CELL PHONE LOCATION AND CELL PHONE FORENSICS

ENVISTA FORENSICS

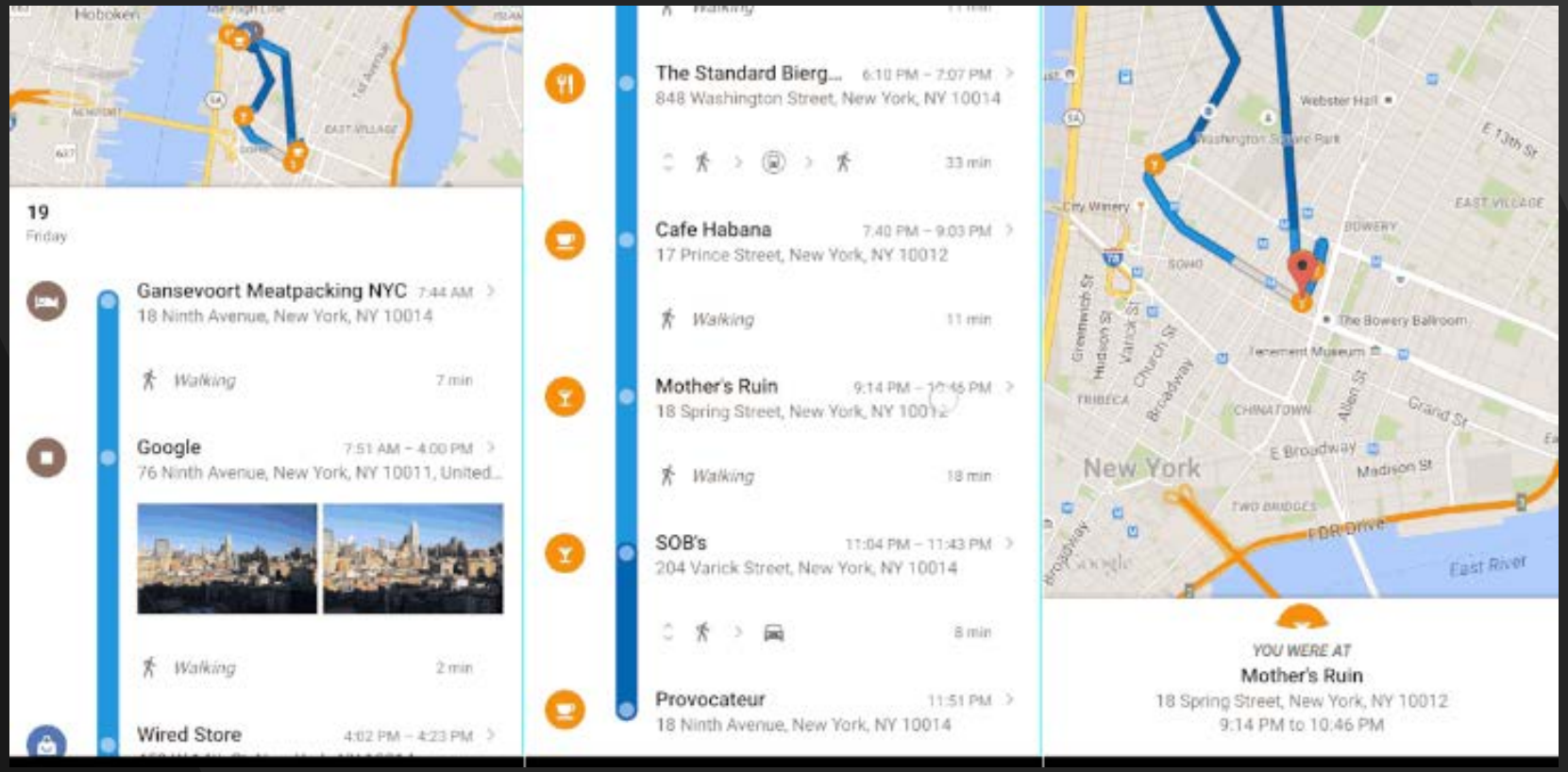
TAKE OUT YOUR PHONE

Location History

What's in your pocket?

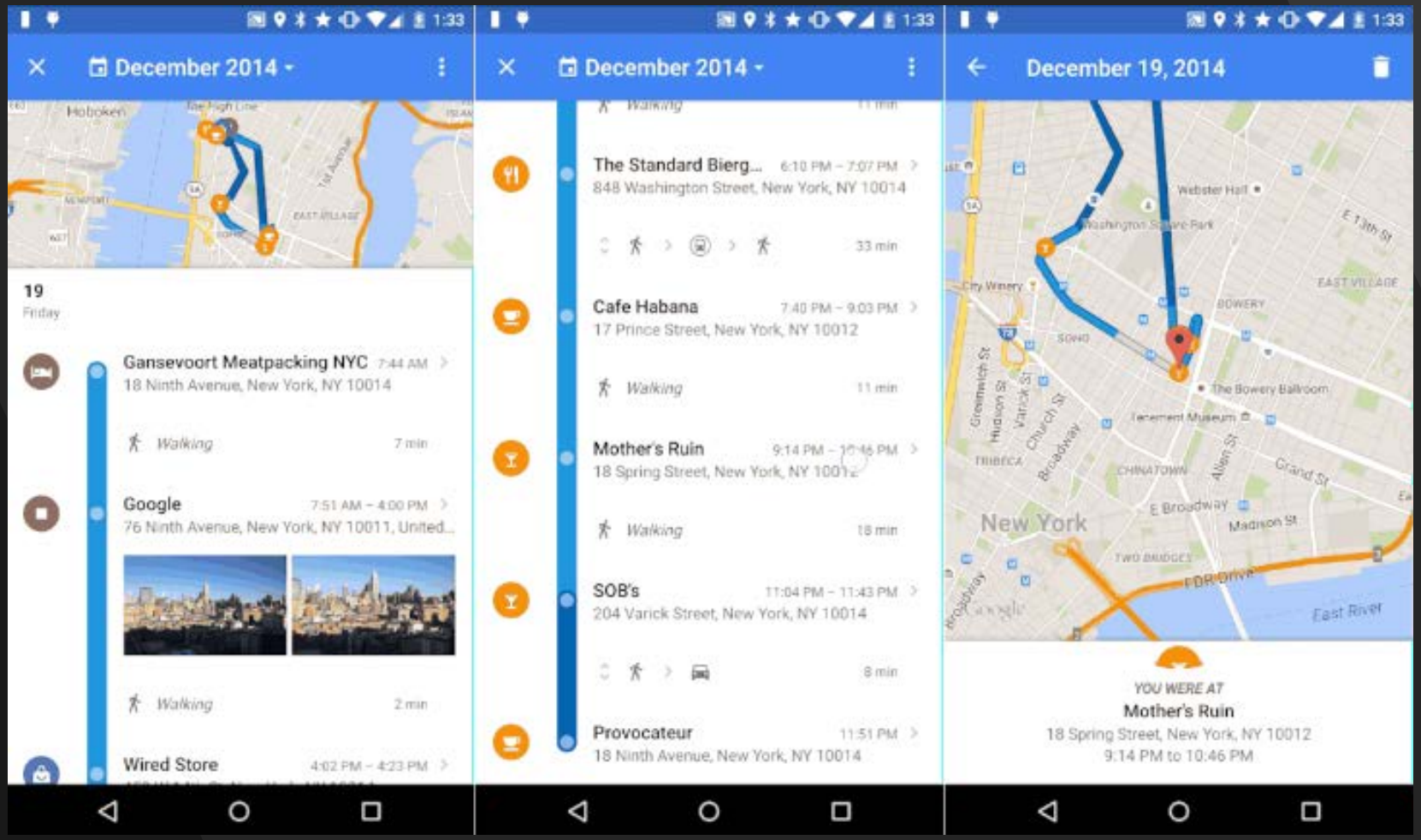
Android/Apple

Open Google Maps > Menu > Timeline (Swipe Left and Right)



Location History

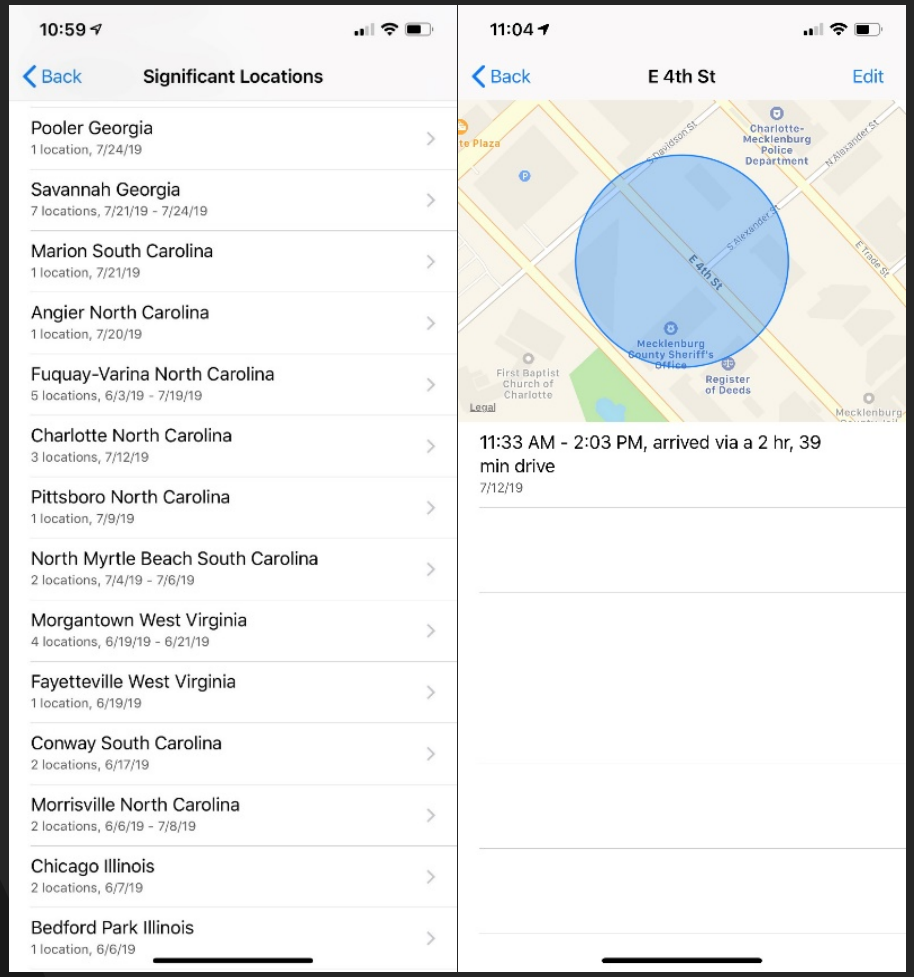
If you have a map like you see below, please let me know in the Chat!



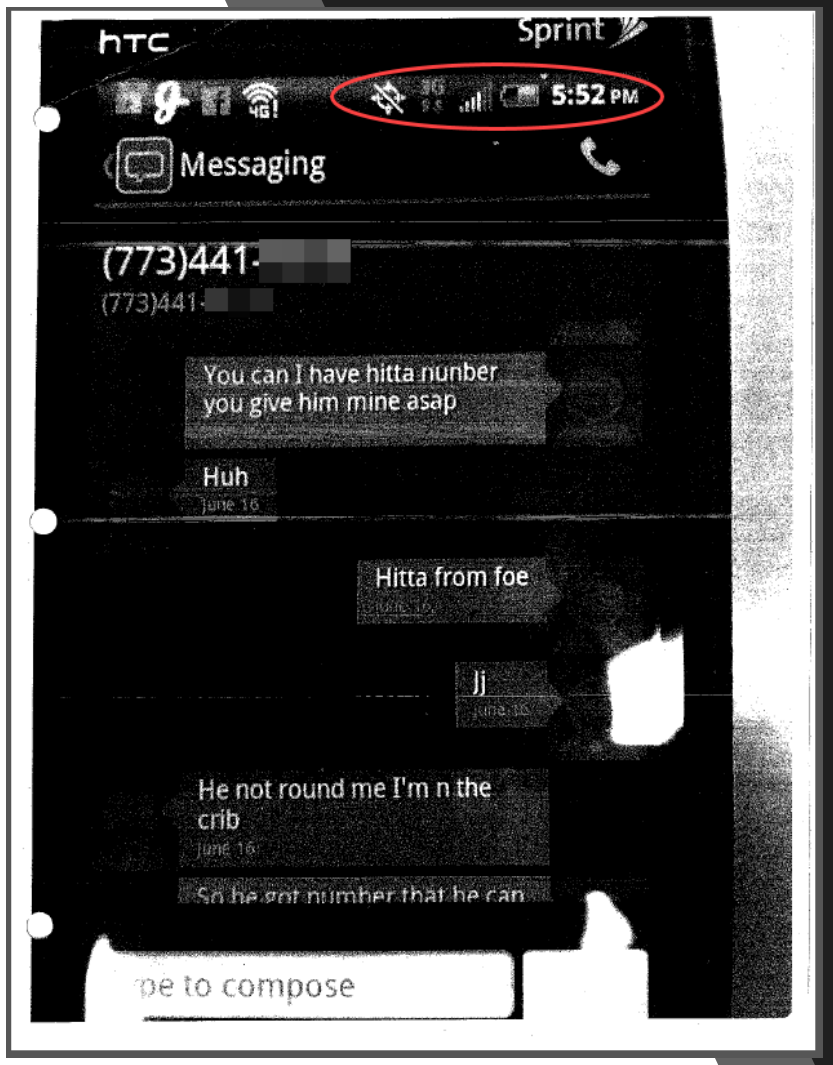
iPhone

What's in your pocket?

Settings > Privacy > Location Services > System Services > Significant Locations (enter passcode)



HOW DO WE PRESERVE DATA?

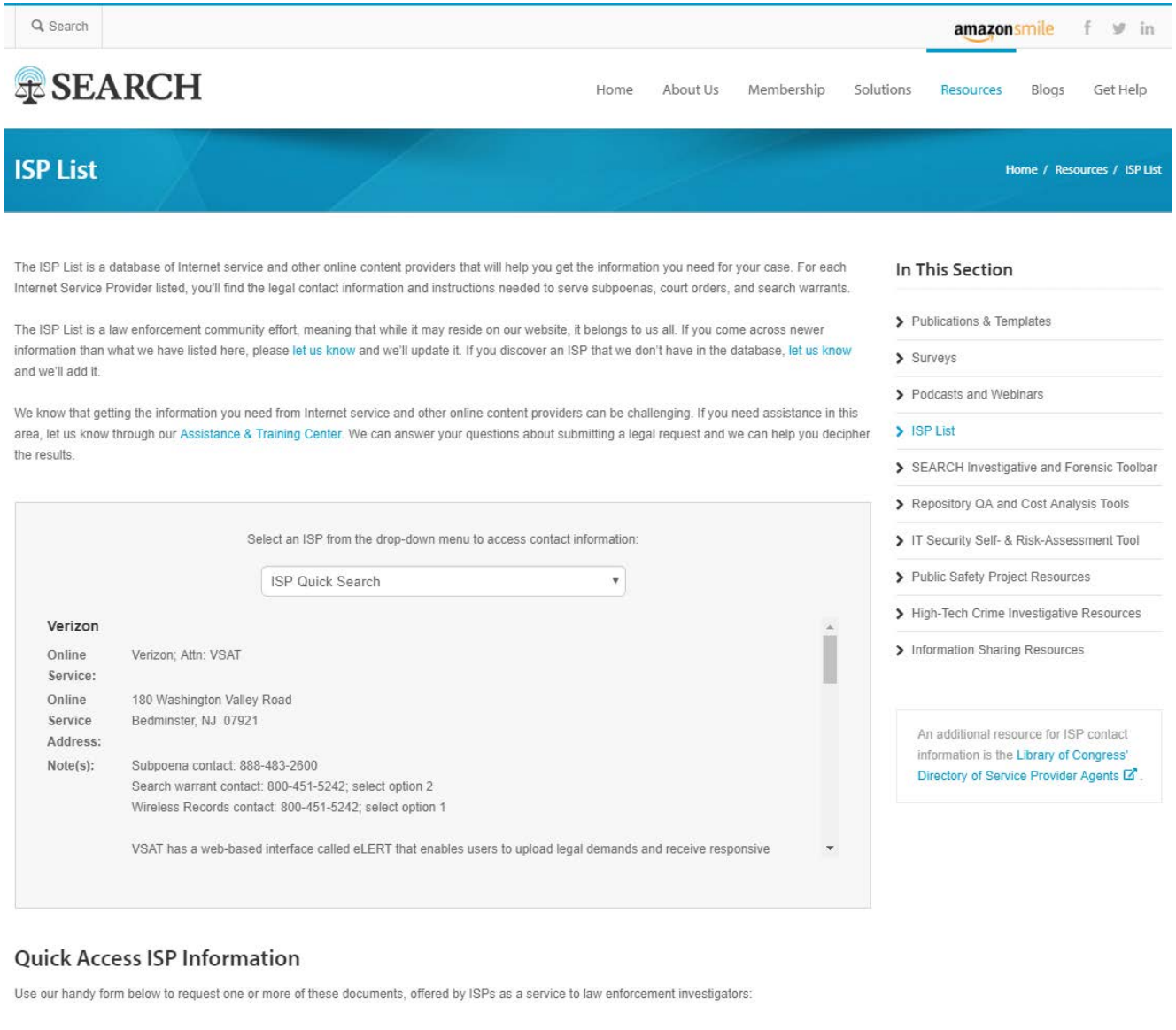


Evidence

- Once we think we have more data, we need to preserve it.
- Mobile Devices: Isolate from the network, store in a safe place, maintain chain of custody
- Records: Send preservation letters

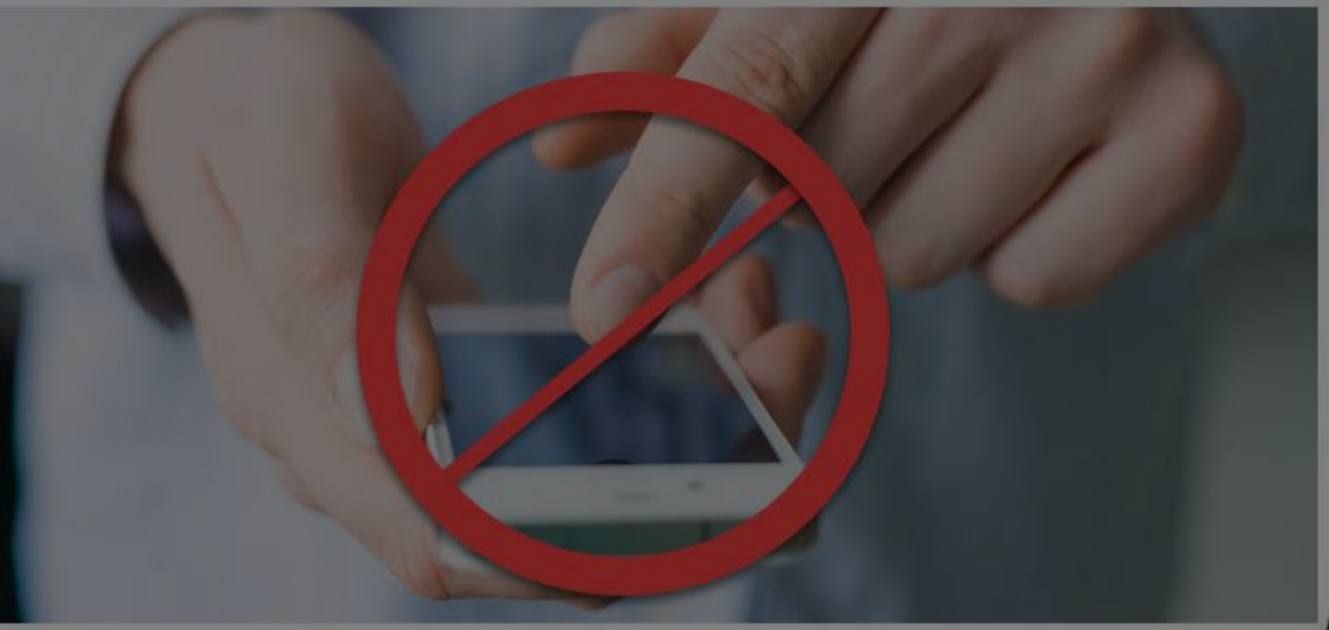
Legal Contact Information

https://www.search.org/resources/isp-list/



ENVISTA FORENSICS

HOW DO WE GET THIS DATA? (PROPERLY)



Right vs. Wrong

Using the right language

- Ensure the most up-to-date language is being used
  - Providers change capabilities and terminology often
  - They may also change their preferred method of service

  (We provide Language, just ask)

TruCall records:

•TruCall records are not readily accessible for production and delivery. Due to the burden involved in production and delivery of TruCall records, T-Mobile will only consider requests for TruCall records in 7 day increments per target telephone number. TMobile will formally object to requests that seek a greater scope.

