Geo Tracking for Welfare Fraud Investigations

DHCS
CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

July 2024

About the Instructor

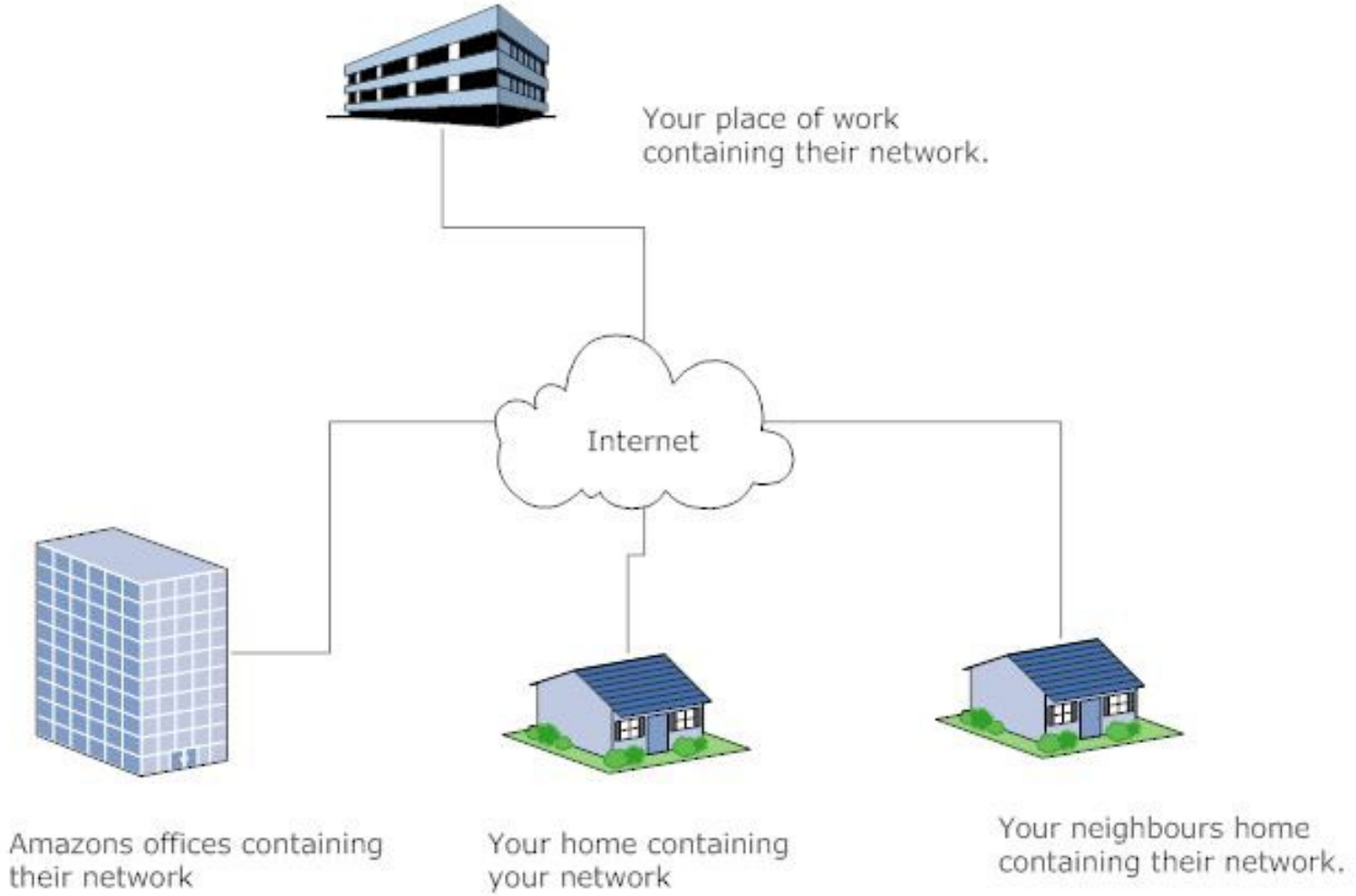
Scan for
contact card

- Fresno native and Fresno State graduate.
- Sworn peace officer since 2012.
- Seven years of patrol experience with a county sheriff’s office and two police departments.
- DHCS Medi-Cal fraud investigator since 2019.

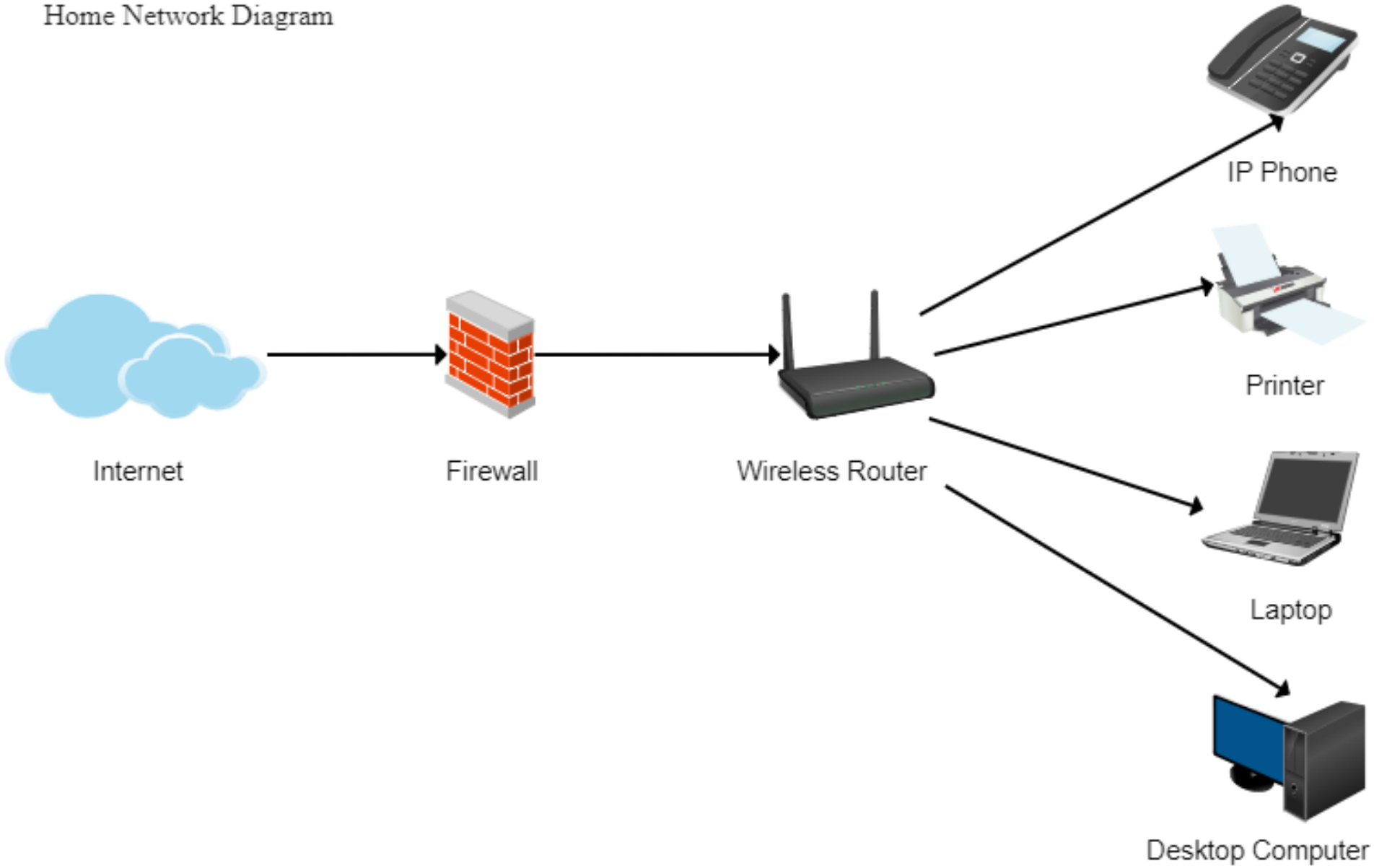
Objectives

Overview of Technology and Digital Data Sources

DHCS


Your place of work
containing their network.
Internet
Amazons offices containing
their network
Your home containing
your network
Your neighbours home
containing their network.

