EVERYDAY TECH-USED AGAINST CRIMINAL DEFENSE
SPENCER MCINVAILLE, CTNS, CWA, CCO, CCPA

CALL DETAIL RECORDS

Call Detail Records (CDRs)
• What are they?
  • Legal proof of a service provided
  • A technical road map of a call
  • A financial transaction record
Call Detail Records (CDRs)

- How to get them
  - Account holder can request with notarized letter
  - Via subpoenas
  - Via discovery
  - Always get copies of the original files
  - Contact us for specific subpoena language...It is free.

- How are they used?
  - Associate a phone call with a cell tower
  - Show connections between phone numbers
  - Show frequency of connections
  - Show "user" activity

What About Prepaid aka "Burner" Phones?
Slide 7

AUTOMATED SOFTWARE
TURBOTAX DOESN'T MAKE YOU A CPA

Slide 8

Automated Software

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

Slide 9

Automated Software

- The State’s “Expert” admitted the software made mistakes. UTC to local offsets set incorrectly.
- EDT = UTC - 4, not +5
- Again faulty and unreliable/unscientific method of standard coverage.
Automated Software

• Again we proved to the Prosecution that the automation and 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.
Slide 13

Find my iPhone – Device Based

• Real time
• Cellular
• WiFi
• Bluetooth

Slide 14

Cell Phone Forensics

• Cellebrite Extractions

Slide 15

Collection and Acquisition

• Unique Preservation Issues
  • Phone must be isolated from network
  • Faraday Bag
Slide 16

Collection and Acquisition

• First responder thumbs through phone at scene
  • not forensically sound
  • Potentially cannot tell if:
    • Something created
    • Something deleted
    • Something manipulated

Slide 17

Collection and Acquisition

• Screenshots are not evidence

Slide 18

Capabilities: Examples

• Location
  • Google Maps

<table>
<thead>
<tr>
<th>Category</th>
<th>Example 1</th>
<th>Example 2</th>
<th>Example 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Maps</td>
<td>1/1/2014, 5414 AM, 4436.03, 7.80 MB</td>
<td>12/20/2014, 9:28 AM, 4436.03, 7.80 MB</td>
<td>1/1/2014, 5414 AM, 4436.03, 7.80 MB</td>
</tr>
<tr>
<td>Location</td>
<td>Google Maps</td>
<td>Google Maps</td>
<td>Google Maps</td>
</tr>
<tr>
<td>Duration</td>
<td>4436.03 MB</td>
<td>4436.03 MB</td>
<td>4436.03 MB</td>
</tr>
<tr>
<td>Size</td>
<td>7.80 MB</td>
<td>7.80 MB</td>
<td>7.80 MB</td>
</tr>
</tbody>
</table>
### Slide 19

**Location Data**

- Location data from multiple sources, from the cell phone.

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Latitude</th>
<th>Longitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/01/2020</td>
<td>00:00</td>
<td>41.3287</td>
<td>-81.3287</td>
</tr>
<tr>
<td>01/02/2020</td>
<td>08:00</td>
<td>41.3287</td>
<td>-81.3287</td>
</tr>
<tr>
<td>01/03/2020</td>
<td>12:00</td>
<td>41.3287</td>
<td>-81.3287</td>
</tr>
<tr>
<td>01/04/2020</td>
<td>16:00</td>
<td>41.3287</td>
<td>-81.3287</td>
</tr>
</tbody>
</table>

### Slide 20

**Location Data**

**Location Data extracted by CellLocation**

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Latitude</th>
<th>Longitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/01/2020</td>
<td>00:00</td>
<td>41.3287</td>
<td>-81.3287</td>
</tr>
<tr>
<td>01/02/2020</td>
<td>08:00</td>
<td>41.3287</td>
<td>-81.3287</td>
</tr>
<tr>
<td>01/03/2020</td>
<td>12:00</td>
<td>41.3287</td>
<td>-81.3287</td>
</tr>
<tr>
<td>01/04/2020</td>
<td>16:00</td>
<td>41.3287</td>
<td>-81.3287</td>
</tr>
</tbody>
</table>

### Slide 21

**Location Data**

**Significant Locations**

- Durham NC
- Fayetteville NC
- Raleigh, NC
- Cary NC
- 2 Locations, 5/31/20 - 6/30/20
Location Data – Google Location Services

• Android OS devices
  • Gmail account required for Google Play Store
  • Also gathers data from other devices signed into Google accounts,
  • Desktops
  • Laptops
  • Tablets
  • iOS devices
• Collection of data dependent upon permissions allowed.
Live Location

- Cell Site Simulators
- E-911 system

Live Location – Pen Register, Trap and Trace

- Pen Register, Trap and Trace orders are used to authorize cell site simulators.
- 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 on a predetermined interval.
- Pen Registers can be established on social media accounts for IP logs.
Questions?

