THE DIGITAL WORLD:

The Role of Digital Information in the Investigation & Prosecution of 21st Century Crime

Lead Author: Justin Fitzsimmons **Contributing Authors:** Timothy Lott, Lauren Wagner, & Dean Chatfield

CHILD ABUSE PROSECUTION PROJECT
ASSOCIATION OF PROSECUTING ATTORNEYS
11 DUPONT CIRCLE NW, 2ND FLOOR
WASHINGTON, DC 20036
CHILDABUSEPROSECUTION.APAINC.ORG

This project was supported by Grant # 2015-CI-FX-K004 Awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. Points of view or opinions in this publication are those of the author/presenter and do not represent the official position or policies of the United States Department of Justice.

OJJDP

ASSOCIATION OF PROSECUTING ATTORNEYS

THE DIGITAL WORLD: The Role of Digital Information in the Investigation & Prosecution of 21st Century Crime[1]

Digital technology now permeates our daily lives.[2] Consider these statistics: According to one study, there were nearly 378 million wireless subscriber connections in the United States at the end of 2015;[3] nearly half of all households in the United States are wireless only;[4] and Americans use over 786 million gigabytes of wireless data a year and average over 156 billion text messages a month.[5] Whether using desktop computers or mobile devices, technology now impacts almost everything we do. It affects how we create, retain and share information: we now store much more including, commonly, our most personal things in the cloud. It has dramatically affected our relationships. As technology increasingly interacts in our daily lives; the digital "footprints" left behind often support investigations and prosecutions of criminal offenses. There are generally at least two repositories of digital evidence: a local digital device and cyberspace – also referred to as the cloud.[6] Each may retain an enormous amount of relevant digital information.

This article-

- describes some of the different types of digital technology currently available and describes how information spawned by that technology may be relevant to an investigation or admissible at trial,
- explains some of the different digital artifacts types that investigators may recover from digital devices,[7]
- highlights several of the available resources to explain the technology in greater detail, and
- clarifies the steps necessary to secure digital evidence and data in the cloud.

How Digital Technology Works

Mobile Devices:

The fastest growing source of digital evidence is mobile or tablet devices.[8] By 2017, it is expected that 63.5% of the U.S. population will use a smartphone device.[9] In 2016, more than 55% of emails were opened using smartphone devices.[10] As with most modern technology, there are at least two repositories of digital evidence: evidence stored on the actual device and evidence that exists in the cloud. Digital information often exists in both places simultaneously and it is important to recognize that different information may be captured by the device as opposed to retained in the cloud. For example, a cloud provider may retain connectivity information, to include IP addresses, where the device may not. Understanding the terminology involved with mobile devices, as well as what information may be recovered from them and what from the cloud, is critical to determining the appropriate investigative avenues, and what may qualify as competent evidence at trial. Introducing evidence from both "repositories" – that is from both the device and the cloud -- may also assist in laying a solid foundation for authenticating the digital evidence.[11]

Two main technologies currently support mobile phones: Code Division Multiple Access (CDMA) and Global System for Mobiles (GSM).[12] Both systems are used in the United States;[13] internationally, the vast majority of the world uses the GSM network. Phones using the GSM network rely on a SIM card.[14] Each SIM card contains the International Mobile Subscriber Identity (IMSI) and its related key. This number authenticates the mobile device to the GSM network. In less technical terms, once the SIM card is activated, the information on the SIM card lets the mobile phone carrier "identify" a specific mobile device to a specific user's account, which then allows the mobile device to access the mobile network.[15] A SIM card may be moved from device to device, but its functionality may be limited by the type of service and/or mobile device.[16]

Additionally, each mobile device on the GSM network comes with a specific International Mobile Equipment Number (IMEI). The IMEI identifies a specific device and is unique to only that device. A device's IMEI remains the same regardless of the mobile device carrier. While the IMEI is often printed on the inside of a mobile device in several locations which can differ from one device model to the next, you may also display it on the phone screen by entering *#**06**# into the phone keypad. On an iPhone, access the IMEI by selecting the "Settings" button, then the "General" and "About" tabs.

The IMEI may help determine the role of a particular device in a crime. For example, if the provider of a mobile service is identified, the provider may be able to supply any and all IMEIs of any devices used by the account in respond to appropriate legal process.[17] With the results, investigators would then know specifically what device they should try to recover. They also could interview witnesses and ask if they ever saw the suspect with the type of device that was identified by the IMEI.

[1] Authors: Justin Fitzsimmons, Lauren Wagner, Dean Chatfield, and Tim Lott. [2] Riley v. California and United States v. Wurie, 578 U.S. ___, 134 S.Ct. 2473 (2014). [3] http://www.ctia.org/industry-data/ctia-annual-wireless-industry-survey [4] Id. [5] Id. [6]For purposes of this article information in the cloud will be considered in 0cyberspace. [7]For purposes of this article, the term "artifacts" refers to specific digital information that may be recovered from digital devices. As more fully explained in the article, this evidence may be used for several different purposes. These include proving identity of the user or that the criminal conduct occurred; demonstrating intent or knowledge by the device user; proving location; and potentially disproving defenses. [8]For purposes of this article, cell phones and tablet devices are referred to as "mobile devices." [9]See https://www.statista.com/topics/2711/us-smartphone-market/ [10]See http://www.emailmonday.com/mobile-email-usage-statistics [11]See Authentication in the Digital Age, in publication in 2017 [12]CDMA and GSM are the two major radio systems that carry the signals for mobile devices. [13]Sprint, Verizon, and U.S. Cellular rely on the CDMA network, while AT&T and T-Mobile use the GSM network. [14]SIM stands for subscriber identity module. A SIM card is the small memory card inside a cellular phone that provides identifying information to a GSM network that authenticates the phone to the network. A SIM card may also store contacts, messages, and other data. 15A user may have an account with multiple SIM cards, however, by changing out SIM cards with a device the user would be using a different number assigned by the carrier. For example, a user may have one SIM card for business and one SIM card everything else, and use them interchangeably on the same mobile device. 16A locked phone is one that is only able to be used by one mobile device carrier. An unlocked phone may be used on any network as long as the SIM card works for the network. For example, a SIM card from a locked phone on the AT&T network may not be compatible with a locked phone from the T-Mobile network. 17See page 38 for a discussion on the appropriate legal process for obtaining different types of material.

