



2023 Transportation Practice Group Seminar

April 26-28, 2023

Call Me!?!

A Discussion Concerning Post-Crash Forensic Analysis of Cell Phones and Other Data, Including Best Practices related to Policies, Procedures and Preservation.

J. Philip Davidson

Moderator

HINKLE LAW FIRM LLC

Wichita, Kansas

pdavidson@hinklaw.com

Lars Daniel

Practice Leader

ENVISTA FORENSICS

Morrisville, North Carolina

lars.daniel@envistaforensics.com

Jeffrey Hickman

Practice Leader

APPLIED SAFETY AND ERGONOMICS, A RIMKUS COMPANY

Richmond, Virginia

jhickman@appliedsafety.com

After the Crash

Spoliation Proofing Mobile Phone Evidence In Trucking Cases

Lars Daniel EnCE, CCPA, CCO, CTNS, CTA, CIPTS, CWA

Practice Leader - Digital Forensics at Envista Forensics

Ashley Brown, Member

Ward, Hocker, Thornton, PLLC (Kentucky)

The aftermath of a motor carrier accident can be a harrowing experience. It is common knowledge that photos, witness statements, alcohol and drug testing, electronic logs, and ECM data must be collected and preserved amid this chaotic scene. However, mobile phone evidence is often an afterthought, if a thought at all. This confusion is partly due to the misunderstanding between evidentiary data on a mobile phone versus what is contained in call detail records.

The Confusion Over Call Detail Records

Call detail records will contain the calls, text messages, and data transmissions from a mobile phone depending on the cellular provider. Regardless, these records will only have the transmission date and time of the text message, not the actual content of what was said. You can also forget about recovering data from messaging applications like Facebook Messenger, Instagram, Kik Messenger, WhatsApp, and Telegram. These applications and the many like them use data to transmit messages, meaning they would create no record of ever existing in a Call Detail Report (CDR).

Further, the data records returned from CDRs are nearly useless for anything other than showing that the phone was powered on at the time. You cannot determine what activity or application the data transmission is related to from call detail records alone. From these records, it is impossible to tell if the data transmission was caused by an automated function of the cell phone or was generated by user activity.

The most inclusive source of evidence for what transpired is contained in the internal storage of the mobile phone.

It needs to be examined using digital forensic software and hardware. With the data contained on the mobile phone, it is possible to determine what was occurred at the time of the accident. By examining the mobile phone's internal memory, it is possible to determine what happened on the phone at the time of the accident, including evidence from applications that only create data records in a CDR, like third-party messaging apps, social media, games, or movie and music streaming services.

Plaintiff Attorneys

Plaintiff attorneys have been requesting Call Detail Records for some time, but it is becoming more common for plaintiff attorneys to seek access to the mobile phone of the truck driver after an accident. For example, in March of 2021, Joe Fried and Michael Goldberg, renowned plaintiff attorneys who specialize in trucking accident cases, wrote:

"The use of cellphones is one of the biggest distractions for truck drivers. The best evidence of cellphone use is a download of the cellphone itself...If the driver refuses to give his password or suddenly cannot "remember" his password, then there is no reason to do anything with the cellphone itself other than to point out to the jury that the driver is most likely failing to remember his password because the contents of the cellphone are harmful to his defense of the case."¹

First Contact: The Critical Link in Evidence Protection

The data contained on a mobile phone is both volatile and fragile. It is volatile in that it is easily altered by mishandling the evidence. It is fragile because critical data can be destroyed if best practices are not implemented when collecting data from a mobile phone.

If the mobile phone is not handled following digital forensics best practices, it can be impossible to determine in some instances what data was changed and if those changes were intentional or unintentional.

According to the Federal Motor Carrier Safety Administration (FMCSA), "No driver may use a hand-held mobile telephone or engage in texting while driving a CMV, according to [49 CFR 392, Subpart H](#). The only occasion where either is permissible is when drivers are communicating with law enforcement officials or other emergency services."²

Keeping the words of the FMCSA in mind, we examine the following scenario.

A catastrophic truck accident occurs. The first to respond to the scene – be that law enforcement, a company representative, or counsel – performs what I call "thumb forensics" on the mobile phone to see if any text messages were sent or read contemporaneous to when the accident occurred.

The driver of the truck received five text messages in the timeframe of interest. However, the driver had never looked at these messages. By thumbing through the phone, the first responder is changing the status of these messages from *unread* to *read*. Now, the knowledge of the content of those messages, as well as having seen those messages would be attributed to the driver. If the phone had been handled properly, those messages could not be used as evidence of driver distraction, because there was no evidence of distraction.

¹ <https://www.friedgoldberg.com/request-trucking-claims-book/cellphone-evidence/>

² <https://csa.fmcsa.dot.gov/safetyplanner/MyFiles/SubSections.aspx?ch=23&sec=68&sub=170>

In other words, the first responder's actions caused all of the evidence on the phone to become suspect. If gone unchecked, this mishandling of the evidence would lead a judge and jury to a false conclusion. As triers of fact, the judge and jury would have wrongly attributed knowledge of the mobile phone's message contents, state, and time stamps to the defendant.

Protecting the Evidence

The initial handling of digital evidence can be divided into four phases composed of identification, collection, acquisition, and preservation. Any deviation by an examiner from these phases can be challenged.

Identification

The identification phase's purpose and scope are to identify sources of digital evidence relevant to the case. This evidence can span multiple devices, systems, servers, and cloud accounts. For mobile phones, relevant data can be located on the internal storage of the phone, in CDRs, cloud accounts like the Apple iCloud or Google Drive, and other synced devices. For example, since messages sync between devices, even if the phone goes missing records of those messages could exist on the user's tablet or laptop computer.

Collection

The primary goal of the collection process, other than ensuring all relevant electronic items are collected, is to protect digital evidence from contamination.

Isolating Device Users

One way this is done is by isolating the devices from their respective users until a forensic acquisition of the mobile device can be performed. While in their custody, the user or first responder could delete, create, or change data before the forensic acquisition (the perfect snapshot in time of the mobile phone data) is performed. They could also factory reset or wipe the device, permanently destroying some data or potentially everything on the mobile phone.

Isolating Devices

Along with isolating the mobile phone from the user, we also need to isolate the device itself. By design, mobile phones are intended for communication, and they are continually sending and receiving data even when they are on the bedside table charging overnight. If data transmission occurs, even with no person physically touching the phone, data can be lost, changed, or destroyed.

Isolation of the device itself is achieved by eliminating all forms of data transmission, including the cellular network, Bluetooth, wireless networks, and infrared connections. Isolating the phone from all networks prevents it from receiving any new data that would cause other data to be deleted or overwritten.

Isolating the device is done by using Faraday technology. A Faraday bag blocks signal that a cell phone might pick by isolating it from electrical fields and radio frequencies. A microwave uses this same technology, utilizing a Faraday cage to contain the magnetron's radio frequency within the cooking

chamber. A cell phone can also be isolated from networks by placing it into Airplane mode with wireless network connectivity turned off. A first responder should do this if they don't have access to Faraday technology.

Forensic Acquisitions

The forensic acquisition process encompasses all the methods and procedures utilized to collect digital evidence in digital forensics. With mobile phones, the acquisition methods used are determined by multiple factors, including the cell phone's make, model, operating system, and physical damage

Regardless of the method used, when a mobile phone is forensically copied, all contents go inside a special forensic file type. The contents recovered from the phone are encapsulated in this forensic file and are tamperproof. If any manipulation did occur, the hash algorithm, or digital DNA, would report a different number. This is a clear indication to an examiner that the evidence is not as it purports to be.

Forensic acquisition puts a bow on the whole process. At this point, you have a perfect snapshot in time of the data that exists on the phone that is tamperproof. However, as we have already discussed, you have to get here first. If a first responder mishandled the phone before the data was forensically extracted, we are extracting potentially compromised data.

Preservation

Chain of Custody

Evidence preservation protects digital evidence from modification. Protection begins by ensuring that anyone who touches the device handles it correctly. A chain of custody must be maintained throughout the life cycle of a case. It should identify who collected the mobile phone, including name, title, organization, and contact information. Whenever the evidence is transferred from persons and locations, it should be documented. Dates and times should accompany all activities.

Digital DNA – Hash Algorithms

The forensic data collection process from the mobile device is commonly called a "forensic extraction" or "forensic acquisition." Following forensic copying comes hashing, where a mathematical algorithm is run against the copied data, producing a unique hash value. This hash value can be thought of as a digital DNA, uniquely identifying the copied evidence exactly as it exists in that point in time.

But My Driver Needs Their Phone

In the United States, 96% of the population owns a cell phone, up from only 35% in 2011.³ Near-complete adoption, progressively faster cellular networks, and the ever-growing list of applications mean that we are more dependent on our phones today than ever before. So it is no wonder that this is the most common objection we encounter to gaining access to the driver or plaintiff's phone.

Taking a driver's phone is sometimes not an option. However, this does not mean that the evidence on the phone is out of reach. The solution is to transfer data from the driver's current phone to a new

³ <https://www.pewresearch.org/internet/fact-sheet/mobile/>

phone so that the evidentiary value is preserved while also providing the driver their data so these road warriors can function unimpeded. Protocols designed for digital forensic experts for laypersons exist for precisely this purpose.