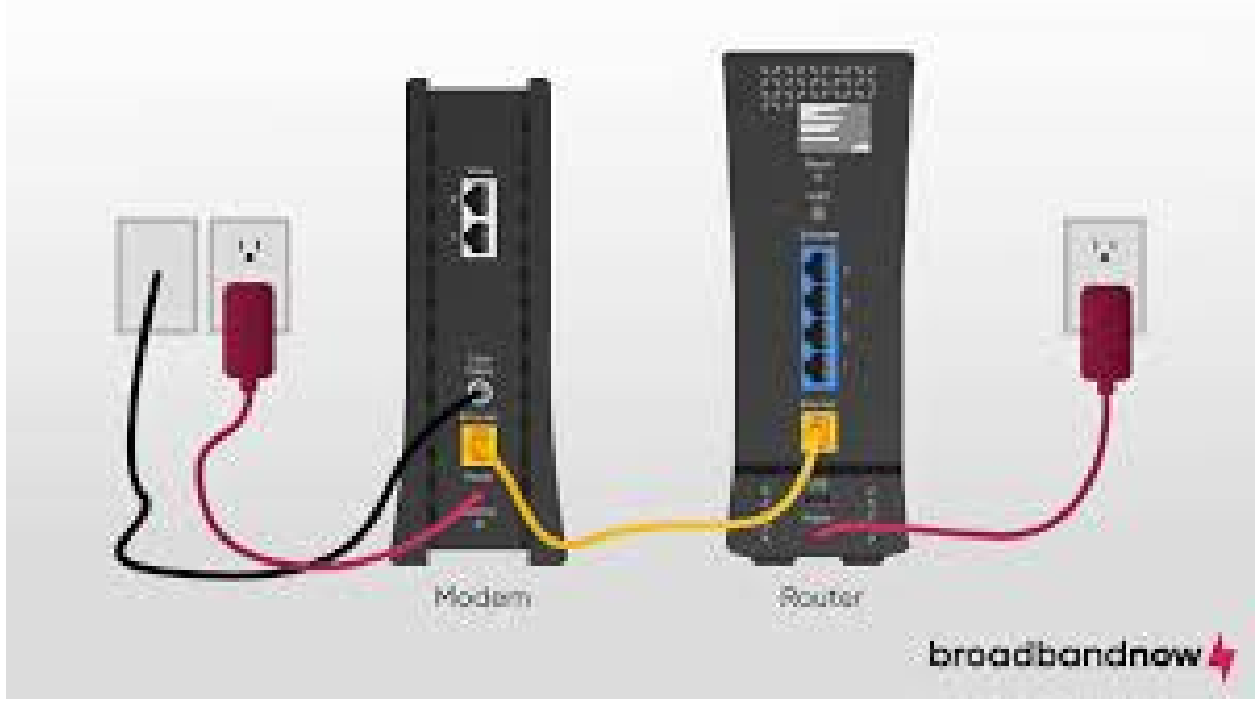
Home Network Diagram



BGW320

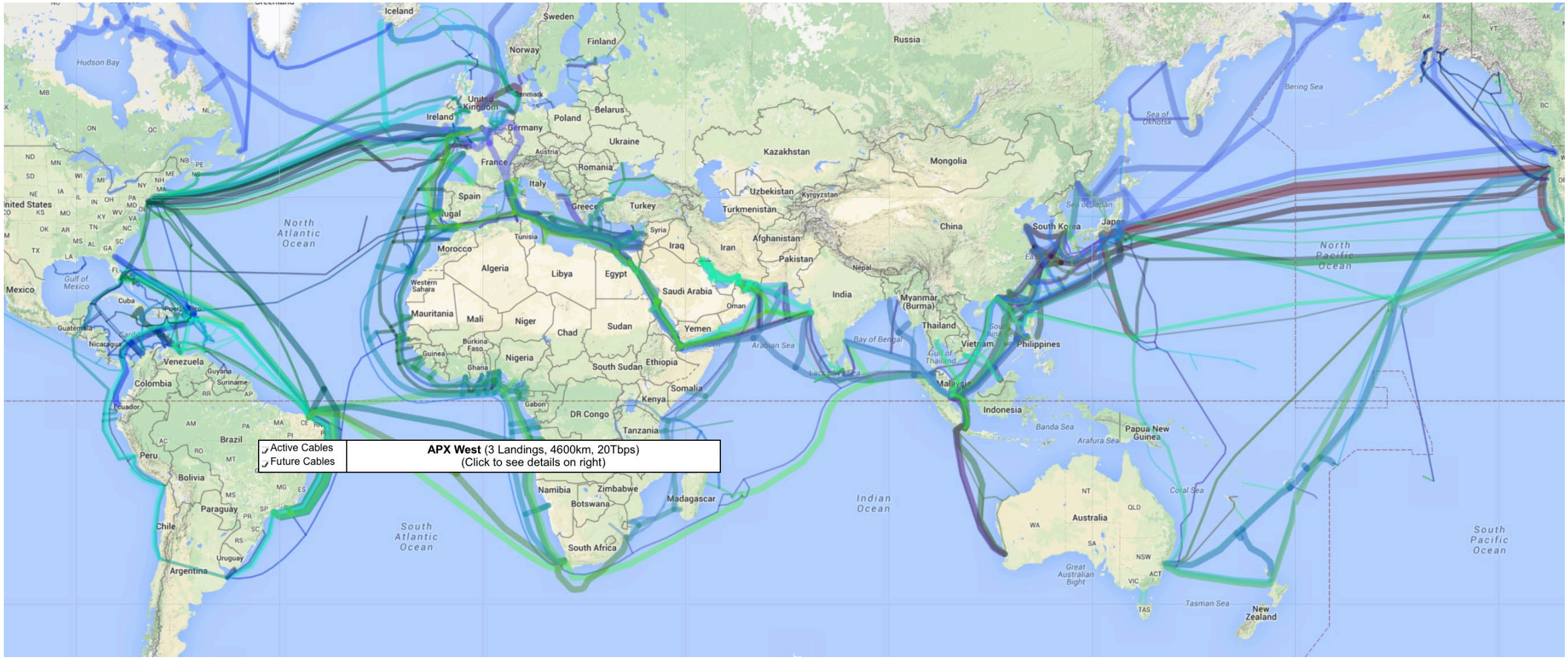
BGW210

PACE 5268



- WAN Port
- Wide area network
- (internet)
  public IP addresses

- LAN ports
- Local area network
- (business or home)
  private IP addresses
- 192.168.0.1
- 192.168.1.1