•T-Mobile does not rely on TruCall data for managing individual accounts and is unable to warrant the accuracy of the data at the account-holder level.

•T-Mobile does not routinely collect TruCall data, which is not available in every market.

•T-Mobile is unable to certify TruCall records and will not provide any testimony that goes to the accuracy of same.

•T-Mobile will preserve up to 7 days of TruCall data per target.

Sept 2017:

T-Mobile US, Inc. (which includes T-Mobile USA and Metro PCS) delivers historical call detail records in Coordinated Universal Time ("UTC"). All requests need to be submitted in UTC values.

July 2017: "T-Mobile/MetroPCS is unable to determine a subscriber or data detail by IPv4 address." However, T-Mobile/MetroPCS has recently provided subscriber information for IPv6 addresses.

THE EVIDENCE
CALL DETAIL RECORDS

Call Detail Records (CDRs)

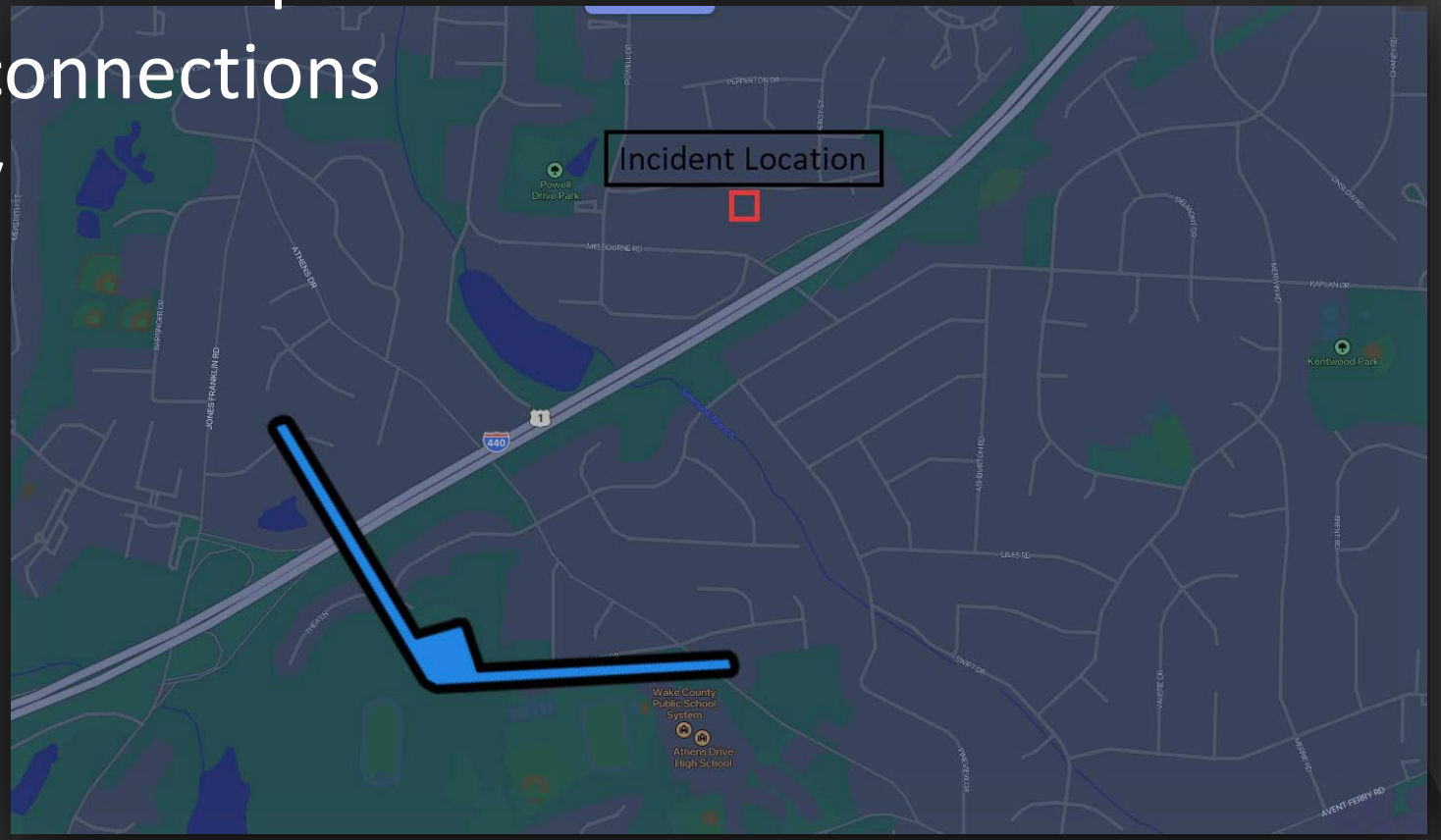
How to get them?

- Account holder can request with notarized letter
- Via subpoena
- Via discovery
  - Always get copies of the original files
- Contact us for specific subpoena language…It is free.
- Search.org (https://www.search.org/resources/isp-list/)

Call Detail Records (CDRs)

How are they used?

- Associate a phone call with a cell tower
- Show connections between phone numbers
- Show frequency of connections
- Show “user” activity



Prepaid Phone F.A.Qs

What are they?

Pre-Paid Phones “Burners”

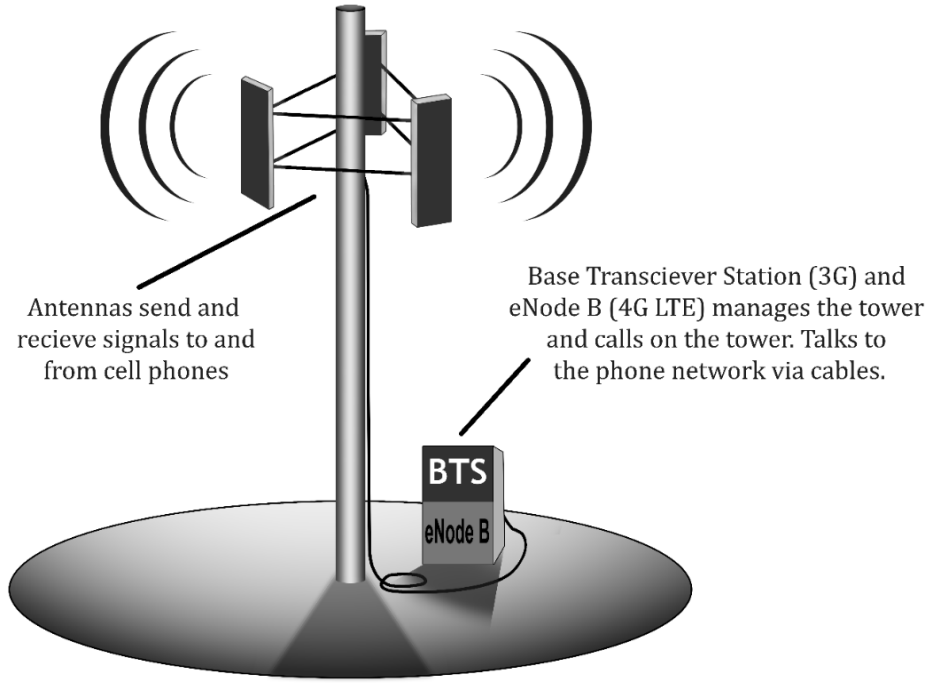
- No verification of identity needed
- Often no valid Subscriber information
- How do you get the records?

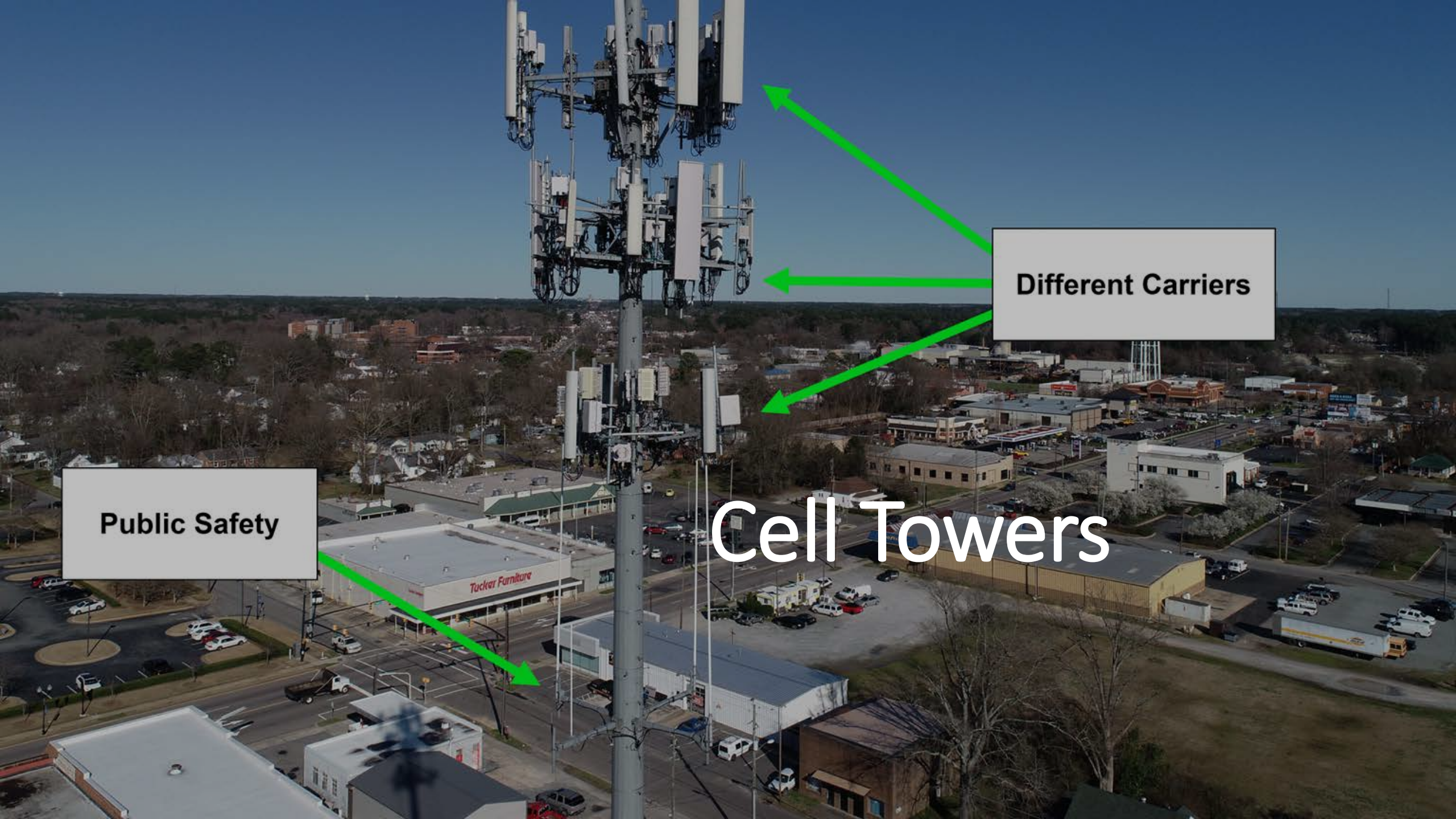
CELL TOWERS

The Cellular System: Cell Site

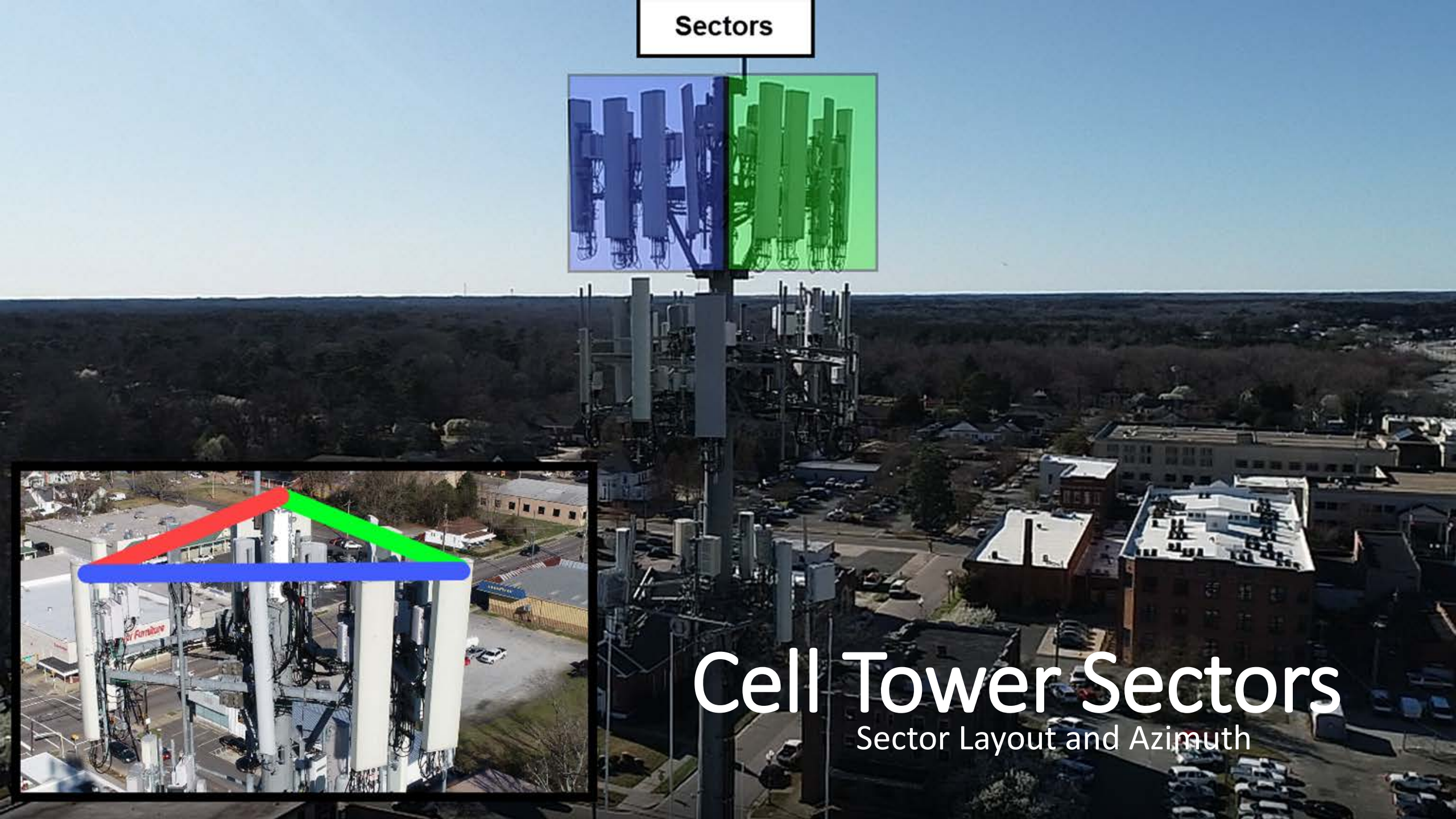
A Cell Site

- Antennas
  - Send and receive signals to and from cell phones
- Base Station Transceiver
  - Manages the tower and calls on the tower
  - Talks to the phone via network cables





Cell Towers

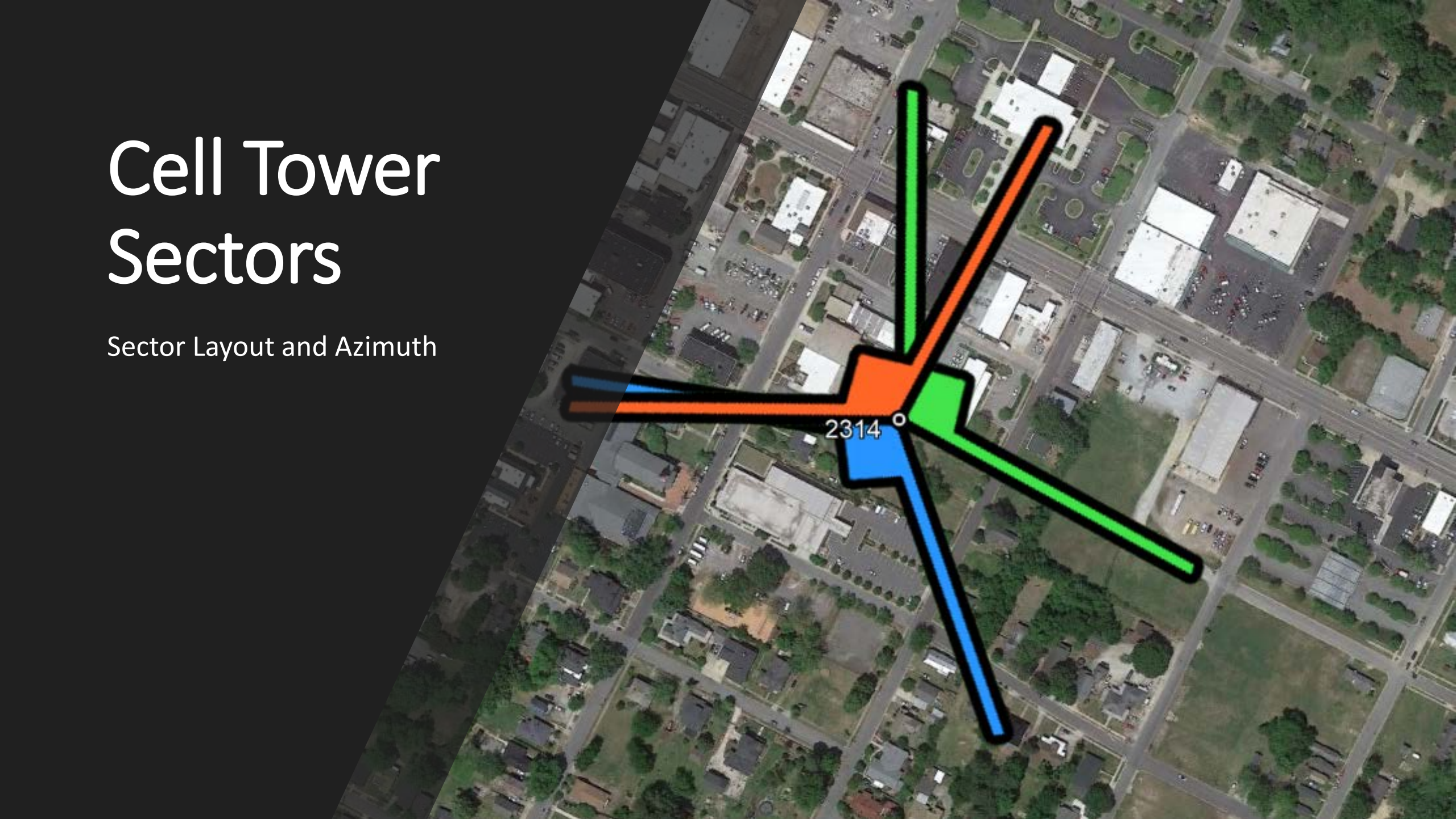


Cell Tower Sectors

Sector Layout and Azimuth

Cell Tower Sectors

Sector Layout and Azimuth



PRECISION?