Mobile devices using a provider that relies on the CDMA network will have neither a SIM card nor an IMEI. However, phones on this network will have a Mobile Equipment Identifier (MEID). This is the CDMA version of an IMEI. The distinction between the two different formats is becoming less and less important as more and more mobile providers are using 4G and LTE technology.[18] The acronym "4G" stands for fourth generation of data technology for cellular networks. "LTE" stands for Long Term Evolution and is the name created within the mobile device industry for the process of reaching a certain minimum speed of data connections.[19] 4G/LTE CDMA devices will contain an IMEI and work more like a traditional GSM device.

A mobile device offers two other identifying numbers: the mobile directory number (MDN) and the mobile identification number (MIN). The MDN is the 10-digit number that is used to communicate with the mobile device. The MIN is the 10-digit number that the mobile service provider uses to register and communicate with the mobile device. While these numbers often match, there are instances where they are different. The most common time that these two numbers will not match is if a phone number is moved from one provider to another provider.

For example, if a subscriber signs up for new service with Verizon and purchases a new mobile device, Verizon will issue that subscriber both an MIN and an MDN, which will be the same number. However, if that subscriber moves to T-Mobile, but wants to take the old Verizon phone number (either with the same device or a new device) with them, the MDN and MIN will no longer match. The MDN will remain the same, but the MIN will have to change. In this scenario, the MIN has to be a T-Mobile MIN for the device to communicate with the new service provider. If both the MIN and MDN are reported (either in the device settings or in a report obtained through mobile device data extraction), it is best to use the MIN to look up the current carrier of service. However, device records will all be recorded and provided using the MDN. An easy mnemonic to remember the difference is MDN has a "D" for the number ***DIALED*** and MIN has an "I" for the number ***INSIDE***.

Mobile Devices Connecting to Networks

Regardless of the network in use, all mobile devices that rely on the cellular network generally work the same. The moment a phone is turned on and available to the network the phone emits a radio signal.[20] The radio signal searches for the nearest cell tower.[21] The number of bars the mobile device displays indicates the signal strength to the closest tower.[22]

There are generally two different types of cell towers: multidirectional and omnidirectional. The multidirectional towers are made up of three sides. Each side is referred to as a "sector." The tower lease holders often assign each sector either a number or a letter designation to represent the sector of each tower, for example A, B, and C. Each sector is responsible for 120 degrees, for a total of 360 degrees. The individual sectors can also be broken down into 40-degree bits that allow for more accurate signal strength.[23] However, the coverage area is not in the shape of a circle, but rather a hexagon, as shown in the Figure 1.[24]

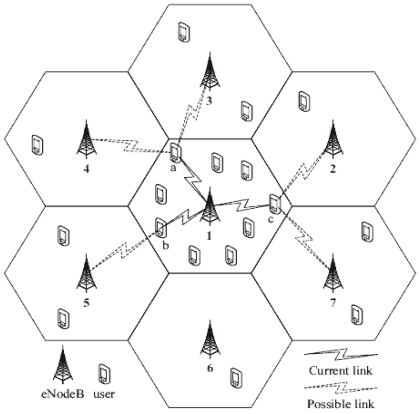


Figure 1: Network model.

Multidirectional towers are generally located in urban areas and may be found mounted on the top of or near the roofline of buildings (photo on the left). The signal strength from each tower depends on the capacity of the transmitter of the cell tower and potential causes of interference to the signal.[25] Omnidirectional towers are most often located in more rural areas (photo below).

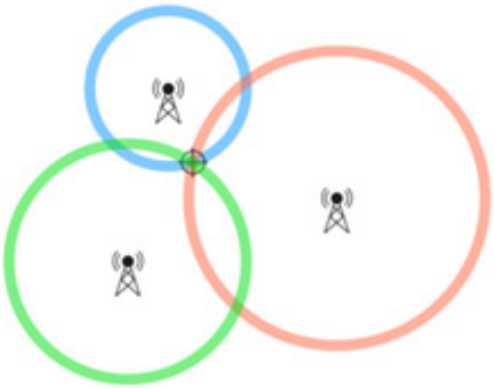
Omnidirectional towers

[18]For an in-depth article on the difference between 4G and LTE, see http://www.digitaltrends.com/mobile/4g-vs-lte/ [19]Id. [20]Mobile devices often have a feature called "airplane mode." Airplane mode simply shuts off the radio signal from the emanating from the device, thus removing it from the mobile device network. On most devices, the airplane mode also restricts the phone from sending or receiving signals through wireless Internet. For additional information, see http://www.howtogeek.com/194421/what-does-airplane-mode-do-and-is-it-really-necessary/ [21]Some carriers also refer to cell towers as "base transmission stations" (BTS) or phone stations. [22]For further information on how mobile devices connect to cell towers, see http://technogog.com/information/how-stuff-works-cell-phone-towers/ [23]Id. [24]Illustration source: http://masters.donntu.org/2013/fkita/benavides/library/2.htm [25]According to one author, cell towers are able to send a signal between 45 to 22 miles. However, he notes that interference—both natural (hills, mountains, trees) and man-made (buildings and other structures)—may significantly diminish the distance. See http://smallbusiness.chron.com/far-can-cell-tower-cellphone-pick-up-signal-32124.html

Whenever the mobile device and the cell tower are communicating through the radio waves a record of that connection is created. This data is referred to as "Cell Site Location Information" (CSLI). Investigators can use CSLI to determine the location of a particular mobile device. There are three methods law enforcement can use to secure the CSLI data, which will demonstrate the connection between a device and a cell tower:

- Ask a cellular provider to provide "real-time" data from a mobile device connecting to a tower immediately after the connection is created.
- Ask the cell tower provider for a list of all of the numbers that have made a connection to the tower within a specific time frame. This is often referred to as a "tower dump."[26]
- Ask for historical data generated by a specific mobile device's interaction with cell towers for a certain period of time from the actual cellular carrier.[27]