The Stakes Have Never Been Higher

From 2010 to 2018, the average verdict size for lawsuits above \$1 million in motor carrier accident cases has increased nearly 1000%, rising from \$2.3 million to \$22.3 million⁴. To quote Joe Fried once again,

"The two main driver distractions that have received most of the publicity in the news is use of cellphones and on-board computer messaging systems. The FMCSA prohibits any texting while driving. Texting is defined as any "electronic text retrieval or entry, short message service, emailing, instant messaging, accessing the internet, or pressing more than a single button to make a or receive a call." Regulations also require a truck driver to use a hands-free cellphone while driving. Most CDL manuals warn against using cellphones in any manner while driving a commercial vehicle."⁵

Plaintiff attorneys know the value of the evidence contained on mobile phones in trucking accident cases. Mishandling a phone opens the door to question the integrity of the mobile phone data and compromises the ability to introduce exculpatory evidence in the case.

Fried notes that drivers should be using hands-free technology, and in doing so, he illustrates our point. We can often tell if a driver used voice commands or hands-free technology to compose or listen to messages using digital forensics. However, using only CDRs, it cannot be determined if the messages were created or viewed with voice commands or with eyeballs and thumbs on the screen.

Properly preserving and handling cell phones following a collision not only protects the evidence; it safeguards potential defenses in the case and saves motor carriers, and their insurers on litigation spend, settlements, and verdict awards.

END

⁴ <https://www.cnn.com/2021/03/24/rise-in-nuclear-verdicts-in-lawsuits-threatens-trucking-industry.html>

⁵ <https://www.friedgoldberg.com/request-trucking-claims-book/theories-of-liability/>

Resource Packet for Legal Professionals

Lars Daniel, EnCE, CCPA, CCO, CTNS, CTA, CIPTS, CWA
Practice Leader – Digital Forensics at Envista Forensics

M: 919-621-9335 // lars.daniel@envistaforensics.com

This document is ever-changing. Our team is consistently adding and updating information. You can contact me to check for the most up-to-date version. *Disclaimer: None of our experts are attorneys, and we do not offer legal advice. Nothing in this resource guide should be viewed as providing legal advice or instruction.*

.....	1
RESOURCE PACKET FOR LEGAL PROFESSIONALS	1
LARS DANIEL, ENCE, CCPA, CCO, CTNS, CTA, CIPTS, CWA PRACTICE LEADER – DIGITAL FORENSICS AT ENVISTA FORENSICS.....	1
CALL DETAIL RECORD SUBPOENA LANGUAGE	3
AT&T WIRELESS	4
VERIZON WIRELESS	6
T-MOBILE/METRO PCS	8
SPRINT CORPORATION	10
CELL SITE LIST REQUEST	12
MOBILE VIRTUAL NETWORK OPERATOR (MVNO) SUBSCRIBER/BILLING REQUEST	13
CALL DETAIL RECORDS – WHAT YOU SHOULD GET IN DISCOVERY FROM OPPOSING COUNSEL.....	14
VERIZON WIRELESS	14
SPRINT	14
AT&T/CRICKET	15
T-MOBILE / METROPCS	15
GOOGLE LOCATION HISTORY SUBPOENA LANGUAGE	16
VIDEO RECORDING SYSTEM (DVR) SUBPOENA LANGUAGE	18
GPS (GLOBAL POSITIONING SYSTEM) RECORDS SUBPOENA LANGUAGE	20
DIGITAL EVIDENCE GENERIC ESI REQUEST	22
WITH REGARD TO ANY ELECTRONIC DATA THAT YOU EXPECT TO USE AS EVIDENCE	22
WITH REGARD TO ANY PERSON WHOM YOU EXPECT TO CALL AS AN EXPERT	22
WITH REGARD TO THE USAGE, OPERATION AND MAINTENANCE OF THE SERVERS	23
CELL PHONE PRESERVATION LETTER	24
CELLULAR ACCOUNT PRESERVATION LETTER	26
VIDEO EVIDENCE PRESERVATION LETTER.....	28
MOTION TO COMPEL PRODUCTION OF CELLULAR PHONE (EXAMPLE).....	29

TEMPORARY RESTRAINING ORDER + ORDER FOR EXPEDITED ESI DISCOVERY	31
DIGITAL EVIDENCE EXAMINATION PROCEDURE (EXAMPLE).....	34
DIGITAL DEVICE EXAMINATION PROCEDURES OF MAKE AND MODEL	34
PRIVACY PROTECTION.....	34
NON-DESTRUCTIVE PROCESS.....	35
EVIDENCE TRANSFER.....	36
CHAIN OF CUSTODY	36
CONDITION	36
RESEARCH	37
REPAIR (If required).....	37
EXTRACTION.....	38
EXTRACTION RESULTS.....	39
POST EXTRACTION	39
VALIDATION	39
ANALYSIS.....	39
EVIDENCE RETURN.....	41
CONFIDENTIALITY	41
FACEBOOK SUBPOENA LANGUAGE/ SELF-DOWNLOAD.....	42
SUBPOENA LANGUAGE	42
DOWNLOAD FACEBOOK ACCOUNT (REASON)	43
DOWNLOAD FACEBOOK ACCOUNT (INSTRUCTIONS).....	45
ADAM WALSH ACT (CHILD EXPLOITATION) LANGUAGE	47
LANGUAGE FOR ACCESS TO EVIDENCE IN CHILD EXPLOITATION CASES.....	47
GUIDE –DIGITAL FORENSICS IN CHILD EXPLOITATION CASES – FINDING YOUR WAY THROUGH	49
<i>About the Authors</i>	49
<i>Introduction</i>	49
<i>Uniqueness of Child Exploitation or Child Pornography cases</i>	49
<i>Law Enforcement Investigations: Before the Search Warrant</i>	49
<i>Law Enforcement Investigations: After the Search Warrant</i>	52
<i>Defense of Child Pornography Cases</i>	54

Call Detail Record Subpoena Language

If you do not see the carrier you are looking for, particularly Tracfone or other prepaid (Mobile Virtual Network Operators (MVNO) 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/>

AT&T Wireless

AT&T Wireless

11760 US Highway 1 Suite 600 North Palm Beach, FL 33408

Contact Phone Number: 800-635-6840

SERVICE BY FAX OR EMAIL: 888-938-4715 or gldc@att.com

Language:

Defendant, by and through their attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records with cell site locations tower location listings, 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. Call Detail Records with cell site location, 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 legend and definition for any and all abbreviations used in the reports provided
7. An explanation of how to read the call detail records.

8. 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.

9. 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:

Mobile Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC), System Identification Number (SID), Network Identity (NID), Tracking Area Code (TAC), Cell ID, E-UTRAN Cell Global Identifier (ECGI), eNodeB ID (eNBID), Technology, Band, Frequency, Channel, EARFCN, Sector Identifier, Sector Orientation (azimuth), Beamwidth, PCI, PSC, PN Offset, and Tower Height.

10. 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

180 Washington Valley Road Bedminster, NJ 07921

Contact Phone Numbers: Subpoena contact: 888-483-2600

SERVICE BY FAX :Subpoenas: 888-667-0028

Orders & Warrants: 888-667-0026

Language:

Defendant, by and through their attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records with cell site locations tower location listings, for cell phone number(s) 000-000-0000 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. Call Detail Records with cell site location, 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 with cell sites.
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 Mobile Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC), System Identification Number (SID), Network Identity (NID), Tracking Area Code (TAC), Cell ID, E-UTRAN Cell Global Identifier (ECGI), eNodeB ID (eNBID), Technology, Band, Frequency, Channel, EARFCN, Sector Identifier, Sector Orientation (azimuth), Beamwidth, PCI, PSC, PN Offset, and Tower Height.

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, ALULTE 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.
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/Metro PCS

4 Sylvan Way

Parsippany, New Jersey 07054

Contact: 866-537-0911

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

Language:

Defendant, by and through their attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records with cell site locations tower location listings, for cell phone number(s) 000-000-0000 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. Call Detail Records with cell site location, 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. Cell Site List including; Mobile Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC), System Identification Number (SID), Network Identity (NID), Tracking Area Code (TAC), Cell ID, E-UTRAN Cell Global Identifier (ECGI), eNodeB ID (eNBID), Technology, Band, Frequency, Channel, EARFCN, Sector Identifier, Sector Orientation (azimuth), Beam width, PCI, PSC, PN Offset, and Tower Height.

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.

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

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 their attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records with cell site locations tower location listings, for cell phone number(s) 000-000-0me 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. Call Detail Records with cell site location, 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;
 - a. Cell Site List including; Mobile Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC), System Identification Number (SID), Network Identity (NID), Tracking Area Code (TAC), Cell ID, E-UTRAN Cell Global Identifier (ECGI), eNodeB ID (eNBID), Technology, Band, Frequency, Channel,

EARFCN, Sector Identifier, Sector Orientation (azimuth), Beamwidth, PCI, PSC, PN Offset, and Tower Height.

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. Include reports for VOVoice (VOWIFI, VOLTE, VOCDMA)
11. Specific information regarding the time stamps / time zones of the records.
12. 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](#)

Cell Site List Request

This request should be used for all carriers, and is important to complete an analysis or cell site survey.

Look up each carrier and their subpoena compliance info using, <https://www.search.org/resources/isp-list/>

Language:

Please include a list of the following information regarding Cell Sites for the State of **Insert State, during Insert Month, Year.**

To include (but not limited to):

Mobile Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC), System Identification Number (SID), Network Identity (NID), Tracking Area Code (TAC), Cell ID, E-UTRAN Cell Global Identifier (ECGI), eNodeB ID (eNBID), Technology, Band, Frequency, Channel, EARFCN, Sector Identifier, Sector Orientation (azimuth), Beamwidth, PCI, PSC, PN Offset, and Tower Height.