Historical Call Detail Record Types for Location

Each Carrier Provides Various Data Sets

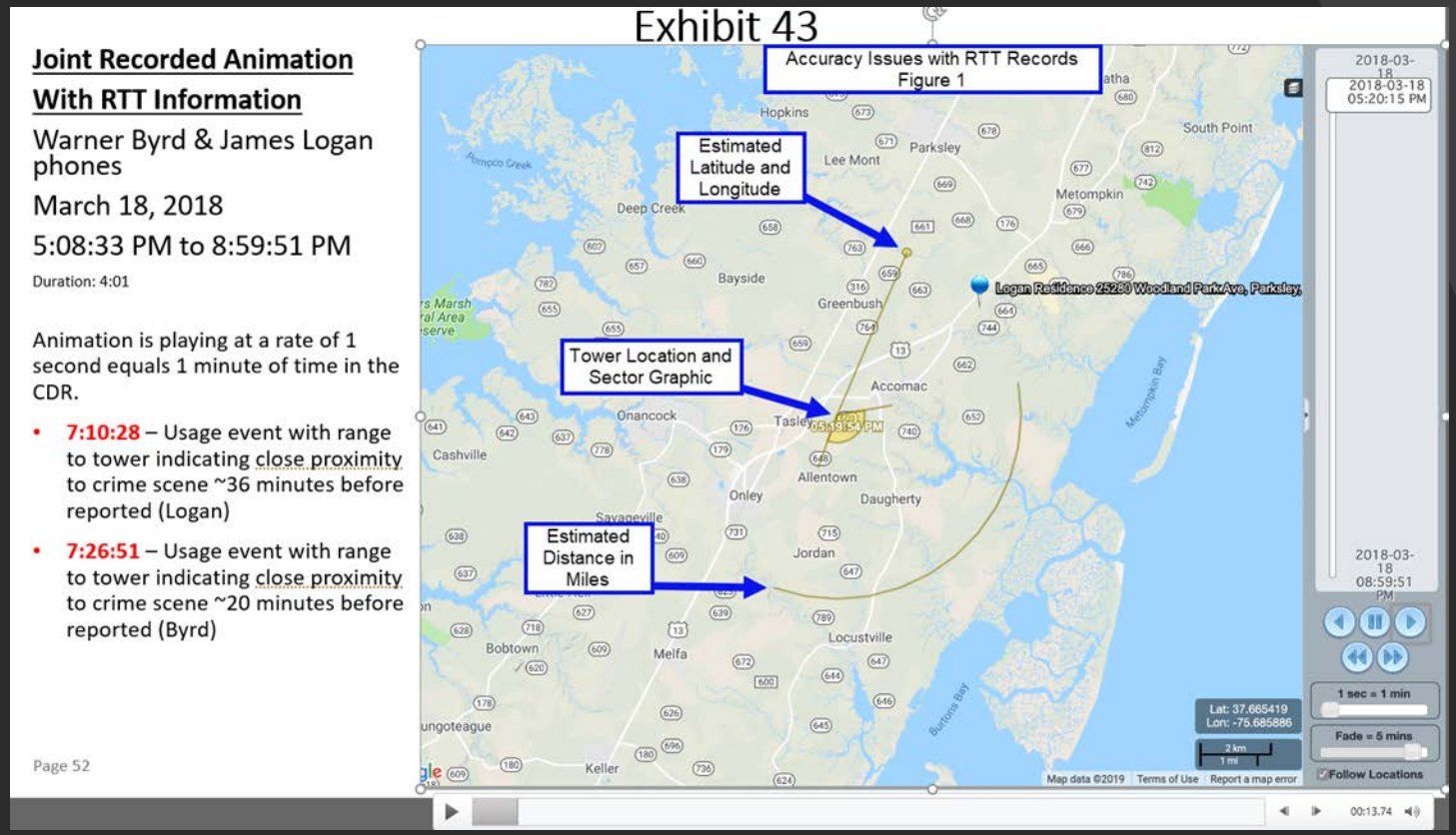
- Call detail records with cell site location
- “Precision location” data
  - NELOS
  - Real Time Tool (RTT)
  - Per Call Measurement Data (PCMD)
  - Time Delay of Arrival (TDOA)
- Tower dump records

	Start m-TMSI	Start Time	Duration	End Time	Start Type
		5/14/2018 21:32	40.925	5/14/2018 21:32	New Connecti
		5/14/2018 21:31	18.21	5/14/2018 21:32	New Connecti
		5/14/2018 21:27	1.39	5/14/2018 21:27	New Connecti
		5/14/2018 21:26	5.439	5/14/2018 21:26	New Connecti
		5/14/2018 21:25	5.176	5/14/2018 21:25	New Connecti
		5/14/2018 21:25	5.256	5/14/2018 21:25	New Connecti
		5/14/2018 21:24	6.182	5/14/2018 21:24	New Connecti
		5/14/2018 21:21	5.512	5/14/2018 21:21	New Connecti
		5/14/2018 21:15	5.331	5/14/2018 21:15	New Connecti
		5/14/2018 21:14	5.182	5/14/2018 21:14	New Connecti
		5/14/2018 21:13	12.798	5/14/2018 21:13	New Connecti
		5/14/2018 21:13	5.675	5/14/2018 21:13	New Connecti
		5/14/2018 21:13	10.76	5/14/2018 21:13	New Connecti
		5/14/2018 21:02	6.06	5/14/2018 21:02	New Connecti
		5/14/2018 21:01	5.53	5/14/2018 21:01	New Connecti

Issues with Precision Location Data

Known Issues

- Latitude and longitude points given have been determined to be less than accurate
- Often presented as if they are GPS based locations



Disclaimers are Important

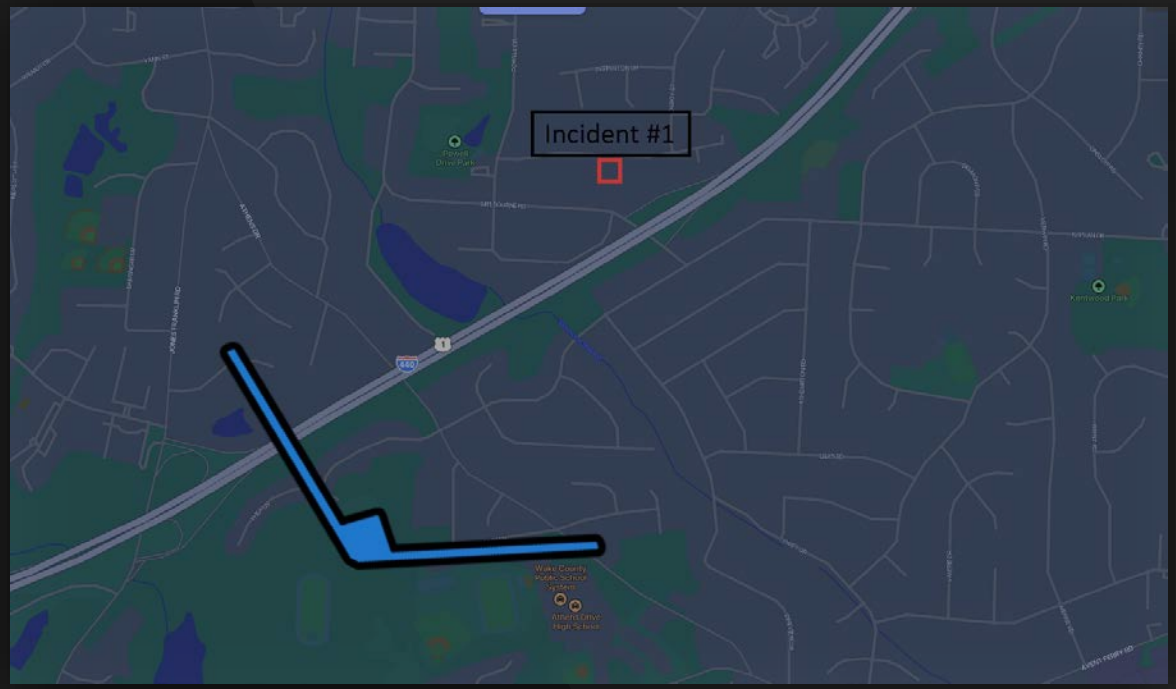
AT&T, Sprint and Verizon all provide disclaimers about the data contained in their reports

- “best estimate”
- “not historical GPS”
- “exercise caution”
- “less than exact”

TOWER DUMPS

Tower Dump Data

- Why are they used?
  - Locate common numbers
  - Determine numbers active in an area
  - Typically requested when suspects are unknown



AUTOMATED SOFTWARE

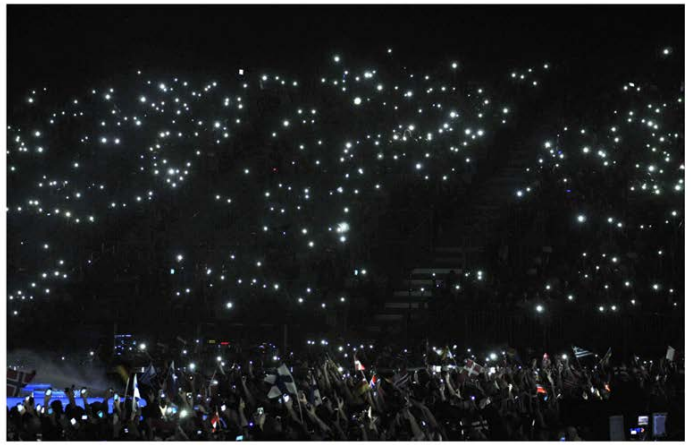
TURBO TAX DOESN'T MAKE YOU A CPA

Automated Software

*Validation Sold Separately

The New York Times

Flaws in Cellphone Evidence Prompt Review of 10,000 Verdicts in Denmark



The first error was found in an I.T. system that converts phone companies' raw data into evidence that the police and prosecutors can use to place a person at the scene of a crime. During the conversions, the system omitted some data, creating a less-detailed image of a cellphone's whereabouts. The error was fixed in March after the national police discovered it.

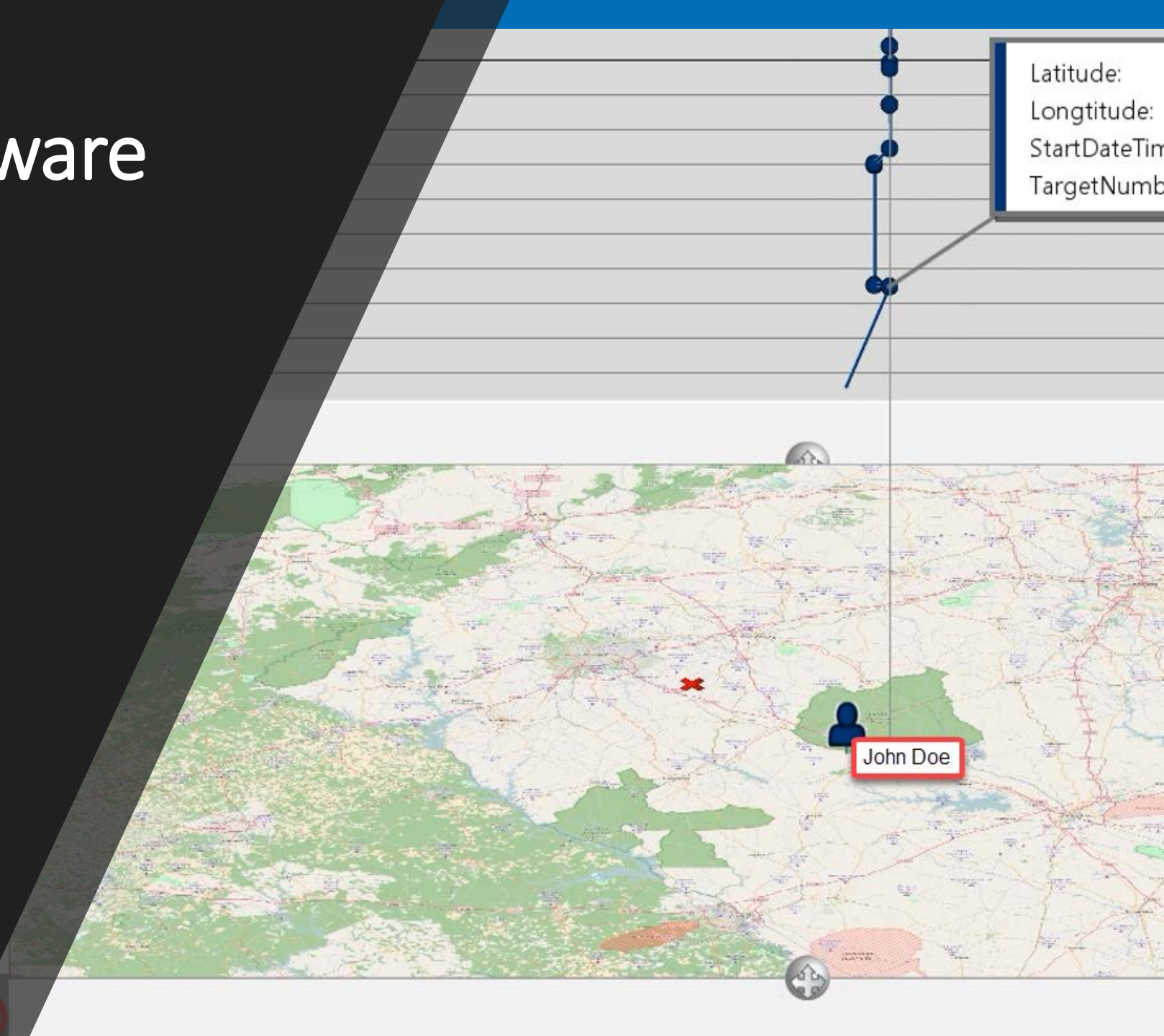
https://www.nytimes.com/2019/08/20/world/europe/denmark-cellphone-data-courts.html

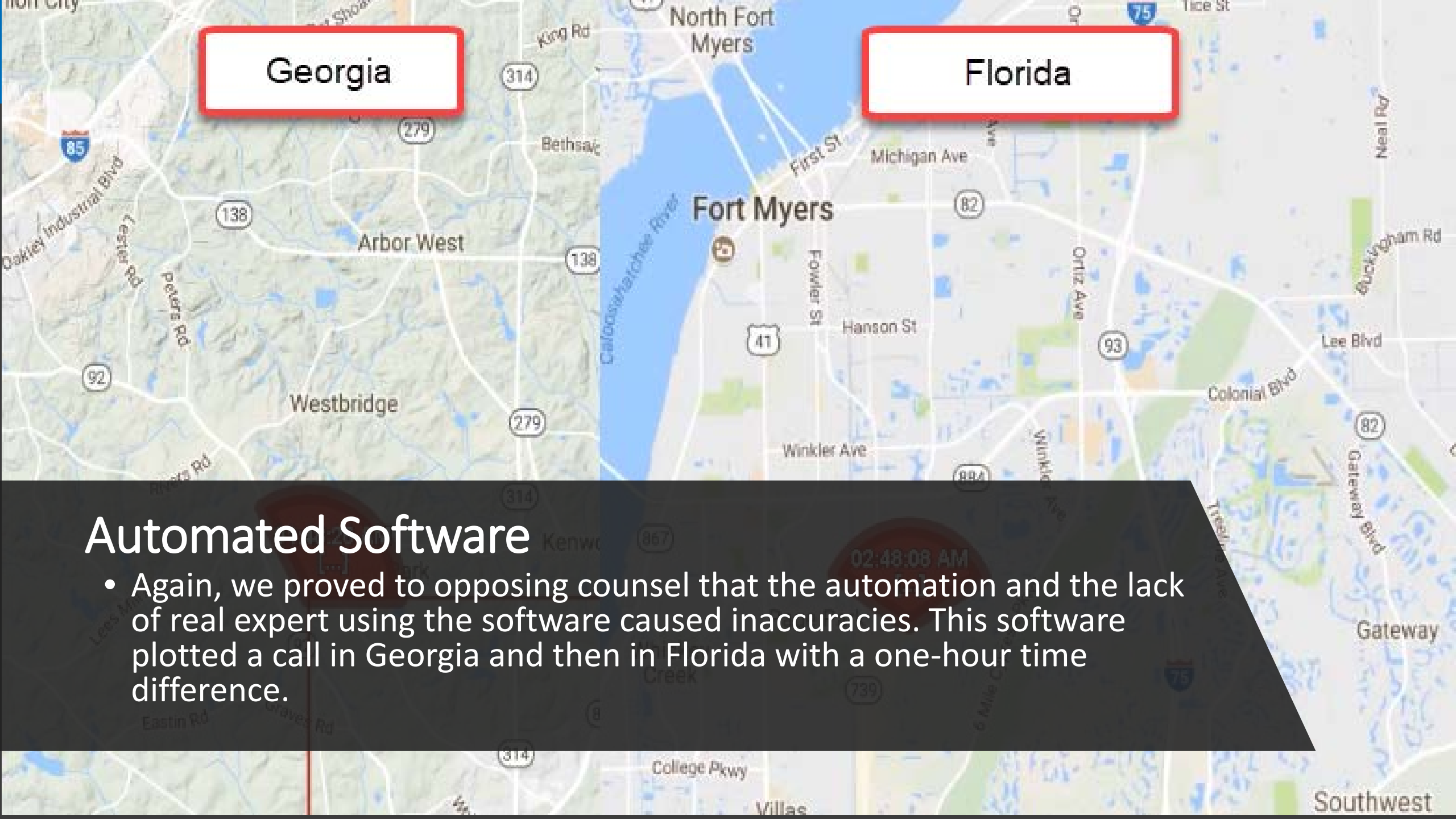
Automated Software

- Coverage area?
- This odd shape is not based on science or any other factual data.

Automated Software

- The State's "Expert" admitted the software made mistakes. UTC to local offsets interpreted incorrectly
- EDT = UTC-4, not +5





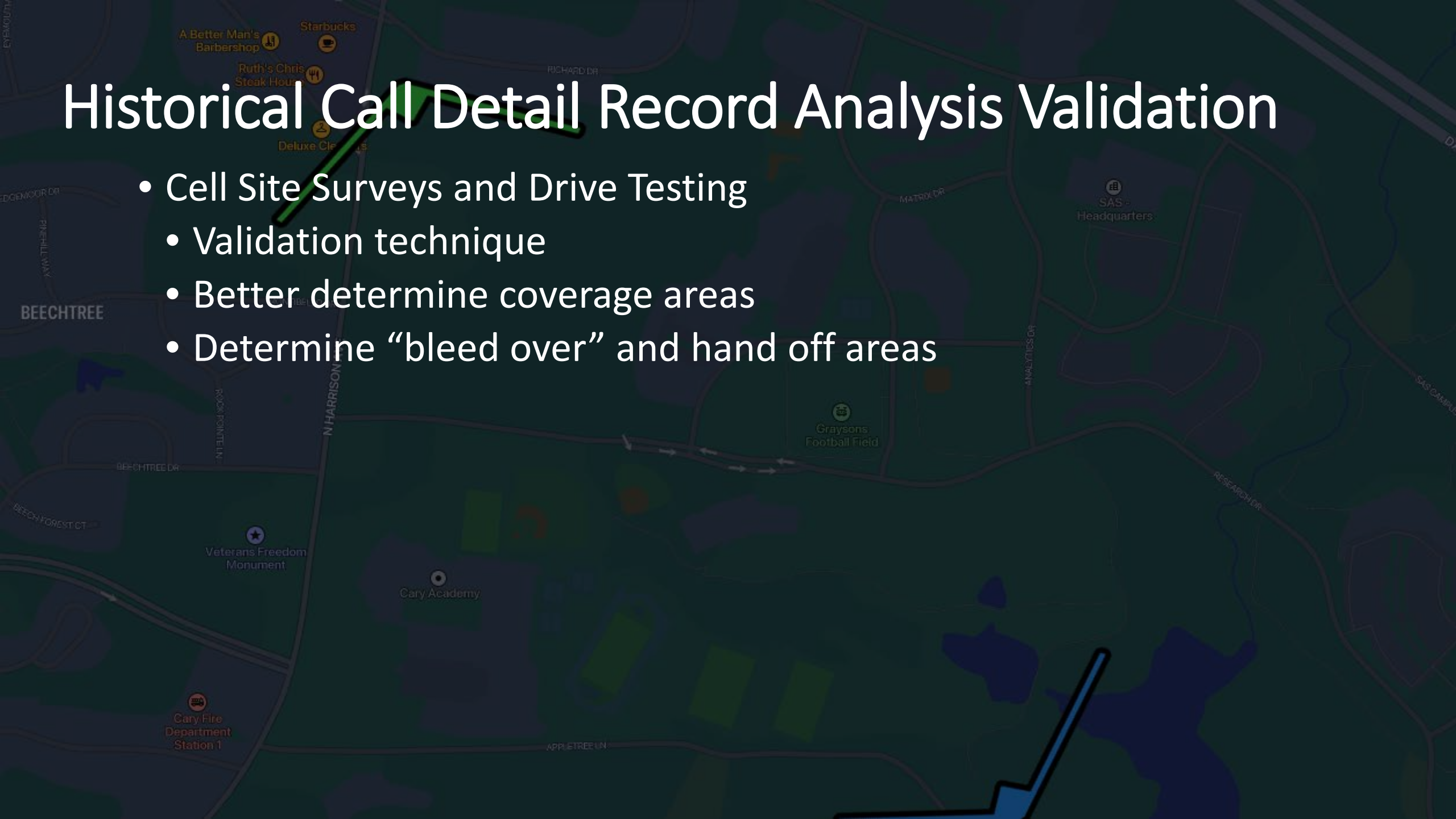
Automated Software

- Again, we proved to opposing counsel that the automation and the lack of real expert using the software caused inaccuracies. This software plotted a call in Georgia and then in Florida with a one-hour time difference.

