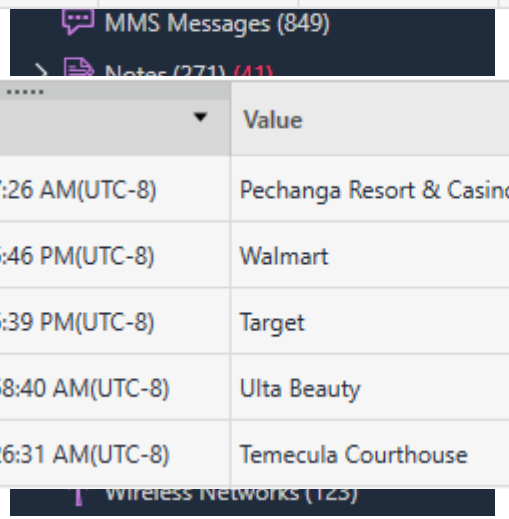
Data Types









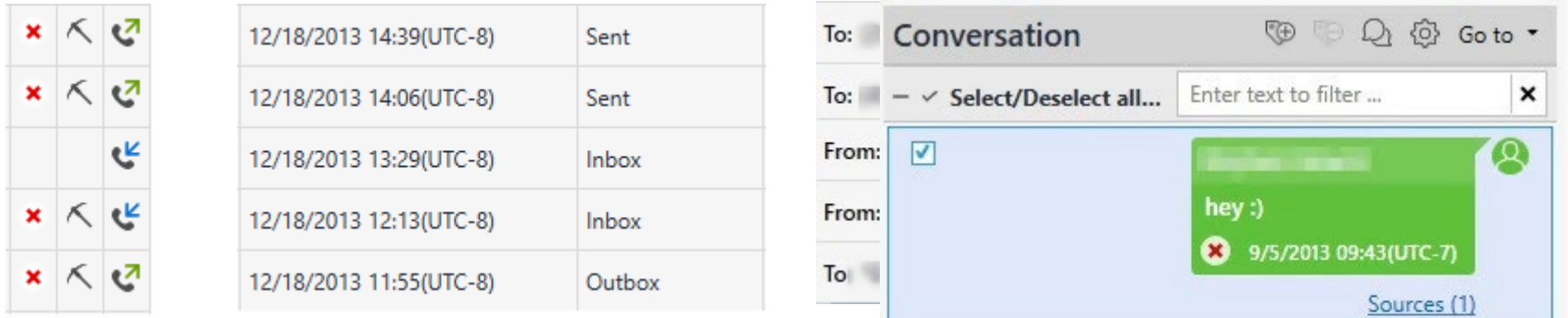


Name	Originates from	Value	Start time	End time
Steps and Distance	Device	393 Steps 233.88 Meters	6/12/2019 2:17:36 PM(U...	6/12/2019 2:36:38 PM(U...
Steps and Distance	Device	268 Steps 148.58 Meters	6/12/2019 2:08:48 PM(U...	6/12/2019 2:15:38 PM(U...
Steps and Distance	Device	293 Steps 170.04 Meters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

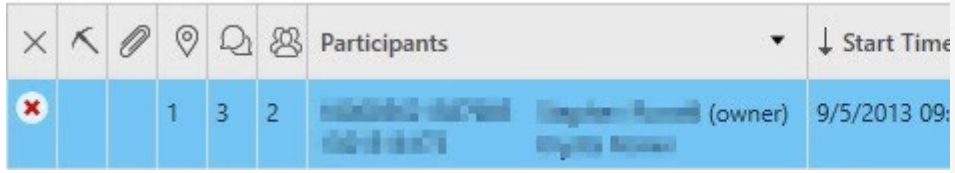
Timestamp	Value	Position	Source
1/19/2019 11:47:26 AM(UTC-8)	Pechanga Resort & Casino	(33.455664, -117.106604)	Waze
12/29/2018 6:35:46 PM(UTC-8)	Walmart	(33.662178, -117.294371)	Waze
12/28/2018 4:55:39 PM(UTC-8)	Target	(33.506343, -117.146342)	Waze
12/28/2018 11:58:40 AM(UTC-8)	Ulta Beauty	(33.527417,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