Please provide the list in excel, .csv or similar format.

Please respond to this subpoena via email to: **your email & Expert with Envista Forensics**

Mobile Virtual Network Operator (MVNO) Subscriber/Billing request

This request can be used for all MVNO, and supplements the call detail record request to the company providing cell service. Look up each carrier and their subpoena compliance info using,

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

A separate request needs to be made to the company providing service (ie. Verizon, AT&T)

Language:

Defendant, by and through their attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records with cell site locations tower location listings, for cell phone number(s) 000-000-0me between 00-00-2000 and 00-00-2000.

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.
3. Records are to include the IMEI, IMSI or other equipment or handset identification information for the target phone number if known.
4. A legend and definition for any and all abbreviations used in the reports provided.
5. An explanation of how to read the call detail records.

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](#)

Call Detail Records – What You Should Get in Discovery from Opposing Counsel

Subpoena responses and warrant returns from wireless phone companies will contain specific files that are delivered via email, on disk or via a secure web portal. It is very important that you received all of the files returned to the requester. Also, copies of the original subpoena and or warrant with the affidavit are very helpful for your expert.

There are spreadsheets and documents that provide such information as subscriber information; the call detail records themselves, cell tower location keys, explanation forms and disclaimers. These disclaimers are important, as they provide pertinent information regarding location accuracy or time-zone information. Each carrier stores their records in various formats and below you will find the specific data you should receive organized by four of the major carriers. Other carriers like US Cellular follow a similar pattern.

Verizon Wireless

Verizon Wireless call detail records also require a cell tower key to determine the location of the towers in the area. Call detail records will often be labeled "Cell sites incoming outgoing" and the tower key will contain a city name and "LEA". Verizon records may also contain Voice Over LTE records which will contain "VOLTE" in the spreadsheet name. If requested in the proper timeframe, you may receive Real Time Tool records, the spreadsheet name will contain "RTTM". Verizon also provides subscriber information, explanation information for each of the different spreadsheets as well as disclaimers. Each of the spreadsheets containing location information will be in Microsoft Excel format and explanation forms are typically in Portable Document Format (.pdf).

Sprint

Sprint also provides call detail records and cell site keys in separate spreadsheets. Again, both are needed to analyze the records. Sprint's records also come in Microsoft Excel format and are typically labeled with a number. There will be several spreadsheets all containing the various information. They may also provide Per Call Measurement Data (PCMD) if requested in the proper timeframe. Sprint also provides need explanation forms and disclaimers.

AT&T/Cricket

provides their call detail records and text detail, with location information, in one spreadsheet. This is typically labeled "Reports AU" and comes in two formats, Text format (.txt) and Portable Document Format (.pdf). This is standard for all requests, unless otherwise specified. At&t will provide subscriber information, as well as needed explanation forms and disclaimers. At&t may also provide, if requested, Network Event Location Service (NELOS) data. It is important for your expert to receive the text format (.txt) files for analysis, this format allows for data to be imported into various software platforms for converting time zones and analysis.

T-Mobile / MetroPCS

T-Mobile / MetroPCS provides call detail records in Microsoft Excel spreadsheets that are typically labeled "CDR Mediations". This spreadsheet will provide the call record as well as the tower location information needed. Subscriber information will be provided and explanation forms will also be provided. Depending on the year the records were provided, they may be kept in different time-zones, for this reason the explanation form is important. No other location information is available from T-Mobile at this time.

Google Location History Subpoena Language

Request the following for accounts: googleuser@gmail.com

INFORMATION SOUGHT: Google location services to include: account information, date, time (UTC), latitude, longitude, maps display radius (accuracy in meters), device source, device tag, and platform.

FOR THE DATE RANGE: **December 5, 2015**

SEND TO:

Google, Inc.

Contact Google Legal Investigations Support

Name:

Online 1600 Amphitheatre Parkway

Service Mountain View, CA 94043

Address:

Phone (844)383-8524

Number:

E-mail uslawenforcement@google.com

Address:

Note(s): For a faster response time, submit your legal requests through the Law Enforcement Request System (LERS). The system requires each user to register for a unique account to submit legal requests. Register for an account at <https://support.google.com/legal-investigations/contact/LERS>

From Googles LERS FAQ:

<https://lers.google.com/u/2/app/faq>

"Notwithstanding Title 18, United States Code, Section 2252A [or similar statute or code] Google shall disclose responsive data, if any, by delivering encrypted files through Google's Law Enforcement Request System"

Oct 2016: telephone number listed for google and the message said the number has changed. The message said the new number is (844)383-8524 or (650)417-9011

Questions can be emailed to USLawEnforcement@google.com

For Emergency Disclosure Requests leave a message with details of the emergency and your contact information at 650-253-3425. Google will only return calls from sworn law enforcement officers handling emergency situations.

Google has launched a new Law Enforcement System. Here is the link to sign up in advance for an account:

<https://support.google.com/legal-investigations/contact/LEERS>

Last Updated: July 2017

Previous Information: As of Feb, 2016: Voice # :650-253-3425 In February 2015, Notes was: For a faster response time, Google has created a web form for submitting legal demands. Use of fax and email are still options for delivering, but the web form is preferred by Google: Google Legal Portal: <https://support.google.com/legal-investigations>. For Custodian of Records and Legal Investigations Support call the "Emergency Disclosure Request" department at: 650-253-3425. Leave a message and an agent will call you back. For search warrant requests, please send them to: Email: USLawEnforcement@google.com (preferred by Google) or by Fax: 650-249-3429. Attention: Custodian of Records Google, Inc. 1600 Amphitheatre Parkway Mountain View, CA 94043 At Google's request, please include the following language in any subpoena: "Please do not disclose/notify the user of the issuance of this subpoena. Disclosure to the user could impede an investigation or obstruct justice." Additionally, please include the following in your search warrant "Google shall disclose responsive data, if any, by sending to [LE's postal address] using the US Postal Service or another courier service, notwithstanding 18 U.S.C. 2252A or similar statute or code." Google will disclose release of information unless in violation of law or court order or if convinced doing so will place a child at risk. A short affidavit arguing the last will be considered. Google does not disclose preservation of data actions to account holders. For Gmail: Custodian of Records and Legal Investigations Support can be reached at: 650-253-3425. For search warrant requests, please submit them to: Email: USLawEnforcement@google.com(preferred by Google) or by Fax: 650-249-3429. Attention: Custodian of Records Google, Inc. 1600 Amphitheatre Parkway Mountain View, CA 94043 At Google's request, please include the following language in any subpoena: "Please do not disclose/notify the user of the issuance of this subpoena. Disclosure to the user could impede an investigation or obstruct justice."

Video Recording System (DVR) Subpoena Language

- 1) Any and all records related to the recording device , specifically for the period of time beginning on _____ and ending upon _____ used in the recording of the interviews of persons _____ and _____

- 2) All information related to the recording device including but not limited to:
 - a. user manuals
 - b. service records
 - c. training materials
 - d. installation manuals
 - e. manufacturer, make, model, and serial number
 - f. date the recording device went into service
 - g. known issues or problems with the recording device
 - h. firmware version
 - i. software version

- 3) Any and all maintenance records for the recording device.

- 4) Any and all information concerning the recording device hardware in regards to the installation and operation. This information is to include, but is not limited to how it is installed in the facility, and any possible errors in the installation that could have an effect on the operation of the recording device.

- 5) Any and all information concerning the software and firmware of the recording device. This information is to include, but is not limited to how the software and firmware are installed on the recording device, how any upgrades to the software and firmware have been performed,

and any possible errors in the installation of the software or firmware that could have an effect on the operation of the recording device.

- 6) The qualifications, resume, curriculum vitae, and any records related to the training of the person who created and/or exported the video and audio recordings from the recording device for the persons _____ and _____.

- 7) Any protocols, operation manuals, guidelines, standard operating procedures, and any and all documents created by the (LAW ENFORCEMENT AGENCY/PRIVATE COMPANY) concerning the particular recording device, audio forensics, video forensics, chain of custody in relation to video and audio, and the preservation methods of video and audio.

- 8) Any and all documentation, reports, narratives, or other documents concerning the method by which the video recordings were extracted from the device to include, but not limited to, the quality settings, file type, and compression ratio.

- 9) Any and all documentation, reports, narratives, or other documents concerning the settings of recording device between the dates of _____ and _____ including, but not limited to, the quality settings, number of cameras, multiplexing, file type, import settings, export settings, compression ratio, encryption, and audio settings.

GPS (Global Positioning System) Records Subpoena Language

- 1) Any and all records related to the GPS records identified by serial numbers _____ specifically for the period of time beginning on _____ and ending upon _____.

- 2) All Information related to GPS units identified by serial numbers _____ and _____, to include but not limited to GPS activity such as powering up, powering down, distance traveled, mileage, latitude and longitude, location by address, speed of travel, distance traveled, long stop, short stop, dilution of precision ratings, and so forth.

- 3) Any information that is available regarding the physical GPS units installed in the vehicle(s) identified by GPS Unit serial number(s) _____. This is to include, but is not limited to; user manuals, installation manuals, owner manuals, manufacturer, make, model, dates units went into service, dates units went out of service, known issues or problems with GPS models such as loss of signal, problems with calibration, pinging, areas of service, problems due to extraneous factors such as weather and so forth.

