

# Digital Evidence

*PART I: THE INVESTIGATIVE STAGE –  
RECOGNITION, COLLECTION, SEARCH*



CATHEE HANSEN  
Digital Evidence Specialist

ADAM BECHTHOLD  
Senior Criminal Investigator

CHRIS GRAY  
Crime Analyst

Denver District Attorney's Office  
720-913-90000



Former FBI Director James B. Comey:

“Used to be in the good old days, you’d roll up and do a search warrant in a drug case and you’d hit the place and you’d find some kilos and some guns and you’d find a black composition notebook where the knuckleheads would have written down who gets how much money, who’s responsible for what drugs. You’d photocopy it and put an exhibit sticker on it and be good to go...

“...Today you’re going to get thumb drives, PDAs, laptops, electronic devices of all kinds, and your ability to understand the digital world and investigate there is the essence of all law enforcement.”

# TOPIC 1

---

You Need to First Know What is Out There



# Practical Topics:

- **Info contained within digital devices**
  - What is available
  - How to preserve data
- **Data contained outside the devices**
  - Service providers
  - Cloud
- **Tracking digital devices**
  - Historical
  - Real-time
- **Info related to motor vehicles**

# Types of Available Data

---

## Cell Service Provider:

Call Detail Records  
SMS/MMS Packet  
Data

## (Specific) App:

Location data  
Social media data  
Financial app data  
Health app data  
Travel App data

## Cloud Storage:

iCloud  
Dropbox  
Google Drive  
Microsoft OneDrive



# Digital Devices

- Types of Data Available
- How to Preserve Data

**Data  
contained  
within the  
device  
itself**

# TYPES OF AVAILABLE DATA

## First Layer:

Calls

Contact Lists

Texts

Email

Photos

Videos

## Second Layer:

Location data

Social media data

Internet history

Financial app data

Health app data

Travel App data

## Third Layer:

Meta data

Deleted data

Encrypted data



## First Layer Data:

- Contact lists, call logs, texts, photos, videos.
- Evidence of the drug trafficking crime.
- Evidence of the participants.
- Evidence of the conspiracy.

## Second Layer Data:

- Location data
- Social media data
- Internet history
- Financial app data
- Health app data
- Travel app data



# Corroboration of criminal activity

- Social media data includes photos, videos, communications
- Internet history can show efforts to learn info related to criminal activity
- Financial app data can show transactions or where suspect keeps his money

Corroboration and/or contradiction of other activity  
and witness statements



Identification of targets and  
co-conspirators/associates  
by their online information

- App data can give you  
usernames and social  
media platforms used

# Third Layer Data

---

## Type of data

- Meta data
- Deleted data
- Encrypted data

## Issues

- Can provide the same info as first and second layer data
- Often requires more work to get it
- Can be inaccessible due to technology limitations





## WHAT IS METADATA?

Info that identifies or “tags”  
the data at issue:

- Date/Time Stamp
- Location Stamp
- Author
- Location information
- Type of device used

# DELETED DATA

---

Always get a physical extraction, if possible, in order to get the deleted data



## ENCRYPTED DATA

*Encrypted data may be available on the device itself*

- WhatsApp
- Snapchat
- Facebook????

# Types of Available Data

---

## Cell Service Provider:

- CDR's
- SMS, voicemail content (maybe)
- Location Data
- Cell Mapping



## Vehicle Location Tracking –

### Other Options:

- Devices used by private parties to monitor their vehicles remotely
- Private onboard systems (OnStar, BMW)
- SIM cards through VINS



## Other Location Tracking Options:

Location history in:

Google

iPhone

Facebook

Instagram

WhatsApp

Snapchat



# Real-Time Geolocation Tracking

---

## Cellphone “pinging”

- Two statutes govern:
  - § 16-3-303.5
  - § 18-9-312(1.5)
- Exigent Circumstances

## IP “trap and trace”

- PC to believe the person is using an account or device connected to the internet
- Get IP address(es) of where the target logged in – in real time – then obtain physical location of IP address
- Companies will honor exigent requests

# TRACKING MOTOR VEHICLES

---

GPS trackers – need warrant

- Get authorization to install, monitor, and maintain, even on private property
- Get permission to “spot monitor” vehicle on an hourly or daily basis if the vehicle leaves CO



## APP DATA TIPS:

- *Think creatively about what might help your case*
- *Know the language/slang while analyzing the data*

# DATA FROM APPLICATIONS/ISPS

## App Data:

- Content
- Account Info
- Location Data



# Google

- Location History
- Google Photos
- Google Maps
- Gmail
- IP Addresses
- Google Pay
- Google Hangout
- Area-based Search Warrants
- And So Much More...