Active Cables
Future Cables
APX West (3 Landings, 4600km, 20Tbps)
(Click to see details on right)
Iceland
Sweden
Finland
Norway
Russia
Hudson Bay
United Kingdom
Ireland
Denmark
Belarus
Poland
Germany
Ukraine
Kazakhstan
Mongolia
France
Austria
Romania
Italy
Spain
Portugal
Greece
Turkey
Uzbekistan
Kyrgyzstan
Turkmenistan
China
South Korea
Japan
North Atlantic Ocean
Syria
Iraq
Iran
Afghanistan
Pakistan
Tunisia
Morocco
Algeria
Libya
Egypt
Western Sahara
Saudi Arabia
India
Nepal
Myanmar (Burma)
Thailand
Vietnam
Philippines
Mexico
Gulf of Mexico
Cuba
Puerto Rico
Guatemala
Nicaragua
Mauritania
Mali
Niger
Chad
Sudan
Yemen
Oman
Arabian Sea
Bay of Bengal
Gulf of Thailand
Burkina Faso
Guinea
Ghana
Nigeria
South Sudan
Ethiopia
Somalia
Kenya
Gabon
DR Congo
Tanzania
Venezuela
Guyana
Suriname
Colombia
Ecuador
Peru
Brazil
Bolivia
Paraguay
Chile
Uruguay
Argentina
South Atlantic Ocean
Namibia
Zimbabwe
Botswana
Madagascar
South Africa
Indian Ocean
Indonesia
Banda Sea
Arafura Sea
Papua New Guinea
Australia
Coral Sea
Great Australian Bight
Tasman Sea
New Zealand
North Pacific Ocean
South Pacific Ocean
Bering Sea
Sea of Okhotsk

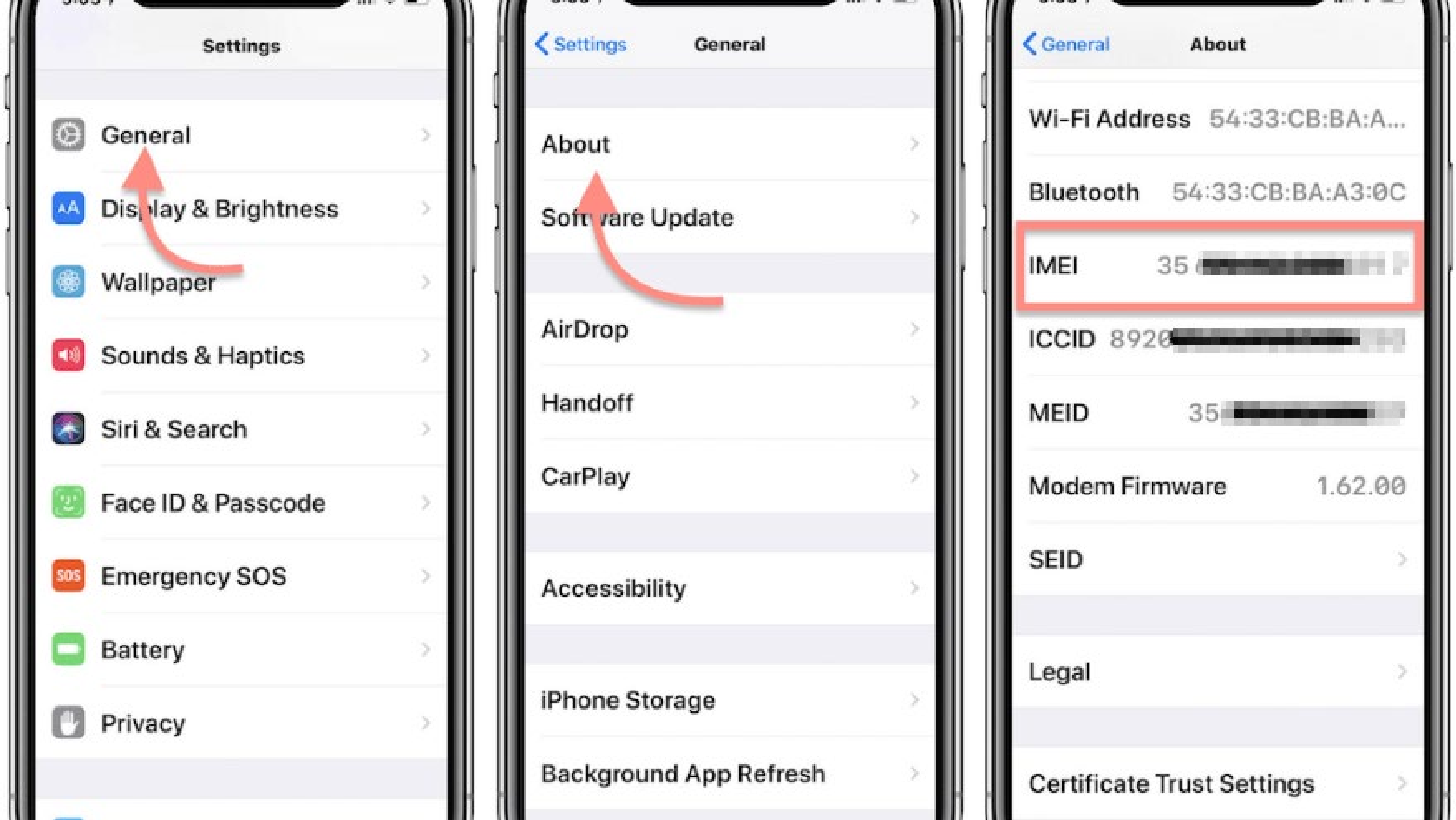
Types of Data

Internal Welfare Program Data

- CalSAWS backend data
- EBT transaction address data
- Healthcare claims data
- Electronic Visit Verification (EVV) data (in home care programs)
- Consider any public facing website, portal, app or online service your program deploys and what data is being logged, contact IT network or server admins

Cellular Network Records and Cell Site Geolocation Data

- Phone number
- International Mobile Equipment Identity (IMEI)
  - serial number of phone (must validate using online tools)
- International Mobile Subscriber Identity IMSI (serial number of SIM)


Settings
General
Display & Brightness
Wallpaper
Sounds & Haptics
Siri & Search
Face ID & Passcode
Emergency SOS
Battery
Privacy
Settings
General
About
Software Update
AirDrop
Handoff
CarPlay
Accessibility
iPhone Storage
Background App Refresh
General
About
Wi-Fi Address 54:33:CB:BA:A...
Bluetooth 54:33:CB:BA:A3:0C
IMEI 35
ICCID 8920
MEID 35
Modem Firmware 1.62.00
SEID
Legal
Certificate Trust Settings

Precise Geolocation Data (mobile device GPS antennas)

- GPS satellite triangulation
- Accuracy measured in meters


337788
337786
337787
337785
337784
337782
Image Landsat / Copernicus
Google Earth


6/17/2020 10:44 pm
6/18/2020 3:07 am
6/11/2020
6/18/2020
ALEY'S MARINE
TOYOTA

Bluetooth Low Energy (BLE)

- Beacons form a mesh network that can precisely locate a device
- Used in department stores and airports
- Apple Air tags use BLE protocols