- 4) Any information that is available regarding the software used by both Vehiclepath.com and their clients. This is to include, but is not limited to; user manuals, installation manuals, owner manuals, online documentation, known problems with the software either used by Vehiclepath.com or their clients, user errors that could have an effect upon GPS records, and so forth.

- 5) Any and all maintenance records for the GPS units identified by serial number(s) _____.

- 6) A list of all GPS units supported by COMPANY NAME'S tracking system up to MONTH of 20XX.

- 7) Any and all information on the GPS units regarding their installation and operation. This information is to include, but is not limited to how and where they are installed in vehicles, possible errors in installation that could have an effect on GPS records, how the tracking ability of GPS units could be manipulated by being turned on and off by the user, otherwise disabling of the GPS unit, the use of software or hardware that could modify the unit, other ways of intentionally causing a GPS unit to function in any way other than intended.

Digital Evidence Generic ESI Request

With regard to any electronic data that you expect to use as evidence in this case, please produce the following:

1. a duplicate of any forensic copies made by the expert of any computer hard drive, digital storage media including but not limited to CD-ROMS, USB flash drives, floppy disks, memory cards, digital camera storage, smart cards and portable hard drives.
2. a complete inventory of all items supplied to the expert that may contain any type of digital data, whether or not such items were examined or copied by the expert.
3. a complete copy of all forensics reports, chain of custody records, and lab notes generated by the expert pertaining to the acquisition, preservation, analysis, and or reporting by said expert.
4. any documents produced from the electronic sources examined by the expert in this case, both in printed and electronic formats, including, but not limited to:
 - a. log files;
 - b. any or all printer artifacts;
 - c. user access histories;
 - d. user account information including all known access times to the server by any of the persons named in this lawsuit;
 - e. user account information including security levels and access control lists;
 - f. user account information including user names, account type and passwords;

With regard to any person whom you expect to call as an expert witness at the trial of this case, please produce the following:

- 1) All materials and documents of any kind in the possession, custody, or control of the expert witness that pertain to the subject matter of this case, including, but not limited to, all correspondence between you and the expert witness, all correspondence between your attorney and the expert witness, all e-mail communications between you and the expert witness, all e-mail communications

between your attorney and the expert witness, all notes that pertain to the subject matter of this case, all diaries or personal journals that pertain in any manner to the subject matter of this case, and all records, depositions, statements, transcripts, reports, writings, drawings, graphs, calculations, estimates, exhibits, charts, photographs, audio tapes, video tapes, plans, invoices, bills, and receipts from any source that relate in any manner to this litigation;

- 2) All documents prepared by the expert that pertain to this case, including, but not limited to, true, correct, and complete copies of all reports concerning this case that have been prepared by the expert. This request for production specifically includes all preliminary drafts of reports as well as final drafts of reports;
 - a) All documents that you or your attorney or any of your representatives have sent to the expert witness that pertain in any manner to this case;
 - b) All documents, data, or other information used, considered, or reviewed by the expert witness that pertain in any manner to this case;
 - c) All documents that pertain to any compensation agreement for the expert's services in this case;
 - d) All documents that have been or will be shown to the expert prior to the expert's trial testimony; and,
 - e) All documents, including current curriculum vitae, used to establish the expert's qualifications as an expert witness.

With regard to the usage, operation and maintenance of the servers,

software and or computers in this case, please provide the following:

- 1) Any and all software manuals, including but not limited to user manuals, training materials, administrator manuals and setup guides for the software that may contain customer data.
- 2) Any and all maintenance records, including invoices, paid or unpaid, from any vendor involved in the maintenance of the servers, patient accounting software, or other electronic sources of information that will be used as evidence in this case. Such records are to include trouble tickets, user setup tickets, service tickets, password changes, password settings, user account lists, administrative changes and training session information.
- 3) Any administrative records regarding the installation, maintenance and or usage of the server, the computer network and the patient records software.

Cell Phone Preservation Letter

Cell Phone Preservation / ESI

[date/address]

Re: Notice to Preserve Electronic Evidence [Legal Matter]

Dear _____ :

Our law firm represents [name] in the above legal matter in which you [your business] are [is] [will be] named as a defendant. This letter requests your immediate action to preserve electronically stored information that may contain evidence important to the above legal matter. Briefly, the matter involves [short statement of facts in case].

This notice applies to your [custodian] cell phone, cell phone backups, removable electronic media, and computer systems. This includes, but is not limited to, e-mail and other electronic communications; electronically stored documents, records, images, graphics, recordings, spreadsheets, databases; calendars, system usage logs, contact manager information, telephone logs, internet usage files, deleted files, cache files, user information, and other data. Further, this notice applies to archives, backup and disaster recovery tapes, discs, drives, cartridges, voicemail and other data. All operating systems, software, applications, hardware, operating manuals, codes, keys and other support information needed to fully search, use, and access the electronically stored information must also be preserved.

The importance of immediate action cannot be overstated. Electronically stored information is easily corrupted, altered, and deleted in normal daily operations. Even booting an electronic device, running an application, or reviewing a document can permanently alter evidence.

The cell phone should be powered off, sealed inside of an evidence container, and placed in secure evidence storage until such a time whereas a cell phone forensics expert can create a forensic image of the device. Full chain of custody should also be kept.

Further, any external media or computer system used to create backups of the cell phone should also be powered off according to digital forensics best practices, placed into sealed evidence containers, and securely stored until forensic images of the evidence items can be created. Full chain of custody should also be kept.

Online accounts associated with the cell phone, including but not limited to, social media accounts, application based accounts, cloud data storage accounts, email accounts, messaging accounts, and/or any other application than can be accessed via the cell phone device should be preserved.

[If known, identify any key persons', officers', supervisors', and employees' computers to which special attention for forensic imaging must be directed.] This preservation notice covers the above items and information between the following dates: [state dates].

Follow the above procedures to preserve electronic information created after this notice. Current law and rules of civil procedure clearly apply to the discovery of electronically stored information just as they apply to other evidence, and confirm the duty to preserve such information for discovery.

You [company] and your officers, employees, agents, and affiliated organizations must take all reasonable steps to preserve this information until this legal matter is finally resolved. Failure to take the necessary steps to preserve the information addressed in this letter or other pertinent information in your possession or control may result in serious sanctions or penalties. Further, to properly fulfill your preservation obligation, stop all scheduled data destruction, electronic shredding, rotation of backup tapes, and the sale, gift or destruction of hardware. Notify all individuals and affiliated organizations of the need and duty to take the necessary affirmatives steps to comply with the duty to preserve evidence.

Sincerely, [attorney/address]

Cellular Account Preservation Letter

Date

Dear Custodian of Records,

Now comes _____, by and through his attorney, and requests the following information be preserved regarding cell phone communications for cell phone number(s) **000-000-0000 and 000-000-0000**. _____ requests that the data and information outlined below be preserved to include the time period of _____ to _____ for a period of 180 days beginning on 00/00/2018. If and when additional preservation time is needed, or if the time that the data is preserved is extended, an additional preservation order will be presented for that purpose.

All information including but not limited to:

Subscriber information for the above listed numbers, including financially responsible party, social security number, billing address, features and services and equipment,

2. Call Detail Records with cell site location, 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, 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, ICCID or other equipment or handset identification information for the target phone number.

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

5. Beginning and ending switch and cell site / tower identifiers for each call, SMS MMS and data transmission.

6. Central office identifiers and or switch identifiers for the area of coverage for the time period requested

7. All connection attempts including completed and failed connections with call duration times to one second

8. Any available information regarding the state of the towers for the time period requested, including trouble tickets, maintenance tickets, maintenance schedules and tower downtime records.

9. Any precise measurement data or call detail records with cell site such as, PCMD, RTT, RTTM, RTTL, ERLTE, ALUTE, NELOS, VOLTE, Truecall, TDOA, VOVoice, VOWIFI, VOCDMA e-911 location data, and or any other data recorded for the timeperiod that will provide additional location data.

10. Any information or event activities related to law enforcement activities regarding these phone number to include, but not limited to, a. Pen trap and trace activity

- Content captured or any other CALEA data provided to law enforcement, with or without a warrant or court order for the phone number or numbers for this request.
- Any location data provided to law enforcement under CALEA or as the result of any filing or request by law enforcement for such data.

Respectfully submitted,

Name

Video Evidence Preservation Letter

DATE:

Dear Legal Department,

My client is the subject of an ongoing criminal investigation in which surveillance video from your location, **(Store name, address, city, state)** was initially collected by the **(police department or agency)**.

In preparation for criminal litigation in this matter, I am requesting that the video device and video data for the surveillance system located at the aforementioned location be preserved in total and specifically for the period of **(date and time through date and time)**.

I am also requesting that you allow our office to have an independent forensics expert travel to the location and collect the original video data for preservation purposes.

Please respond immediately as time is of the essence due to the limited storage capability of video surveillance systems. It is imperative that we collect this data as soon as possible.

You can respond to this request via email to email@email.com or via facsimile to 555-555-5555.

Sincerely,

ATTORNEY NAME

Motion to Compel Production of Cellular Phone (Example)

Motion to Compel Production of Cellular Phone

Please modify the facts to suit your case.

Comes now DEFENDANT, by and through his attorney ATTORNEY NAME, and moves this Court to compel production of the alleged victim's cellular phone for forensic examination.

DEFEDANT is charged with _____, of the most serious offenses under STATE law. Considering the seriousness of this charge, it is absolutely imperative that DEFENDANT have all relevant resources available for his defense.