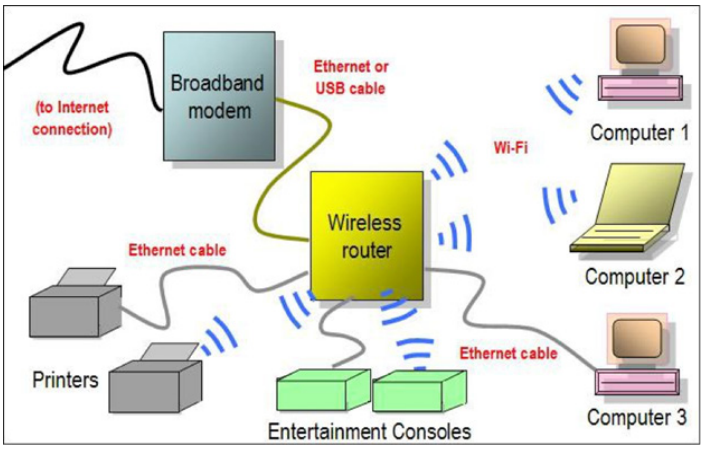
Using this CSLI data, it is possible to locate a mobile device through the process of triangulation. The mobile network is made up of a grid of cells. Towers broadcast a signal into each cell. Investigators can determine an approximate location of the device by measuring the signal strength of the different towers broadcasting into the cell that the mobile device was—as illustrated in the graphic.[28]



Mobile WiFi Connectivity

Another potential area of recoverable location or connection data relates to mobile devices connecting to wireless Internet—in these cases, the data can reside either in the mobile device or in cyberspace. Smartphones and many tablet devices now offer consumers the option of both cellular and WiFi-enabled data.[29] Instead of connecting to the cellular tower to send radio waves, the WiFi-enabled device accesses the Internet through a Wireless Access Point (WAP).[30] The router creates a WAP that broadcasts a unique Service Set Identifier, or SSID to any nearby devices.[31]

The SSID creates a wireless local-area network (WLAN). The mobile device receives the signal and then communicates through radio waves to gain access to the Internet through the router's unique SSID. These are often referred to as "hot-spots."[32] Any device that accesses the Internet through a WAP may create connection logs with the router, with the Internet provider, and on the device itself (see illustration).[33]



Some home routers have the ability to log information about the devices that connect to it: this feature is disabled by default on most routers and must be turned on by the user. The average home user does not know how to activate this feature. Additionally, many businesses and hotels offer wireless Internet to which their customers – and sometimes others in parking lots outside may connect. While most business routers have the ability to log connected devices, most do not. However, all routers have an Internet Protocol (IP) lease table, which records information about the devices currently connected to the router. Depending on the router configuration, their leases are usually active for 24 hours, but may be less for a router that has many devices that connect to it. For example, in a coffee shop where multiple customers come in and out during the day, the router may be set to release IP addresses after an hour to allow other devices to connect to the network. In this example, after the passage of an hour, the IP addresses would no longer be in the router log.

Another example may help illustrate this: An offender checks into a hotel room. Once in his room, he connects to free hotel wireless network using that hotel's credential requirements of room number and last name. He then accesses his personal social media account and checks his email, both of which require user identification and passwords. Once he has completed those tasks, he engages in the criminal activity of creating an email account and sending harassing emails. Each one of those actions *may*

---

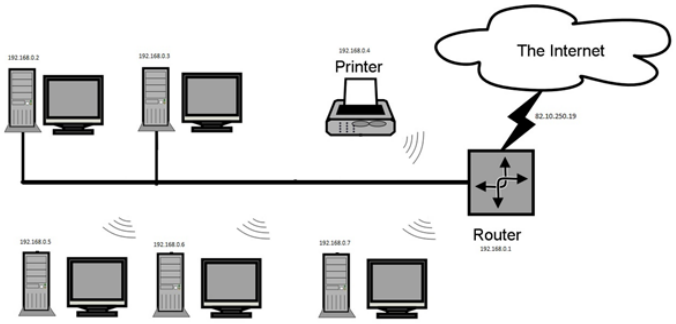
[26]For the legal process required to lawfully examine records from a cell tower, see section on search and seizure on page 35. [27]Id. [28]Illustration source: http://www.neilson.co.za/mobile-network-geolocation-obtaining-the-cell-ids-the-signal-strength-of-surrounding-towers-from-a-gsm-modem/ [29]See https://www.att.com/shop/wireless/data-plans.html?&WT.srch=1&source=ECPS0000000PSM00P. [30]See http://www.explainthatstuff.com/wirelessinternet.html [31]An SSID is a case-sensitive, 32 alphanumeric character unique identifier attached to the header of packets sent from a particular wireless hot spot. An easy way to think of it a SSID is an analogy to an address at the top of a letter. The address describes the physical location where the letter originated. [32]A hot spot is simply a router that is available to the public for anyone within range of the broadcast signal of the router. Generally the router can carry a signal that will carry anywhere between 90–300 feet, depending upon what type of obstacles are in the path of the signal. Id. [33]Illustration source: https://blog.peerless-av.com/wi-fi-101-wi-fi-works/

leave connection logs on the hotel router, with the Internet service providers, the social networking providers, and on the device itself.[34]

To add another layer of complexity to acquiring location data, some Internet Service providers and mobile networks now port IP addresses. An Internet Protocol (IP) address identifies a device on a network, and is assigned to each user by an Internet Service Provider (ISP). Law enforcement often uses IP addresses to identify Internet connections that are related to an investigation. One important aspect of IP addresses, as it relates to an investigation, is that the IP addresses identify the *Internet connection*, not necessarily the specific device that was used. When investigators encounter an IP address and trace it back to the ISP, they can query the ISP to determine the customer or controlling authority, for a specific date/time, for that connection—which is usually the name of a business or subscriber. Investigators may need to conduct follow-up investigations to actually determine the specific device of investigative value that was used.

Multiple devices can use the same IP address through either Network Address Translation (NAT) or port forwarding. NAT uses a piece of hardware (router) to translate one public IP address into multiple private IP addresses. A device needs to have a public IP address to connect to the Internet—but if every device needed its own public IP address these addresses would very quickly be used up. NAT allows a router to share one public IP address with multiple devices each with its own private IP address. A good analogy is to think of an IP address like a phone number. One phone number may ring to multiple phones within a residence. When someone answers a ringing phone, the caller may ask for a specific person in the household. That person may be the person who picked up the phone, or he or she may have to hand the phone to someone else, or instruct someone else to pick up another phone in the household. Many people within a household may all access multiple phones within a household, but they all share one telephone number.

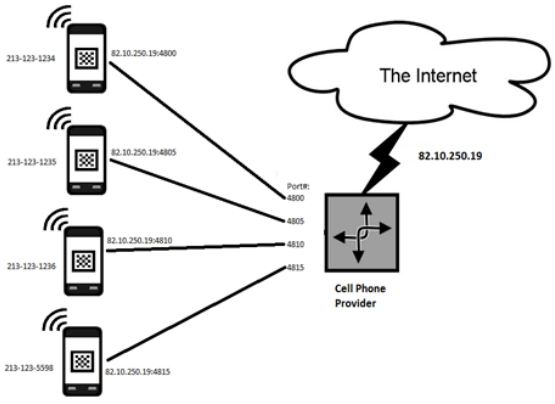
Routers use a "router table" to keep track of devices that share an IP address. This router table takes a device's media access control (MAC) number, which acts similarly to a serial number, and assigns that device an internal IP address. When traffic from the Internet is sent to the router, the router will route that traffic to the specific targeted device. The other devices on the network do not get that information.