- spencer.mcinvaille@envistaforensics.com
- Ask for a copy of our Cell Location Guide and Example Language!

[Images of books with titles: Digital Forensics for Legal Professionals, Cell Phone Location Evidence for Legal Professionals, and Digital Forensics for Legal Professionals, 2nd Edition]
Example Subpoena Language for Call Detail Records

Please contact the Digital Forensics Division for any questions or case inquiries regarding call detail records and location information. dfassign@envistaforensics.com

Table Of Contents:

- Page 2-3: AT&T Wireless, servicing Cricket Wireless
- Page 4-5: Verizon Wireless
- Page 6-7: T-Mobile, servicing Metro PCS and Metro by T-Mobile
- Page 8-9: Sprint Corporation, Servicing Boost Mobile and Virgin Mobile
- Page 10-11: Tracfone Wireless, servicing Net10 and SafeLink

If you do not see the carrier you are looking for, particularly Tracfone or other prepaid companies, or have any questions regarding call detail records, please contact us.

Other important steps prior to sending legal process:

- If your matter is civil litigation, please contact our experts for assistance as the service process may vary from these samples.
- Contact the carrier to ensure they are the correct carrier to request data.
- Send preservation letters to hold all available records, this can be done for 90 days at a time.
- Refer to search.org for the most current contact numbers and delivery methods for legal process. https://www.search.org/resources/isp-list/
Defendant, by and through his or her attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records and tower locations, for cell phone number(s) 000-000-0000 for the period of time between 00-00-2000 and 00-00-2000.

All information including but not limited to:

1. Subscriber information for the above listed numbers, including financially responsible party, billing address, features and services and equipment,

2. All call originations, call terminations, call attempts, voice and text message transactions, including push to talk, data communications, SMS and MMS communications, and voice communications, LTE and/or IP sessions and destinations with cell site information, including the originating and receiving phone numbers or network IDs for all incoming and outgoing call transactions, data transactions and push to talk sessions.

3. Records are to include the IMEI, IMSI or other equipment or handset identification information for the target phone number if known.

4. All stored SMS content, MMS content and / or Browser Cache if available.

5. Beginning and ending switch and cell site / tower identifiers for each call, SMS MMS and data transmission, including the location information and azimuth for the tower and sector used for the call.

6. A complete table of cell towers / cell site information for all cell towers / cell sites in the LAC, NEID or service area and or for all switches used, active at the time period for the call detail records requested. This shall include:
   a. cell tower location information including latitude and longitude
   b. cell tower / cell site designation information / identification numbers
   c. information for each cell site sector including azimuth.
   d. equipment type used at the cell site, i.e. Lucent or Nortel, etc.
   e. NOTE TO ATT MOBILITY: Even though the tower location information is in the call detail records, this subpoena also requests a list of cell tower locations with the latitude, longitude of each tower, the sector azimuth and the beam width, if known, for the time period covered, in comma delimited or Excel
format, for every tower referenced in the call detail records responsive to this subpoena.

7. a legend and definition for any and all abbreviations used in the reports provided

8. An explanation of how to read the call detail records.

9. Any precise measurement data such as e-911 location data, NELOS data and or any other data recorded for the time period that will provide additional location data.

10. Specific information regarding the time stamps / time zones of the records.

Provide the following information regarding cell tower locations for the following areas containing cell towers actively in service between 00-00-2000 and 00-00-2000.

Include the below AT&T cell tower information:

LAC
CID
Latitude
Longitude
Sector Azimuth

11. Any records or information regarding cell towers that were undergoing maintenance, or were out of service the time period in this request.

All responsive data is to be provided in both Adobe PDF format and Microsoft Excel format, .TXT or .CSV format.

Please indicate in your response to this subpoena if there is any data loss due to the time difference between the date of the receipt of this subpoena and the time period requested, and if so, a detailed description of what data is not recoverable versus what data would be recoverable based on the carrier’s retention period for call detail records.

Please respond to this subpoena via email to: your email & Expert with Envista Forensics
Verizon Wireless (formerly Cellco DBA Verizon Wireless)

180 Washington Valley Road
Bedminster, NJ 07921

Contact Phone Numbers:
- Subpoena contact: 888-483-2600
- Search warrant contact: 800-451-5242; select option 2
- Wireless Records contact: 800-451-5242; select option 1
- Wireless Voice, Text, Email, IP, etc.: (888) 483-2600

SERVICE BY FAX OR MAIL:
- Subpoenas: 888-667-0028
- Orders & Warrants: 888-667-0026
  OR
  Verizon Security Assistance Team
  180 Washington Valley Road
  Bedminster, NJ 07921

LANGUAGE:

Defendant, by and through his or her attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records and tower locations, for cell phone number(s) 000-000-0000 for the period of time between 00-00-2000 and 00-00-2000.