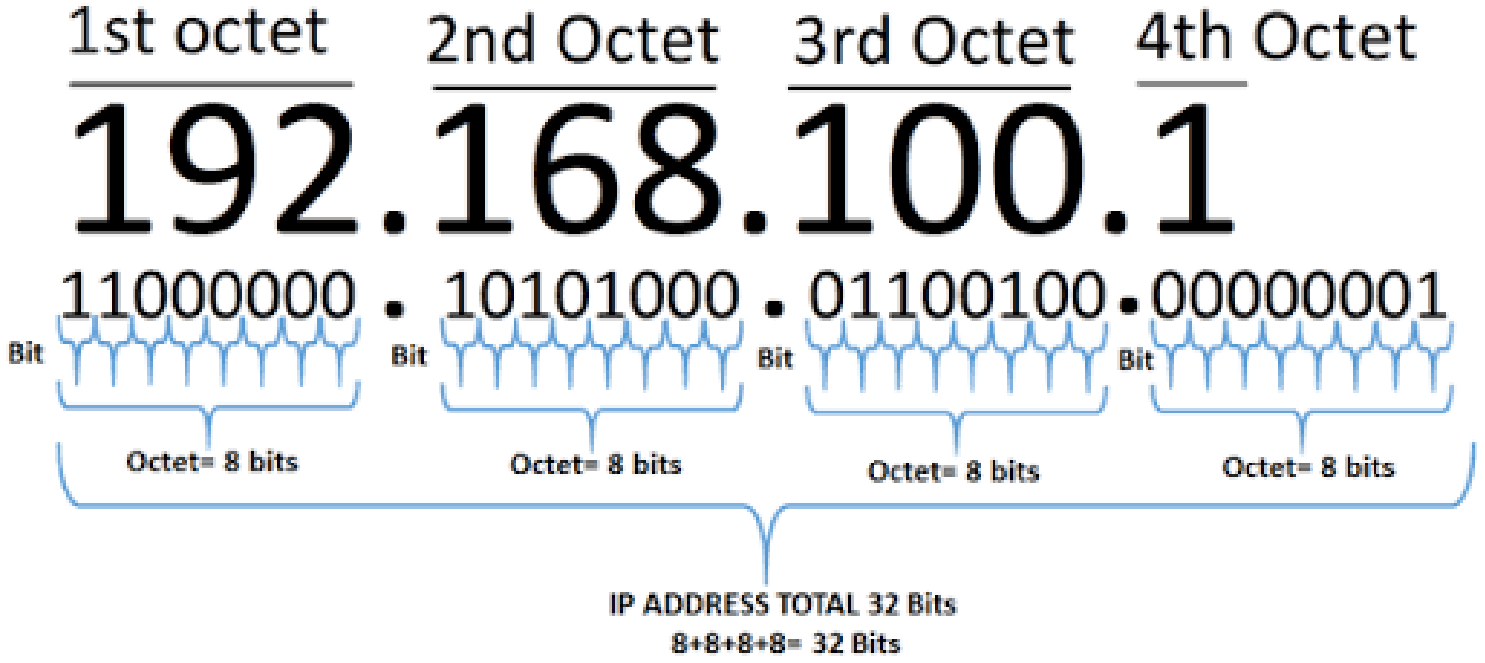
Near Field Communication (NFC) & Radio Frequency Identification (RFID)

- These communications are likely logged by payment processing companies and access control systems
- Apple Pay & Google Pay

Internet Protocol (IP) Addresses

Internet Protocol (IP) Addresses

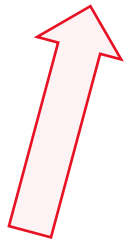
- Come in two flavors
  - Version four (IPv4), four octets (192.168.1.1)



Internet Protocol (IP) Addresses

- Version six (IPv6), eight octets
  (2001:0db8:85a3:0000:0000:8a2e:0370:7334)

  - A double colon in IPv6 abbreviates octets of zeros
    2001:0db8:85a3::8a2e:0370:7334