Communications

SMS / MMS



CHATS

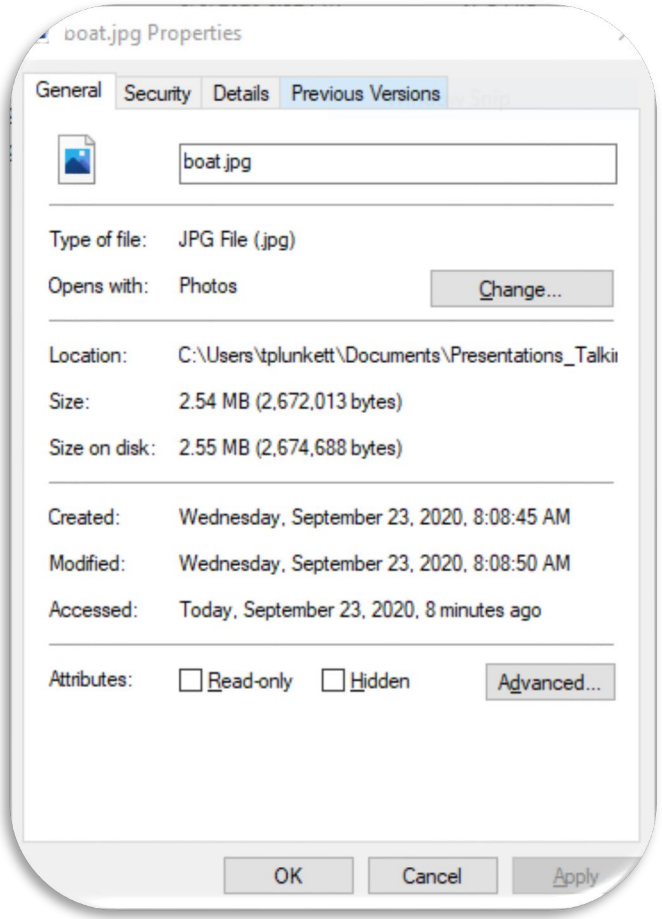


Metadata

- 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

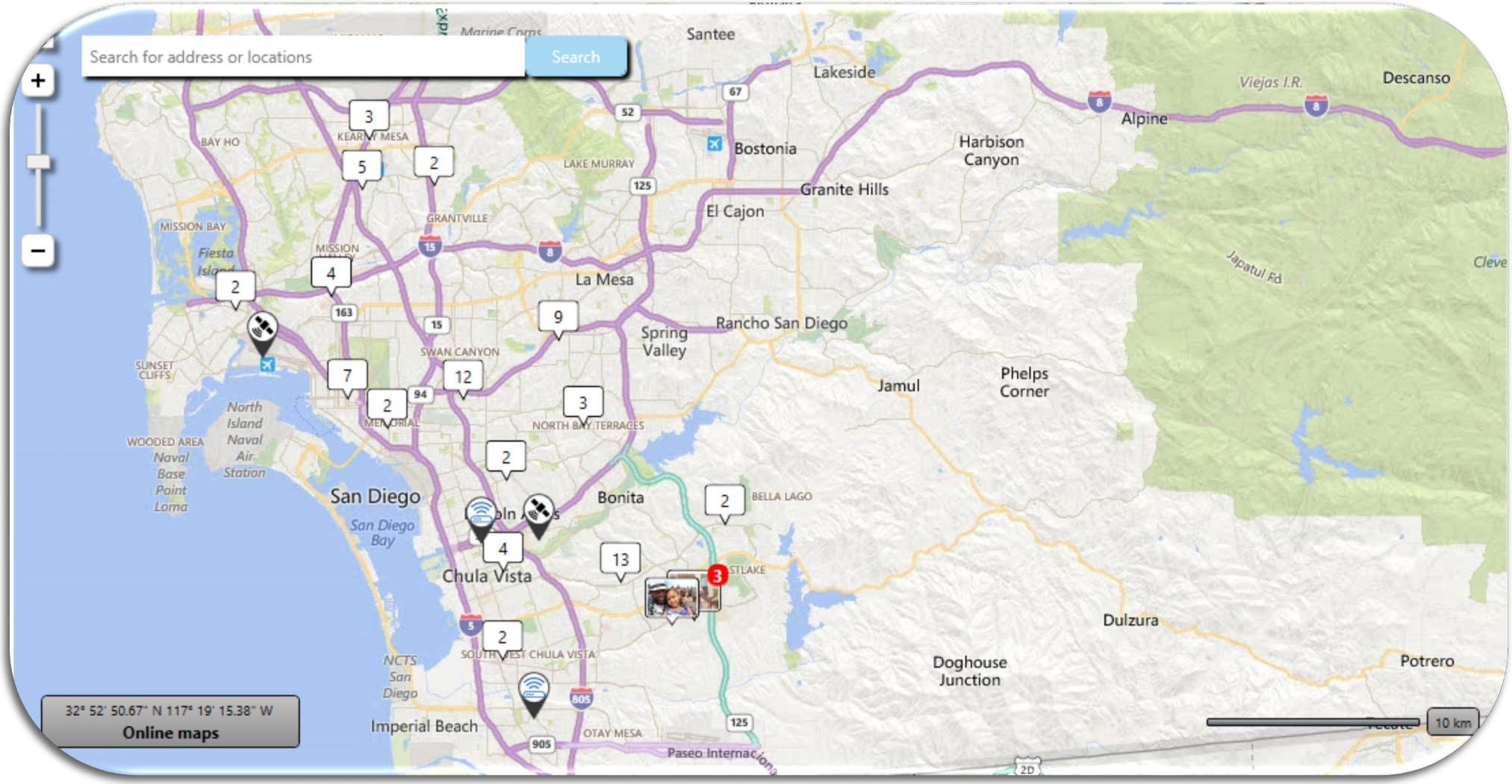


Internal Metadata

```
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
```

```
Shutter Speed                   : 1/625
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
```