NAT diagram: In the above figure, the public or external IP address is 82.10.250.19, which is assigned by the ISP service provider. The router has an internal IP of 192.168.0.1. Any device attached to the router by either hard wire or wireless connection has a similar address of 192.168.0.xx. All requests to access the internet from the internal devices (192.168.0.xx) go to the router, which then makes the request of the ISP through the external address of 82.10.250.19. The internal devices do not communicate directly with the ISP or the Internet.

Port forwarding works the same way that NAT works, but rather than have a router assign multiple private IP addresses to connected devices the router assigns a separate port number to each device using a singular IP address. Port forwarding is used in IPv6 addressing.[36]

As IPv6 addressing has become more common, port forwarding is of increasingly greater concern to investigators because ISPs now share a single IP address with multiple subscribers. Without the specific port associated to the IP address, an ISP will not be able to identify a singular subscriber; instead, it would only be able to offer a table of all subscribers who share that IP address. Investigators need to ask the original source of data for not only the IP address relevant to the investigation, but also the IP address ***with all associated port information*** relevant to the investigation.



[34]In addition to the connection log or lease information left on the router, and depending on the make and model of the mobile device, it may be possible to also demonstrate the connection between the mobile device and the SSID of a router at a particular location through the internal memory of the mobile device. [35]See https://en.wikipedia.org/wiki/Computer_network_diagram#/media/File:Sample-network-diagram.png. [36]Historically, and until 2012 IP addresses used what was called IPv4; however, with the explosion of devices attaching to the Internet, there were not enough IPs available. To alleviate this issue, IPv6 was created. For a more detailed discussion of IPv6 and its capabilities, see http://www.search.org/resources/e-crime-investigative-tools/.

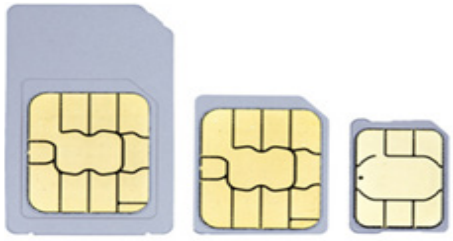
Cell Phone Port Forwarding: In the above diagram the cell phone company subdivides an IP address (82.10.250.19) by appending port numbers to the IP address. The port-forwarded IP address, 82.10.250.19:4810, now directs to cell phone number 213-123-1236.

Let's say a photo is discovered on a Facebook profile, depicting a gun used in a robbery. An investigator might send legal process to Facebook to obtain the information of the user who uploaded that photo. One of the identifying pieces of information would be the IP address that was used to upload that photo, because a person must be connected to the Internet to upload a photo to Facebook. Traditionally, asking for the IP address would allow the investigator to identify a business (like a Starbucks) or a residence that the investigator could use to continue the investigation. However, if this IP address has been port forwarded and the legal process lacks a request for port information, the investigator might receive information on 100 businesses or residences in response to the inquiry. This would make the investigation much more difficult. Port addresses, in addition to IP addresses, must be an item that is specifically demanded in legal process to narrow the investigation to a single business or residence.[37]

Information Recoverable from Mobile Devices

The fragmented market of mobile devices presents a real challenge to acquiring data, as each device presents unique nuances. Most smartphones rely on either the iOS (iPhone operating system) or Android OS (operating system). Apple released the first iOS in June 2007, while Google released the first Android OS in September 2008. Apple has released seven generations of iPhone models (1st gen, 3G, 3GS, 4, 4S, 5, 5C/5S, 6/6+, 6S/6S+, 7/7+) and 10 generations of their iOS. Android interfaces are much more fragmented.[38] As of August 2015, OpenSignal reported 24,093 distinct Android devices covering 1,294 brands.[39] Android has released 14 "flavors" of OS (alpha, beta, cupcake, donut, eclair, froyo, gingerbread, honeycomb, ice cream sandwich, jelly bean, KitKat, lollipop, marshmallow, nougat), and as of June 2016 has current distribution on 9 flavors.[40]

Generally, if you can hear, see or watch data or material on a mobile device, it may be recoverable from the actual device using a variety of extraction techniques. Mobile devices typically offer three areas where evidence may be recovered: internal memory, a media card, or a SIM card. The internal memory is the amount of storage space on the mobile device at the time of purchase.[41] A media card is a small storage device made up of flash memory. These cards are also referred to as "memory" or "flash memory" cards. Several memory card manufacturers currently advertise micro SD cards with storage capacities of 512 gigabytes.[42] The third potential area of internal memory is the SIM card on GSM network-enabled mobile devices. A SIM card can come in one of three formats: standard, micro, and nano. The SIM card will generally contain the personal information of the account holder, contacts or address book, and text messages. The most current model of SIM cards is embedded with Secure Elements to also retain credit card information.[43] This graphic demonstrates the different sizes of SIM cards.



Standard ***Micro*** ***Nano***

From these three sources investigators may recover data that includes text messages, calendar events, images and movies, emails, notes, voice notes or audio files, and application data. Text messages come in two formats: SMS (Short Messaging Service) and MMS (Multimedia Messaging Service). The SMS format limits the message to 160 characters.[44] And while the name MMS implies that the message will contain audio or a visual component, this is misleading. On a smartphone, any text message over 160 characters is designated as an MMS message. Think back to the days of flip phones and early BlackBerry phones. When you sent or received a "long" text message from another device, it was usually broken up into parts (one of three, two of three, etc.). Today, that message will come in as one complete text.

Phones use flash memory, which like a USB drive stores data in pages and blocks. Just as data can be recovered on a USB device, if it has not been over written, it can be recovered from a mobile device. However, the ability to recover deleted data from a mobile device is not guaranteed and is device specific.[45]

Data Extraction Methods

The process of acquiring data from a mobile device is often referred to as "mobile device extraction."[46] Regardless of the nomenclature used to describe the process, there are generally five different extraction methods: manual, logical, filesystem, physical, and JTAG.