All information including but not limited to:

1. Subscriber information for the above listed numbers, including financially responsible party, billing address, features and services and equipment,

2. All call originations, call terminations, call attempts, voice and text message transactions, including push to talk, data communications, SMS and MMS communications, and voice communications, LTE and/or IP sessions and destinations with cell site information, including the originating and receiving phone numbers or network IDs for all incoming and outgoing call transactions, data transactions, VOLTE and push to talk sessions.

3. Records are to include the IMEI, IMSI or other equipment or handset identification information for the target phone number if known.

4. All stored SMS content, MMS content and / or Browser Cache if available.

5. Beginning and ending switch and cell site / tower identifiers for each call, SMS MMS and data transmission, including the location information and azimuth for the tower and sector used for the call.
6. A complete table of cell towers / cell site information for all cell towers / cell sites in the Switch, Market, Site ID, Sector ID or service area and or for all switches used, active at the time period for the call detail records requested. This shall include:
   a. cell tower location information including latitude and longitude
   b. cell tower / cell site designation information / identification numbers
   c. information for each cell site sector including azimuth and beamwidth.
   d. equipment type used at the cell site, i.e. Lucent, Samsung, Nortel, etc.

7. a legend and definition for any and all abbreviations used in the reports provided

8. An explanation of how to read the call detail records.

9. Any precise measurement data such as e-911 location data, RTT, RTTL, RTTM, erlte or reports of similar nature data that provide estimated locations of the device or distances from the base station. Any other data recorded for the time period that will provide additional location data.

10. Specific information regarding the time stamps / time zones of the records.

Provide the following information regarding cell tower locations for the following areas containing cell towers actively in service between 00-00-2000 and 00-00-2000.

11. Any records or information regarding cell towers that were undergoing maintenance, or were out of service the time period in this request.

All responsive data is to be provided in both Adobe PDF format and Microsoft Excel format, .TXT or .CSV format.

Please indicate in your response to this subpoena if there is any data loss due to the time difference between the date of the receipt of this subpoena and the time period requested, and if so, a detailed description of what data is not recoverable versus what data would be recoverable based on the carrier’s retention period for call detail records.

Please respond to this subpoena via email to: your email & Expert with Envista Forensics
T-Mobile, service Metro PCS, and Metro by T-Mobile

4 Sylvan Way
Parsippany, New Jersey 07054

Contact: 866-537-0911

SERVICE BY E-MAIL AND FAX: Lerinbound@T-Mobile.com, 973-292-8697

LANGAUGE:

Defendant, by and through his or her attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records and tower locations, for cell phone number(s) 000-000-0000 for the period of time between 00-00-2000 and 00-00-2000.

All information including but not limited to:

1. Subscriber information for the above listed numbers, including financially responsible party, billing address, features and services and equipment,

2. All call originations, call terminations, call attempts, voice and text message transactions, including push to talk, data communications, SMS and MMS communications, and voice communications, LTE and/or IP sessions and destinations with cell site information, including the originating and receiving phone numbers or network IDs for all incoming and outgoing call transactions, data transactions and push to talk sessions.

3. Records are to include the IMEI, IMSI or other equipment or handset identification information for the target phone number if known.

4. All stored SMS content, MMS content and / or Browser Cache if available.

5. Beginning and ending switch and cell site / tower identifiers for each call, SMS MMS and data transmission, including the location information and azimuth for the tower and sector used for the call.

6. A complete table of cell towers / cell site information for all cell towers / cell sites in the Region, Market, Site ID, Sector ID or service area and or for all switches used, active at the time period for the call detail records requested. This shall include:
   a. cell tower location information including latitude and longitude
   b. cell tower / cell site designation information / identification numbers
   c. information for each cell site sector including azimuth and beamwidth.
   d. equipment type used at the cell site, i.e. Lucent or Nortel, etc.

7. a legend and definition for any and all abbreviations used in the reports provided
8. An explanation of how to read the call detail records.

9. Any precise measurement data such as e-911 location data, TDOA (Time Delay of Arrival) Truecall, Timing Advance or reports of similar nature data and or any other data recorded for the time period that will provide additional location data.

10. Specific information regarding the time stamps / time zones of the records.

Provide the following information regarding cell tower locations for the following areas containing cell towers actively in service between 00-00-2000 and 00-00-2000.

11. Any records or information regarding cell towers that were undergoing maintenance, or were out of service the time period in this request.

All responsive data is to be provided in both Adobe PDF format and Microsoft Excel format, .TXT or .CSV format.

Please indicate in your response to this subpoena if there is any data loss due to the time difference between the date of the receipt of this subpoena and the time period requested, and if so, a detailed description of what data is not recoverable versus what data would be recoverable based on the carrier’s retention period for call detail records.