FACTS of the case:

On _____, 20XX, VICTIM claimed that DEFENDANT sexually assaulted her in her hotel room. Her claim is that she left her hotel room door open in anticipation of a friend's later arrival and then fell asleep. She further claims that the defendant entered her room and sexually molested her.

It is the defendant's belief that evidence contained in the electronic storage of her cellular phone (smart phone), specifically related to Twitter messages she sent to the Internet and subsequently deleted from her Twitter timeline can be recovered from the cellular phone device and that such "tweets" are critical to his defense.

In the same way that evidence collected from a cellular phone can be used to link a perpetrator to a victim, in this case, such evidence can be used to show that the victim posted information related to the alleged assault to the Internet via the service, Twitter, via "tweets", that is in conflict with her account of the crime.

Therefore the defendant respectfully requests that the court compel the alleged victim to produce the cellular "smart" phone for forensic examination for evidence of said "tweets" and other electronic communications, including email and other correspondence that would prove exculpatory to the defendant.

Forensic examinations of cellular phones are conducted every day on a routine basis by law enforcement agencies in the US and such examinations yield a great deal of evidence that is brought to bear in cases by the government. _____ is simply asking the court to allow an expert in cellular phone examinations to provide the same services for the purpose of producing exculpatory evidence

that the victim may have produced communications that are in conflict with her claims via the use of her cellular phone.

Such forensic examinations are well known at this point in time with current forensic examination methods to have the ability to recover information and data that has been deleted from cellular phones, even for a significant period of time after such a deletion has occurred.

Due to the personal nature of a cellular phone, in that such devices are carried on or about a person nearly at all times, this makes the cellular phone a critical repository of evidence and as such, should be produced for examination by the defense's expert, in the same way that a defendant's cellular phone would have been examined by the government's expert in a criminal case with an accusation of such a serious crime as this one.

Temporary Restraining Order + Order for Expedited ESI Discovery

Temporary Restraining Order and Order for Expedited Discovery

THIS CAUSE came on to be heard before the undersigned Superior Court Judge Presiding over the Civil Session of _____ County Superior Court, on ____, on Plaintiff's Motion for Temporary Restraining Order and for Expedited Discovery.

The Court, having reviewed the pleadings of record, finds that the Plaintiff has shown that reasonable grounds exist to believe the following:

1. This is an action by Plaintiff seeking damages and injunctive relief relating to Defendants _____ and _____ breach of a contract containing a covenant not to compete: and relating to all Defendants misappropriation and use of Confidential Information and trade secrets of Plaintiff.
2. Defendants do business in competition with Plaintiff, and using Confidential Information and trade secrets of Plaintiff, _____, from a location whose address is _____ (“The Business Location”).
3. Defendants have misappropriated and used Confidential Information and trade secrets of Plaintiff: the Confidential Information and trade secrets are stored on computers owned or operated by Defendants which are a the Business Location (and which may be at other locations): and Defendants may secrete or destroy evidence of their use of the same irreparably and immediately injuring the Plaintiff if they are not enjoined from doing so.

BASED UPON THE FOREGOING FINDING OF FACT, THE COURT CONCLUDES AS A MATTER OF LAW that a temporary restraining order should be entered, preventing Defendants from removing, destroying, or tampering with any of the computers; hard drives, disks, CDs, DVDs, memory sticks, thumb drives, or any other medium upon which information is stored electronically, that they may have at any location.

BASED UPON THE FOREGOING FINDINGS OF FACT, THE COURT FURTHER CONCLUDES AS A MATTER OF LAW that an order should be entered granting expedited discovery by permitting Plaintiff's inspection and copying of all of the computers; hard drives, disks, CDs, DVDs, memory sticks, thumb drives, magnetic tapes, or any other medium upon which information is stored electronically, which are at the Business Location.

NOW, THEREFORE, IT IS HEREBY ORDERED, ADJUDGED AND

DECREED AS FOLLOWS:

1. Defendants are temporarily restrained and enjoined from removing, destroying, or tampering with any of the computers; hard drives, disks, CDs, DVDs, memory sticks, thumb drives, magnetic tapes, or any other medium upon which information is stored electronically, that they may have under their possession, custody or control, at any location.
2. Hearing on Plaintiff's motion for preliminary injunction, extending the restraints set forth herein, shall be held in the _____, _____ of _____ at _____ on the ____ day of ___, 2010, or as soon thereafter as may be reached.
3. Plaintiff shall post as a bond, with respect to entry of the restraints set forth, the principal amount of \$_____.

IT IS FURTHER ORDERED, ADJUDGED AND DECREED as follows:

1. Defendants shall allow representatives of Plaintiff to enter the Business Location (_____) and conduct an examination of any of the computers; hard drives, disks, CDs, DVDs, memory sticks, thumb drives, or any other medium upon which information is stored electronically, which are at the Business Location. Such examination may include copying of all hard drives, disks, CDs, DVDs, memory sticks, thumb drives, or any other medium upon which information is stored electronically. Defendants may permit Plaintiff's representatives to remove such items to expedite copying process, or may permit the inspection and copying to be performed at the Business Location, as Defendants may elect.

2. Defendants shall permit the entry and copying described above beginning at ___ on the ___ day of _____, 2010 and continuing until finished.
3. The _____ Sheriff shall serve this Temporary Restraining Order and Order for Expedited Discovery upon Defendants as immediately as possible.
4. The information discovered in response to the inspection and copying permitted herein shall be used by Plaintiff solely for the prosecution of its claims, and for no other purpose whatsoever, unless and until the Court orders otherwise.

Superior Court Judge

DATE AND TIME ENTERED: _____

Digital Evidence Examination Procedure (Example)

If an expert is appointed or retained onto a case, they should provide a procedure detailing how evidence will be handled and examined. If they have no such protocol, I would question their capability and training. Protocols provide a roadmap for you, opposing counsel, and their expert.

A comprehensive procedure can help you get things done, moving the ball forward in your case. Often, both parties want the evidence contained on the mobile phone. However, concerns of those involved can impede the process. These concerns center on how evidence will be handled and if the examiner will properly protect the device's data or the device itself, as well as how much of the data the examiner and opposing attorney have access to.

Here is an example protocol our team developed for a transportation (trucking) accident case:

Digital Device Examination Procedures of MAKE AND MODEL

PRIVACY PROTECTION

A representative of Envista Forensics' Digital Forensics group will perform a forensically sound acquisition or extraction of data from the computers, cell phones, GPS devices, or electronic storage devices.

The forensic hardware and software employed by Envista Forensics is considered the industry standard and is in use all over the world by a large number of private forensic consulting firms and law enforcement agencies worldwide, including the Federal Bureau of Investigation (FBI), Homeland Security, the Department of Defense, Naval Criminal Investigation Services (NCIS), the Secret Service and hundreds of other national, state and local agencies.

Software and hardware tools in use by Envista include Cellebrite, Logicube Forensic Falcon, MacQuisition, EnCase Forensic Software, Forensic Tool Kit (FTK), Paladin, Magnet Axiom, Tableau Write Blockers, Image MASSter, Encase Portable, WeibeTech Forensic UltraDock, DI USB 3.0 Media Card Write Blocker and other tools as needed.

In the particular case of cell phones, the Cellebrite tool does not allow the examiner to restrict the data retrieved from the phone. The data that is ultimately delivered to the parties involved can be limited to a particular time frame and limited to a selected portion of the complete data set, such as only producing text messages or call history.

The digital forensic examiners at Envista Forensics are trained and experienced in the collection and protection of data so that nothing is exposed that is outside of the parameters set in civil agreements, court orders, or protective orders.

All of the data collected during the forensic extraction process is secured and stored in our locked, secure storage area. No data is provided to anyone outside the scope of the disclosure limits agreed to by the parties of this matter unless so ordered by a court of law.

NON-DESTRUCTIVE PROCESS

All of the processes, hardware, and software used in the acquisition (copying) of data from cell phones, computers, GPS devices, or other electronic storage devices are non-destructive.

The basic tenet of forensic acquisitions (forensic copying) and examination of digital evidence from electronic storage devices of all kinds are that the process must protect the original data from any change. There is a built-in method of verification to ensure that the original data matches the forensic copy of the data at the time the data is forensically copied. This verification is in the form of a "hash value."

A hash value is a mathematical calculation using the contents of the data to create a computed value unique to the contents of the data as it exists when acquired.

To prevent the engagement of possibly destructive processes (Brute Force, JTAG, ISP, Chip Off), Envista Forensics should be provided the following:

- Device PIN (Personal Identification Numbers), typically between four and six digits
- Device Passwords (alphanumeric combination containing letters and numbers)
- Device Unlock Patterns
- Encryption Passwords
- Smart Lock

Presence of Mobile Device Management (MDM) applications such as AppTec360 Enterprise Mobility Management, Baramundi Management Suite, ManageEngine Mobile Device Manager Plus, SOTI MobileControl, Citrix XenMobile, IBM MaaS360, Microsoft Intune, VMware AirWatch, and MobileIron.

MDM applications are typically utilized by government, businesses, and schools

EVIDENCE TRANSFER

After completing the below-described chain of custody form, the evidence custodian should package the evidence to prevent damage during shipment.

Regardless of the shipping vendor the custodian chooses, Envista typically requests the following:

- Shipment Tracking Number
- Overnight Shipping (if authorized by paying party)
- Direct Signature Required
- Please ship evidence to the following:

ENVISTA FORENSICS

ATTN: Jake Green

2700 Gateway Centre Blvd, Suite 100

Morrisville, NC 27560

Please provide the tracking number, estimated delivery date, and time by email to jake.green@envistaforensics.com

CHAIN OF CUSTODY

Complete a chain of custody form for receipt of the computer, cell phone, GPS device, or electronic storage device and any accessories.