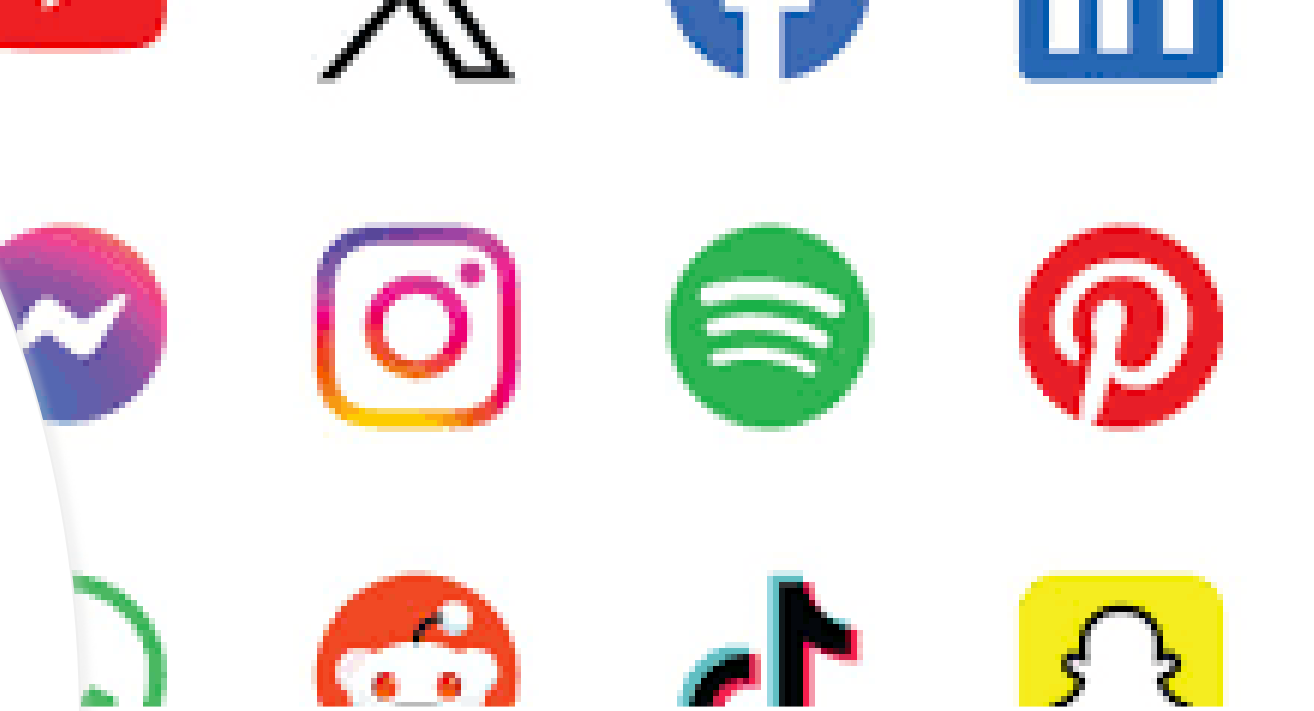
Connected Cars

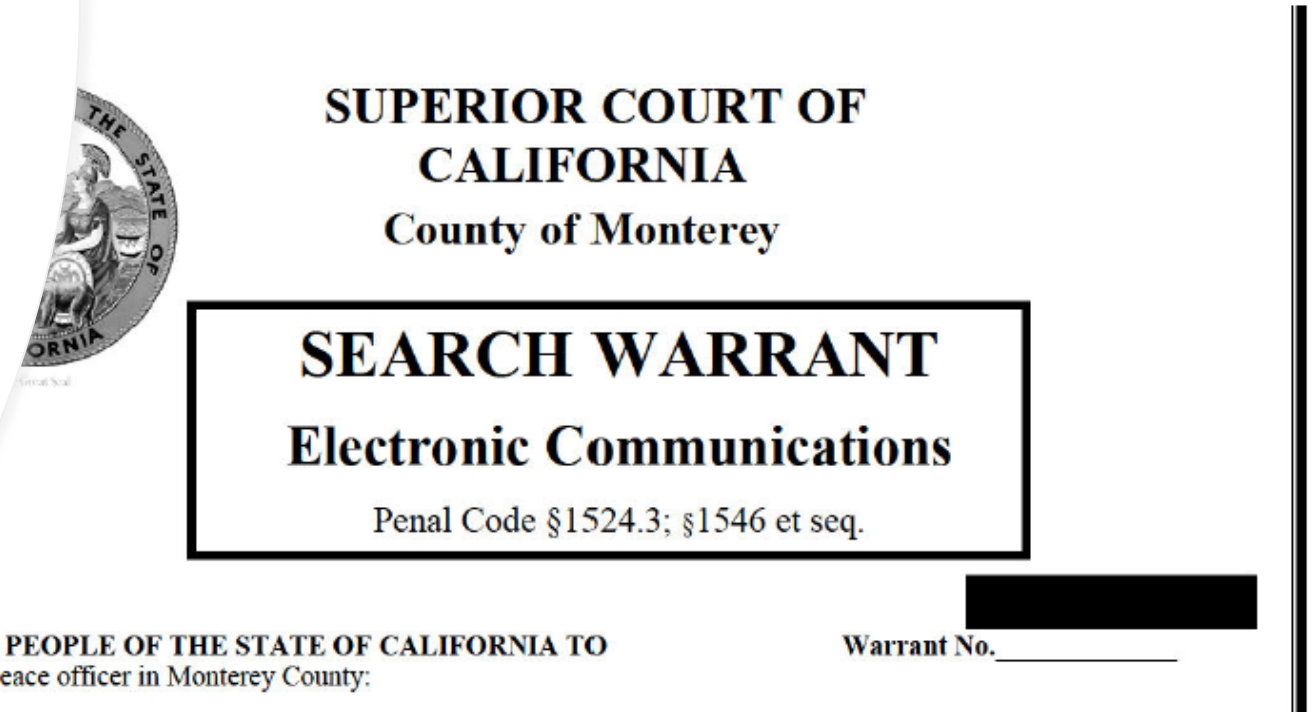
Obtaining Geolocation Data

DHCS

Legal Process

- Legal process
  - Search Warrants/Subpoenas
    - California Electronic Communications Privacy Act (ECPA)
    - Retention periods
    - Preservation requests





SUPERIOR COURT OF CALIFORNIA

County of Monterey

SEARCH WARRANT

Electronic Communications

Penal Code §1524.3; §1546 et seq.

[redacted]

THE PEOPLE OF THE STATE OF CALIFORNIA TO any peace officer in Monterey County:

Warrant No._____

◆ EXHIBIT 1A ◆

PLACE TO BE SEARCHED:

THE INTERNET SERVICE PROVIDER known as: Google LLC
1600 Amphitheatre Parkway
Mountain View, CA. 94043
Attn: Custodian of Records
Phone: (844) 383-8524
Email: uslawenforcement@google.com
Service via digital upload: Law Enforcement Request System (LERS)

◆ EXHIBIT 1B ◆

EVIDENCE TO BE SEIZED:

Records from Google LLC for the Target Account: [redacted]**@gmail.com**

In compliance with Penal Code § 1546.1(d)(1), each of the types of records specified below associated with the Google LLC account shall be from **06/18/2018 0000 PDT to 04/28/2022 2359 PDT**. The provided records shall be reviewed by your Affiant or other Investigators with the California Department of Health Care Services, Monterey County District Attorney's Office, and the U.S. Department of Health & Human Services – Office of Inspector General as needed.

Account Subscriber Information: Basic registration or customer information to include name, address, phone number, contact information, additional accounts, and dates associated with account creation and/or suspension for the above listed Target Account.

Device Information: Records identifying the devices used by the Target Account to access Google LLC services. The records shall include device attributes such as make/model/operating system/serial/IMEI numbers. A report or document shall be included that associates each device linked to the Target Account to Google's respective device ID numbers or device tags as commonly seen in data reports produced to law enforcement.

Location History: Records containing location-related information of all devices associated with the Target Account. Location records shall include dates and times, GPS coordinates, display radiuses, location data sources, precise device locations, IP addresses and any other records commonly included in data reports produced to law enforcement.

Google Photos/Videos containing Geolocation Metadata: Records of any stored photographs/videos associated with the Target Account and their respective metadata which shall include location based data of where the photos/videos were taken, e.g. latitude, longitude, radius, date, time, and location source.

Order to Send Information
Google LLC's production/response may be delivered by notifying:
Investigator Robert Musso
7112 N. Fresno Street Suite #200, Fresno, CA 93720
(559) 612-4460
robert.musso@dhcs.ca.gov

Preservation Requests

18 USC 2703(f) Preservation Request in reference to T-Mobile cellular number - (5555555555)

This fax serves as a formal request for the preservation of records and other evidence pursuant to 18 U.S.C. § 2703(f) pending further legal process.

You are hereby requested to preserve, for a period of 30 days, the records described below currently in your possession. You also are further requested not to disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request may result in a permanent or temporary termination of service to the accounts described below, or otherwise alert the subscriber or user of these accounts as to your actions to preserve the referenced files and records, please contact me before taking such actions.

This preservation request applies to the following records and evidence during the time period 01/01/2024-1/31/2024:

1. All Call Detail Records, SMS Records, MMS Records, and Data Records, to include all related Cell Site Data
2. All Location information including estimated or known locations, commonly referred to as TDOA or Timing Advance Information
3. All text messages (content) currently available
4. All picture messages (content) currently available
5. Any information on file in reference to the current subscriber, to include billing information, activation information, and device information.
6. Any document, files, or media currently in the possession of T-Mobile in reference to the above listed customer number.

This request will be followed by a Search Warrant for the above listed information.

Consent

Google Takeout

Your account, your data.
Export a copy of content in your Google Account to back it up or use it with a service outside of Google.

CREATE A NEW EXPORT

1 Select data to include — 65 of 67 selected

Products — Deselect all

Access Log Activity
Collection of account activity logs

Due to the size of content found in the Access Log Activity product, exports may take longer to process.

Multiple formats | All activity logs selected

Google Takeout

1 Select data to include — 65 of 67 selected

Home App
Device, room, home and history information from the Home App. More info

Multiple formats

Keep
Notes and media attachments stored in Google Keep. More info

Multiple formats

Location History (Timeline)
Your Timeline data, like settings and locations.