# Facebook

- Different kinds of available data
- Messenger data is a gold mine
- Proper identification of account holder:

[www.Facebook.com\[uid\]-](http://www.Facebook.com[uid]-)



# CLOUD DATA

- iCloud, Dropbox, Google Drive, Mega, Microsoft One Drive, NextCloud
- Can give additional info beyond the device
- Preservation request should be done ASAP, even if you have device

# Digital Devices

**More than cell phones...**



# OTHER DIGITAL DEVICE SOURCES

- Cars
- Drones
- LPRs
- Gaming devices

## Internet of Things [IoT]

- Echo, Google home
- Refrigerators
- Watches and Fitbits
- Smart home devices
- Home surveillance cameras
- Video doorbells
- Kids' toys



## VEHICLES – EDRs

### Event Data Recorder:

- Records data related to vehicle's speed, direction, etc.
- Based on a tamper-proof, read-write memory device.
- Some continuously record data, overwriting the previous few minutes vehicle stops.
- Others are activated by crash-like events

# In-Vehicle Infotainment (IVI) In-Car Entertainment (ICE)

---

- Collection of hardware and software in vehicles that provides audio or video entertainment.
- Systems can include steering wheel audio controls and hands-free voice control
- Includes: automotive navigation systems; video players; USB and Bluetooth connectivity; Carputers; In-car internet and WiFi



# VEHICLE DATA

## What can you get?

- All or most communications data downloaded when phone is synced to system.
- Doesn't matter if phone is locked or not

- Doors open/closed
- Bluetooth connections
- Gear Shifts
- Lights on/off
- USB attachments
- GPS location data
- Calls made
- Wifi connections
- System reboots

# Topic 2

---

You Then Need to Know How to Collect it Properly



# Digital Devices

## How to Preserve Data

- In the field (no warrant)
- In search warrants

# Preservation of cellphones

---



# Search Warrants

Two kinds of search warrants:

General – search warrant to take/seize all mobile devices recovered at a particular location (including associated hardware and storage media).

Specific – search warrant to access/seize all the data in a particular device.

## Preservation requests to include in general warrant

Ask for authorization to take steps to preserve and safeguard the data in any mobile devices encountered during the search.

- Request to access the phone to put it in airplane mode and turn off WiFi and Bluetooth
  - NOTE: keep phone powered on
- Request on-scene extraction to preserve the data.
- Request authority for biometric unlock



USE YOUR CREATIVITY TO OBTAIN PASSWORD AND/OR CONSENT

# Victim-Witness Devices

- Device(s) belonging to victims and uninvolved witnesses require special privacy protections
- Consent – remember what YOU see, you will likely have to provide to the defense
- Limit search if necessary and document the limitation.
- Protective orders for discovery purposes
- Be careful of screenshots – some apps will notify the sender that a screenshot was taken



# Digital Evidence

---


- Data contained outside the device
  - Service Provider
  - Cloud Storage
- Types of Data Available
- How to Preserve and Obtain Data

# PRESERVATION OF RECORDS

---

- Records from ISPs, social media accounts, email accounts, phone records – all electronic records
- Probable cause NOT required for preservation request
- Preservation requests:
  - Most companies accept preservation requests online
  - If not – send preservation letter immediately





---

basics related to DE  
search warrants

Key principles: specificity, probable cause

## PARTICULARITY of the location to be searched

---

- The easy part – identify the device to be searched or the business entity that you are seeking records from
- If seeking records, list name and address of business, registered agent, and LE portal (if available)
- Search.org – list of ISP providers with contact info



# PARTICULARITY of the data you want to receive

---

- ❖ List all the data you want to want to receive
  - ❖ For records: some data types are consistent between ISPs and some are different, find a good template or check the company's TOS/PP
- ❖ Don't forget data which tends to show possession and control of the device or account

# Overbreadth

- The need for attribution and authentication can justify a broad search, but...
- “*Any and all data*” IS NOT OK...nor is “including but not limited to...”



## Additional Court Orders

- Order for Nondisclosure  
18 U.S.C. §2705
- Order to Not Cancel Account
- Order to Seal  
C.R.S. §16-3-304(2)

# Topic 3

---

You Next Need to Know How to Search and Seize the Data



# Search of Devices

---

- Physical devices:
  - Obtain the device
  - Unlock if necessary
    - Cellebrite Advanced Services
    - GrayKey
  - Extract the data
    - Software-based tools: Cellebrite, Oxygen, Magnet, Final Mobile
    - Other methods: JTAG, ISP, Chip Off
  - Parse/Carve the data to put it in readable form

# Search of Records

---

- Electronic records:
  - Preserve the account – AS SOON AS POSSIBLE!
  - Submit a warrant or subpoena for the records
  - Subject the returns to a tool that will ingest the data and provide it in a more readable form



# FINAL THOUGHTS

## CONSIDER:

- What type of evidence is available?
- What is the source of the evidence?
- Do you have access to the evidence or do you need a warrant for it?
- What is the extent of the search authorized by your facts?