- Each item is to be listed separately on the chain of custody form.
- The device will be inspected at the Envista Forensics Lab office in Morrisville, NC.
- The device is logged into custody, identified, and assigned a unique identifying lab number.
- The device is identified by make, model, and unique identifying number (IMEI, DEC, ESN)
- The device is tagged with a lab number.
- The device is isolated from network/internet connections.
- The device is physically inspected.

CONDITION

All items of interest will be photographed before any work is performed for chain of custody purposes.

If the computer, cell phone, GPS device, or electronic storage device is in a bag or other container, take a photo of the container before removing the computer, cell phone, GPS device, or electronic storage device for inspection from the front, back, and top of the container.

If the computer, cell phone, GPS device, or electronic storage device is not in a container, take a photo of the computer, cell phone, GPS device, or electronic storage device in its current state of the top, bottom, front, back, left side and right side.

Take close-up photos of any identifying information, including any asset tags, the serial number, MEID HEX, product number, ESN, and any other identifying information.

If the computer, cell phone, GPS device, or electronic storage device is a flip phone or a clamshell design, open the device to show the screen and keypad. Take photos of the screen and the keyboard area.

Have the producing custodian sign the chain of custody form indicating that they have reviewed the inventory on the Chain of Custody form and are transferring the items to a representative of Envista Forensics.

RESEARCH

The device is fully researched before extraction. Research includes:

- Operating system
- CPU Chipset
- Memory type/size
- Carrier limitations
- Manufacturer limitations
- Forensic tool compatibility
- Research sources include:
- Lab notes
- Peer networks
- Internet
- Manufacturer

REPAIR (If required)

- Physical damage will be closely assessed and triaged.

- Physical part damage
- Internal component damage
- Liquid damage
- Physical part damage will be repaired by part replacement.
- Screen
- Buttons
- USB port
- Battery
- Sensors
- Internal component damage will be repaired by component replacement.
- Liquid damage will be repaired by following liquid damage protocols.
- Isolation
- Ultra-Sonic cleaner

The repair goal is to achieve an extractable device, not a permanent repair. Repair methods/techniques will move towards that goal.

EXTRACTION

An extraction method is chosen based on research and device status. The least invasive, non-destructive method that produces the desired results will be used.

Desired results in order of importance (most preferred to least preferred)

- Full Physical extraction
- File system extraction
- Logical/Advanced Logical extraction

Only industry-accepted digital forensic methods will be used for extraction. User data WILL NOT be modified.

ENVISTA EXPERT NAME will conduct the extraction at the Envista Forensics Lab in CITY, STATE.

Equipment/Software used MUST be licensed to Envista Forensics Laboratory or individual examiner.

Extraction Tools for the MAKE AND MODEL: (in order of preference)

- Cellebrite UFED

- Axiom

EXTRACTION RESULTS

- A successful extraction will result in a forensic copy of the device's memory.
- The result will be a .bin file or forensic container.
- Results will be assigned a hash value for self-authentication
- Counsel for the parties may be present during the extraction process.
- Opposing counsel's expert may be present during the extraction process to monitor the work.

POST EXTRACTION

Open the forensic image of the computer, cell phone, GPS device, or electronic storage device in the associated forensics software program to ensure the image was completed successfully, thoroughly, and verifiably.

Have the producing custodian sign the chain of custody form indicating that they have reviewed the inventory on the Chain of Custody form and are receiving the items back into their custody from Envista Forensics.

Create master and working copies of the forensic image on separate storage locations for backup redundancy.

VALIDATION

Validation is conducted whenever possible to ensure equipment/software operation.

ANALYSIS

Data carving/parsing will be conducted on the extracted forensic copy (.bin file, .rar file) only. Only industry-accepted digital forensic software will be used for Analysis.

Analysis software includes (in order of preference):

- Cellebrite Physical Analyzer
- Axiom

Analysis TBD after the acquisition and not completed until scope has been agreed on by both parties.

- Experts will be authorized to review data during the following timeframe:
- 90 minutes before and after 12:00 PM on January 1, 2020

- No other data may be exported or retained.
- Defendant's expert will retain the originally extracted data.
- REPORTING
- The scope of Analysis governs the final examination report.
- Final examination report formats:
 - Adobe PDF,
 - Microsoft Excel, or
 - UFDR (with reader)
 - Included with the final examination report:
 - Analyst report (PDF of technical data)
 - The report will be on electronic media (depending on size)
 - DVD
 - Flash Drive

Envista Forensics' disclosure to Defendant, _____, shall be limited to a written report summarizing recovered electronically stored data of Defendants usage of device functions during the aforementioned period including, but not limited to, application usage, voice usage, messaging usage, GPS usage, Bluetooth pairings, locations, SIM Data, and wireless network usage.

Envista Forensics shall not disclose or shall redact any "Personal Information" extracted from the device.

Envista Forensics acknowledges and agrees to the term "Personal Information" as used herein and as defined below. Forensic expert agrees it shall keep secret, retain in the strictest confidence and prevent the unauthorized duplication, use, and disclosure of the Personal Information. Personal Information shall be used and duplicated (as is reasonably required) only so that Forensic Expert may accomplish the Extraction and Analysis and for no other purpose. Forensic expert agrees, except when required by law, to maintain and keep confidential Defendants Personal Information and not disclose the same to the Receiving Parties or third parties to this Agreement. "Personal Information" includes the following data during the period of time analyzed pursuant to the Analysis: email content (recipient name and number, subject line, body text), text message content (recipient name and/or number, body text), SMS/MMS content (recipient name and/or number, body text), Instant Messenger (IM) content (recipient name and/or number, body text), social media posting content made during the period in question, photographs, videos, website addresses or URLs, Social Security numbers, PINs (Personal Identification

Numbers), user names, passcodes, passwords, voicemails, recorded messages, notes, cookies, browser history, bookmarks, phone numbers, the identification of callers to or from the Mobile Device(s).

Plaintiff's counsel will receive an additional copy of the complete raw binary extraction (.bin file or.rar file)

EVIDENCE RETURN

The device is resealed in its original evidentiary container and marked with initials/date.

If the device is submitted without an evidentiary container, it will be sealed in a new container and marked with initials/date

The device will be immediately returned to plaintiff's counsel via a prepaid shipping label or FedEx.

CONFIDENTIALITY

Envista Forensics acknowledges that it may be held liable for disseminating Personal Information to parties other than opposing counsel unless and until such time as the Trial Court approves of such dissemination by written order.

Except as required by law, Envista Forensics agrees to take commercially reasonable steps to protect from disclosure to third parties any confidential and proprietary information of the plaintiff that may be exchanged in connection with this examination. Except as required by law, Envista Forensics agrees to take commercially reasonable steps to protect the confidentiality of information in or on electronic data and media made available or furnished to them for examination. Plaintiff agrees that if during the course of this examination, Envista Forensics shall find within any electronic data or media evidence of child exploitation (e.g., child pornography) or of a credible threat of physical harm to any person, Envista Forensics shall be entitled to immediately bring such matters to the attention of federal or state law enforcement authorities and that no assertion of privilege, confidentiality or breach of contract will be raised as a bar to such action.

PLAINTIFF

DEFENDANT

Facebook Subpoena Language/ Self-Download

Facebook can be difficult to obtain records from via subpoena. Included in this section is Facebook's reasoning , and how to do a self-direct download of Facebook data.

Subpoena Language

Facebook

Facebook, Inc.

Contact Name: Security Department/ Custodian of Records

Online Service Address: 1601 S. California Avenue
Palo Alto, CA 94304

Fax Number: 650-644-3229

E-mail Address: subpoena@fb.com

Note(s): Requests may be faxed, emailed, or mailed.

Any and all subscriber records regarding the identification of Facebook friend ID(s): **10000000000**, emailaddress@email.com to include real name, screen names, status of account, login log, ip address log, detailed billing logs, date account opened and closed, method of payment and detailed billing records. Also, to be included, but limited to, are all stored emails and all profile pages including wall posts, communications and chat logs.

Such stored information is to include any deleted and or archived pages or email or communications, that Facebook has retained as part of its normal business operations for the period of _____ to _____.

In the case of archived or deleted pages for the above account, the archive URLs for the pages may be returned as part of this request, provided that the URLs are accessible via the Internet. If any credentials are required to access the archive URLs, then those must be provided as part of the response to this request.

Download Facebook Account (Reason)

The following is Facebook's response to the question, "May I obtain any account information or account contents using a subpoena?"

Account Contents

Federal law does not allow private parties to obtain the content of communications (example: messages, timeline posts, photos) using subpoenas. See the Stored Communications Act, 18 U.S.C. § 2701 et seq.

Parties to litigation may satisfy party and non-party discovery requirements relating to their Facebook accounts by producing and authenticating the content of communications from their accounts and by using Facebook's ["Download Your Information" tool](#), which is accessible through the Settings drop down menu. Facebook does not respond to requests to disclose information that are accompanied by purported user consent because Facebook account holders may access, produce and authenticate information from their accounts.

If a person cannot access their content, Facebook may, to the extent possible, attempt to restore access to deactivated accounts to allow the person to collect and produce their content. However, Facebook cannot restore account content that has been deleted.

Account Information

Facebook may provide the available basic subscriber information (not content) where the requested information is indispensable to the case, and not within a party's possession upon personal service of a valid subpoena or court order and after notice to affected account holders.

