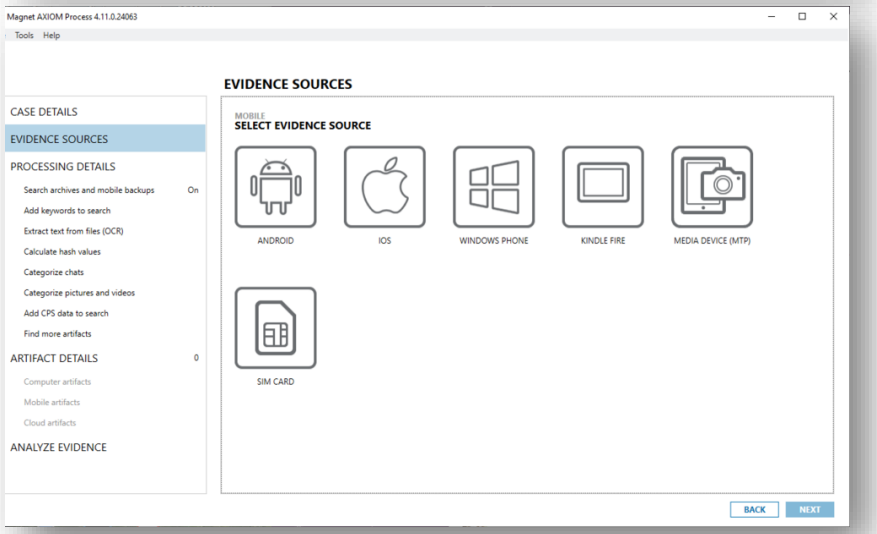
Cellebrite

GRAYSHIFT

Mobile Device Forensic Tools (MDFTs)