CELL SITE SURVEYS AND DRIVE TEST

Historical Call Detail Record Analysis Validation

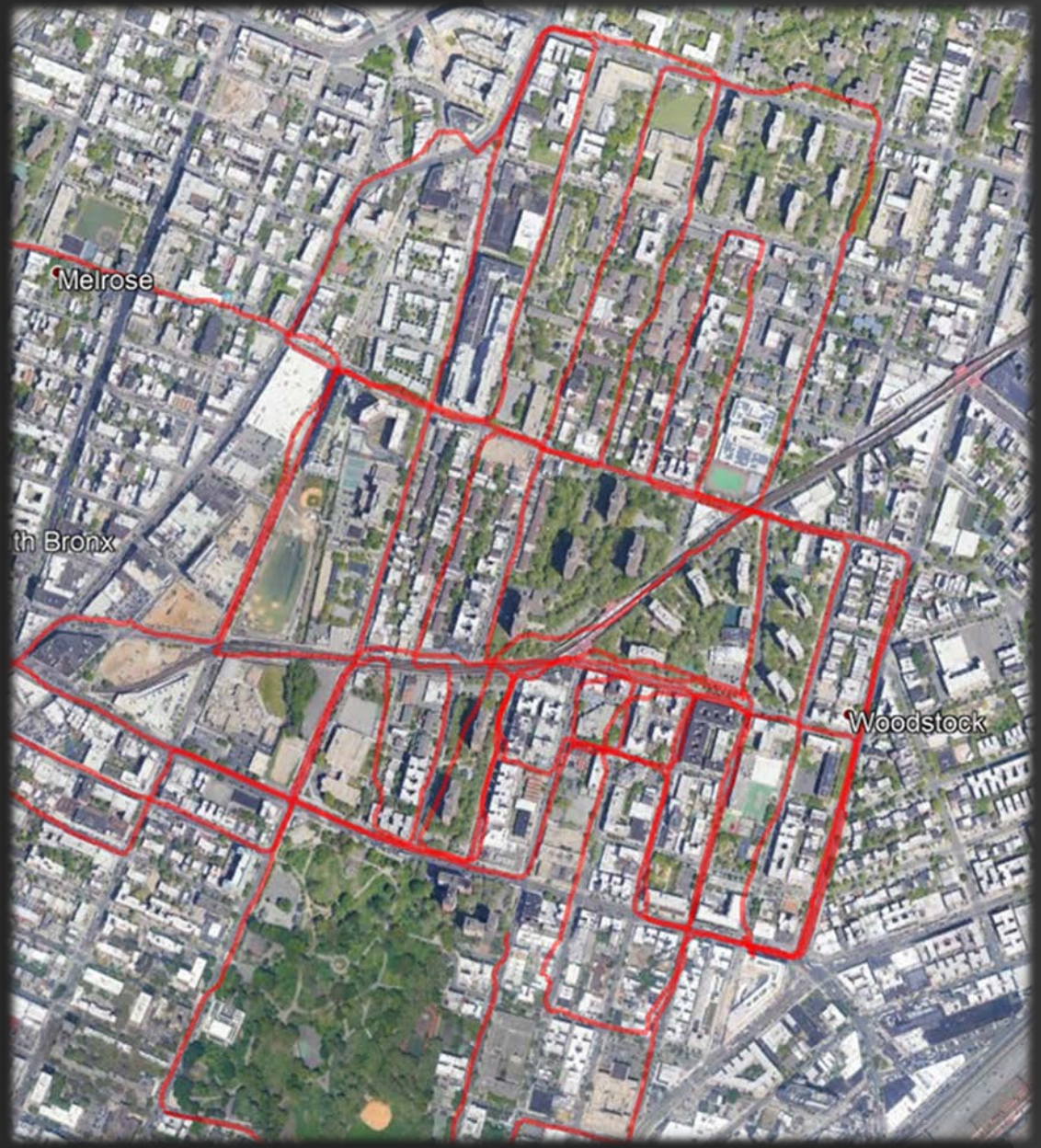
- Cell Site Surveys and Drive Testing
  - Validation technique
  - Better determine coverage areas
  - Determine “bleed over” and hand off areas



Surveys or Drive Test

Collect data from the area in question;

- Signal Strength
- Sector Information
- Frequencies available
- Serving coverage?



Coverage?

We want to know what is possible

LIVE LOCATION DATA

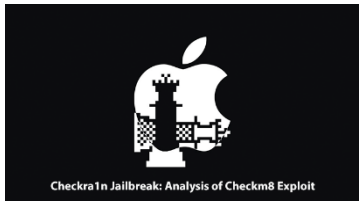
Live Location

- Pen register, trap and trace orders (no content)
- Wire Taps (content included)
- These orders allow for new data to be obtained, as well as request historical data.
- After a Carrier has received the order, they will begin to provide location information
- All carriers can provide real time GPS for tracking
- Pen registers can also be installed for IP logs

DEVICE BASED LOCATION DATA

GRAYSHIFT

OXYGEN FORENSICS
Helping good people make this world safer



BlackBag TECHNOLOGIES

Cellebrite
Digital intelligence for a safer world

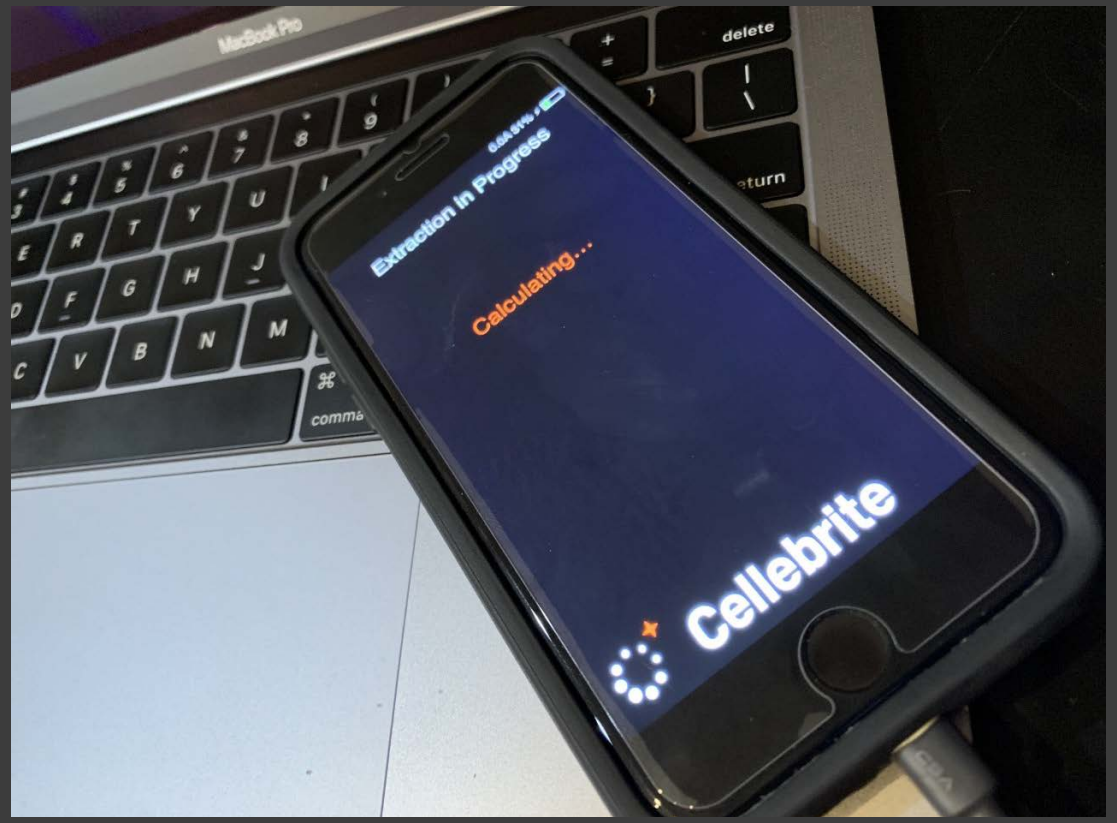
Cell Phone Forensics

Forensic Extraction Tools

ENVISTA FORENSICS

Capabilities

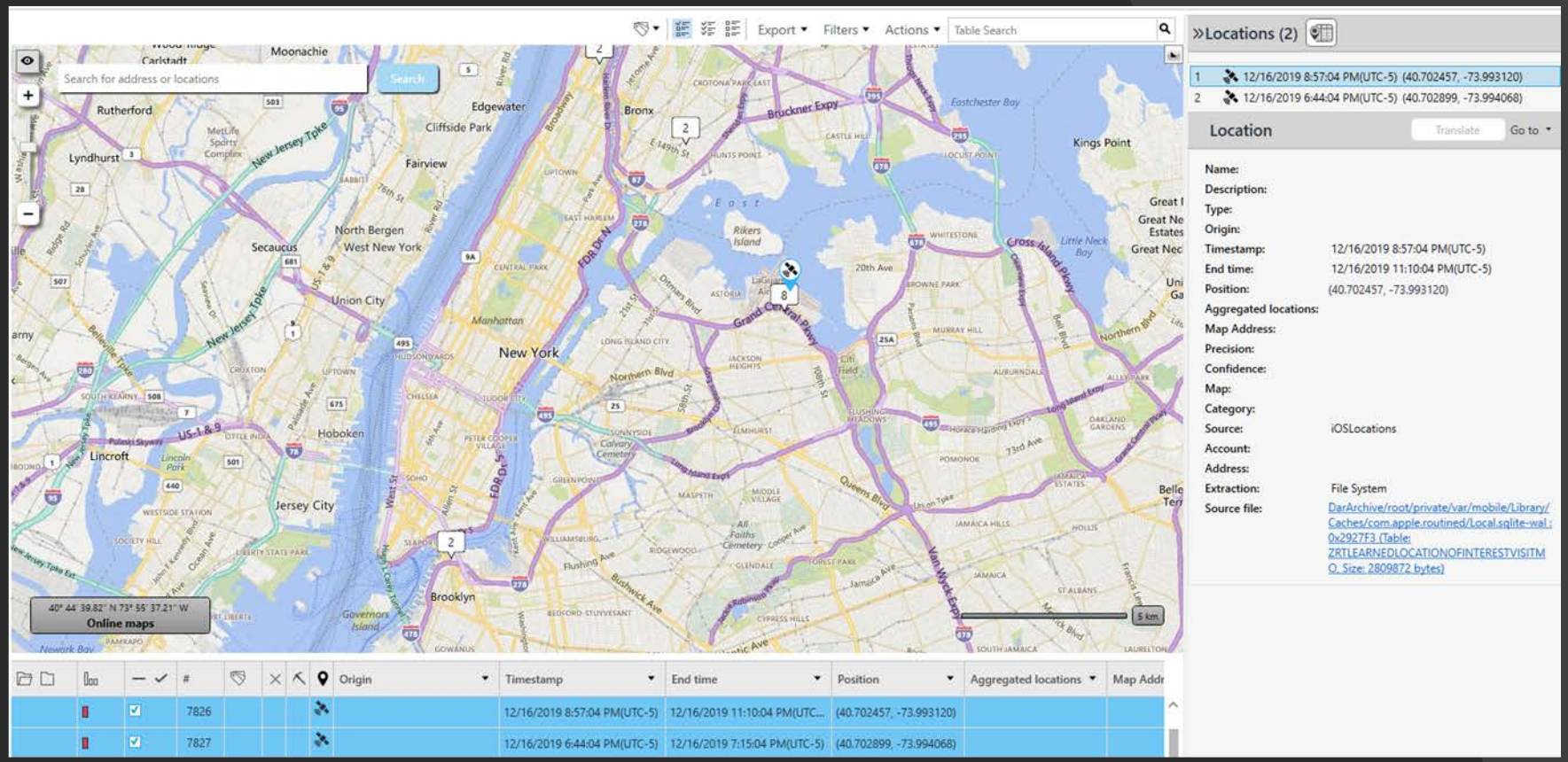
iOs Full File System Extraction



- Call Log (280) (1)
- Cell Towers (1393) (188)
- Chats (310) (23)
- Contacts (1748) (45)
- Cookies (1154)
- Device Connectivity (1140) (121)
- Device Events (2762)
- Device Locations (9401) (317)

iOS Significant Locations

- Device Locations (9401) (317)
  - Journeys (9)
    - Apple Maps (5)
    - Google Maps (3)
    - Mails (1)
  - Locations (9254) (317)
    - Apple Maps (11)
    - Calendar (385)
    - Find My (1)
    - Google Maps (5) (3)
    - iMessage: +19842975158
    - iOSLocations (5910) (3)
    - Mails (10)
    - Native (2748) (311)
    - Uber (5)
    - Waze (178)



CELL PHONE DATA "CELLEBRITE"

DID YOU RECEIVE ALL DISCOVERY?

Standard discovery request for extraction data

"Cell Phone Forensic Extraction Files believed to have been collected with Cellebrite or similar forensic extraction software: UFED Files, .BIN (Binary Files), .TAR (or other archival files)

a. Evidence Log of all digital Evidence with full chain of custody for each item

b. Complete Search Warrants, Signed Consent to Search Forms, or documentation of exigent circumstances that were utilized to access and download these devices

c. All data as originally produced by Cellebrite UFED (Universal Forensic Extraction Device) to include the original folder structure and all files.

d. All exported reports in native format (i.e. PDF, Excel, HTML, UFDR, etc.)

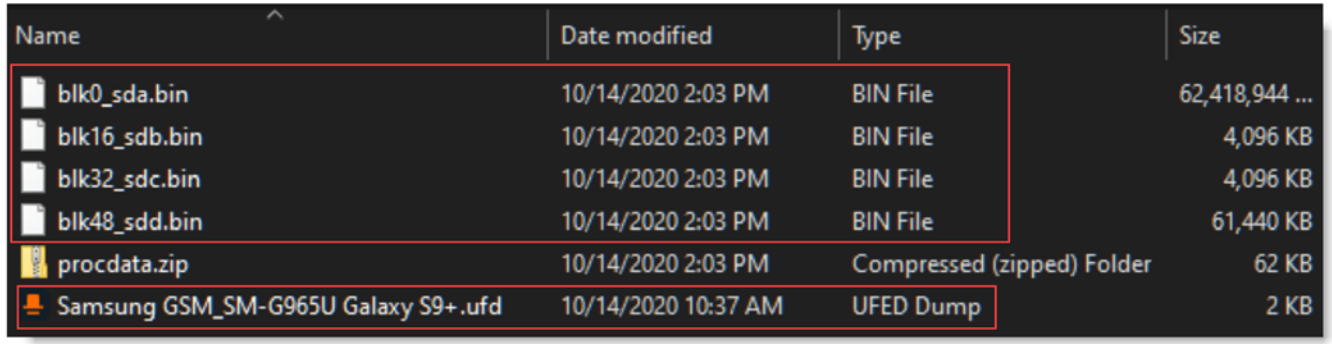
e. Any passwords (security or encryption), PIN, pattern locks collected during the law enforcement investigation to unlock said devices."

f. Any Cellebrite Project files (.pas files)

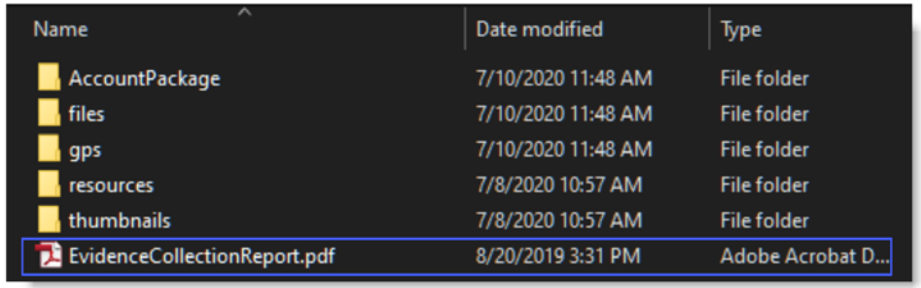
g. Any Cellebrite Multiple Dumps (UFDX files)

h. Any photographs taken of the device at time of seizure and examination

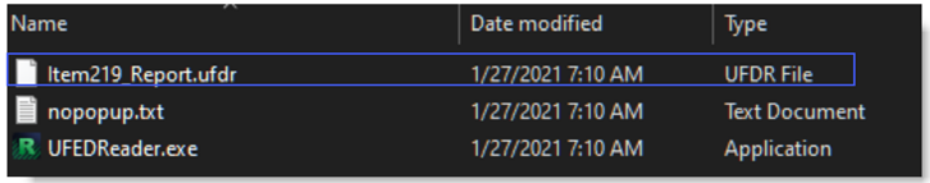
i. Any notes written by police regarding their handling, examination, or analysis of the digital evidence."



Name	Date modified	Type	Size
blk0_sda.bin	10/14/2020 2:03 PM	BIN File	62,418,944 ...
blk16_sdb.bin	10/14/2020 2:03 PM	BIN File	4,096 KB
blk32_sdc.bin	10/14/2020 2:03 PM	BIN File	4,096 KB
blk48_sdd.bin	10/14/2020 2:03 PM	BIN File	61,440 KB
procdata.zip	10/14/2020 2:03 PM	Compressed (zipped) Folder	62 KB
Samsung GSM_SM-G965U Galaxy S9+.ufd	10/14/2020 10:37 AM	UFED Dump	2 KB



Name	Date modified	Type
AccountPackage	7/10/2020 11:48 AM	File folder
files	7/10/2020 11:48 AM	File folder
gps	7/10/2020 11:48 AM	File folder
resources	7/8/2020 10:57 AM	File folder
thumbnails	7/8/2020 10:57 AM	File folder
EvidenceCollectionReport.pdf	8/20/2019 3:31 PM	Adobe Acrobat D...



Name	Date modified	Type
Item219_Report.ufdr	1/27/2021 7:10 AM	UFDR File
nopopup.txt	1/27/2021 7:10 AM	Text Document
UFEDReader.exe	1/27/2021 7:10 AM	Application

Data Aquired during extraction vs. Reports and exports

Pourpose: Forensic Analysis by Qualified Examiners

.UFED, UFDX, .BIN, .TAR or similar files are used by Forensic Examiners for analysis of data. Examples of those files are located below. You cannot open and view the content without forensic tools

Name	Date modified	Type	Size
blk0_sda.bin	10/14/2020 2:03 PM	BIN File	62,418,944 ...
blk16_sdb.bin	10/14/2020 2:03 PM	BIN File	4,096 KB
blk32_sdc.bin	10/14/2020 2:03 PM	BIN File	4,096 KB
blk48_sdd.bin	10/14/2020 2:03 PM	BIN File	61,440 KB
procdata.zip	10/14/2020 2:03 PM	Compressed (zipped) Folder	62 KB
Samsung GSM_SM-G965U Galaxy S9+.ufd	10/14/2020 10:37 AM	UFED Dump	2 KB

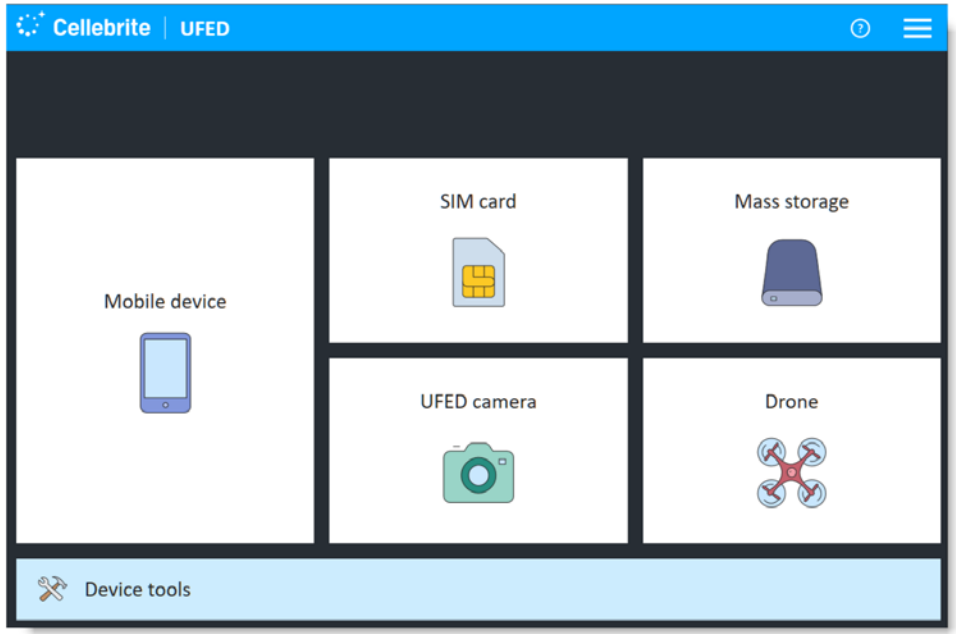
Name	Date modified	Type
FileSystem Android Backup 01	6/4/2019 2:29 AM	File folder
Logical 01	6/4/2019 2:29 AM	File folder
Physical ADB 01	6/4/2019 2:29 AM	File folder
EvidenceCollection.ufdx	6/26/2016 12:41 PM	UFED Multiple Dumps

Pourpose: Reporting Findings to Non-Experts

PDF, UFED Reader, Excel or other report formats are for reporting findings and opinions from forensic analysis. They do not provide the details needed by a Forensic Examiner to conduct an analysis. Examples of those files are located below.