Location Data - Automated



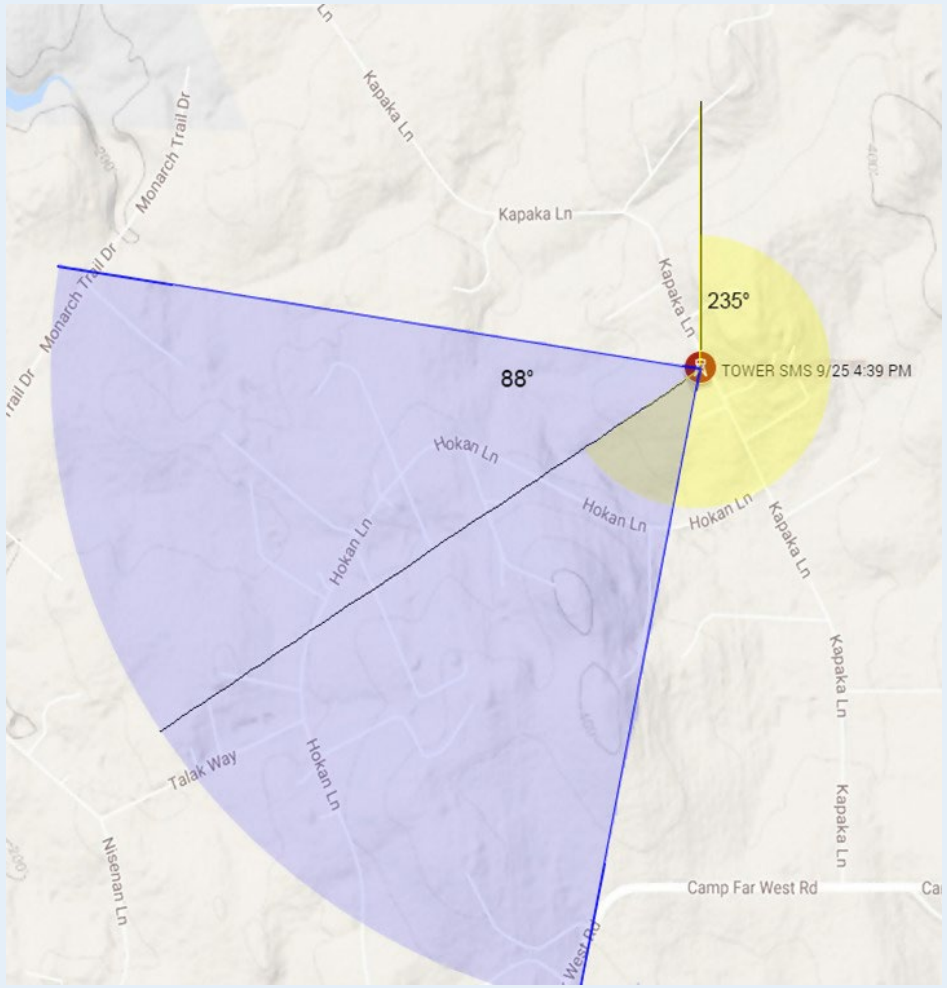
Location Data – Manually Extracted

Plot from Wahoo Fitness app