Multiple formats

Mail
Messages and attachments in your Gmail account in MBOX format. User settings from your Gmail account in JSON format. More info

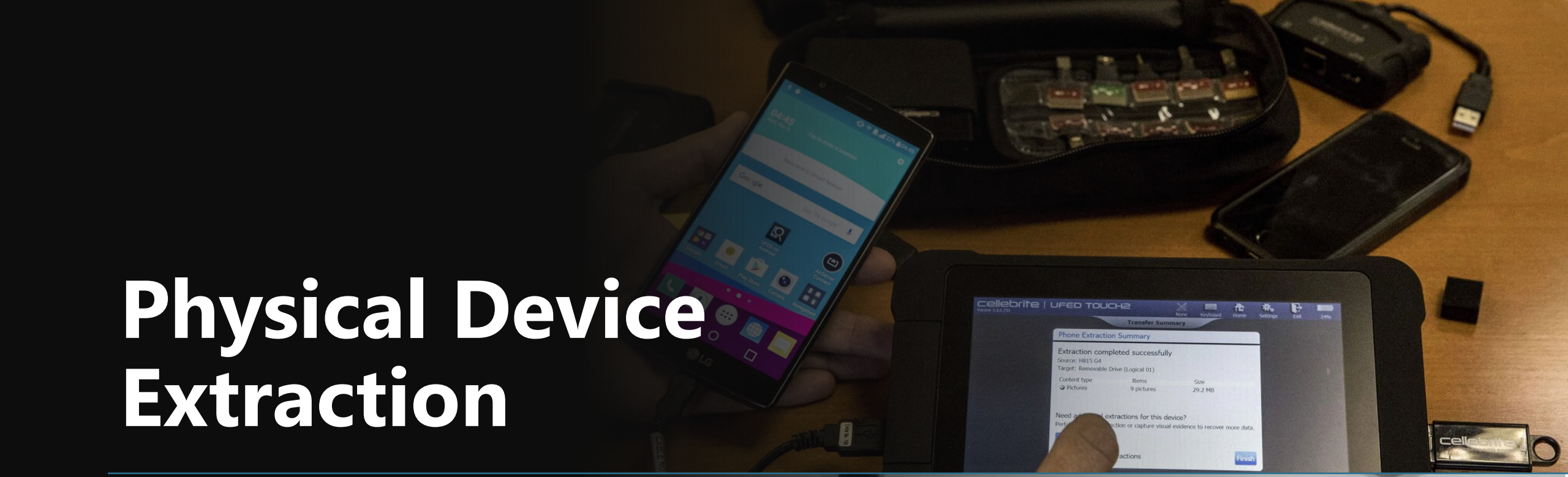
Multiple formats | All Mail data included

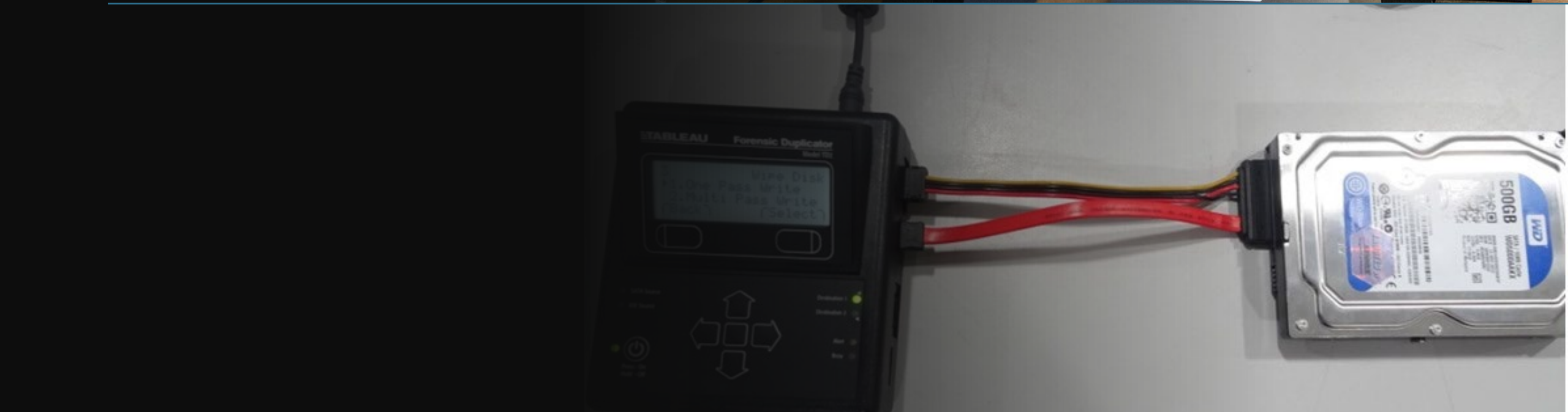
Internal Program Authority

Query data possessed by program under known authorities

THIS IS FAKE INFO CREATED BY AI FOR DEMONSTRATION PURPOSES			
Name	Date of Birth	SSN	Address
Vanessa Yang	5/3/1964	287-XX-XXXX	684 Kevin Haven Suite 763, Port Ariana, MT 09102
Gabriel Davis	11/13/1939	781-XX-XXXX	92338 Walton Landing Apt. 790, Port Melissaside, PA 98956
Elizabeth Smith	2/16/1967	932-XX-XXXX	34998 Kristina Walks Suite 484, Kelseyland, OH 01427
Patricia Williams	7/13/1972	448-XX-XXXX	134 Laura Pass, South Douglas, LA 38069
Alexandra Ali	10/28/1958	676-XX-XXXX	13352 Jimenez Parkway Suite 308, Nelsonview, IA 80354
Paige Ross	1/8/1986	169-XX-XXXX	153 Johnson Parkways Suite 575, Howardborough, MS 74934
Virginia Edwards MD	8/26/1983	895-XX-XXXX	052 Smith Well, West Lauren, TX 10214
Erik Gordon	3/26/1991	620-XX-XXXX	3193 Anita Valleys, North Timothyton, DC 26430
Anthony Evans	4/11/1945	633-XX-XXXX	631 Fields Burg, Ryantown, KY 88506
Shannon Ware	4/8/1984	920-XX-XXXX	139 Jessica Plains, New Sandra, UT 40863
Michele Lara	8/14/1951	902-XX-XXXX	9404 Gaines Dale, Jennifertown, VA 47828
Carlos Harris	6/5/1957	510-XX-XXXX	722 Tara Ferry, Lake Brandonview, WA 75668
Briana Drake	3/22/1997	127-XX-XXXX	USNV Atkins, FPO AP 13352
Amanda Martinez	3/24/1953	444-XX-XXXX	3999 White Stravenue Apt. 032, Port Jill, AR 12955
Sophia Black	4/2/1997	471-XX-XXXX	988 Raymond Lake, New Virginia, CO 17204
Joan Dodson	11/13/1996	789-XX-XXXX	73900 Johnny Ports, North Danielleberg, DE 54666
Michael Rosales	5/10/1949	291-XX-XXXX	342 Kayla Terrace, East Anna, CO 88092
Robert Fleming	1/11/2002	144-XX-XXXX	3344 Destiny Spring, West Ashleychester, VA 28247

Physical Device Extraction





Open-Source Intelligence OSINT

- OSINT relies on information that is legally and openly accessible.
- Great for anyone in eligibility/program integrity/quality assurance
- Requires skill in filtering out noise and verifying the credibility of the information.
- Training classes are available from various orgnizations

GitHub Repositories

- GitHub is a popular web-based platform used primarily for software code version control and collaborative software development.
- Community based open source and free software
- There are public repositories “repos” of various OSINT tools you can download.
- Consult with your IT dept or get a separate OSINT computer that is not connected to your department’s network.
- *Be careful what you install*