Please respond to this subpoena via email to: your email & Expert with Envista Forensics
Sprint Corporation, Servicing Boost Mobile and Virgin Mobile

6480 Sprint Pkwy
Overland Park, Kansas 66251

Contact: 800-877-7330

SERVICE BY FAX: 816-600-3111; To receive status updates for Subpoenas and Search Warrants by contacting 800-877-7330 extension 3.

LANGUAGE:

Defendant, by and through his or her attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records and tower locations, for cell phone number(s) 000-000-0000 for the period of time between 00-00-2000 and 00-00-2000.

All information including but not limited to:

1. Subscriber information for the above listed numbers, including financially responsible party, billing address, features and services and equipment,

2. All call originations, call terminations, call attempts, voice and text message transactions, including push to talk, data communications, SMS and MMS communications, and voice communications, LTE and/or IP sessions and destinations, eHRPD with cell site information, including the originating and receiving phone numbers or network IDs for all incoming and outgoing call transactions, data transactions and push to talk sessions.

3. Records are to include the IMEI, IMSI or other equipment or handset identification information for the target phone number if known.

4. All stored SMS content, MMS content and / or Browser Cache if available.

5. Beginning and ending switch and cell site / tower identifiers for each call, SMS MMS and data transmission, including the location information and azimuth for the tower and sector used for the call.

6. A complete table of cell towers / cell site information for all cell towers / cell sites in the NEID/REPOL, Switch, Market, Site ID, Sector ID or service area and or for all switches used, active at the time period for the call detail records requested. This shall include:
   a. cell tower location information including latitude and longitude
   b. cell tower / cell site designation information / identification numbers
   c. information for each cell site sector including azimuth and beamwidth.
   d. equipment type used at the cell site, i.e. Lucent, Samsung, Nortel, etc.
7. A legend and definition for any and all abbreviations used in the reports provided.

8. An explanation of how to read the call detail records.

9. Any precise measurement data such as e-911 location data, Per Call Measurement Data (PCMD) or reports of similar nature data that provide estimated locations of the device or distances from the base station. Please provide a PCMD report for each Vendor/Call type. Any other data recorded for the time period that will provide additional location data.

10. Specific information regarding the time stamps / time zones of the records.

Provide the following information regarding cell tower locations for the following areas containing cell towers actively in service between 00-00-2000 and 00-00-2000.

11. Any records or information regarding cell towers that were undergoing maintenance, or were out of service the time period in this request.

All responsive data is to be provided in both Adobe PDF format and Microsoft Excel format, .TXT or .CSV format.

Please indicate in your response to this subpoena if there is any data loss due to the time difference between the date of the receipt of this subpoena and the time period requested, and if so, a detailed description of what data is not recoverable versus what data would be recoverable based on the carrier’s retention period for call detail records.

Please respond to this subpoena via email to: your email & Expert with Envista Forensics.
Tracfone Wireless Inc. d/b/a Simple Mobile, also servicing Net10 and SafeLink

Tracfone Wireless Inc. d/b/a Simple Mobile

ATTN: Subpoena Compliance

9700 NW 112th Avenue

Miami, FL 33178

Contact: 800-810-7094

SERVICE BY E-MAIL (PREFERRED) AND FAX: subpoenacompliance@tracfone.com, 305-715-6932

LANGUAGE:

Defendant, by and through his or her attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records and tower locations, for cell phone number(s) 000-000-0000 for the period of time between 00-00-2000 and 00-00-2000.

All information including but not limited to:

1. Subscriber information for the above listed numbers, including financially responsible party, billing address, features and services and equipment,

2. All call originations, call terminations, call attempts, voice and text message transactions, including push to talk, data communications, SMS and MMS communications, and voice communications, LTE and/or IP sessions and destinations with cell site information, including the originating and receiving phone numbers or network IDs for all incoming and outgoing call transactions, data transactions and push to talk sessions.

3. Records are to include the IMEI, IMSI or other equipment or handset identification information for the target phone number if known.

4. All stored SMS content, MMS content and / or Browser Cache if available.

5. Beginning and ending switch and cell site / tower identifiers for each call, SMS MMS and data transmission, including the location information and azimuth for the tower and sector used for the call.

6. A complete table of cell towers / cell site information for all cell towers / cell sites in the Region, Market, Site ID, Sector ID or service area and or for all switches used, active at the time period for the call detail records requested. This shall include:
   a. cell tower location information including latitude and longitude
   b. cell tower / cell site designation information / identification numbers
   c. information for each cell site sector including azimuth and beamwidth.
d. equipment type used at the cell site, i.e. Lucent or Nortel, etc.

7. a legend and definition for any and all abbreviations used in the reports provided

8. An explanation of how to read the call detail records.

9. Any precise measurement data such as e-911 location data, TDOA (Time Delay of Arrival) Truecall, Timing Advance or reports of similar nature data and or any other data recorded for the time period that will provide additional location data.