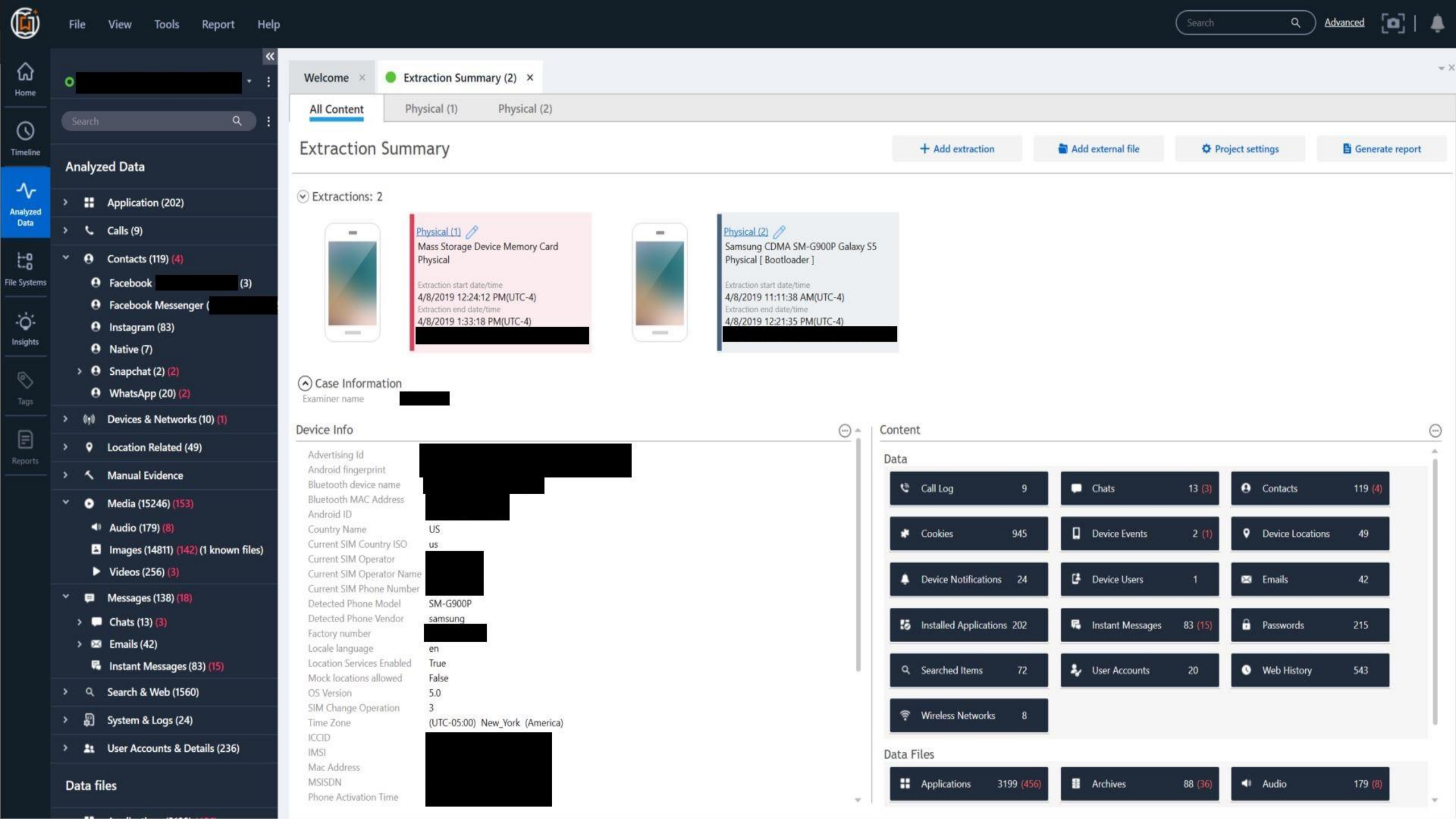
MAGNET FORENSICS

OXYGEN FORENSICS



Cellebrite & Magnet Forensics

- What is an Extraction?
- The type of Extraction that can be performed depends on the device, its operating system, and the status of the device
- Extractions vs. Reports
- Cellebrite UFED Touch2, UFED 4PC, Physical Analyzer, and more
  - UFED = Universal Forensic Extraction Device
- Magnet AXIOM, Outrider, Review, and more
  - Partnered with Grayshift to provide GrayKey to its law enforcement customers


File
View
Tools
Report
Help
Search
Advanced
Home
Timeline
Analyzed Data
File Systems
Insights
Tags
Reports
Search
Analyzed Data
Application (202)
Calls (9)
Contacts (119) (4)
Facebook [redacted] (3)
Facebook Messenger (
Instagram (83)
Native (7)
Snapchat (2) (2)
WhatsApp (20) (2)
Devices & Networks (10) (1)
Location Related (49)
Manual Evidence
Media (15246) (153)
Audio (179) (8)
Images (14811) (142) (1 known files)
Videos (256) (3)
Messages (138) (18)
Chats (13) (3)
Emails (42)
Instant Messages (83) (15)
Search & Web (1560)
System & Logs (24)
User Accounts & Details (236)
Data files
Welcome
Extraction Summary (2)
All Content
Physical (1)
Physical (2)
Extraction Summary
Add extraction
Add external file
Project settings
Generate report
Extractions: 2
Physical (1)
Mass Storage Device Memory Card
Physical
Extraction start date/time
4/8/2019 12:24:12 PM(UTC-4)
Extraction end date/time
4/8/2019 1:33:18 PM(UTC-4)
[redacted]
Physical (2)
Samsung CDMA SM-G900P Galaxy S5
Physical [Bootloader]
Extraction start date/time
4/8/2019 11:11:38 AM(UTC-4)
Extraction end date/time
4/8/2019 12:21:35 PM(UTC-4)
[redacted]
Case Information
Examiner name
[redacted]
Device Info
Advertising Id
Android fingerprint
Bluetooth device name
Bluetooth MAC Address
Android ID
Country Name
US
Current SIM Country ISO
us
Current SIM Operator
Current SIM Operator Name
Current SIM Phone Number
Detected Phone Model
SM-G900P
Detected Phone Vendor
samsung
Factory number
Locale language
en
Location Services Enabled
True
Mock locations allowed
False
OS Version
5.0
SIM Change Operation
3
Time Zone
(UTC-05:00) New_York (America)
ICCID
IMSI
Mac Address
MSISDN
Phone Activation Time
Content
Data
Call Log 9
Chats 13 (3)
Contacts 119 (4)
Cookies 945
Device Events 2 (1)
Device Locations 49
Device Notifications 24
Device Users 1
Emails 42
Installed Applications 202
Instant Messages 83 (15)
Passwords 215
Searched Items 72
User Accounts 20
Web History 543
Wireless Networks 8
Data Files
Applications 3199 (456)
Archives 88 (36)
Audio 179 (8)

Cellebrite Advanced Services & Premium

- Cellebrite Advanced Services (CAS)
- Cellebrite Premium
- Unlocks phones that the commercially available software and hardware cannot
- On-site or remote mobile device access services
- Premium = law enforcement only
- Advanced Services = law enforcement only for the most part

GrayKey

- GrayKey is made by Grayshift
- Grayshift has now partnered with Magnet Forensics
- Unlocks previously unlockable iPhones like CAS and recently expanded into Android devices
- Law enforcement only

Frye & *Daubert* Challenges

Frye v. United States, 293 F. 1013 (D.C. Cir. 1923)