Lawful Ruse Tactics

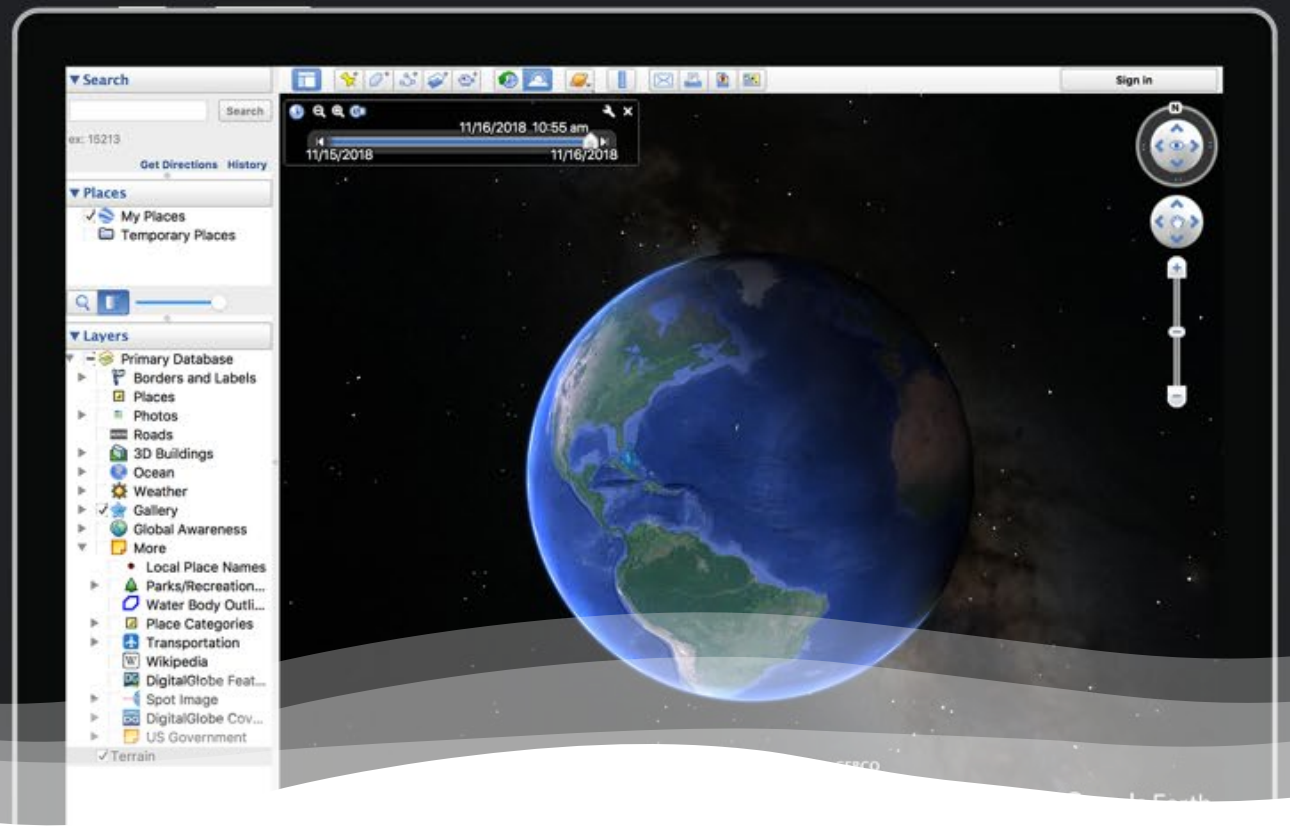
- Grabify IP Logger https://grabify.link/
- Create or send communications to targets in effort of obtaining IP addresses for legal process and geolocation data.
  - Phishing for public IP addresses
- *Consult with prosecutor*

Grabify Demo


GRABIFY
IP Logger
Create or Track URL's
Enter a URL or tracking code...
Create URL
Tracking Code
Total Logs: 365,976,661

Analyzing Data

DHCS



Create maps with advanced tools

Google Earth Pro on desktop is available for users with advanced feature needs. Import and export GIS data, and go back in time with historical imagery. Available on PC, Mac, or Linux.

Download Earth Pro on desktop

Geocoding & Mapping Address or Coordinate Data

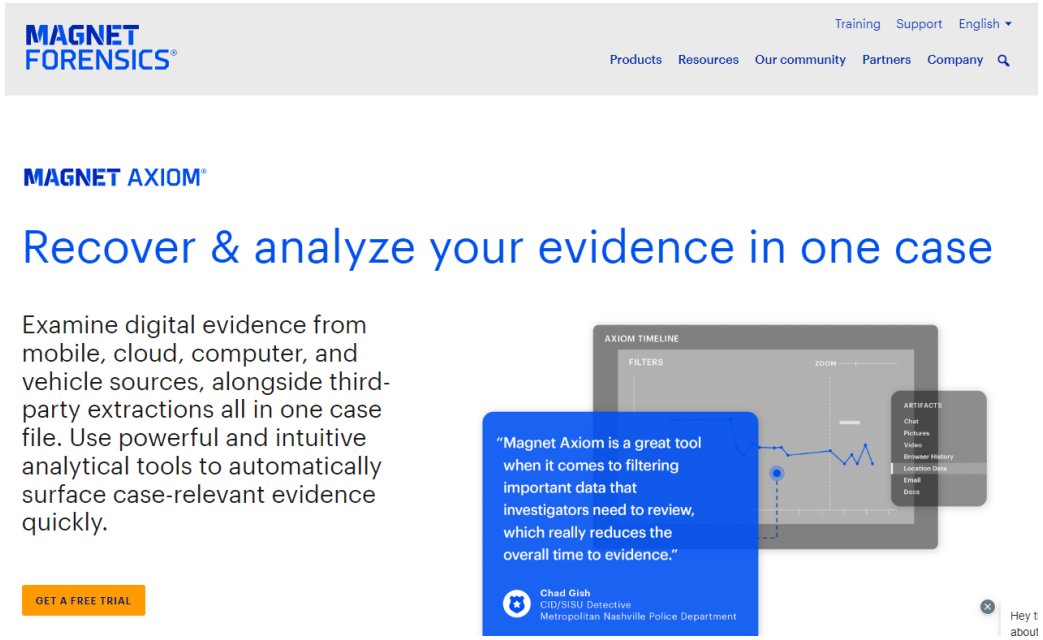
- Internal welfare program data
  - Google Earth Pro desktop