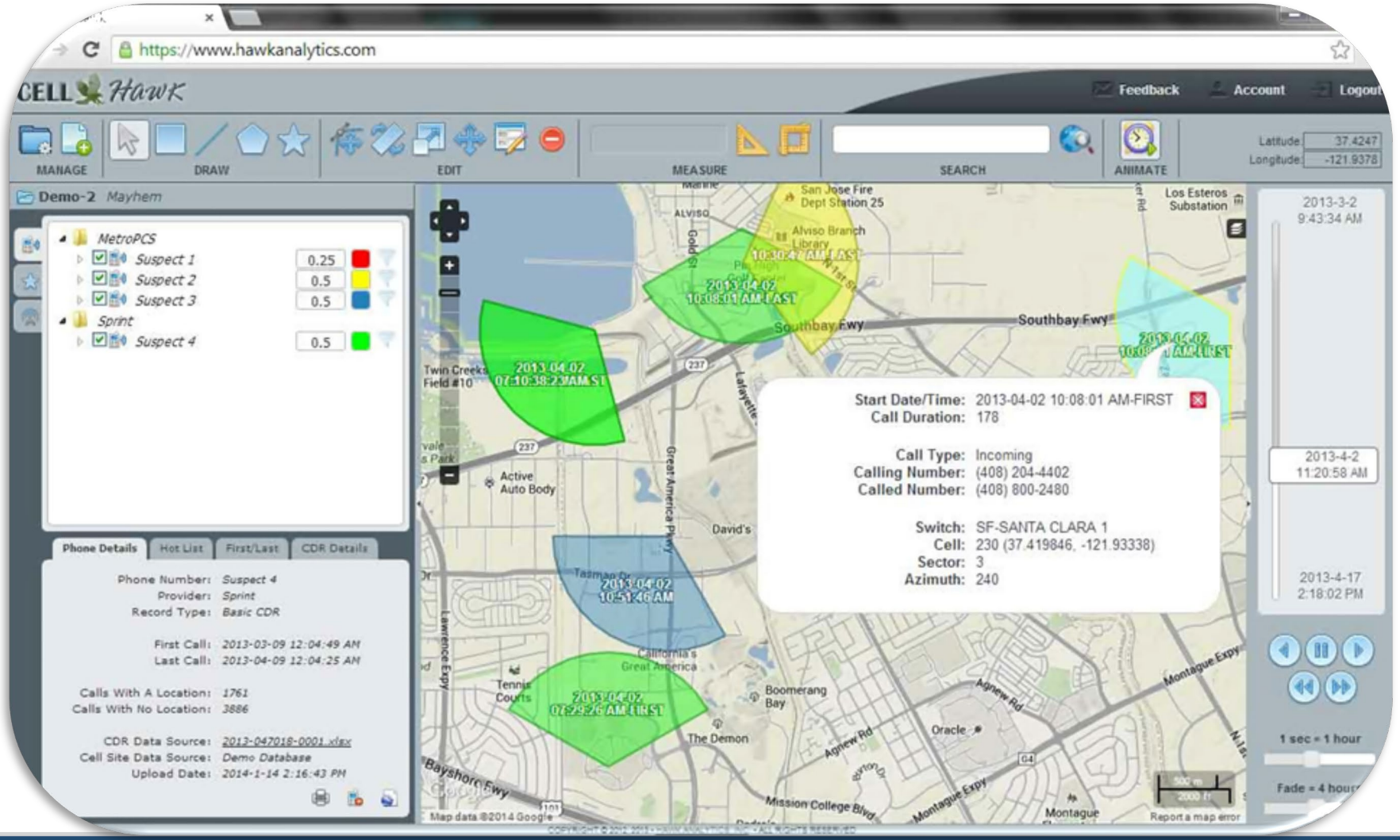
Location Data Animated

Location Data – Mapping Tower Data

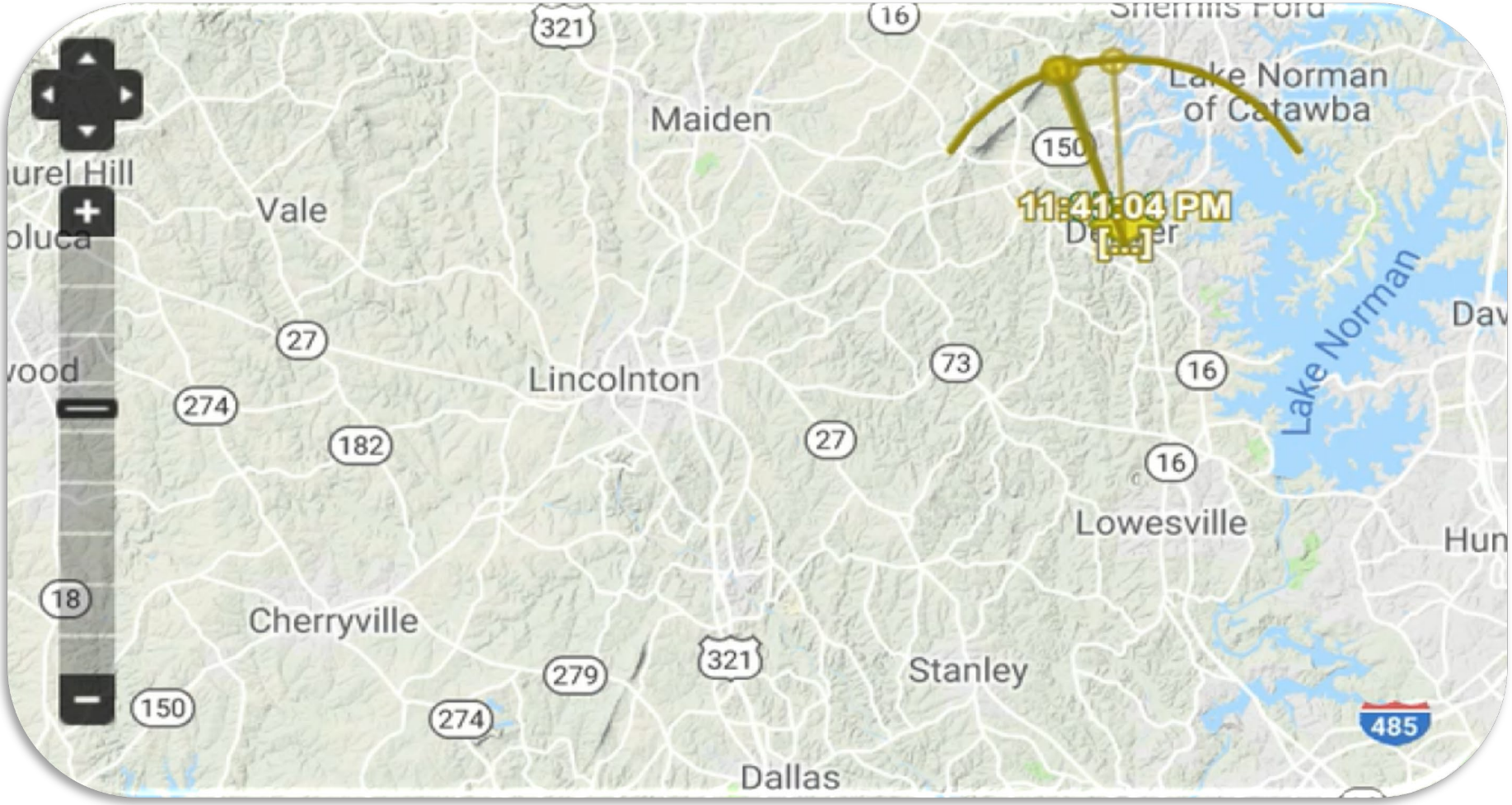
- **LAC/CID Longitude, Latitude**
  - Location of the Tower
- **Azimuth**
  - Sector angle from due North
- **Beam Width**
  - Angle of coverage of sector.