Your subpoena or Court order must be directed to the entity mentioned in the Terms of Service that are applicable to your use of the Facebook service (i.e. Facebook Ireland or Facebook, Inc., depending on where you are domiciled meaning if serving the subpoena on Facebook, Inc., the subpoena must be a valid federal, California or California domesticated subpoena, addressed to and served on Facebook, Inc. If serving Facebook Ireland Limited, the subpoena or court order must be addressed to and served on Facebook Ireland Limited.")

Any such subpoena or court order should be limited in scope to seek basic subscriber information only, and set out the specific accounts at issue by identifying them by URL or Facebook user ID (UID). Names, birthdays, locations, and other information are insufficient.¹

1


https://www.facebook.com/help/133221086752707?helpref=related&ref=related&source_cms_id=133221086752707

Download Facebook Account (Instructions)

This is the method Facebook provides for users to download Facebook accounts:

If you want to download a copy of your information from Facebook, you can use the **Download Your Information** tool.

To download a copy of your Facebook data:

Click  in the top right of Facebook.

Select **Settings & Privacy**, then click **Settings**.

In the left column, click **Your Facebook Information**.

Next to **Download Your Information**, click **View**.

To add or remove categories of data from your request, click the boxes on the right side of Facebook.

Select other options, including:

The format of your download request.

The quality of photos, videos and other media.

A specific date range of information. If you don't select a date range, you'll request all the information for the categories you've selected.

Click **Create File** to confirm the download request.

After you've made a download request, it will appear as **Pending** in the **Available Copies** section of the **Download Your Information** tool. It may take several days for us to finish preparing your download request.

Once we've finished preparing your download request, we'll send a notification letting you know it's ready.

To download a copy of data you requested:

Go to the **Available Copies** section of the **Download Your Information** tool.

Click **Download** and enter your password.

You can also click **Show more** to view information about your download request, such as the format and when it will expire.

Note: You can always view your [Privacy Shortcuts](#) to learn about the ways you can control your data and privacy on Facebook. If you want to review recent activity on your Facebook account or want to review your Facebook account information, you can use the [Access Your Information](#) tool.

Adam Walsh Act (Child Exploitation) Language

Contraband cases are unique in the sense that they are covered by the Adam Walsh Child Safety and Protection Act of 2006. Because of this federal law, barriers are in place to prevent actions that would result in the distribution of the materials to defense attorneys and defense experts. An expert working on behalf of the defense must perform their examination onsite at a law enforcement facility and under their supervision. Data can be taken from this examination, such as log files, file listings, and other forensics artifacts. However, no images or videos of contraband, even suspected contraband, should be taken.

Language for Access to Evidence in Child Exploitation Cases

ACCESS TO FORENSIC EVIDENCE

The Defendant requests that government's agent provide to the Defendant's expert access to the physical evidence seized by the State in the course of its investigation under the following conditions:

1. The defense expert will supply in advance an external hard drive, factory new, if required by the law enforcement agency, for the purpose of providing forensic copies of the evidence to be examined during the defense expert's forensic examination and will be kept in the custody of law enforcement at all times.
2. The law enforcement agency shall copy to the provided hard drive any FTK, Encase or other type of forensic image files that are an exact forensic copy of the hard drive(s), CD-ROM or DVD-ROM media, flash cards, floppy disks, smart media cards or any other digital evidence seized and copied by law enforcement.
3. The law enforcement agency shall provide to the defense expert an un-redacted copy of any computer forensic reports for the use of the defense expert while performing the forensic examination. Such un-redacted reports shall be returned to the law enforcement agent at the end of each day's examination period at the discretion of the supervising agent.
4. The law enforcement agency shall have available for inspection by the defense expert copies of any derivative evidence created and supplied to the prosecution, including but not limited to media created for the purpose of prosecution review, submission to the National Center for Missing and Exploited Children, or for the use by other law enforcement parties to the investigation of the charges, pending or otherwise.

5. The expert will perform all of his work on the provided hard drive, using forensic analysis equipment provided by the law enforcement agency, provided that hardware provided by the law enforcement agency is no more than 18 months old, has a current version of 64 bit Windows OS (7, 8 or 10), and current versions of Microsoft Office Professional, Adobe PDF reader, a video player that is fully configured to play all types of video files such as VLC Media player, and any other software normally used in the course of forensic examinations, excepting actual forensic software. The expert may install other forensic analysis software on the provided computer for the purpose of performing his examination as needed and will bring his own licensing keys or USB dongles for that purpose.
6. At the end of the forensic examination session, the examination hard drive will be sealed in the presence of the defense expert and given to the law enforcement agent and kept in the custody of the police in case further review is needed at a future time or the review room will be locked so that processes on the computer can continue overnight as needed.
7. The law enforcement agency shall make such supervisory arrangements as deemed appropriate in accordance with the law enforcement agencies' policies and procedures for the forensic examination of contraband material by a defense expert.
8. The expert will show to the law enforcement agent any items he wishes to copy or print, to provide to defense counsel as part of his analysis or reporting, to ensure that no contraband images are copied or transferred.
9. The expert will be given a minimum window of 6 hours per day, scheduled in advance, to perform the analysis.
10. All items and information discovered by the expert are to be treated as attorney work product, and protected as such even though the law enforcement agent will review said documents and information for the presence of contraband.

GUIDE –Digital Forensics in Child Exploitation Cases – Finding Your Way Through

Justin Ussery, Digital Forensics Examiner

Jake Green, Digital Forensics Examiner

Copyright 2020, Envista Forensics, All Rights Reserved.

About the Authors

Jake and Justin have are both Former Law Enforcement Officers who were assigned as Digital Forensic Examiners and Task Force Officers of the United States Secret Service Electronic Crimes Task Forces in South Carolina and California. Jake and Justin both work matters and cases involving all aspects of Digital Forensics, including Cellular Phones, Tablets, Computers, and Cloud data. This article is meant to give you a brief overview of the frequently and daunting amount of confusing electronic evidence you receive in discovery and an overview of this information you often find in the discovery process of a Child Exploitation matter.

Introduction

This article is meant to give you a brief overview of what is frequently a daunting amount of confusing electronic evidence you may receive via discovery in a child pornography case.

Uniqueness of Child Exploitation or Child Pornography cases

Child pornography cases present unique difficulties because of how attorneys can view the evidence and how experts can examine that evidence. These cases are controlled at the federal level by the Adam Walsh Child Safety and Protection Act of 2006. This act explicitly says government examiners cannot send a report containing child pornography in any form to any person outside of law enforcement. The evidence review likely will take place at a government facility, and we are often supervised by law enforcement officials, often the same ones who performed the original forensics. The Adam Walsh Act prevents child pornography from being disseminated, which is a good thing. However, this places a burden on the defense, as examinations of forensic data need to occur at a law enforcement facility. The examiner may only leave with certain artifacts, which do not contain images or videos, making the onsite review of the evidence critical, as this typically does not take place more than once due to the cost of placing a forensic examiner on site.

Law Enforcement Investigations: Before the Search Warrant

CyberTips

Law Enforcement typically deals with two main entities when it comes to dealing with child pornography: Internet Crimes Against Children (ICAC) and The National Center for Missing and Exploited

Children (NCMEC). NCMEC acts as a clearinghouse for business and Electronic Services Providers (ESPs) to report possible illicit media.

After ESPs notify NCMEC, a "CyberTip" is created and forwarded to a Regional ICAC Task Force or local law enforcement agency. The Regional ICAC Taskforce or agency then investigates and collects evidence. The investigating officer may perform a forensic examination of this evidence or may assign this to a qualified forensic examiner.

All of this activity originates with the Cyber Tip.

The Cyber Tip will generally include dates and times of said activity, Internet Protocol (IP) addresses during the period of the event, and account information such as email addresses, phone numbers, mailing addresses, and possible user names of the account utilized during the actions.

Online Law Enforcement Investigation Tools and Resources

Detectives and investigators across our country conduct digital or online investigations with a variety of digital tools and software. Many of these tools are deemed to be "law enforcement sensitive" and in our experience as law enforcement examiners, a court order may be required to gain access to these specific tools for review by a forensic examiner working with defense counsel.

Several keywords and processed should be defined at a basic level before continuing:

IP Addresses

An Internet Protocol address is an identifying number for a computer network. A unique Public IP address is assigned by an Internet Service Provider (ISPs like CenturyLink, RCN, Frontier, Verizon, or AT&T). These assignments are unique to physical locations (modems or gateways), which can distribute the connection physically via a wired network switch or a broadcast wireless network via a Wi-Fi router. Public IP addresses are unique to physical locations (home, business, public Wi-Fi) and are not typically unique to physical devices like cellphones, computers, and tablets.

Once an IP address is documented, the owner of the IP address can be found. IP addresses are owned by Internet Service Providers (ISP).

This identification process proceeds in steps:

The IP address is obtained by law enforcement from an online investigation.

The owner of the IP address is identified using a "reverse" lookup to locate the company that owns the IP address. This is accomplished using a "WHOIS" lookup service. One such service is "whatismyip.com". For instance, looking up a text IP Address shows that the owner of the IP Address is Charter Communications.

Once the owner of the IP address is known; the law enforcement officer will create a warrant or subpoena and send that to the owner of the IP address to obtain the subscriber information for the IP address on the date of interest.

GUID: Globally Unique Identifier

GUIDs are an alphanumeric series of numbers that can be assigned by a computer system. For this article, a GUID is assigned to each asset or device within a P2P network. This GUID is unique but can be changed or updated by the P2P network.