10. Specific information regarding the time stamps / time zones of the records.

Provide the following information regarding cell tower locations for the following areas containing cell towers actively in service between 00-00-2000 and 00-00-2000.

11. Any records or information regarding cell towers that were undergoing maintenance, or were out of service the time period in this request.

All responsive data is to be provided in both Adobe PDF format and Microsoft Excel format, .TXT or .CSV format.

Please indicate in your response to this subpoena if there is any data loss due to the time difference between the date of the receipt of this subpoena and the time period requested, and if so, a detailed description of what data is not recoverable versus what data would be recoverable based on the carrier’s retention period for call detail records.

Please respond to this subpoena via email to: your email & Expert with Envista Forensics
Preparing Testimony about Cellebrite UFED in a Daubert or Frye Hearing
Table of Contents

The Cellebrite UFED is among the best known and most used mobile forensic extraction and analysis tools in the digital forensics industry. However, its complex technical processes are not as well understood outside of training. The following information is presented in an effort to help attorneys prepare themselves and their witnesses for Daubert\(^1\), Frye\(^2\), or related challenges to the admissibility of UFED-extracted mobile device evidence.

Tested Theory or Tool.....................................................................................................................3

   Examiner’s personal tool validation..........................................................................................3

Peer Review. ..................................................................................................................................4

   Test methodology.....................................................................................................................5

   Known or potential error rates...............................................................................................5

   Putting CFTT findings in context............................................................................................6

Expert qualifications and stature...............................................................................................7

General Acceptance...................................................................................................................8

Appendix.....................................................................................................................................10

   Foundational questions.........................................................................................................10

2009 NIST CFTT............................................................................................................................11

2010 NIST CFTT............................................................................................................................11

2012 NIST CFTT............................................................................................................................12

\(^1\) Daubert v. Merrell Dow Pharmaceuticals (92-102), 509 U.S. 579 (1993)

\(^2\) Frye v. United States. 293 F. 1013 (D.C. Cir 1923)
Cellebrite’s tools are commercial, meaning that their underlying code is proprietary. In the interests of competitive advantage, its code is not open for review. However, Cellebrite makes available an overview of how its processes work, and how they support forensically sound extractions, decoding and analysis, in its white paper “What Happens When You Press that Button? Explaining Cellebrite UFED Data Extraction Processes.”

Generally it is extremely difficult to falsify UFED results because the extractions are read only. Furthermore, physical extractions are subjected to hash calculation at the time of extraction. Multiple methods exist to validate UFED findings.

### Examiner’s personal tool validation

Cellebrite supports the regular practice of tool validation. Our customers may validate their results in one of several different ways:

1. Manually view results—for instance, the contents of a text message, or an email’s date/time stamp—compared to the UFED’s report. (This will not be possible with deleted data.)

2. Test the tool on two different devices of the same make and model. However, because this risks replicating errors, it is wise for examiners to create content on a test device(s) with which to compare evidence extractions—and to use additional validation methods.

3. Compare the UFED’s results from the evidence device with the results of one or more additional mobile forensic tools.

4. Compare call and text messaging logs with carrier call detail records.

5. For file system and physical extractions, go into the hexadecimal code and use manual decoding methods to verify results.

In addition to validating that their tools work properly, examiners should authenticate their evidence, either independently or in collaboration with case investigators, referring to relevant rules of evidence. Hash values, witness statements, and process are explored in great detail in Guidance Software’s 2011 EnCase Legal Journal.

---

*Examiners should not use their own personal devices. This risks being asked to introduce personal data at trial.

Cellebrite UFED hardware and software has been independently tested three times by the National Institute of Standards and Technology (NIST) and once by the National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence (ECTCoE). All four reports are in the public domain and available for download online.

NIST evaluated Cellebrite UFED hardware and software in 2009, 2010 and 2012 as part of its Computer Forensic Tool Testing (CFTT) Project. In all three years, the UFED completely and accurately acquired all supported objects, with few anomalies:

- In 2009, the tested UFED 1.1.0.5 version acquired all supported data objects from an LG VX5400, LG VX6100, Motorola V710, Samsung SCH–u410, Samsung SCH–u740, and Samsung SPH–a660.

- In 2010, the tested UFED 1.1.3.3 version acquired all supported data objects from an iPhone 3Gs, Blackberry Bold 9700, HTC Tilt 2, Nokia E71x, HTC Touch Pro 2, Blackberry Tour 9630, Samsung Moment, and Palm pixi.

- In 2012, the tested UFED 1.1.8.6’ acquired all supported data objects from an Apple iPhone 4 running iOS 4.3.3 and 4.2.10, BlackBerry Torch 9800, Samsung SGH-i917, Nokia 6350, Motorola Tundra, HTC Thunderbolt, Palm Pre2, and Samsung Haven. UFED Physical Analyzer 2.3.0.1, and UFED Report Manager 1.8.3.171110 were also assessed in this test.