Name	Date modified	Type
AccountPackage	7/10/2020 11:48 AM	File folder
files	7/10/2020 11:48 AM	File folder
gps	7/10/2020 11:48 AM	File folder
resources	7/8/2020 10:57 AM	File folder
thumbnails	7/8/2020 10:57 AM	File folder
EvidenceCollectionReport.pdf	8/20/2019 3:31 PM	Adobe Acrobat D...

Name	Date modified	Type
Item219_Report.ufdr	1/27/2021 7:10 AM	UFDR File
nopopup.txt	1/27/2021 7:10 AM	Text Document
UFEDReader.exe	1/27/2021 7:10 AM	Application



Forensic Software/Hardware for extraction

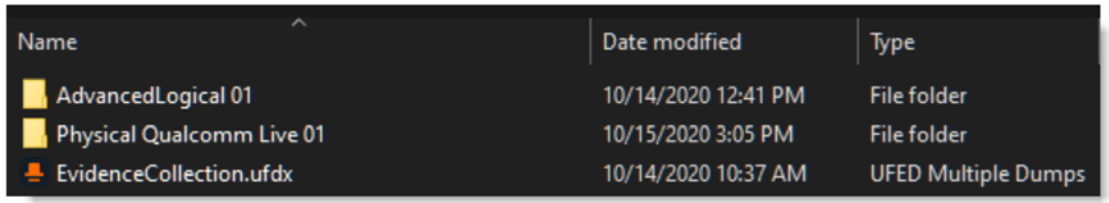
Evidence Device

Depending on the device and methods used, Cellebrite UFED Software will produce similar files.

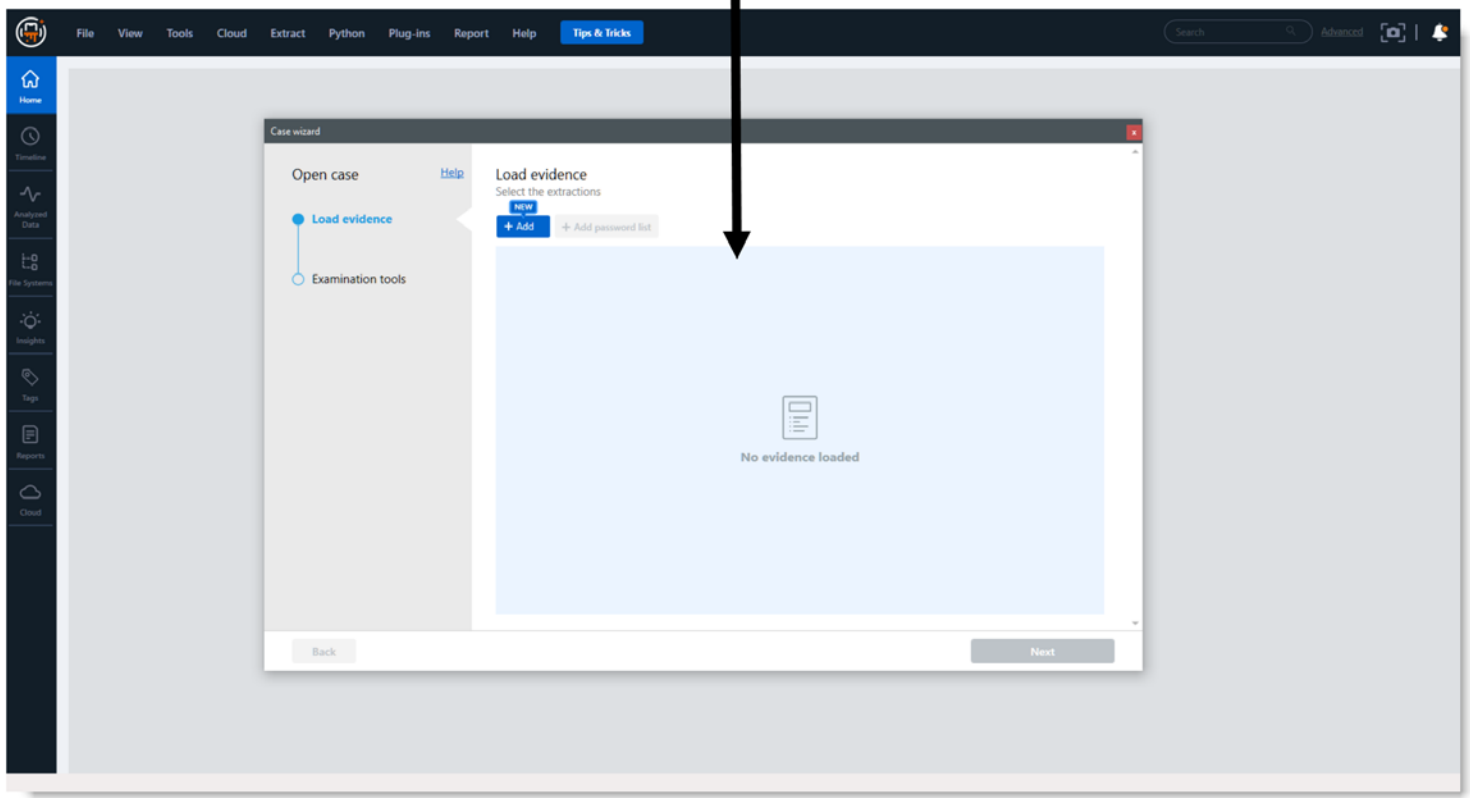
Name	Date modified	Type
AdvancedLogical 01	10/14/2020 12:41 PM	File folder
Physical Qualcomm Live 01	10/15/2020 3:05 PM	File folder
EvidenceCollection.ufdx	10/14/2020 10:37 AM	UFED Multiple Dumps

Name	Date modified	Type	Size
blk0_sda.bin	10/14/2020 2:03 PM	BIN File	62,418,944 ...
blk16_sdb.bin	10/14/2020 2:03 PM	BIN File	4,096 KB
blk32_sdc.bin	10/14/2020 2:03 PM	BIN File	4,096 KB
blk48_sdd.bin	10/14/2020 2:03 PM	BIN File	61,440 KB
procdata.zip	10/14/2020 2:03 PM	Compressed (zipped) Folder	62 KB
Samsung GSM_SM-G965U Galaxy S9+.ufd	10/14/2020 10:37 AM	UFED Dump	2 KB

This is the original data that is extracted from the device. Without forensic tools this data cannot be viewed.



This data is then loaded to a seperate forensic software for parsing and analysis.



File View Tools Cloud Extract Python Plug-ins Report Help **Tips & Tricks** Search Advanced

Home Timeline Analyzed Data File Systems Insights Tags Reports Cloud

Samsung GSM_SM-S12... | Extraction Summary (1) ×

All Content | Physical

Extraction Summary

+ Add extraction | Add external file | Project settings | Generate report | Open Virtual Analyzer

Extractions: 1

Physical
Samsung GSM SM-S120VL Galaxy Luna
Physical [Bootloader]

Extraction start date/time

Extraction end date/time

Image Hashes

Extraction images are verified.

Insights from Installed Apps

- Chat applications (10 apps)
- Hide files or pictures (1 apps)
- Clean mobile (7 apps)
- Games (112 apps)
- Browser (2 apps)
- Social networking (18 apps)
- Spoofing (1 apps)
- Lifestyle (15 apps)

View all

Device Info

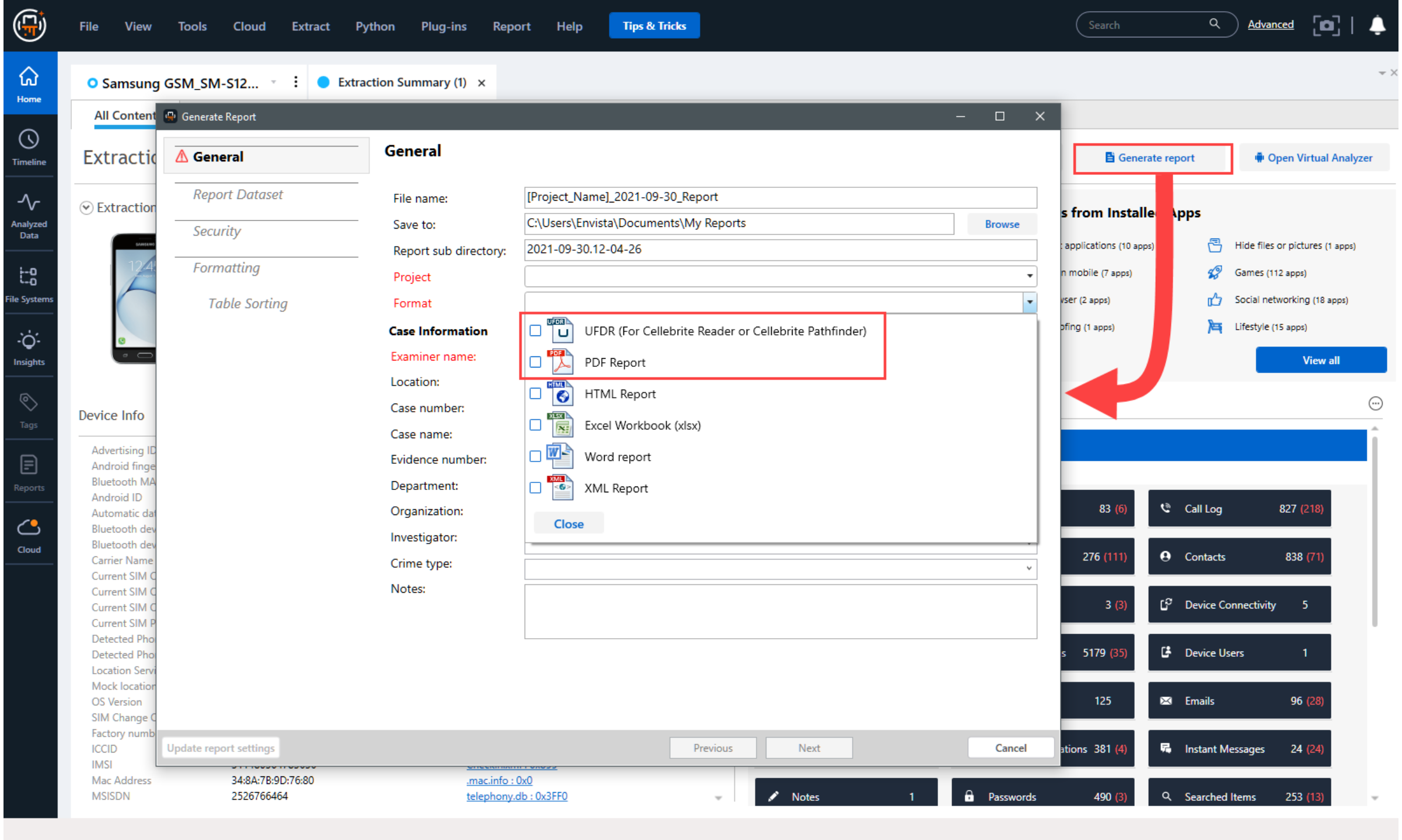
Advertising ID #1	adid_settings.xml : 0x99
Android fingerprint	build.prop : 0x537
Bluetooth MAC Address	bt_addr : 0x0
Android ID	settings_secure.xml : 0x23E1
Automatic date & time	com.android.settings_preferences.xml : 0x7EE
Bluetooth device address	settings_secure.xml : 0x3085
Bluetooth device name	settings_secure.xml : 0x1F91
Carrier Name	telephony.db : 0x3FD7
Current SIM Country ISO	SimCard.dat : 0x9F
Current SIM Operator	SimCard.dat : 0xB5
Current SIM Operator Name	SimCard.dat : 0xD3
Current SIM Phone Number	SimCard.dat : 0x11D
Detected Phone Model	build.prop : 0x252
Detected Phone Vendor	build.prop : 0x26D
Location Services Enabled	googlesettings.db-wal : 0x339BD7
Mock locations allowed	
OS Version	build.prop : 0x134
SIM Change Operation	SimCard.dat : 0x157
Factory number	serial_no : 0x0
ICCID	com.android.phone_preferences.xml : 0x3CE
IMSI	Checkin.xml : 0x855
Mac Address	.mac.info : 0x0
MSISDN	telephony.db : 0x3FF0

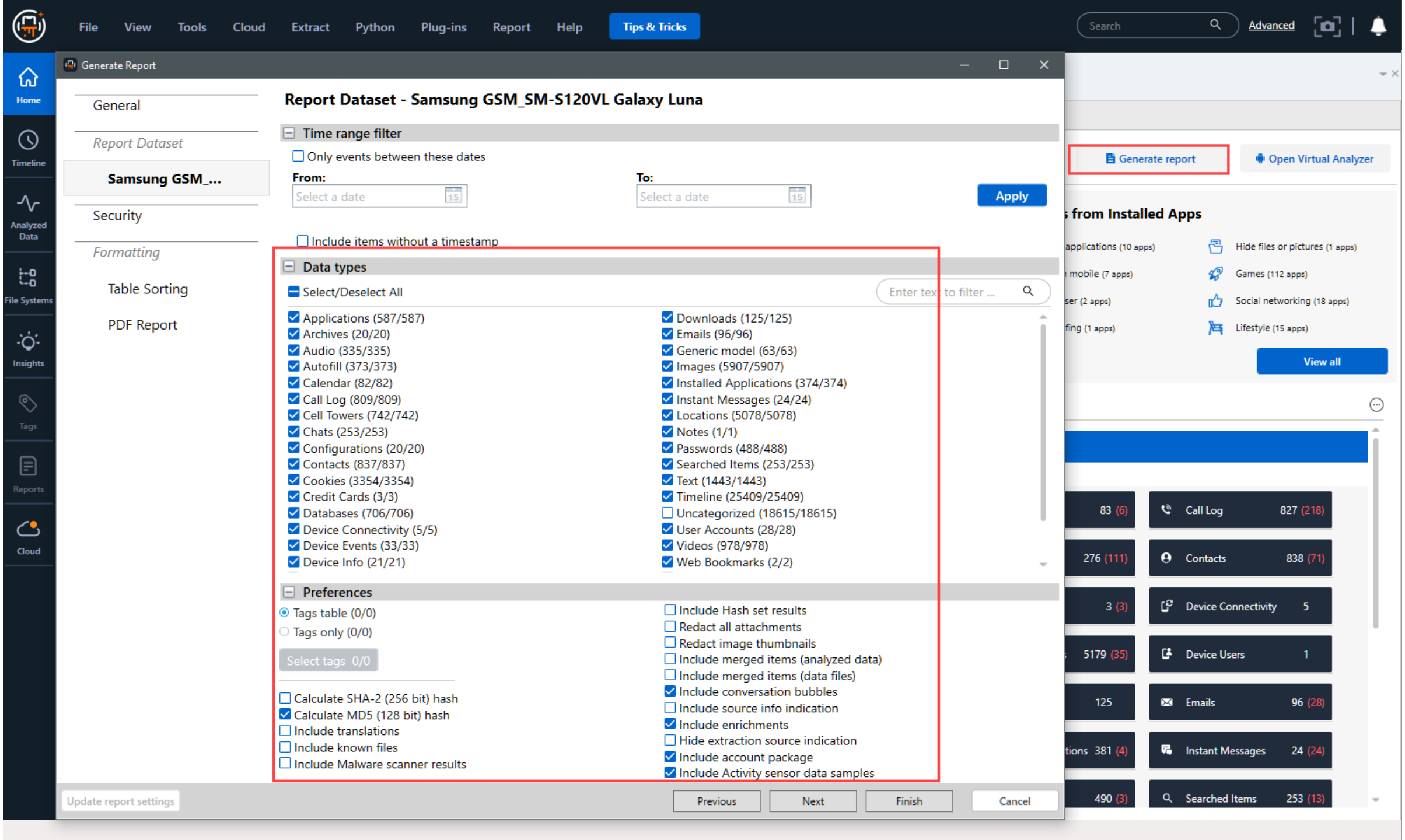
Content

23 data sources can be extracted using UFED Cloud

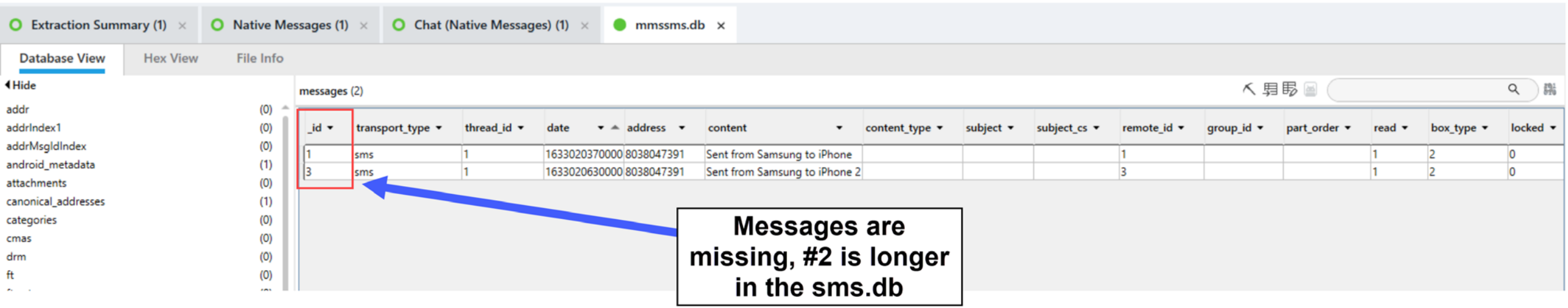
Data

Autofill 374 (2)	Calendar 83 (6)	Call Log 827 (218)
Cell Towers 747	Chats 276 (111)	Contacts 838 (71)
Cookies 3410 (91)	Credit Cards 3 (3)	Device Connectivity 5
Device Events 45 (44)	Device Locations 5179 (35)	Device Users 1
Devices 5	Downloads 125	Emails 96 (28)
Generic model 63	Installed Applications 381 (4)	Instant Messages 24 (24)
Notes 1	Passwords 490 (3)	Searched Items 253 (13)