---

[37]While the best course of action is to always ask for the IP address with all associated port information, there may be companies who do not keep this information. [38]See https://en.wikipedia.org/wiki/IPhone [39]See https://opensignal.com/reports/2015/08/android-fragmentation/ [40]See https://en.wikipedia.org/wiki/Android_version_history and https://en.wikipedia.org/wiki/Android_version_history#/media/File:Android_historical_version_distribution_-_vector.svg). [41]For example, Verizon Wireless is offering the iPhone 7 with internal memory storage capabilities of 32, 128, or 256 gigabytes. See https://www.verizonwireless.com/smartphones/apple-iphone-7/#sku=sku2150065 (last accessed November 20, 2016). [42]See http://www.bestproducts.com/tech/gadgets/g658/best-sd-memory-cards/ and https://www.mymemory.co.uk/SDXC [43]See http://security.stackexchange.com/questions/134527/what-is-the-difference-between-secure-element-and-smart-card [44]See http://latimesblogs.latimes.com/technology/2009/05/invented-text-messaging.html [45]For example, data deleted from a mobile device through a remote wipe—Apple and Google offer this functionality—is unrecoverable. [46]There is currently a rather significant debate among digital analysts about whether pulling data from a cell phone is considered forensics. Rather than getting caught up in that debate and creating potentially confusing testimony, SEARCH posits that the better terminology is extraction and when referring to the process adopt the language of the Massachusetts Digital Evidence Consortium and refer to the process as a digital device examination.

Manual Extraction. The most basic extraction method is the manual process. This is sometime referred to as the "low-tech" or "thumb" technique, in which the investigator physically manipulates the user interface to connect with the phone, and then examines the visible data to look for and capture data. An investigator generally documents the data by taking screenshots of what appears on the phone. This method has severe limitations in terms of what may actually be recovered, and also should be assiduously documented as it is most likely to alter information on the device.

Logical Extraction. The second type of device extraction is a logical extraction. This process involves using specialized software to extract the data containers in the mobile device.[47] These containers typically include the Contacts, Call Logs, SMS/MMS messages, media, and some app content.

Filesystem Extraction. The filesystem extraction process involves using specialized software to make a copy of the complete filesystem on a mobile device. This provides all the data from a logical extraction as well as files and hidden files on a mobile device. Some examples of data that might be contained in these files and hidden files include user-deleted data, EXIF data on images, and email header information. *Physical Extraction.* The physical extraction process involves using specialized hardware and software to not only obtain all the information from the file system of the phone, but also create a bit-for-bit copy of the flash memory of the phone. This will provide all the data from a logical extraction, the files and hidden files from a filesystem extraction, and also the deleted content and the content the device is collecting without the user's involvement knowledge, such as GPS information, Wi-Fi networks, and passwords. This process often requires the use of a specialized software programing called a "boot loader" to accomplish a physical extraction.[48] It is extremely important to understand that the use of a boot loader will make changes to the underlying flash memory of the phone. Investigators should make sure to carefully document those changes in a report that can be tendered in discovery.

JTAG/Chip-Off Extraction. The fifth and final method of extracting data from a mobile device is referred to as JTAG or Chip-Off. A "chip-off" is an advanced extraction and analysis of the data from a mobile device. This method requires that the memory chips from the device be physically removed so investigators can then acquire the data. A chip-off will make the digital device inoperable because the memory chip is removed from the device and cannot be re-attached. However, the data on the chip is preserved during the chip off process.[49]

Data Encryption

Anyone reading the news in the past year will undoubtedly have stumbled across a headline claiming *"FBI, Apple Eye New Fight Over Encryption,"* or one substantially similar.[50] Encryption is the process of changing information through a cypher in such a way that no one other than the person who holds the key will be able to read it. Data stored on digital media normally is stored in plain text. In order to secure the data from an unintended recipient the user would need to encrypt it.[51] Encryption turns part or all of a message, file, folder or hard drive into unreadable text using a particular encryption algorithm. The process usually involves the use of a unique encryption key that specifies how the data will be encoded. While anyone is able to see the scrambled encrypted text, the underlying actual data is incomprehensible. The only way to decode the encrypted text is to use the correct decryption algorithm, which requires the specific decryption key that will translate the data back to plain text. Without the key to unlock or translate it the encrypted data remains unintelligible. There are now multiple cloud-based data sites that market services that encrypt data.[52] The robustness of the encryption key determines whether an investigator can crack the key without it having been provided.

An emerging phenomenon occurring with application communications is that application providers are offering end-to-end encryption, often referred to as "E2EE."[53] E2EE means that when a communication is in transmission—that is, moving from one digital device through cyberspace to and arriving at another digital device—the entire communication is encrypted. Legal process to obtain the communications from the server side of would produce unusable data: without the encryption key, the data would be unreadable.

Recovering Evidence from Non-Mobile Digital Media

With the plethora of devices capable of storing digital evidence, it is important to understand how to properly examine these devices to recover relevant artifacts. In addition to mobile devices, crime scenes today often contain desktop or laptop computers, gaming devices, USB drives, and memory cards. Evidence from these digital media will often be recovered from one or two areas: digital media and random access memory (RAM).

---

[47]There are multiple software programs on the marketplace to complete logical, filesystem, and physical extractions of mobile devices. Based on the number of different mobile devices and operating systems, SEARCH staff has not discovered one program that is compatible with every device. [48]A boot loader is a program that will install an operating system while a device is running. For example, a boot loader will allow a specific data extraction program's operating system to be added to a mobile device that will pull the information from the phone's memory However, by adding the bootloader, the file system on the phone will undergo some changes. [49]A chip-off is the last resort for accessing data stored on a mobile device. Generally, if the process is going to be used for a criminal investigation notice of the destruction of the underlying digital device should be given as required by state or federal statutes. [50]See http://thehill.com/policy/cybersecurity/299853-fbi-apple-eye-new-fight-over-encryption [51]With encryption, there is a distinction between data in transit and data at rest. For an in-depth explanation of the difference see: https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest [52]See http://spideroak.com for an example of one company that offers three different versions of encryption of data, communications, and encryption password protection. [53]As of the drafting of this article, the following applications have instituted E2EE for their users: Facebook Messenger (secret conversation), Allo-Google (incognito mode), Viber, Line (letter sealing), Signal, Cyber Dust (messages deleted once read), Telegram (secret chat), and What's App.