The ECTCoE study, completed in July 2012, tested seven devices—an LG VX-9900, a Motorola V3M, a Nokia 2610, a Motorola V3xx, an LG C729 Double Play, an Apple iPhone 4S, and an Apple iPhone 3GS—against UFED 1.1.7.6, UFED Physical Analyzer 2.2.0.8966, and (now discontinued) UFED Report Manager 1.8.3.171110 as part of the NIJ Research, Development, Testing and Evaluation (RDT&E) process.

It concluded: “Cellebrite’s UFED performed consistently well during the testing. Connectivity issues between the UFED and phones tested were rare. In these tests, the UFED only had difficulty connecting to certain GSM phones that did not contain a SIM card, and these issues most likely could be remedied by creating a cloned SIM card.”

---

5 Test Results for Mobile Device Acquisition Tool: Cellebrite UFED 1.1.05, https://cyberfetch.org/sites/default/files/Mobile_Cellebrite_UFED_1_1_05_2009.pdf, September 2009, accessed March 11, 2014
6 Test Results for Mobile Device Acquisition Tool: Cellebrite UFED 1.1.3.3 - Report Manager 1.6.5, https://cyberfetch.org/sites/default/files/Mobile_CelleBrite_UFED_1_1_3_3_Report_Manager_1_6_5_2010.pdf, October 2010, accessed March 11, 2014
7 In 2012 NIST misidentified UFED 1.1.8.6 as UFED software application “UFED Logical Analyzer 1.1.8.6“ rather than the version of UFED firmware used to extract the device.
8 Test Results for Mobile Device Acquisition Tool: Cellebrite UFED 1.1.8.6 – Report Manager 1.8.3/UFED Physical Analyzer 2.3.0, https://cyberfetch.org/sites/default/files/Mobile_CelleBrite_UFED_1_1_8_6_Report_Manager_1_8_3_UFED_Physical_Analyzer_2_3_0_2012.pdf, October 2012, accessed March 11, 2014
Test methodology

NIST’s CFTT is ongoing research that evaluates a broad spectrum of digital forensic software and hardware. The CFTT follows a set of standards which NIST itself developed. According to its 2010 and 2012 reports, NIST states:

“In all four tests, the vast majority of anomalies had to do with reporting known data (see Appendix for details). With the exception of some NIST results in 2010, no acquisition errors occurred across hundreds of tested devices, and reporting/interpretation anomalies were rare:

- In 2009, out of 79 NIST test cases among six devices, eight anomalies were reported for a 10 percent error rate. Three of those anomalies were very minor misidentification of MIN/MSISDN; one was related to connectivity. All were related to reporting rather than acquisition.

- In 2010, out of 188 NIST test cases among eight devices, 11 anomalies were reported for a 6 percent error rate. Both acquisition and reporting errors occurred. Certain file types were not acquired in four test cases; the rest of the errors had to do with reporting.

- In 2012, out of 227 NIST test cases among nine devices, 17 anomalies were reported for a 7.5 percent error rate. These anomalies were either a failure to report, or misreporting, of data including address book, MMS text, memo entries, and call log data.

- In all but one case in the ECTCoE study, logical extractions were verified upon manual examination. (The exception was a device that did not contain a SIM card.)

The ECTCoE disclosed its test methodology based on its test bed and installation procedures, but did not reflect how it came to select test cases.

Known or potential error rates

Unlike the ECTCoE study, NIST’s research did not break out results by logical, file system, or physical extraction (although its 2012 report appears to indicate reliance on UFED Logical).
Putting CFTT findings in context

File system extractions were successful in all seven cases, although in one case could not be decoded for examination within UFED Physical Analyzer. In the three cases where physical extraction was attempted, only one could not be performed, likely because of a lack of SIM card.

Digital forensics tools should also not misreport one type of data as another, for example, a text message as an email.

By contrast, misattribution—reporting a text message as sent when it was actually received, or not reporting part of a message’s or image’s metadata, even when the content and its location are correct—may have more to do with the device than the forensic tool.

A logical extraction, for instance, relies on the device manufacturer’s API to request data from the device. If the API doesn’t support the transfer of that particular piece of data, the UFED cannot report it. In addition, smartphones’ operating systems may make attributions or interpretations (for instance, a cellular tower’s location) which the UFED, rather than interpreting, simply reports.

In these cases, focus should be on the fact that the content was found to be on the device and that during a forensically sound extraction, could not have been placed there during a previous extraction or other manipulation. Expert witnesses should be able to help explain how mobile devices store data, how their forensic tools extract and report it, what may result in errors in that process, and again, how they validated their process.

In addition, it should be possible to show that even when a logical extraction misreports data, a physical extraction (when possible for that model) identifies the data’s location within the device’s memory.