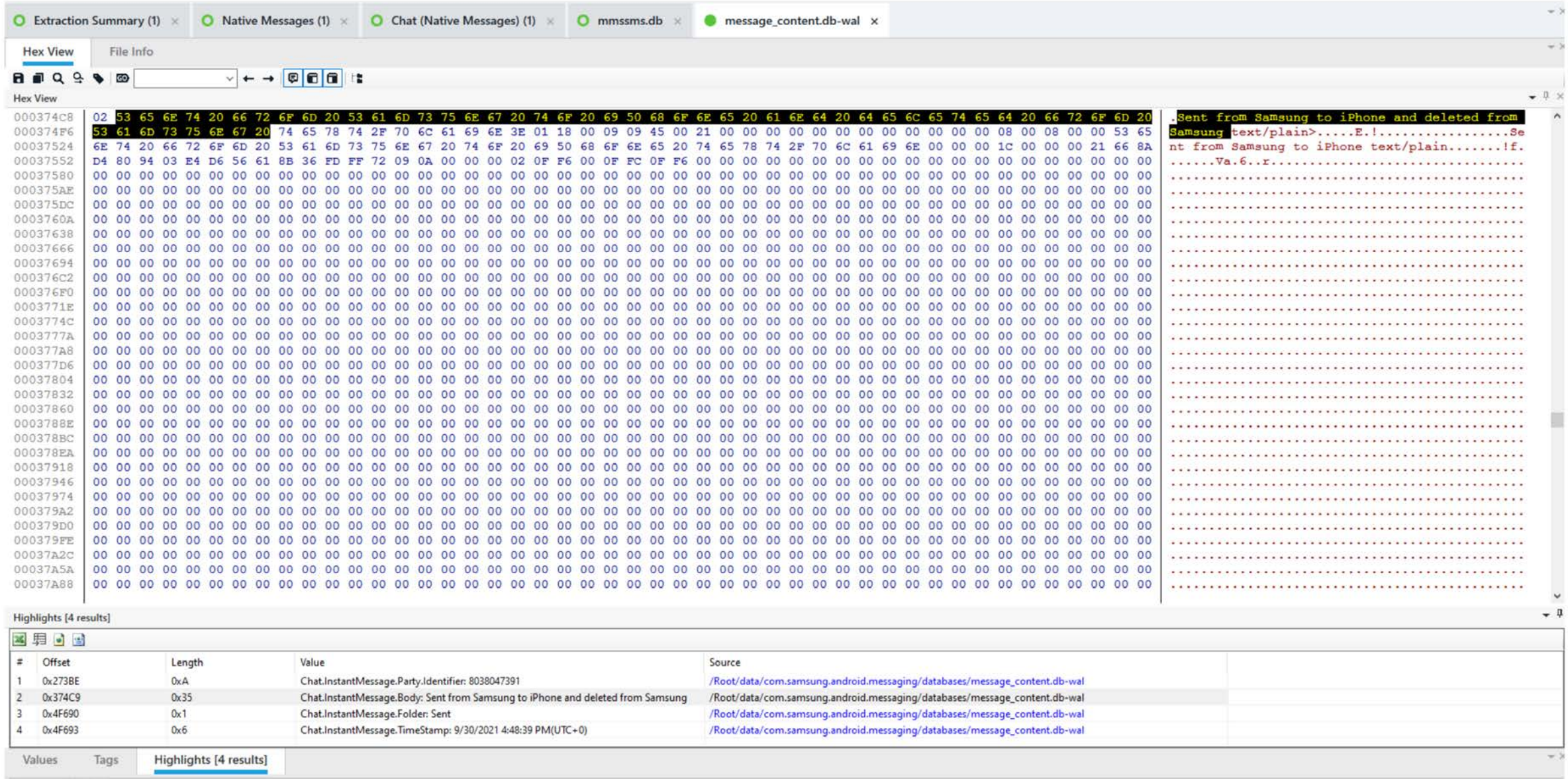

File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Search
Advanced
Home
Timeline
Analyzed Data
File Systems
Insights
Tags
Reports
Cloud
Samsung GSM_SM-S12...
Extraction Summary (1)
All Content
Generate Report
General
Report Dataset
Security
Formatting
Table Sorting
General
File name:
[Project_Name]_2021-09-30_Report
Save to:
C:\Users\Envista\Documents\My Reports
Browse
Report sub directory:
2021-09-30.12-04-26
Project
Format
Case Information
Examiner name:
Location:
Case number:
Case name:
Evidence number:
Department:
Organization:
Investigator:
Crime type:
Notes:
UFDR (For Cellebrite Reader or Cellebrite Pathfinder)
PDF Report
HTML Report
Excel Workbook (xlsx)
Word report
XML Report
Close
Update report settings
Previous
Next
Cancel
Generate report
Open Virtual Analyzer
Device Info
Advertising ID
Android ID
Bluetooth MA
Carrier Name
Mac Address
34:8A:7B:9D:76:80
MSISDN
2526766464
.mac.info : 0x0
telephony.db : 0x3FF0
Hide files or pictures (1 apps)
Games (112 apps)
Social networking (18 apps)
Lifestyle (15 apps)
View all
Call Log 827 (218)
Contacts 838 (71)
Device Connectivity 5
Device Users 1
Emails 96 (28)
Instant Messages 24 (24)
Notes 1
Passwords 490 (3)
Searched Items 253 (13)


File
View
Tools
Cloud
Extract
Python
Plug-ins
Report
Help
Tips & Tricks
Search
Advanced
Home
Timeline
Analyzed Data
File Systems
Insights
Tags
Reports
Cloud
Generate Report
General
Report Dataset
Samsung GSM_...
Security
Formatting
Table Sorting
PDF Report
Report Dataset - Samsung GSM_SM-S120VL Galaxy Luna
Time range filter
Only events between these dates
From:
Select a date
To:
Select a date
Apply
Include items without a timestamp
Data types
Select/Deselect All
Enter text to filter ...
Applications (587/587)
Archives (20/20)
Audio (335/335)
Autofill (373/373)
Calendar (82/82)
Call Log (809/809)
Cell Towers (742/742)
Chats (253/253)
Configurations (20/20)
Contacts (837/837)
Cookies (3354/3354)
Credit Cards (3/3)
Databases (706/706)
Device Connectivity (5/5)
Device Events (33/33)
Device Info (21/21)
Downloads (125/125)
Emails (96/96)
Generic model (63/63)
Images (5907/5907)
Installed Applications (374/374)
Instant Messages (24/24)
Locations (5078/5078)
Notes (1/1)
Passwords (488/488)
Searched Items (253/253)
Text (1443/1443)
Timeline (25409/25409)
Uncategorized (18615/18615)
User Accounts (28/28)
Videos (978/978)
Web Bookmarks (2/2)
Preferences
Tags table (0/0)
Tags only (0/0)
Select tags 0/0
Calculate SHA-2 (256 bit) hash
Calculate MD5 (128 bit) hash
Include translations
Include known files
Include Malware scanner results
Include Hash set results
Redact all attachments
Redact image thumbnails
Include merged items (analyzed data)
Include merged items (data files)
Include conversation bubbles
Include source info indication
Include enrichments
Hide extraction source indication
Include account package
Include Activity sensor data samples
Update report settings
Previous
Next
Finish
Cancel
Generate report
Open Virtual Analyzer
from Installed Apps
applications (10 apps)
mobile (7 apps)
ser (2 apps)
fing (1 apps)
Hide files or pictures (1 apps)
Games (112 apps)
Social networking (18 apps)
Lifestyle (15 apps)
View all
83 (6)
Call Log
827 (218)
276 (111)
Contacts
838 (71)
3 (3)
Device Connectivity
5
5179 (35)
Device Users
1
125
Emails
96 (28)
tions 381 (4)
Instant Messages
24 (24)
490 (3)
Searched Items
253 (13)

Locating messages in the database and confirming sequence of the primary key



Deleted messages were stored in the write ahead log and not the sms.db



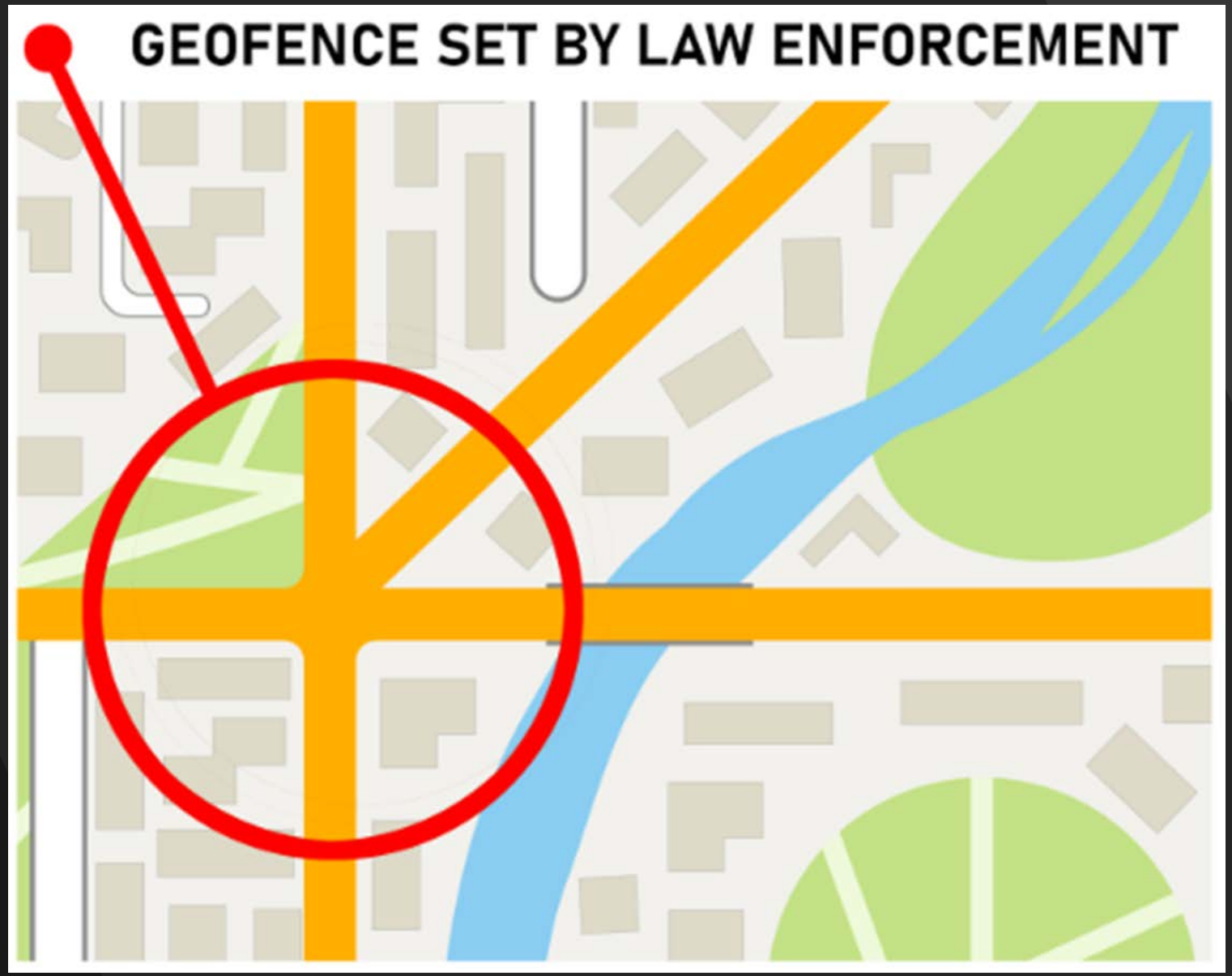
GOOGLE GEOFENCE

"NUMEROUS TENS OF MILLIONS" = 592 MILLION

What a Geofence Warrant Demands

- Historical Locations
  - Obtained via search warrant
  - Search warrant templates are marketed by many of the automated software program companies
  - Geofence for area of incident(s)
  - Location History (required)

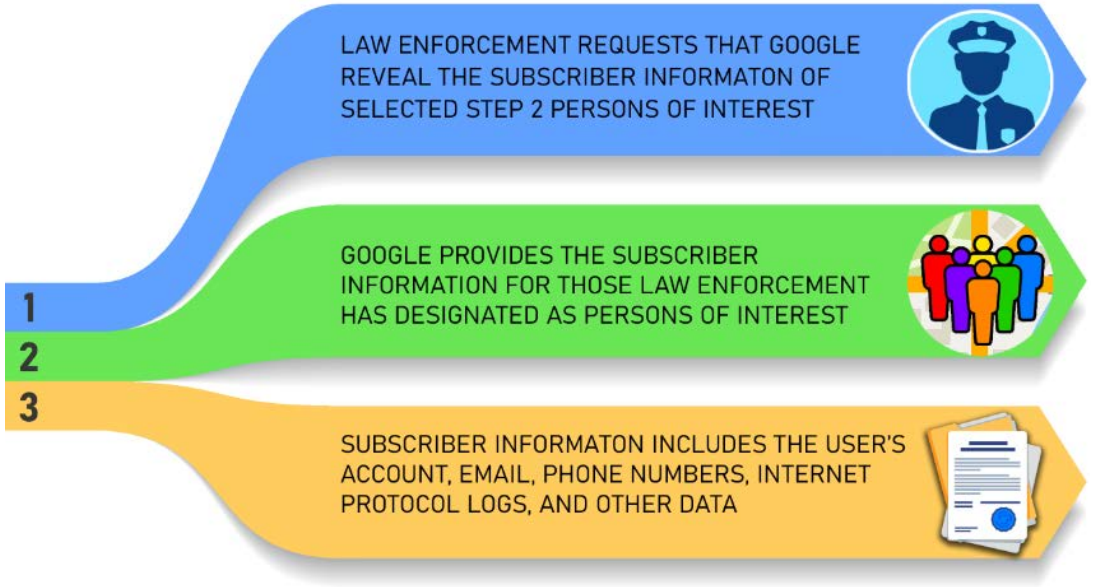
Geofence – Step 1



Geofence – Step 2

Geofence – Step 3

- The final step allowing the gathering of subscriber information.
- Users may receive notification in email with instructions for submitting motions to quash.

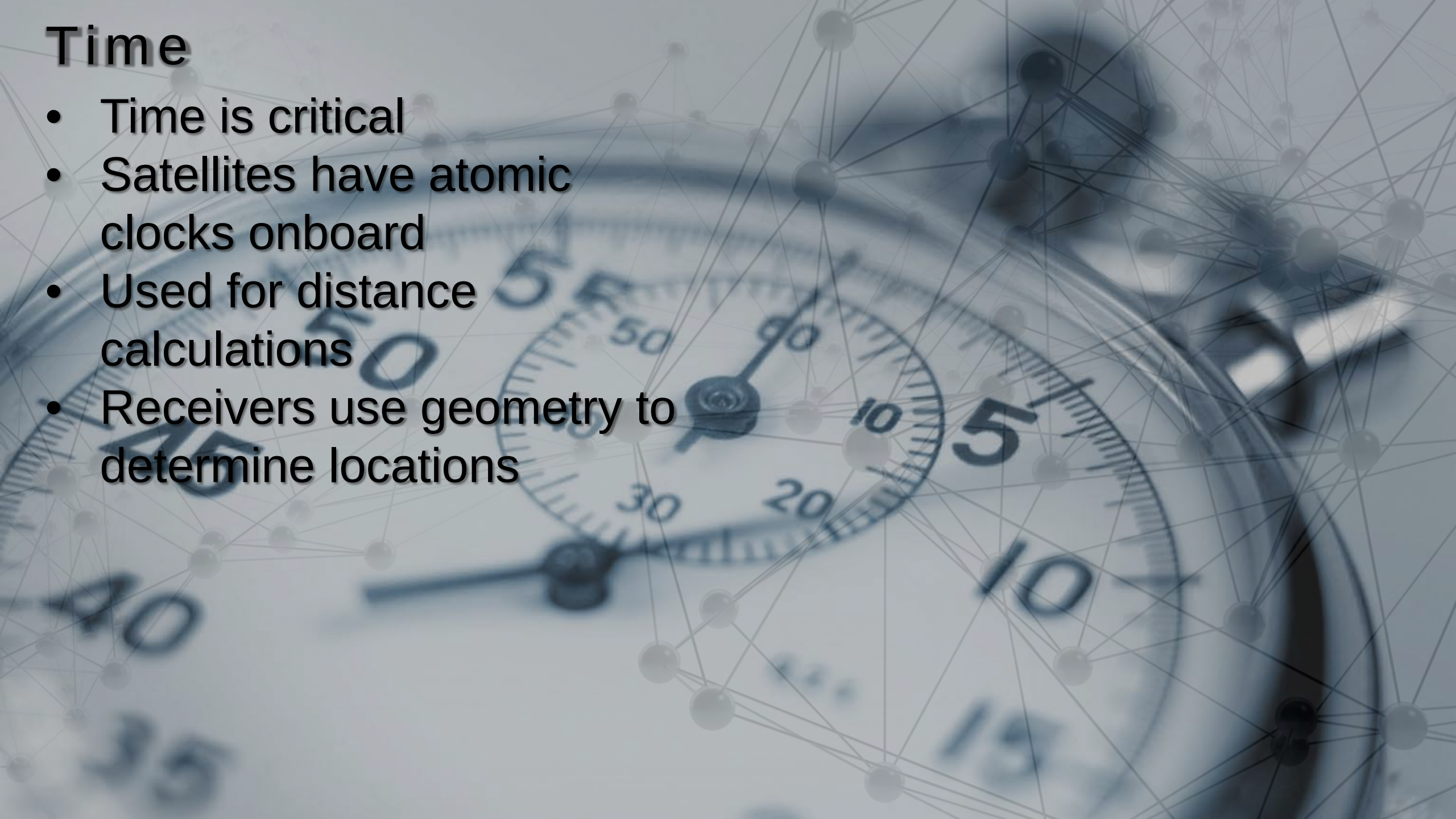


GPS AND ELECTRONIC MONITORING

ENVISTA FORENSICS

Time

- Time is critical
- Satellites have atomic clocks onboard
- Used for distance calculations
- Receivers use geometry to determine locations