Digital Media

The term "digital media" refers to the physical devices known as hard drives, thumb drives, and the memory cards that exist on the device itself. Digital media is designed to store data, be it documents, pictures, music, or videos. Hard drives fall into one of two categories: the traditional platter hard drive and the new solid-state or flash memory drive.

traditional platter hard drive

solid-state or flash memory drive

Traditional hard drives consist of platters with read/write heads floating on top of and below each platter. This allows data to be read or written to both sides of the platter. Solid-state drives contain memory chips where data is written. How the data is actually written in either type of drive is proprietary to each manufacturer. All drives are equipped with software, called firmware, which handles the actual read-and-write function of the drive. The firmware communicates with the operating system in a virtual mode that allows the operating system to use a file system to organize the storage of data.

Digital media using Microsoft Windows as an operating system is made up of small storage units called sectors. Sectors are numbered sequentially, starting with zero. Each sector generally holds either 512 or 2048 bytes of data. (Each character that you type on the keyboard is one byte. The character "A" = 1 byte). Digital media based on the MAC OS is made up of allocation blocks, generally these also hold 512 bytes of data.

A digital media device only does two things: it reads or writes data to/from the sectors. It never deletes data, but it can overwrite the existing data with new data. It does not track ownership of the data, nor does it track if the data is modified once it is written.

The management system that tracks which sectors store the data that make up the files is called the file system. It manages all of the sectors on the media assigned to it. The file system is also stored in sectors on the digital media, and is similar to a database or spreadsheet. The file system database tracks the name of the file, the size of the file, the date it was created, the date if the file has been modified, which sectors store the data, and if the file has been deleted.

```
Directory of D:\

autorun  inf              182 04/09/2015  03:14 PM
BOOTMGR                398,356 03/18/2014  07:29 AM
bootmgr  efi         1,601,880 03/18/2014  07:29 AM
bootmgr  exe           651,096 03/18/2014  04:18 AM
grldr                  279,239 09/26/2014  07:32 AM
menu     lst             1,457 04/09/2015  03:22 PM
PECMDEXT INI             1,095 04/09/2015  03:11 PM
WIN81~1  CD                  0 04/09/2015  03:15 PM
BOOT          <DIR>            04/09/2015  03:22 PM
efi           <DIR>            04/09/2015  03:22 PM
sources       <DIR>            04/09/2015  03:22 PM
dir      txt                838 12/01/2016  03:36 PM
               9 File(s)      2,934,143 bytes
               3 Dir(s)   1,039,872,000 bytes free
```

Before hard drives, data was stored on small storage devices called floppy disks. When hard drives were introduced as data storage devices, they could hold much larger amounts of data. However, the file systems on floppies had mathematical limitations as to how much data they could track. To work around the limitation of the early file systems, programmers devised a method to divide the hard drive into discrete areas called partitions.

A drive may be partitioned into one large zone in which all of the data, such as the operating system files, programs files, and data files is comingled. Alternatively, multiple partitions may be used to separate the operating system and program files from data files. One partition would hold the operating system and program files while a separate partition would hold all of the data files.[54] Whichever partitioning method is used, each partition is managed by a separate file system that manages the files within that partition.

Random Access Memory (RAM)

The second area of information is the random access memory, or RAM.[55] RAM is separate from the memory used for data storage, such as hard drives, thumb drives, and DVDs. RAM is used by the computer to link the programs that are running on the system to all hardware devices in the computer. As an example, when creating a Word document, the Word application is running in RAM. While working on the document, it is displayed on the monitor from RAM. When it is printed, Word sends the document through RAM to the printer. When it is saved, Word tells the operating system to save the document to the hard drive. The operating system then sends the data from RAM to the selected storage device. The computer performs various tasks effectively simultaneously, using RAM memory to allow it to run multiple programs or applications and

[54]Unless the offender has exceedingly strong technology skills it is likely that the hard drive is set up with a specific partition that hides all of the contraband material or criminal activity. [55]RAM is the acronym for Random Access Memory. This is also referred to as volatile memory, meaning that it has to have a power source to remain active.

perform various processes.[56] Once the machine is turned off, the RAM is deleted and unrecoverable. However, if the computer is up and running, the RAM may contain useful information on settings, passwords, and other recent activity that may be critical to a case.[57] The acquisition of RAM is often referred to as a "RAM dump."

Useful Digital Media Forensic Artifacts

A successful investigation and prosecution for any criminal prosecution requires more than a digital device analyst taking the stand, pointing to a piece of digital evidence, and testifying that the contraband was found on the device. In addition to the evidence supporting the charges being found on the digital device, our criminal justice system requires evidence that a person bears responsibility.[58] There are several specific artifacts that appear during digital evidence analysis of digital media that may provide evidence of intent, knowledge, modus operandi, and absence of mistake.[59]

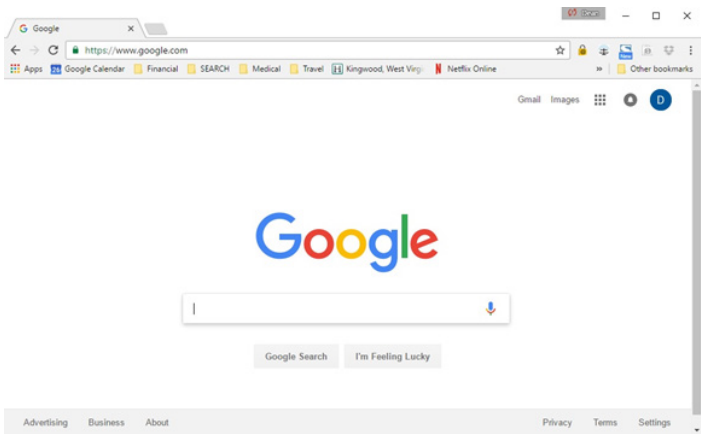
The process of extracting data from a hard drive, USB, or other media device is often referred to as a computer forensic examination.[60] Usually the examination consists of three parts: the acquisition, authentication, and analysis of digital media:[61]

- Generally, the acquisition consists of using a write-blocking device to forensically image the contents of the suspect drive to a separate drive or digital media.[62] This device is used to ensure that the contents of the original digital media is not altered.[63]
- After imaging the data recovered is compared to the contents of the original digital media most commonly through a hash match.[64]
- The final step of the forensic process is to analyze the contents of the forensic image of the digital media.[65]

The analysis done is dependent on the legal authority and the type of case being investigated. However, there are some common forensic artifacts that are likely to be universally useful.