It is important to understand the nature of these anomalies and the context of NIST’s CFTT reports. First, Cellebrite’s tools—both extraction and analysis software—are updated every four to six weeks. As any software updates do, these improve performance and fix bugs in addition to introducing new features and/or device support.

Second, the CFTT project cannot account for every device make, model, operating system or network protocol that exists; instead, the independent protocol that NIST developed exists to evaluate overall tool performance. Thus, use of the NIST reports should not focus so much on whether the device(s) you are introducing into evidence at trial was also tested by NIST.

Instead, focus on the reports’ broader meaning. Digital forensics tools should not be found to report content that exists someplace it does not (whether as part of the file system structure or in unallocated space).
At that point, the examiner must use his/her personal expertise to identify all the data, metadata, and attributes.

**Expert qualifications and stature**

As with any digital forensic tool or technique, it is not recommended that a mobile device examiner rely on a single UFED tool to interpret the data. Examiners should be trained and qualified to validate what is on the device and where it is located, especially after performing a physical extraction. This includes:

- Current certification for the type of examination performed. Prior to late 2013, examiners could expect to earn UFED Logical certifications (typically granted after a 2-day course) or UFED Ultimate certifications (granted after a 3-day course). Following Q4 2013, Cellebrite has standardized its training curriculum and is delivering Cellebrite Certified Logical Operator (CCLO) and Cellebrite Certified Physical Analyst (CCPA) certifications, while honoring previous certifications for two years from the date of issue. Cellebrite recommends that training in the rapidly evolving field of mobile forensics should be refreshed every two years to stay current with the evolution of Cellebrite tools and methodology, as well as the evolution of mobile device technology.

- Whether the examiner regularly updates his or her tools, and whether the most current versions of UFED software were available and used at the time each extraction and analysis were performed. For validation purposes, it is useful for an examiner to create and maintain a known mobile data set, so as to parse that data on each subsequent release of analytical tools like UFED Physical Analyzer. It can be likewise beneficial for the examiner to keep a known mobile device with certain known artifacts on hand, and use this non-evidentiary test device for extraction each time there is a subsequent release of UFED firmware. (As technology develops, new artifacts may be revealed, but the loss of artifacts may indicate issues with the validity of the new software release, indicating a “rollback” is in order.)

* More details about the UFED extraction solution can be found in the white paper, “What Happens When You Press that Button? Explaining Cellebrite UFED Data Extraction Processes.”
Whether it was possible for the examiner to validate the tool using a test version of device(s) relevant to their case—both make and model—as well as the same operating system version, and any pertinent apps installed on the device. The examiner should also understand and be prepared to explain the differences between device models, operating system versions, and app versions, as well as accounting for any potential variances between results from test and evidence devices.

Whether the examiner and/or lead investigator validated and authenticated his or her results with other tools and resources, including other mobile forensics tools, carrier call detail records, witness interviews, known case details, manual decoding of the hex code, etc.

Whether the examiner maintained logging and reporting per their organization’s standard operating procedure and digital forensics best practices, thus resulting in a repeatable and reproducible process.

General Acceptance

Cellebrite UFED hardware and software is used by investigators in both the public and private sectors worldwide. More than 90,000 hardware units have been sold to law enforcement at local, county, state or provincial, and federal levels; corporate legal and security teams; private investigators and consultants; and military field personnel in more than 100 countries. Securities, customs and border protection, immigration, and various task forces all use the UFED to investigate narcotics, human trafficking, fraud, homicide, sexual assault, and numerous other types of cases.

No independent national or international standard exists for the development of mobile forensics extraction and analysis tools.

However, Cellebrite UFED extraction processes are generally accepted as a valid scientific process. This is because of the UFED’s read-only transfer of data from source device to target drive, and its physical analysis software’s “hex view.” Hex view enables examiners to check the device’s underlying data to verify parsed information from a raw “dump” or extraction.

Part of Cellebrite’s broad appeal is its relationships with more than 150 wireless carriers and original equipment manufacturers, owing to its retail business unit. In order to facilitate the transfer of data from mobile consumers’ old phones to new phones, Cellebrite receives more than 100 new
handsets per month from its global partners. Each device is tagged, tested and, once certified, added to the list of mobile phones supported by the UFED system. Ongoing quality assurance helps to reinforce consistent support across makes, models and operating systems.