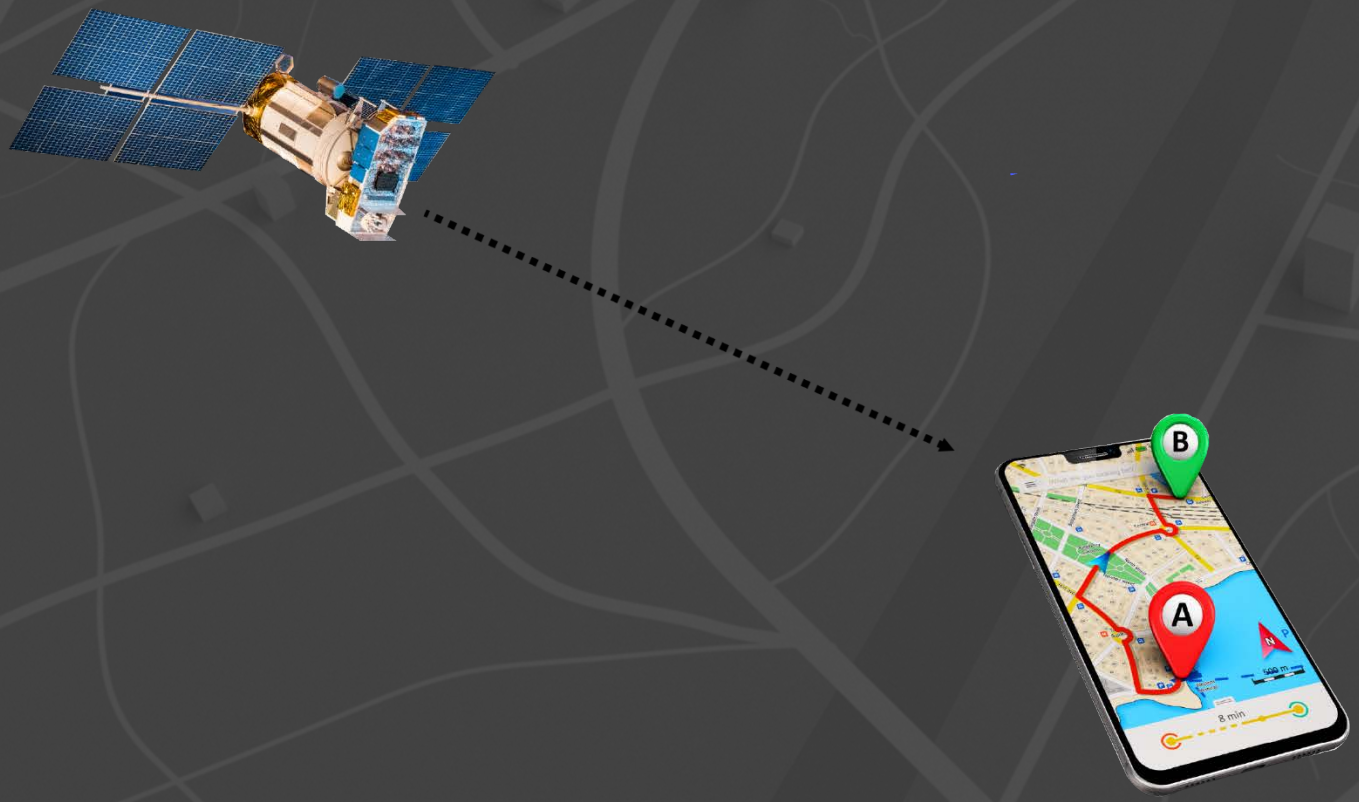
Satellite Coverage

- 24 Satellites
- Ground Stations

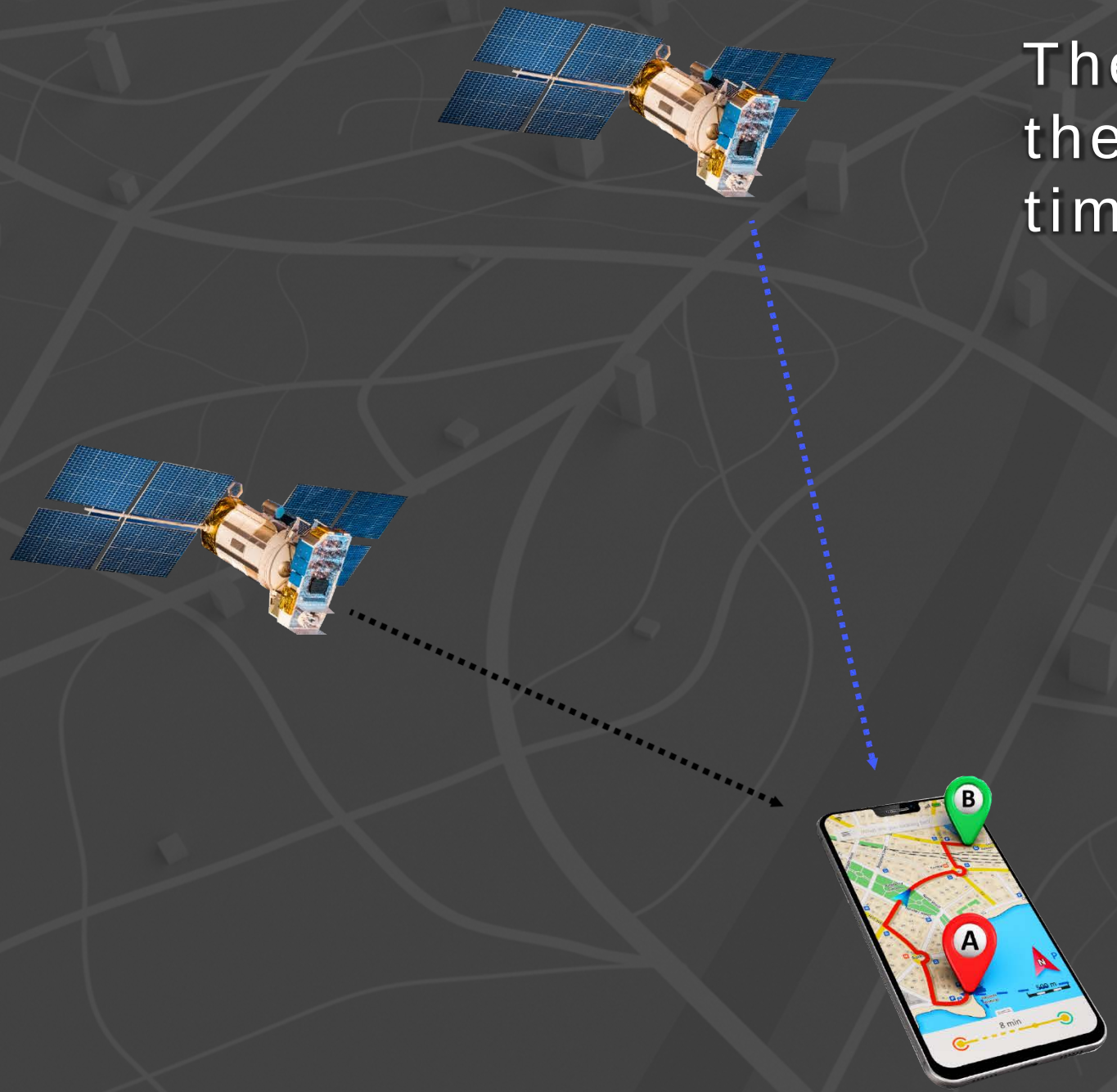
Satellite Coverage

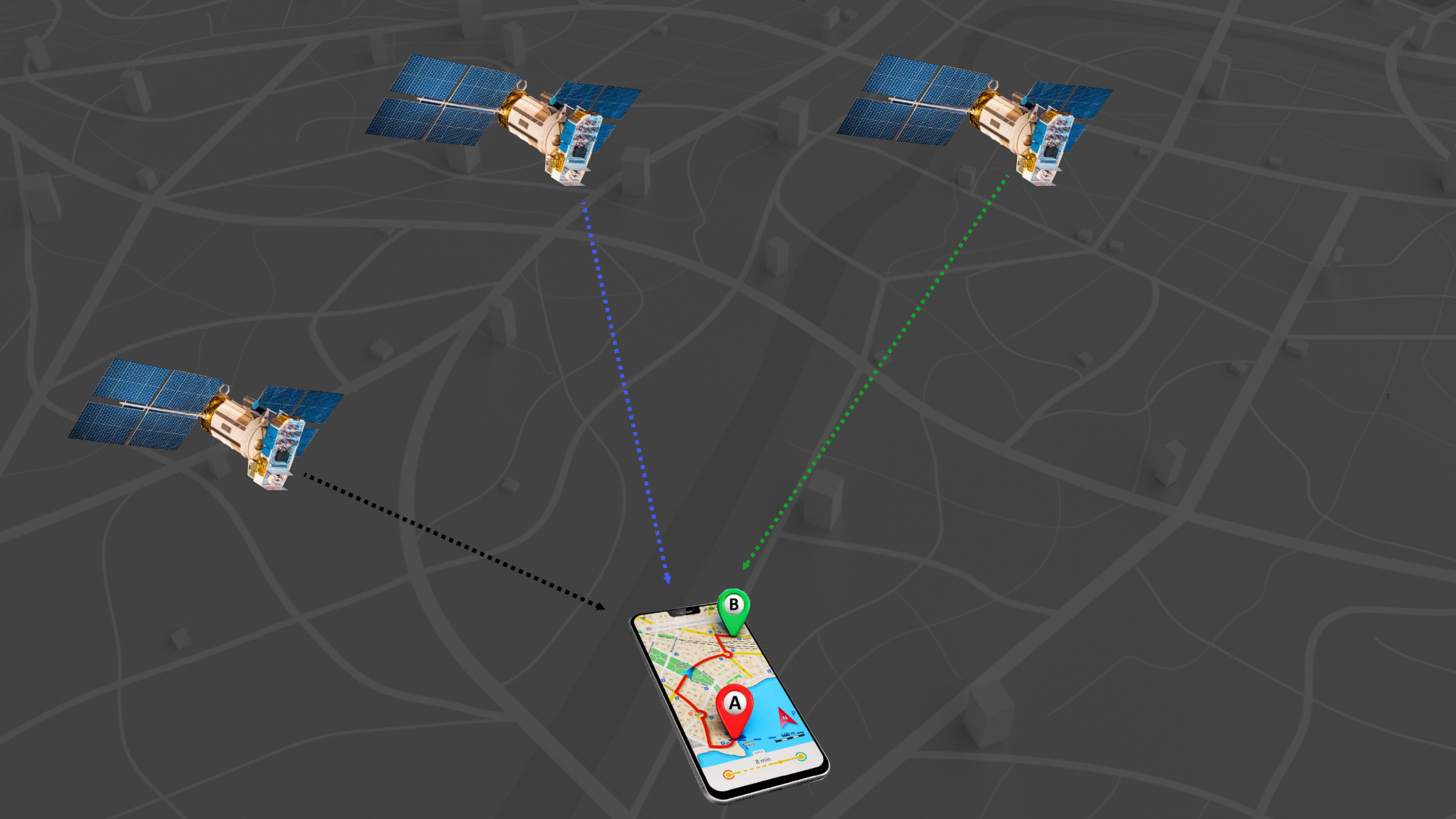
- 24 Satellites
- Ground Stations

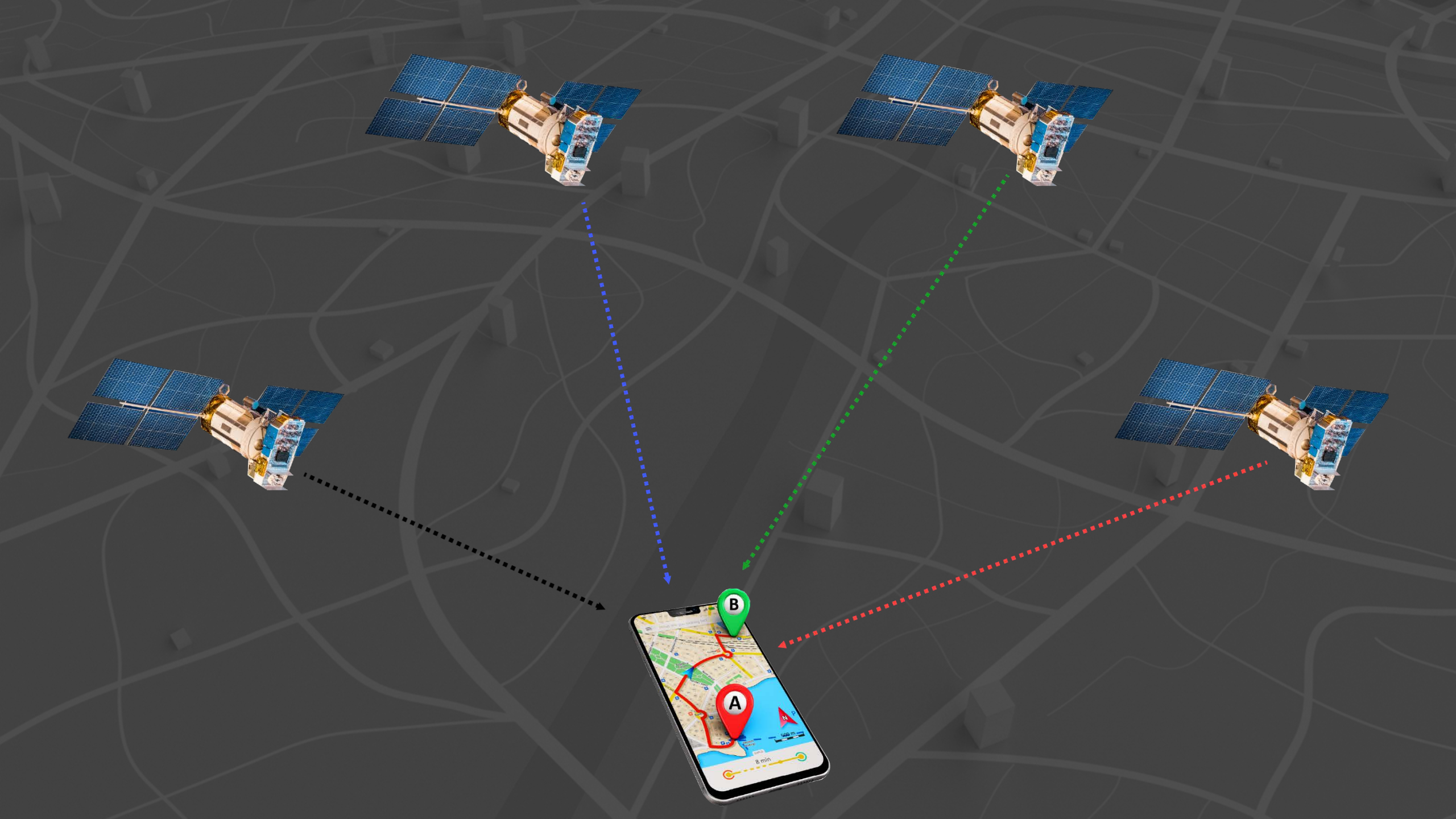
The GPS Satellites send information via radio signals to Earth. GPS enabled devices gather this information to calculate their position.



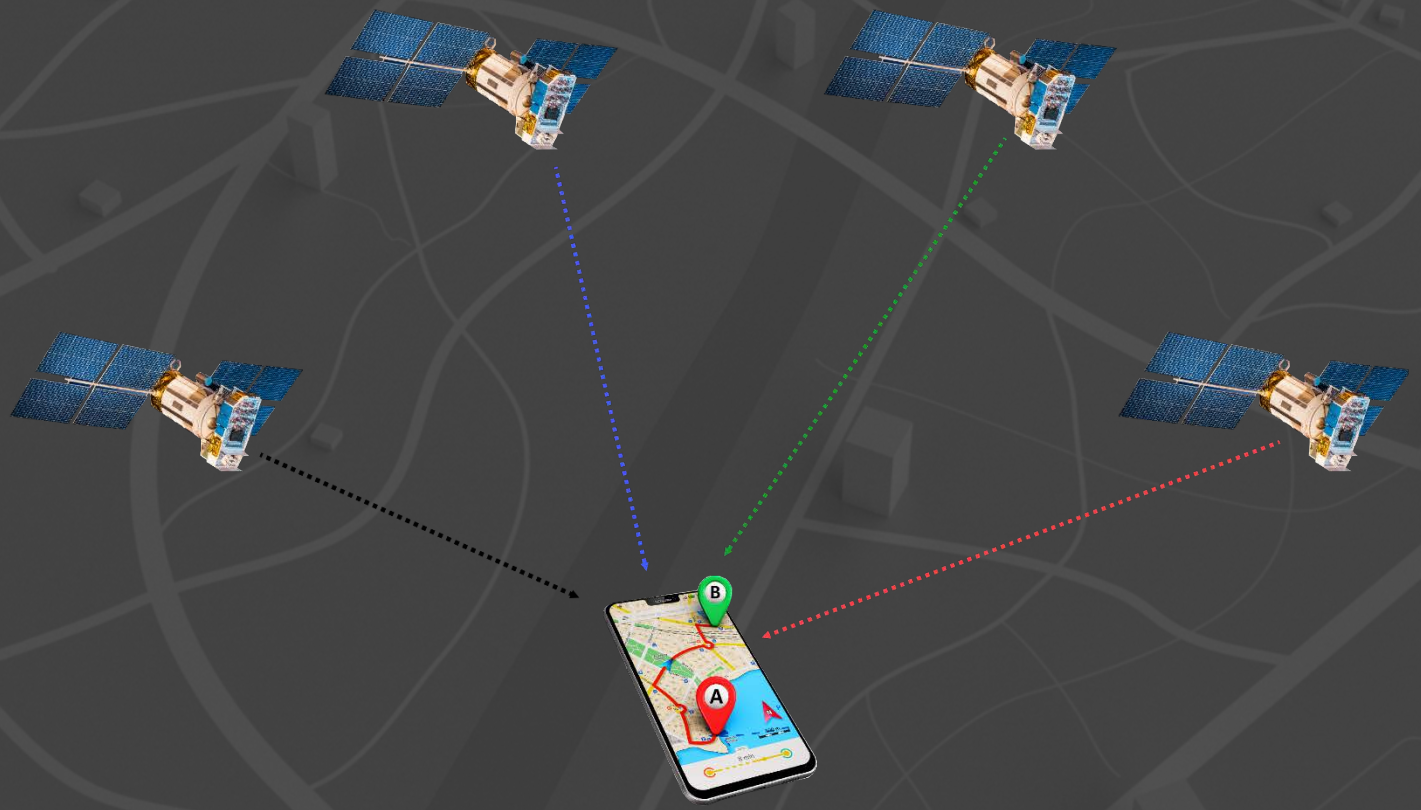
The GPS Satellites provide their position in space and timing information.

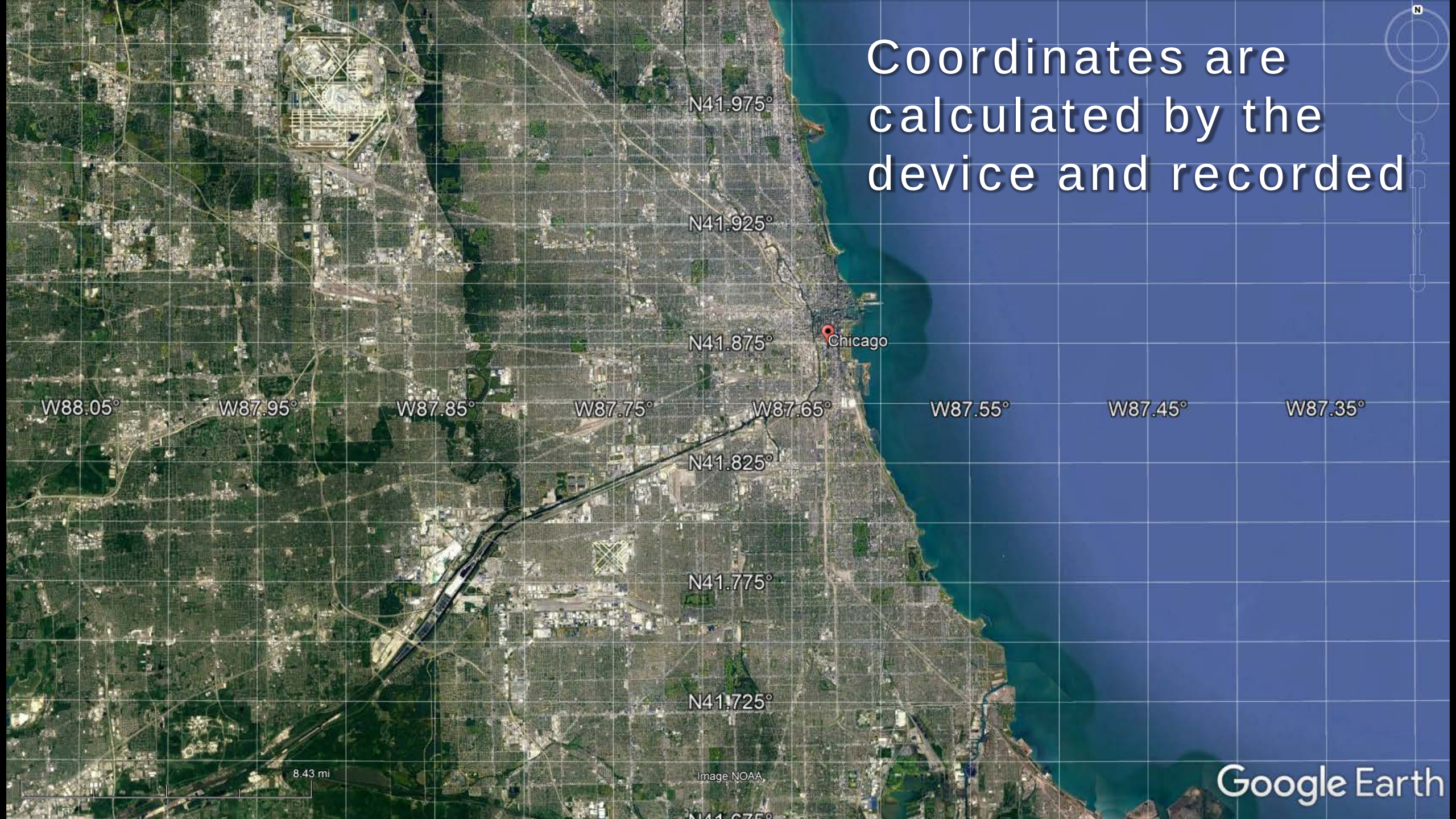



B
A
N
8 min


B
A
N
8 min

The GPS receivers require 4 satellites to accurately locate their position



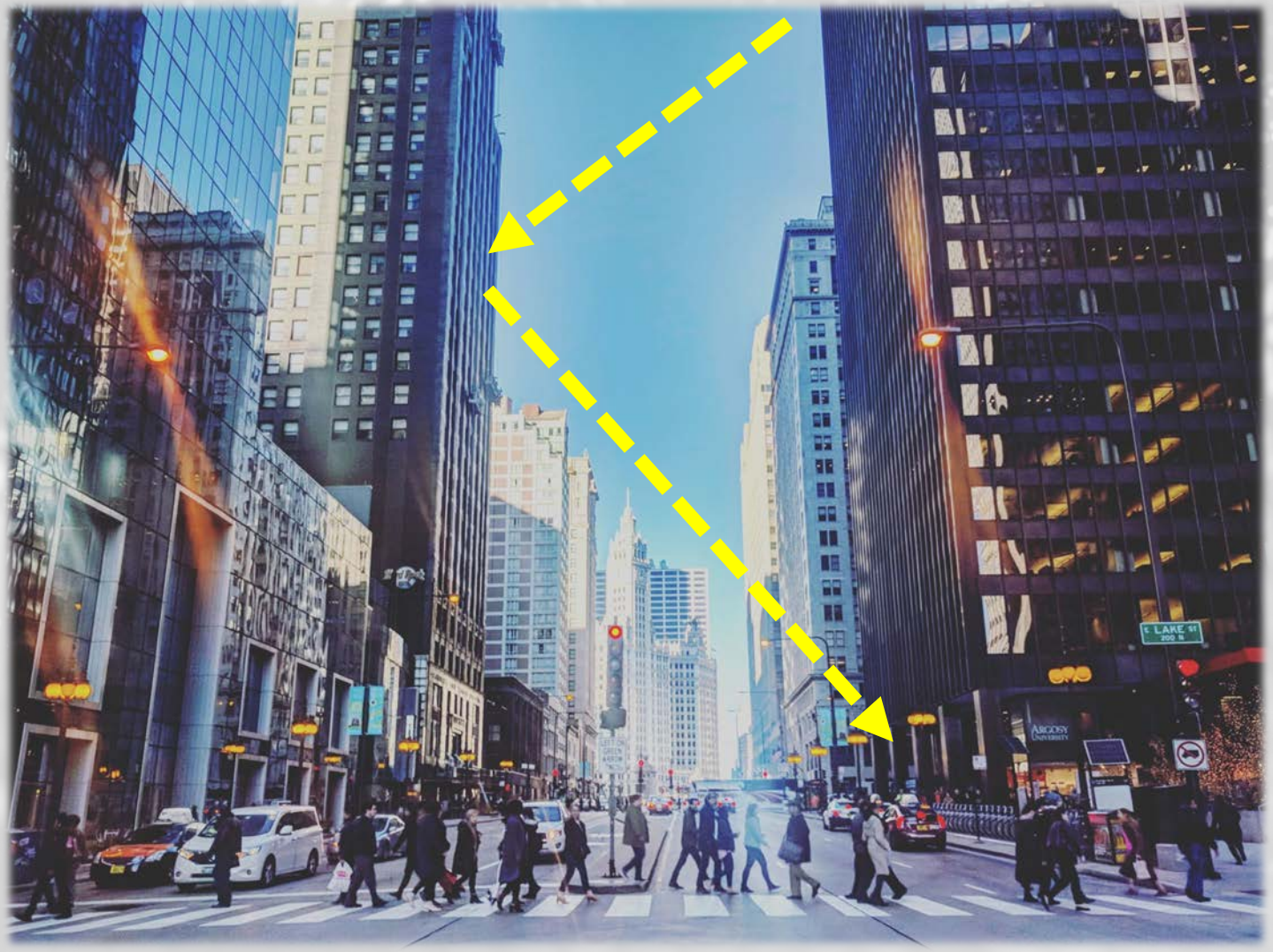

Coordinates are calculated by the device and recorded
N41.975°
N41.925°
N41.875°
Chicago
W88.05°
W87.95°
W87.85°
W87.75°
W87.65°
W87.55°
W87.45°
W87.35°
N41.825°
N41.775°
N41.725°
8.43 mi
Image NOAA
Google Earth