Metadata: "Data about data."

While the colloquial definition "data about data" is often used, we prefer "information about data." Metadata is a collection of information about the source or creation of data. This information could be the manufacturer or model of a camera, GPS location, file metadata such as date and time of creation; or modifications, source, author, or editor.

Hash Value: Electronic DNA

A hash value is the application of a mathematical formula (algorithm) to produce a unique alphanumeric string associated with a single file or a set of files. Changes to the data (even a single bit) will result in the change of the hash value. Hash values allow investigators to identify known images, accurately preserve and reproduce data. Common hash values are MD5 (message-digest algorithm), SHA-1, and SHA-256 (Secure Hash Algorithm).

Through our background, experience, and review of software documentation, we're able to offer some insight into these investigative aids. We cover three unique pieces of software used by law enforcement to conduct online investigations. It should be noted that the log files discussed in each section are unique to each piece of software and should be requested through discovery or court order. The below listed log files do not contain illicit content, images, or media and can be released by law enforcement to a civilian defense examiner.

ShareazaLE

One of the most common investigative tools is a variant of the peer to peer (or "P2P") program, Shareaza, that has enhanced features for investigations. This piece of software allows law enforcement to single out an IP address (known as a "single source download"). ShareazaLE produces a log called "ShareazaLE Summary Report for IP: "0.0.0.0"," where "0.0.0.0" is the target or identified IP address.

Torrential Downpour

This is another free piece of software that has been modified to suit the needs of law enforcement investigators. However, this piece of software operates using a different protocol, called torrents. In the most basic sense, torrents are a series or set of files. The torrent file itself is a set of instructions related to the source file and metadata. These source files can be a single file (i.e., movie) or an archived folder containing multiple files (i.e., sets of photos or music from an album). Torrent files are typically sourced from search engines, websites, or forums, but some Bit Torrent software packages have built-in search features. Torrential Downpour produces a series of log files: Datawritten.xml, Details.txt, Downloadstatus.xml, Netstat.txt, summary.txt, and Torrentinfo.txt. It should be noted that the torrent file itself is not illegal to possess as it contains only metadata.

RoundUp eMule

RoundUp was designed to investigate the eD2K or eDonkey2000 file-sharing network. EMule and similar P2P networks are built around keyword searches. A user enters a general keyword (like "porn"), and the search results in the return of any files containing the keyword (i.e., "child porn" or "adult porn"). RoundUp produces logs named: SummaryLog.txt, DetailedLog.txt, Netstat.txt, IdentityLogging.txt, and IdentitySignatures.xml.

Law Enforcement Investigations: After the Search Warrant

Major Software Vendors

There are several major software vendors utilized by both government examiners and private examiners alike. For cellular device forensics, you will likely see Cellebrite UFED with Physical Analyzer, Oxygen Forensics Detective, Axiom by Magnet Forensics, and GrayKey by Grayshift. Most cellular device tools rely on three general types of extractions from the phones, but all produce very similar results with a few caveats. There are thousands of applications operated on four major smartphone operating systems: Android, Apple iOS, Windows Mobile, and Blackberry OS. Not every tool can decode and make

sense of every single application in the world and that is a primary reason why it is beneficial to utilize a variety of different tools during examinations.

As for computer forensics, you will see Axiom or IEF by Magnet Forensics, Forensic Tool Kit by Access Data, Encase by OpenText, Analyze by Griffey, Forensic Explorer by GetData and BlackLight by Cellebrite (formerly Blackbag Technologies).

Many of these tools can redact child pornography images and safely provide a good deal of metadata about the activities without the dissemination of child pornography by Law Enforcement or prosecutors.

Review of Digital Forensic Evidence

If law enforcement recovers electronic evidence and utilizes forensic tools, the scope of their investigation should not be limited to the simple question of "Is illicit media on this device?" Digital investigations need to be a great deal more comprehensive. An expert should search for any known evidence such as suspect IP Address, GUID, hash values, user attribution, as well as a possible indication of file use and knowledge.

Many law enforcement forensic tools and Cyber Tips identify IP Addresses and GUIDs. A review of these records is essential to identify the physical location of an IP address (possibly the defendant's home or work). The subsequent investigation of a network, like a broadcasting Wi-Fi router, may be necessary to determine what devices were connected at a location. While gathering evidence, an investigator should collect and review network connection logs (if logging is enabled) or records from an ISP. Knowing when and what devices were connected to a network can significantly assist in the identification of a suspect. Failing to gather these logs can result in their overwriting or deletion.

If a law enforcement investigator is adequately trained and utilizes online tools, like those outlined above, they should retain the available logs. These logs should become part of the investigator's digital case file. The logs should be maintained as a unique piece of digital evidence, as printing will result in the loss of file metadata (i.e., the creation and modification dates and times).

This metadata is critical to what is referred to as "user attribution."; putting a specific person behind the keyboard at the time of the offense. This will likely make or break the case for a prosecutor. These indicators of user attribution are often forgotten or overlooked by examiners who are providing evidence to the investigating officer or prosecutor.

These user attribution indicators are held in a variety of places on a computer and consist of jump lists, .lnk files (pronounced "Link"), Shellbags, Windows MRU, and search terms found within browsing histories.

Jump Lists

A "jump list" is a system-provided menu that appears when the user right-clicks a program in the taskbar or on the Start menu. It is used to provide quick access to recently or frequently used documents and offers direct links to app functionality.

Link Files

An LNK (short for LiNK) is a file extension for a shortcut file used by Microsoft Windows to point to an executable file. LNK file icons use a curled arrow to indicate they are shortcuts, and the file extension is typically hidden from the computer user. Generally, if the "linked" or source file is deleted, the LNK file will remain behind and will contain information not only of when the LNK file was created, but about the target file of interest.

Shellbags

Windows uses the "Shellbag" to store user preferences for folder display within Windows Explorer. Everything from visible columns to display mode (i.e., icons, details, or list) to sort order and are tracked.

Most Recently Used files (MRU)

The Most Recently Used "MRU" is a list that contains a history of recent activity on a computer. MRUs can include open documents or webpages.

If user attribution indicators are disregarded for any reason, the case weakens. The user attributes held within these specific items can show a pattern of behavior by a computer user. This makes it much more unlikely that this offense was an isolated incident and was occurring over an extended time period. Again, these crucial artifacts frequently go unexamined. These are in many cases, "make or break" items worth looking at when it comes to a defense strategy.

Defense of Child Pornography Cases

U.S. vs. Flyer

In *U.S. vs. Flyer*, defense counsel made successful arguments regarding the lack of possession for images found in unallocated space. Unallocated space is not accessible by ordinary users. We have reviewed many cases where government examiners find child pornography in unallocated space but do not

identify additional forensic artifacts. An inability to exercise "dominion and control," no proof of "file use and knowledge," and lack of user attribution makes a case easier to defend as there is a lack of knowing possession and intent.

Thumbnails and Cache Files

Thumbnail images are an image that is a smaller representation of the original photograph. These thumbnail images by themselves usually are devoid of metadata and are created by the operating system without user interaction.

The Internet browser cache contains images saved by the browser to help speed up your rendering of web pages. By avoiding downloading the same image again and again the computer user experiences a faster web page viewing experience.

In both instances, the operating system or web browser application is automatically doing this as an automated process. The computer user has no knowledge of or access to these files.

ISP Connections

The way that the law enforcement agency determines where to go for a search warrant or "knock and talk" is to find out the subscriber account for an internet download.

When law enforcement performs a lookup of the IP address for a download, they will then research to determine which Internet Service Provider owns that IP address.

Once the owner of the IP address is determined, i.e. Spectrum or Charter Cable, the law enforcement officer will send a subpoena to the ISP and find out who the subscriber is for that IP address on the date and time of the download.

The subscriber account information will also provide a physical address for the internet connection.

Once the law enforcement officer has that information in hand, he or she will then apply for a warrant to search the residence or business at the address, This is based on the probable cause in the form of the download history from one of the tools used for the online investigation and the subscriber information from the ISP.

There are times when the connection is not being made from the address, i.e. someone is stealing a connection from a nearby address.

"The sound of his door being broken down awoken the man at 6:20 a.m. on March 7. Seven armed officers greeted the homeowner, whose name has not been released. He was forced to lie down on the floor while the officers pointed guns at him while calling him a pedophile and a pornographer. According to the Associated Press, the officers had the initials of I.C.E. on their jackets, which the man didn't know stood for Immigration and Customs Enforcement, and we don't blame him.

The agents searched the man's desktop for about two hours that morning looking for evidence, and eventually confiscated the computer, as well as his and his wife's iPads and iPhones. It took three days for investigators to realize the man, who had told the officers at the time of the intrusion that they had the wrong guy, was actually telling the truth and was indeed not the kiddie-porn downloader. A week later, investigators arrested a 25-year-old neighbor and charged him with distribution of child pornography. However, he did not get in trouble for piggybacking off the man's WiFi signal."

Source: <https://www.geek.com/news/man-wrongly-accused-of-child-porn-learns-to-password-protect-wifi-the-hard-way-1347033/>

Conclusion

Nearly every case in today's digital age has an electronic evidence component. These components can supply both supporting and damning information for your case. The question is: How do you obtain and interpret the evidence? A qualified and experienced expert can assist you with a thorough discovery review and comprehensive analysis of the electronic evidence.

i 633 F.3d 911 (9th Cir. 2011).