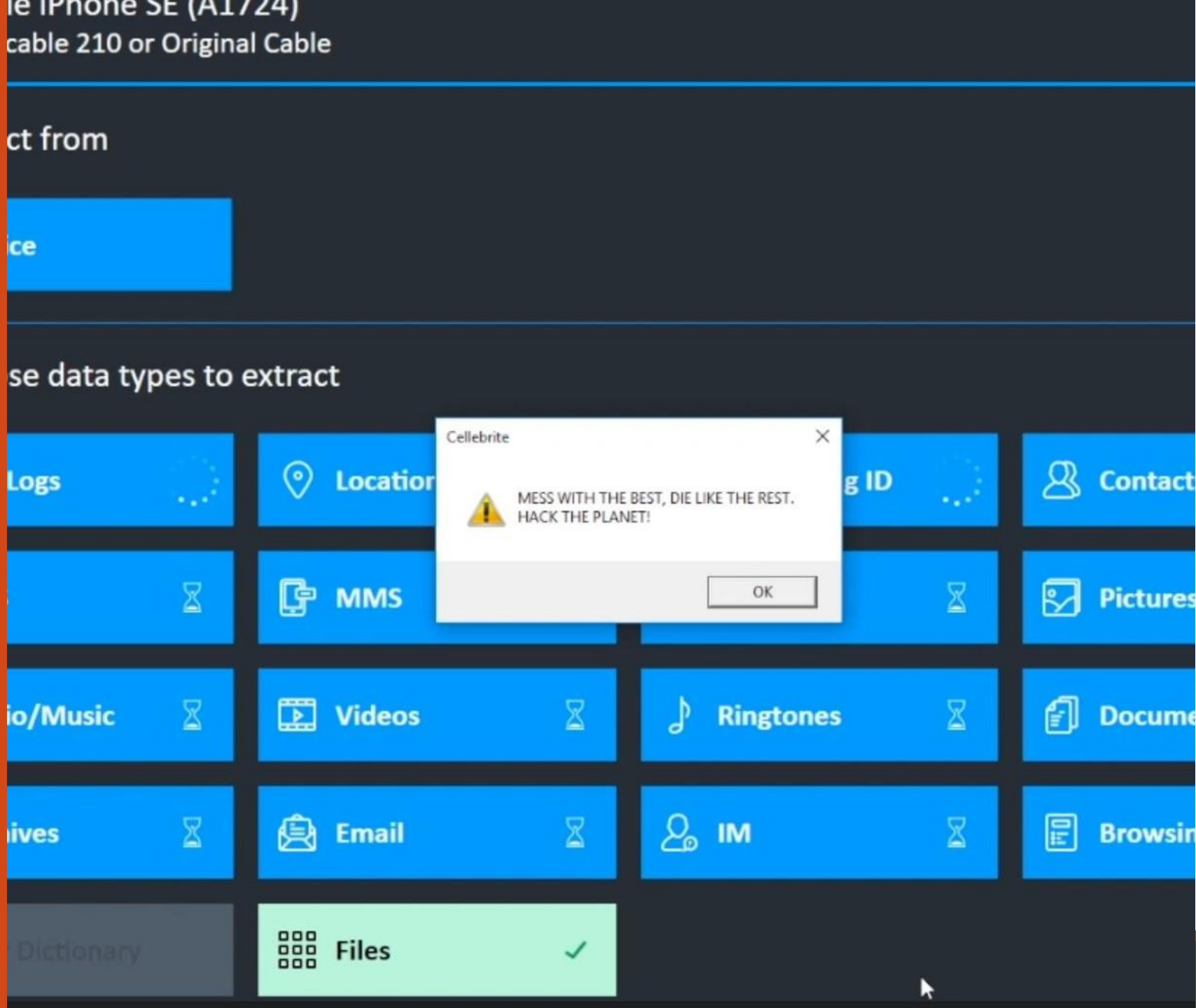
- "Somewhere in this twilight zone the evidential force of the principle must be recognized, and while courts will go a long way in admitting expert testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs." *Frye* at 1013-14.

Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993)

- Federal Rules of Evidence Rule 702
  - A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if: (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue; (b) the testimony is based on sufficient facts or data; (c) the testimony is the product of reliable principles and methods; and (d) the expert has reliably applied the principles and methods to the facts of the case.

Signal App Takes on Cellebrite

- “Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective”
  - https://signal.org/blog/cellebrite-vulnerabilities/
- What actually happened?
- How can we use this?
- How significant is the exploit Signal revealed?



Challenging “Experts” and Law Enforcement Only Tools

Actual experts vs. button pushers

- Certifications
- Trainings
- Degrees
- Not just which buttons to push but why

Law enforcement only tools

- Cellebrite Premium
- Grayshift GrayKey
- How do they work?
- How can it be verified?

Miscellaneous Issues

- How long can law enforcement hold on to a mobile device before getting a warrant?
  - *United States v. Smith*, 967 F.3d 198 (2d Cir. 2020)
    - (1.) the length of the delay, (2.) the importance of the seized property to the defendant, (3.) whether the defendant has a reduced property interest in the seized item, and (4.) the strength of the state's justification for the delay
  - Strategic considerations
- "Do-over" search warrants
  - *People v. Dominguez-Castor*, 2020 COA 1, 469 P.3d 514, cert. denied, No. 20SC130, 2020 WL 4915827 (Colo. Aug. 17, 2020)
  - How many times can the prosecution get a search warrant for a mobile device?
- Seize and search every device
  - *United States v. Griffith*, 867 F.3d 1265, 1276 (D.C. Cir. 2017) (citations omitted)
    - "The warrant's overbreadth is particularly notable because police sought to seize otherwise lawful objects: electronic devices. Courts have allowed more latitude in connection with searches for contraband items like 'weapons [or] narcotics.' But the understanding is different when police seize 'innocuous' objects. Those circumstances call for special 'care to assure [the search is] conducted in a manner that minimizes unwarranted intrusions upon privacy.'"