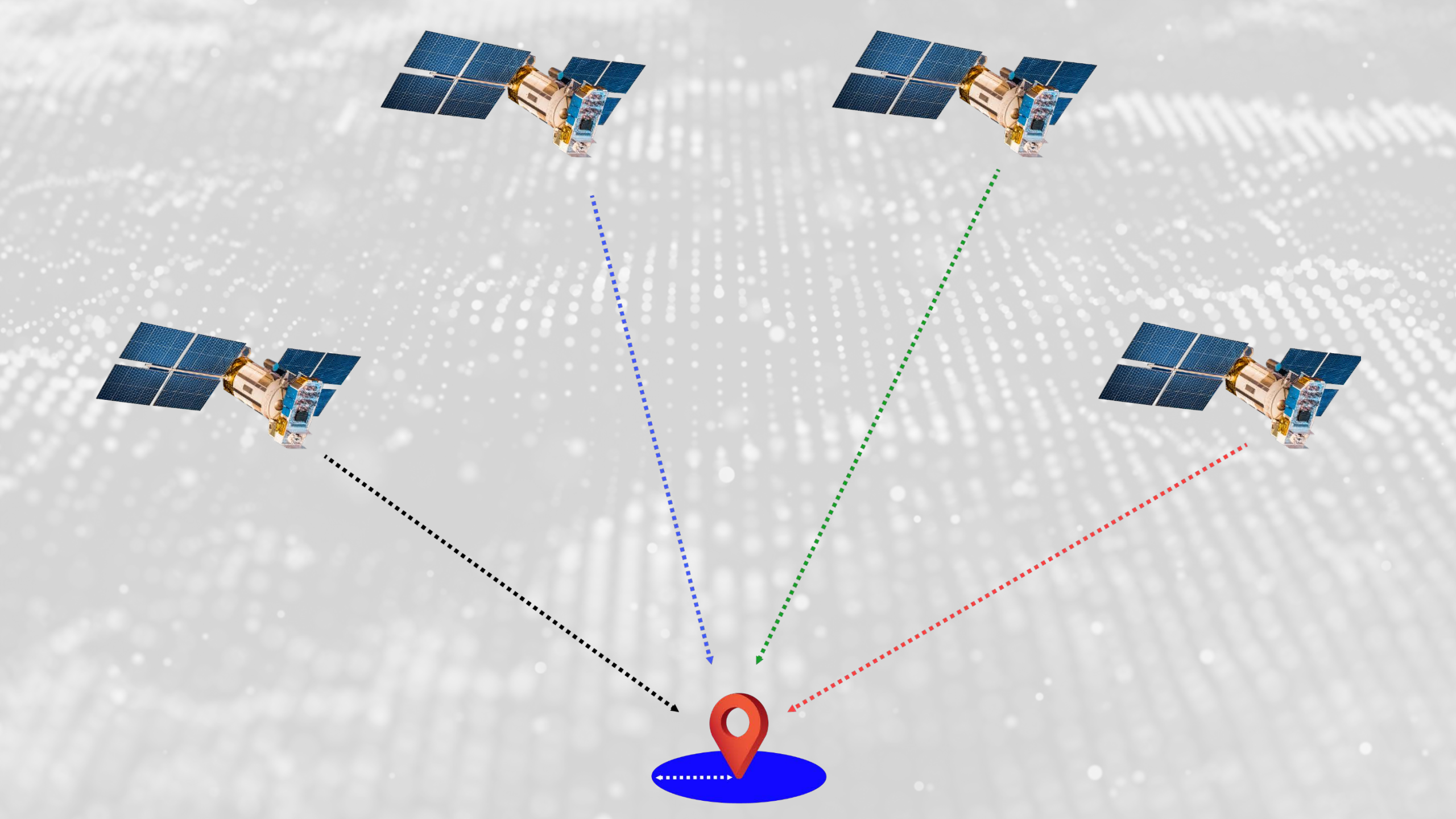

N41.975°
N41.925°
Latitude
N41.875°
Chicago
W88.05°
W87.95°
W87.85°
W87.75°
W87.65°
W87.55°
W87.45°
W87.35°
Longitude
N41.825°
N41.775°
N41.725°
8.43 mi
Image NOAA
Google Earth

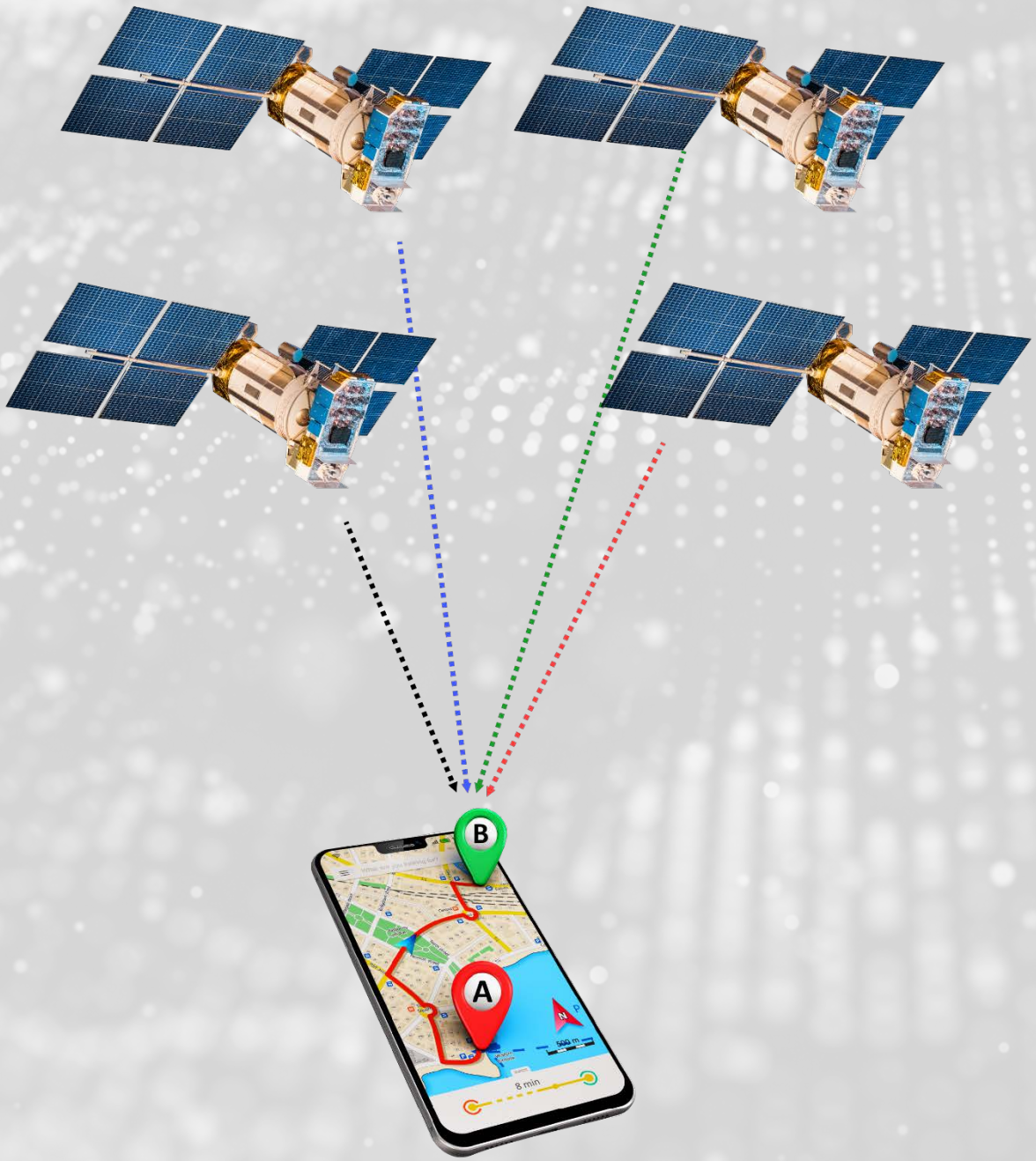
GPS Accuracy

What causes accuracy to diminish?

- Blocked Signals
- Less Satellites
- Satellite Positioning
- Signal Multipathing



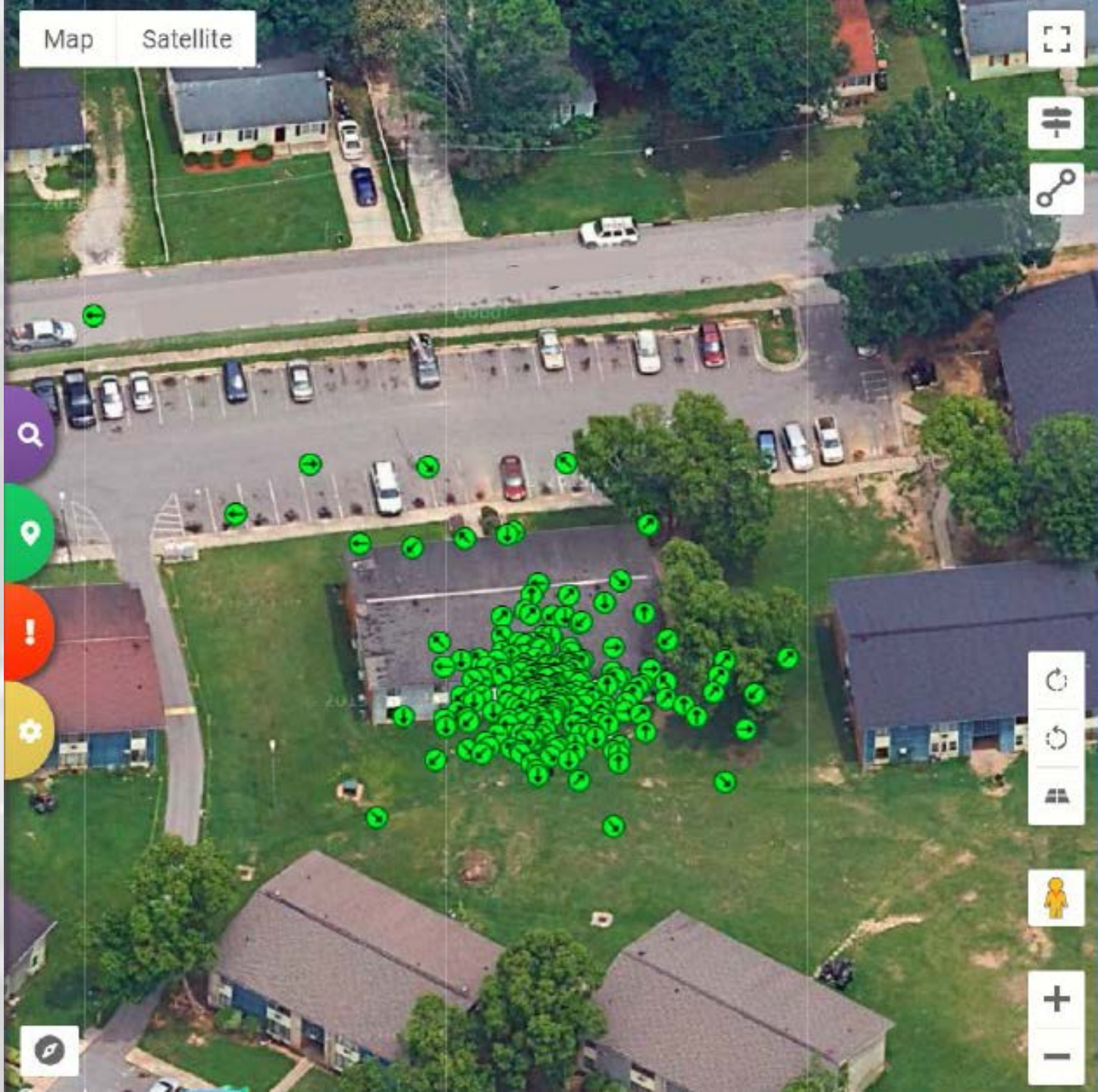




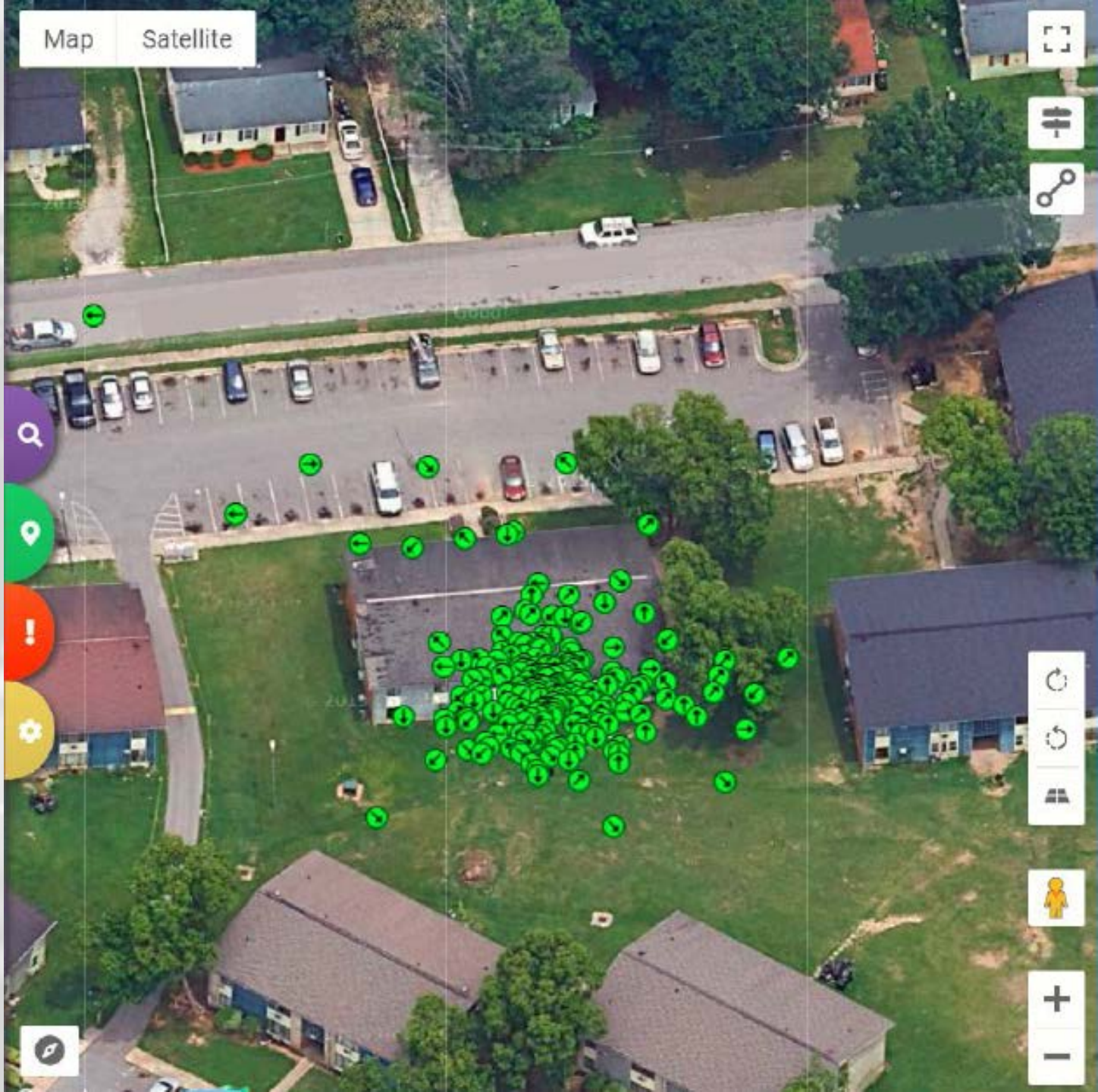
The position of satellites used can dimmish accuracy

Is the Latitude and Longitude the Absolute position of the device?

Is the Latitude and Longitude the Absolute position of the device?

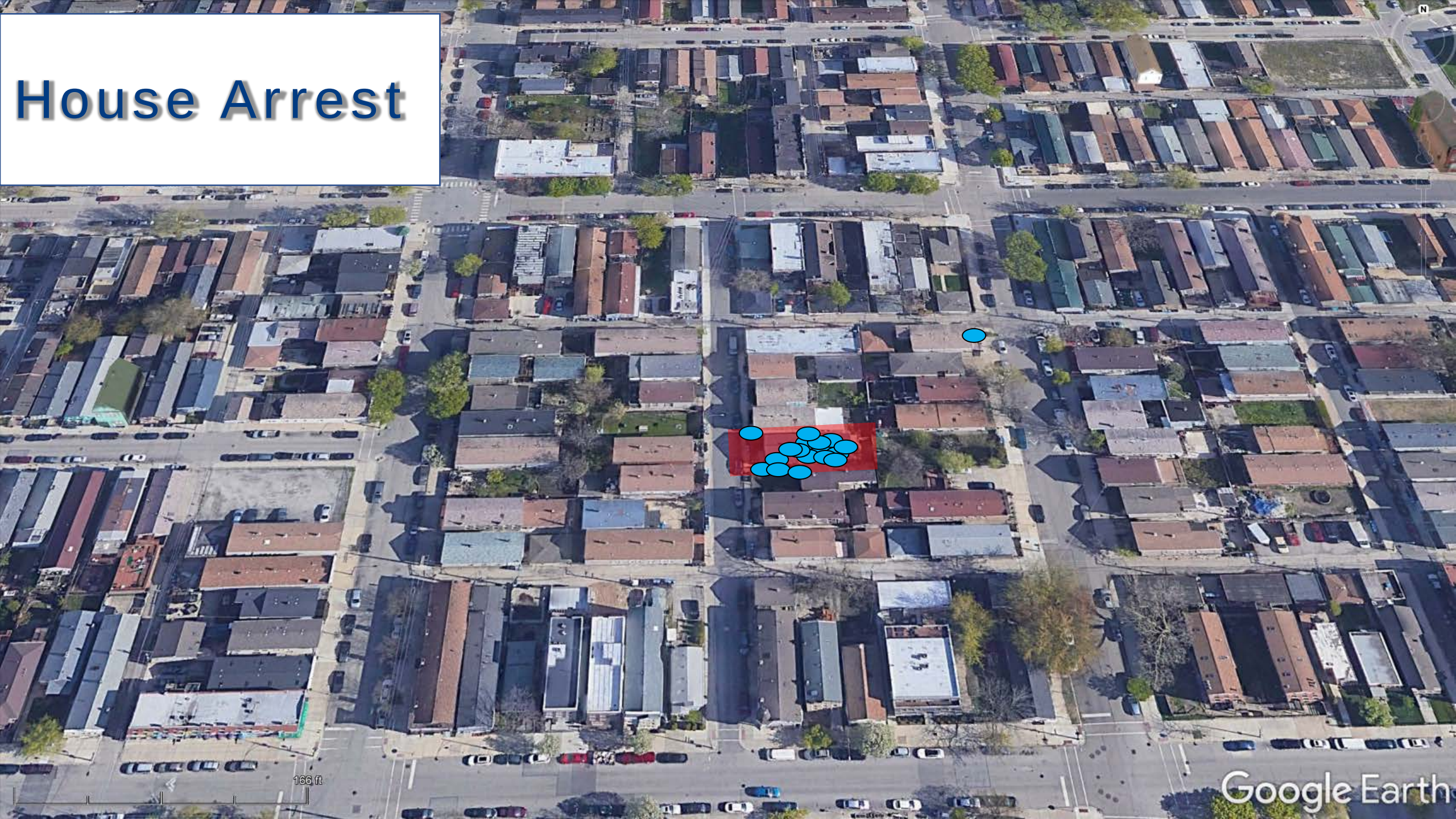


GPS Float



Common EM Issues

House Arrest



Exclusion Zones

Validate Automated Violation Reports

Validate Automated Violation Reports

- Verify Violations with Analysis of data
- Accuracy Issue?
- Actual Violation?