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

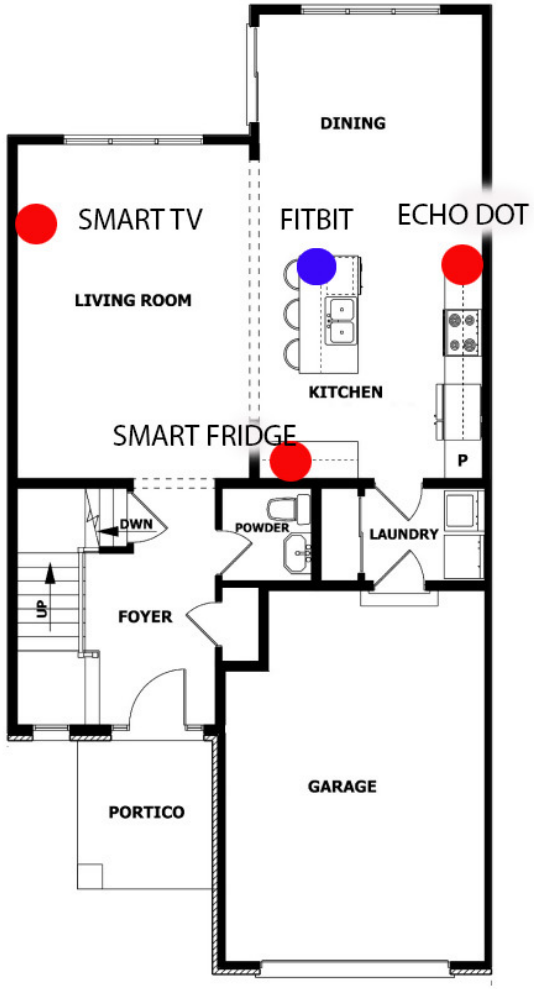
Allows opposing party to review responsive content for privilege prior to delivery to you

THE FUTURE

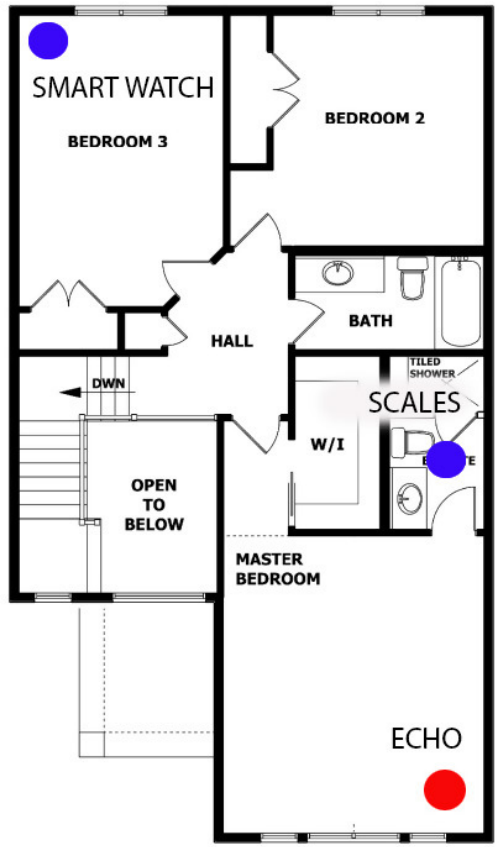
ARCHERHALL
AIM HIGH

Forensic Trails

- IOT and Smart Homes and wearables provide much more info

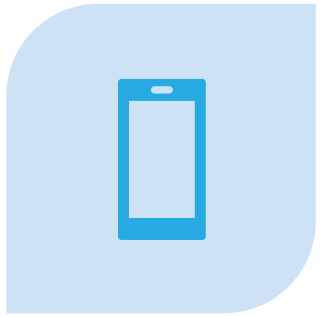


1ST FLOOR PLAN



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).