Cellebrite is not aware of any challenges to admissibility based on UFED tools passing Daubert tests, Cellebrite UFED tools have been referenced in several cases at the appellate level, and a 2008 customer testimonial references successful expert witness testimony. In this case, State of Texas v. Deaver, defense mounted its appeal based on consent rather than forensic process.
Appendix

Foundational questions

- What is the Cellebrite UFED?
- Is this tool commonly used by law enforcement to extract data from cell phones?
- Are you trained and experienced in using the device?
- Are you certified to use this device at the level of extraction you used it for? When did you obtain your certification?
- Are there articles, white papers, or publications about the Cellebrite UFED?
- Has the device been accepted as a forensic tool in other courts across the country?
- Is there any one tool that can extract all data from a phone?
- Is it common for forensic examiners to use multiple tools depending on the phone make/model in question?
- Did you use the Cellebrite UFED device to extract data in this case?
- Have you validated that the Cellebrite is unable to write data to an evidence device?
- What type of phone did you examine in this case?
- What type of information did the UFED indicate it was capable of extracting from the defendant’s phone?
- Were you able to extract that information using the UFED?
- Have you validated that the Cellebrite extracts the data it says it will extract from this device?
- Did you also verify that the UFED parsed the information correctly? (same number of text messages, contact info, call history)
- During this validation, had the UFED changed or deleted any of the data from the cell phone?
- If the phone is a GSM phone, did you examine the SIM card and the handset separately?
- If the UFED did not extract all the data you extracted from the phone or SIM, what other method did you use to extract that information?
- If you reexamined this device today, would you get the same information?

* This list is a sampling and is not meant to be exhaustive. Attorneys may come up with their own foundational questions.
Except for the following test cases, the tested tool (UFED 1.1.05) acquired all supported data objects completely and accurately from the selected test mobile devices. The exceptions are the following:

- Connectivity disruptions between the mobile device (i.e., LG VX6100) and interface were not adequately presented to the examiner. Test Case: CFT–IM–03 (LG VX6100)
- The MIN was extracted instead of the MSISDN for the following Samsung devices: SCH–u410, SCH–u740, SPH–a660. Test Case: CFT–IM–05 (SCH–u410, SCH–u740, SPH–a660)
- Missed calls are reported as both Incoming and Missed, representing two calls rather than one. Test Case: CFT–IM–07 (MOTO V710)
- Text messages with a status of UNREAD were altered to READ. Test Case: CFT–IM–08 (MOTO V710)
- Outgoing text messages did not contain the outgoing date/time stamp. Test Case: CFT–IM–08 (MOTO V710)
- All outgoing text messages present in internal memory were not reported. Test Case: CFT–IM–08 (MOTO V710)

---

2010 NIST CFTT

Except for the following test cases, the tested tools (UFED 1.1.3.3; UFED Report Manager\(^2\) 1.6.5) acquired all supported data objects completely and accurately from the selected test mobile devices. The exceptions were the following:

- Maximum length address book entries reported were truncated. Test Case: SPT–06 (iPhone 3Gs, HTC Tilt2, Palm pixi)
- Graphics files associated with address book entries were not reported. Test Case: SPT–06 (iPhone 3Gs, Palm pixi)
- Email addresses associated with address book entries were not reported. Test Case: SPT–06 (Palm pixi)
- Graphics files of type .gif and .bmp were not acquired. Test Case: SPT–10 (iPhone 3Gs)
- Videos of type .flv were not acquired. Test Case: SPT–10 (HTC Tilt2, Nokia E71x)
- Connectivity was not established using the supported interface. Test Case: SPT–01 (Samsung Moment)
- Subscriber and equipment related information was not acquired. Test Case: SPT–05 (Palm pixi)

---

\(^2\) UFED Report Manager is no longer being distributed. It was discontinued in 2012 and replaced by reporting within UFED Logical Analyzer and UFED Physical Analyzer; however, it may still be in use, and/or may have been used to create reports for cases only now entering trial or appeals.
The tools (UFED 1.1.8.6, UFED Report Manager 1.8.3 and UFED Physical Analyzer 2.3.0) were tested for the ability to acquire active and deleted data from the internal memory of mobile devices and SIMs. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all nine mobile devices tested.

- Graphics files associated with address book entries were not reported. (iPhone4 GSM, iPhone4 CDMA, HTC Thunderbolt, Palm Pre2)

- Address book entries with fields for a first, middle and last name were reported incorrectly. The first name field was appended with a semicolon. (Samsung Focus)

- Regular-length address book entries with a value in only the first-name field were reported incorrectly. The first-name field was duplicated. (Motorola Tundra)

- Memo entries were not acquired. (Motorola Tundra)

- Address book entries with fields for a first, middle and last name were reported incorrectly. The middle-name field was not reported. (Palm Pre2)

- Maximum-length address book entries were truncated — 54 out of 126 characters were reported. (Palm Pre2)

- Email addresses associated with address book entries were not reported. (Palm Pre2)

- The textual portion of MMS messages was not reported. (BlackBerry Torch, Nokia 6350, HTC Thunderbolt)

- Acquisition of call log data ended in errors. (Motorola Tundra)

- Equipment-related information was not reported. (Palm Pre2)

- Acquisition of address book entries containing non-ASCII characters were reported incorrectly. (BlackBerry Torch)

- When connectivity was interrupted, the tool failed to notify the user that the acquisition had been disrupted. (Palm Pre2)