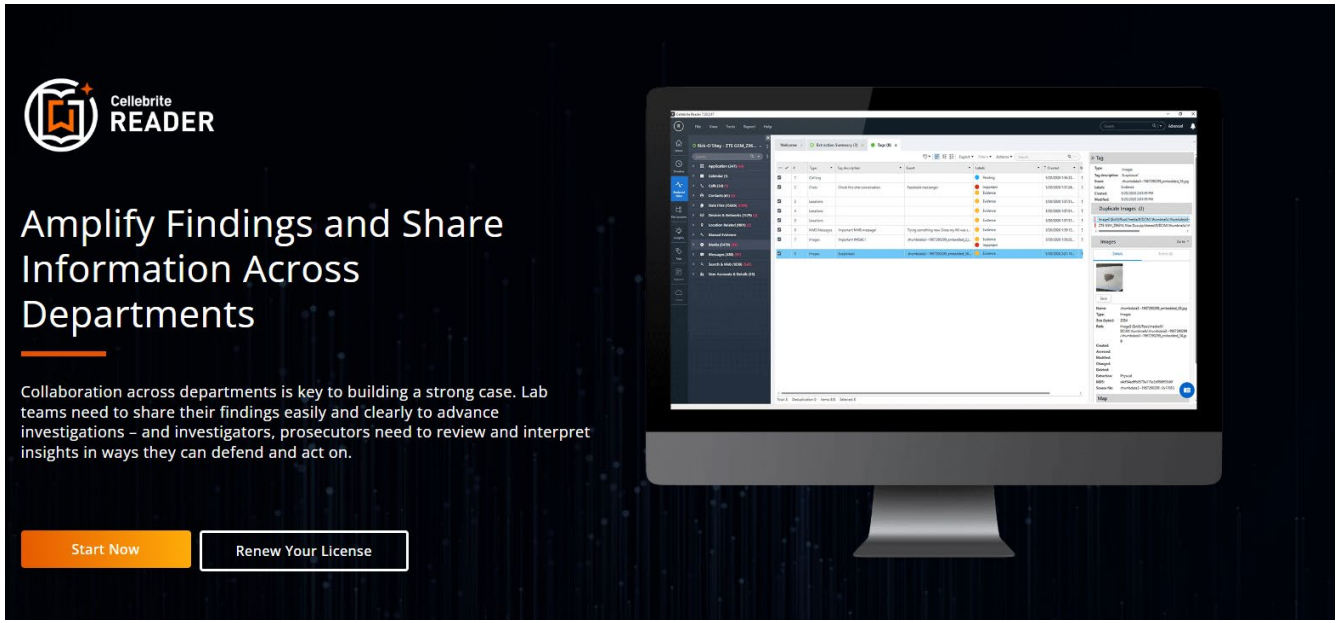
IP Address Registry Lookups

Social Media Data Parse Tools

Physical Device Extraction Analysis

- Cellebrite Reader
- Magnet Forensics AXIOM Examine





Exploring Proprietary ISP and Cellular Company Records

- Use https://fileinfo.com/ to learn about uncommon file types and what programs are required to open them
  - .eml files for example

.KMZ File Extension

Google Earth Placemark File

Developer Google

Popularity 3.6 | 349 Votes

Open with Google Earth Pro

What is a KMZ file?

A KMZ file is a Zip-compressed .KML file that stores map locations viewable in various geographic information systems (GIS) applications, most notably Google Earth. It contains one or more placemarks that may include a custom name and the latitudinal and longitudinal coordinates of the location. KMZ files may also include COLLADA 3D models, overlays, and images referenced by the KML file.

More Information

Google designed KMZ files to reduce the space taken up by KML files to make them easier to distribute and share with multiple users. Common uses for KMZ files include sharing placemarks or tours with users via email or when publishing on a webpage.

Various programs may create KMZ files, but Google Earth Pro primarily creates the files. To create a KMZ

Ask AI

Organizing Information

- Spreadsheets
  - Pivot tables
- Microsoft OneNote
  - Great for workups and OSINT
  - Collect and distill information to identify target accounts and devices to gather geolocation data

Geolocation Data Conversion Tools and Specialized Software

- Google Earth Pro
- LexisNexis Accurint TraX
- LeadsOnline Cellhawk
- NDCAC LE Portal
- FBI CastViz
- Badge Apps

Google Earth Pro Address Data Import Demo

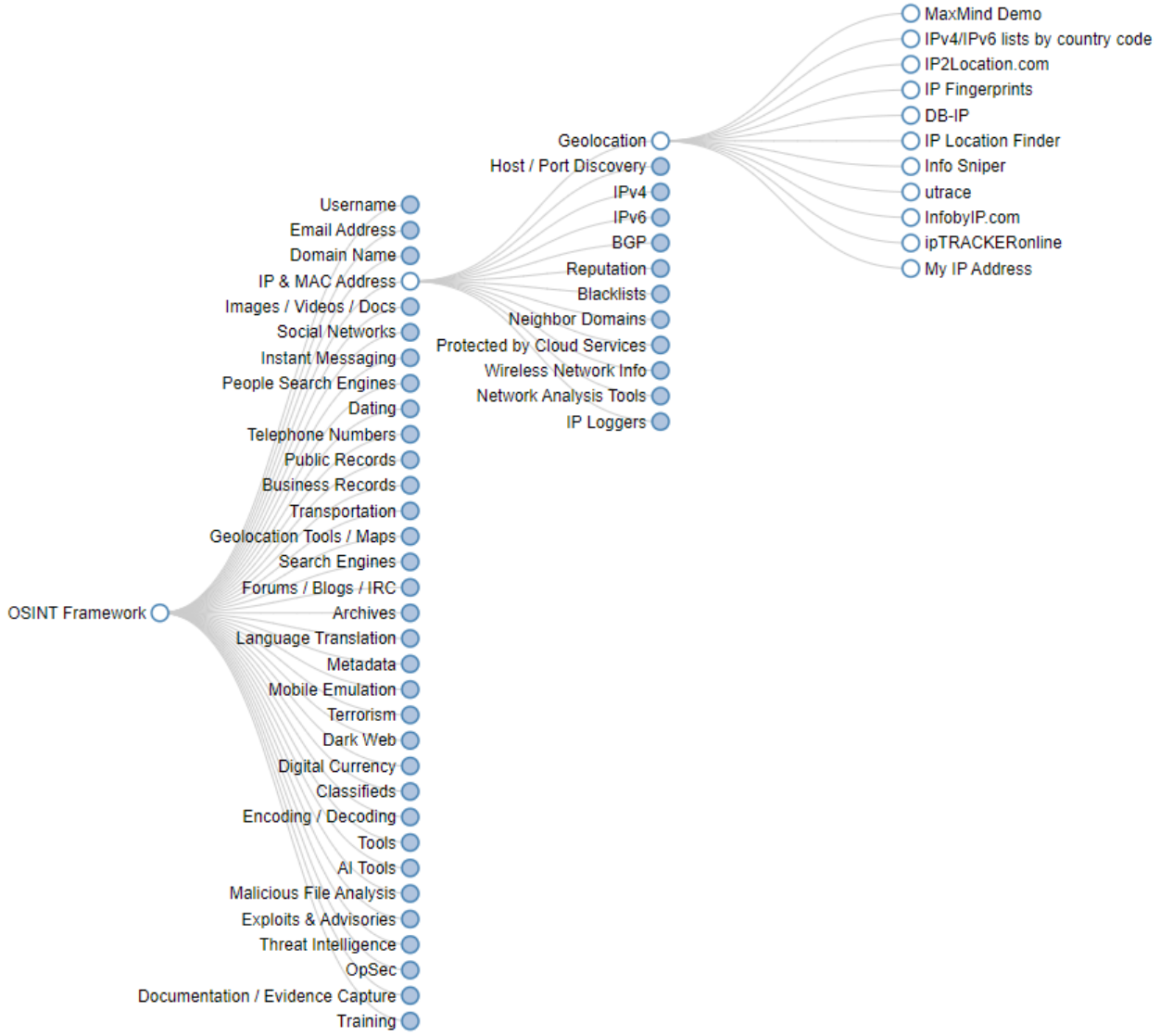
Accurint TraX Geo Data Conversion Demo

Law Enforcement Resources

- Search.org
- NDCAC
- Kloving.net
- NW3C
- Badge Apps
- Leads Online

Open-Source Intelligence (OSINT) Resources

» https://osintframework.com/



Case Examples

Open Discussion

Questions?

Do you have a case type to discuss as a group?

Scan the below QR code or visit this URL to download bookmarks of OSINT tools.

https://docs.google.com/spreadsheets/d/1TBLYhMe39eJWlAeYQTLMSSRaGL1qFlCq/edit?usp=sharing&ouid=110761610925557932464&rtpof=true&sd=true

Scan Me

Contact Information

Scan for
contact card

Investigator Robert Musso
California Department of Health Care Services
Investigations Division
7112 North Fresno Street Suite 200, Fresno CA 93720-2949
559-612-4460
Robert.Musso@dhcs.ca.gov