Device Registry Artifacts

In cases involving a Windows based digital device, one of the most important areas to understand in digital media analysis is the device registry. The registry is the location on the drive that contains configuration settings, controls, account information, and stored passwords associated with the device. In a MAC OS digital device, this data resides in the PList and Log Files. Regardless of the specific operating system the digital device is using, think of these areas as the digital media's brain or the equivalent of the human brain stem. The registry also contains a list of recently opened, extracted, or viewed files and which program on the device was used to open the files. The registry also records the URLs, Uniform Resource Locators, the device visited in the past. The URL is the address typed into a web browser to take a device user to a particular website.[66] For example, a person who knows they want to go to the Google website would open a web browser and type in the URL www.google.com. The action of typing in www.google.com would be stored in the typed URL's folder within the registry.



Another area to explore in the digital media's registry is the saved passwords.[67] Using our example above, the offender not only wants to go the Google page, but also wants to access his Gmail account. In an effort to save time, when his default web browser, Internet Explorer, offered him the option of saving his user name and password for subsequent visits to the site, he readily checked the box. As a result, that user name and password is stored within the computer registry.[68]

A .lnk file, also called a link file, may also be recoverable from the computer's registry.[69] These files create a path for the operating system of a digital device to a specific executable file (an .exe file). In essence, the .lnk file is a shortcut that allows the operating system to navigate to the executable file more quickly.[70] Digital media devices do not automatically create .lnk files. Instead, the device accessed a program that looked for a specific file to create the .lnk shortcut. External devices plugged into a computer may also create a .lnk file. For example, let's say an offender has placed all his contraband movies on an external USB device and plugs that device into his Microsoft Windows machine. He then uses the Windows Media Player program to access one of the movies on the external drive to watch it on the computer. The actions of accessing the external device with Windows Media Player would create a .lnk file, which would

[56]http://searchstorage.techtarget.com/definition/RAM-random-access-memory Technically the computer is not performing the actions simultaneously but rather serially but incredibly quickly, and it thus appears to the user as though the actions are simultaneous. (At least I think that's right.) [57]The failure to secure RAM from a live machine could have significant consequences. The defense may argue that the failure to secure the RAM deleted exculpatory evidence. Additionally, if a device is encrypted and the password is not obtained before shut down, it may be impossible to gain access to the device (depending on how robust the password is). [58]See United States v. Lowe, 795 F.3d 519 (6th Cir. July 28, 2015) in which the Appellate Court reversed a jury's guilty finding holding that no reasonable jury could have concluded the defendant's guilt based on the lack of evidence that the defendant was controlling the computer at the time the contraband material was being downloaded or offered for download on a peer-to-peer network. This case is an excellent example of the need to adequately present the forensic artifacts from a digital device analysis in court. [59]The phrase "digital evidence analysis" was coined by the Massachusetts Digital Evidence Consortium to describe the best practice analysis of any type of digital media. [60]The phrase "computer forensic examination" was first conceived at a training in Portland, Oregon in 1991, by the International Association of Computer Investigative Specialists (IACIS). [61]There are several digital media scholars who posit that a computer forensic examination also includes providing testimony in court. This article focuses only on the acquisition, authentication, and analysis stages of the process. [62]For further information on write-blocking devices, see http://www.cru-inc.com/data-protection-topics/write-blockers/ [63]Write blockers only work in a read-only format on the original digital media. [64]For further explanation of what a hash value is, see Authentication in the Digital Age, in publication in 2017. [65]All analysis or other use of the evidence from a case should take place on the forensic image and the original evidence of digital media should be placed into secure storage. [66]Technically a URL can also point to an FTP site or to other parts of the Internet, but those are much less common than web addresses. Note also that a URL can point to a location on the device itself – the URL means only that the file was opened with the browser. [67]Depending on the operating system, and the choices selected by the user it is possible that some saved passwords and user names may not appear in the registry, but in other places, for example within the web browser files of the user. [68]The specific file path within the registry for auto complete passwords is: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2. For additional file path locations for other stored passwords, see http://www.nirsoft.net/articles/saved_password_location.html [69]The file directory of a particular partition of a digital media device may also create .lnk files. [70]The actual .lnk will not be found within the registry, however the MRU(most recently used) file path will be found in the registry. This path will provide the .lnk for the file that was recently accessed. For additional information on .lnk files, see http://whatis.techtarget.com/fileformat/LNK-Shortcut-file-Microsoft-Windows-9-x

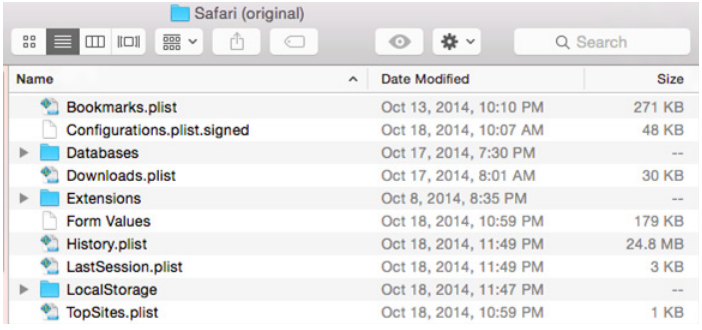
show the shortcut the operating system took to access the specific movie played from the external storage device. It is important to note that the .lnk file will likely be resident on the digital device itself, not on the external storage device. A computer analysis thus may identify additional external storage devices of interest.

In some instances, the most recently used files, generally designated as either MRU (Most Recently Used) or MRA (Most Recently Accessed) will be of importance.[71] MRU is a term used in computing to refer to the list of programs or documents that were last accessed. It is a feature of convenience allowing users to quickly see and access the last few used files and documents.[72] Digital evidence analysts can review the MRU/MRA file for objects of interest.