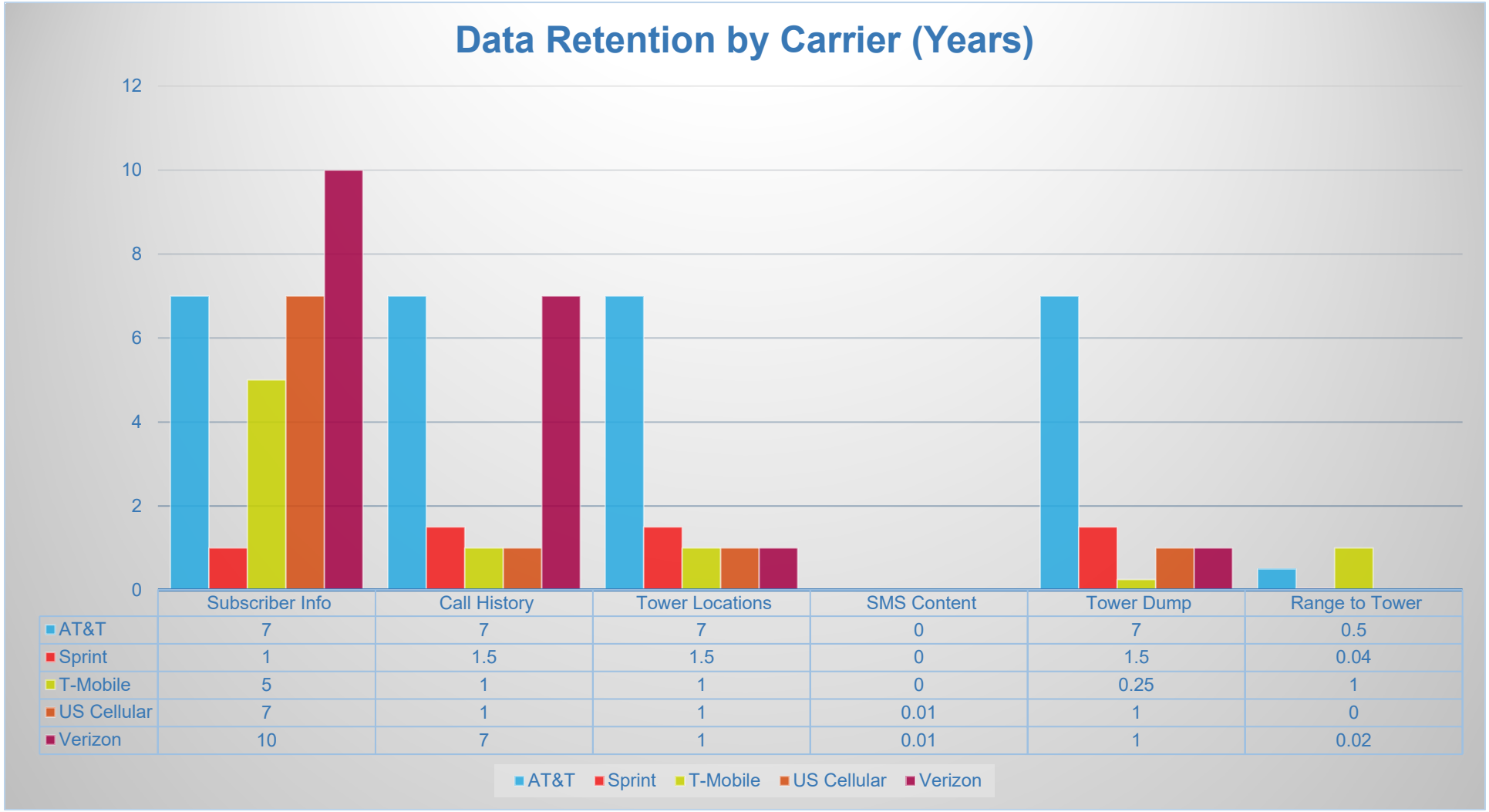
- **The loss or destruction of relevant cell phone texts, intentional or not, can lead to sanctions under Federal Rule of Civil Procedure 37(e).**
  - Rule 37(e) authorizes courts to issue sanctions where four conditions are met:
    - the ESI at issue should have been preserved in the anticipation or 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



	Subscriber Info	Call History	Tower Locations	SMS Content	Tower Dump	Range to Tower
AT&T	7	7	7	0	7	0.5
Sprint	1	1.5	1.5	0	1.5	0.04
T-Mobile	5	1	1	0	0.25	1
US Cellular	7	1	1	0.01	1	0
Verizon	10	7	1	0.01	1	0.02