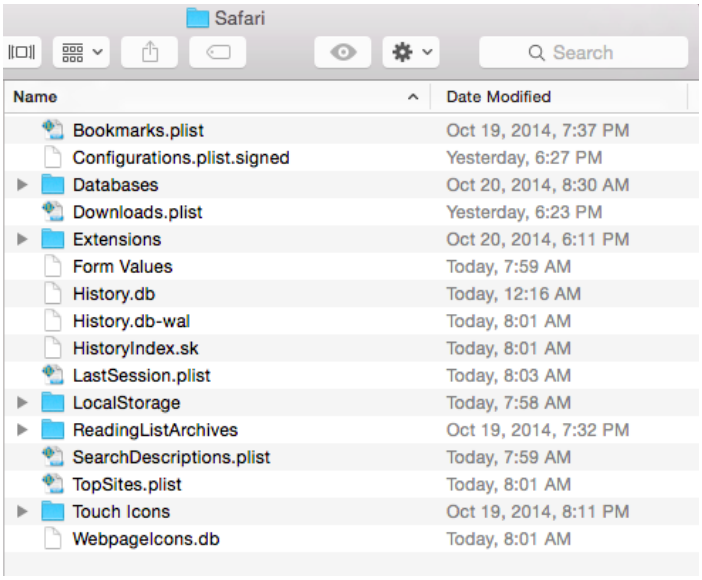
Web Browsing History

There are many useful artifacts outside of the computer's registry as well. One of the most useful is to look at the web browsing history of a particular device.[73] While there are multiple web browsers available, there are six main ones that are commonly encountered: Firefox, Google Chrome, Internet Explorer (Soon to be Edge), Abri and Safari. Windows-based machines—specifically those that run operating systems prior to Windows 7 or Internet Explorer 7 and above—create an index.dat file.[74] The index.dat file will contain information about the Internet sites the user visited, including dates and times. The web browsing programs in Windows 8 and newer operating systems replaced the index.dat file with a different file called WebCacheV01.dat. Within the WebCache file are subfolders called container.dat.[75] The details of the web browser history and websites visited that used to be in the index.dat are now all in the container.dat files.

In MAC OS digital devices Safari is the default web browser. Prior to the Yosemite OS upgrade, Safari used a folder similar to an index.dat; however, the MACOS called it the history.plist file.[76]



With the update to Yosemite, Apple discarded the single history.plist file and instead replaced it with several files, including History.db, History.db-wal, and HistoryIndex.sk. The data that once was in the single file has now been spread across the three files.[77]



The information contained in the web browser history may provide clues and additional information that demonstrate the identity of the user at the time offenses were committed. A hypothetical will help explain. An offender opened Internet Explorer and started a web session where he ran Google searches for terms normally associated with child exploitation. In this particular case, the terms he used were PTHC and DaddyDoesDaughter.[78] Google returned multiple websites that were responsive to his search terms. The offender then selected one of the sites by using his mouse to select the hyperlink pointing the web browser to the specific website. He then selected several movies that were available to download and saved them to an external USB that was plugged into the computer. While he was downloading the movies, he also opened up several other search windows within his browser and checked his Facebook account, his bank account, paid his utility bill online, and looked at his credit card statement on the issuer's website. Once the movies were downloaded, he used Windows Media Player and watched each video. Each one of these activities may create a separate record in the .dat or .db files of where the web browser went on the Internet.[79] Each one of those activities may require the use of a password and user name. Investigators could send the appropriate legal process to the separate companies to secure records demonstrating ownership of the underlying account.[80]

In the same hypothetical, the digital media would also create a .lnk file path showing the shortcut from Windows Media

[71]For a list of locations of MRU lists, see http://forensicswiki.org/wiki/List_of_Windows_MRU_Locations [72]See https://en.wikipedia.org/wiki/Common_menus_in_Microsoft_Windows#Most_Recently_Used_menu [73]There are several different methods to limit the collection of web browsing history, and several web browsers have specifically created modes of searching that do not retain data. For example, Firefox allows users to open a private window under the File tab on the tool bar that opens a web browser session that proclaims "Private Browsing with Tracking Protection" and then details the information they do not keep, but takes it one step further and explains how the browsing pattern may be recorded by other entities. [74].dat files stand for data files in either text or binary format. [75]For additional information on the specific file path to recover web browser history, see http://www.thewindowsclub.com/index-dat-file-windows [76]Illustration source: https://discussions.apple.com/thread/6615000?start=0&tstart=0 [77]Illustration source: https://discussions.apple.com/thread/6615000?start=0&tstart=0 [78]The acronym PTHC stands for pre-teen hard core and is one of the more common terms used in file names of child pornography. [79]It is possible that a software or hardware program was being run that eliminates web history from the .dat files, container.dat files, history.plist, or history.db files on the digital media. [80]For the proper type of legal process and potential information to search for, see infra Search and Seizure: Securing Evidence from the Cloud, pg 32.

Player to the external USB drive. It is a compelling argument to break down the multiple, intentional, separate steps the offender had to take to acquire the child exploitation material: opening a web browser, picking a search engine, entering the terms to find the material, selecting the website where the material was found, plugging in an external USB to the computer device, selecting and downloading each movie file, opening Windows Media Player, searching for the external USB device, and selecting each individual movie for viewing.

Digital Photographs

When a digital camera is used to create photographs, it also embeds data with the file that contains the digital image. The additional data is referred to as "exchangeable image file" format or EXIF data. EXIF data may contain a myriad of information about the digital photo, including the type of camera, or smart phone camera used to take the photo, the camera make and model, the serial number of the camera lens, the camera settings, if enabled, GPS data, the camera owner's name. A person looking at a digital photograph will not be able to see the accompanying EXIF data. Readily available, specialized software is necessary to see EXIF data. However, digital photographs do not always contain EXIF data.[81] Using certain types of editing software allows the user to remove or edit and change the EXIF data. Likewise, a photo downloaded from a social networking website likely will not have any EXIF data, as many of these sites strip that information before the image is uploaded for viewing by other site users.[82]

Data from Cars

Technology advances in automobiles provide the additional repositories of digital information. Automobiles are becoming more computerized. According to one article, the average car has between 25 and 50 central processing units to operate certain functions.[83] One of those systems is the Event Data Recorder.[84] Commonly referred to as "black boxes," EDRs are required to store the data for 15 different processes when the car engages in certain crash type activity. In addition, there are approximately 30 other voluntary processes that the EDR may record.[85] In addition, after-market services such as Hum, the Verizon program, allow for monitoring of a car, such as geofencing the car when a certain person drives it, setting speed governors.

Mobile Device Apps

Every mobile device owner has the option to download individual applications. An application is simply a program or complete software or hardware process that allows a user to engage in certain activity. If you think back to the days of installing programs on computers from floppy disks, a rather complex program would require multiple disks. A user would have to install each disk one at time, one of 10, two of 10, etc. With applications, the entire program is downloaded to the mobile device at one time. Once the entire application is downloaded, the user may then open the app and begin to use the program. For many of these applications the first three questions that are posed to the user request access to the user's contact list, the ability to push notifications to the user, and to turn on location services when the application is in use. Often the program is not just self-contained to the device, but reaches out through a data connection to the servers in the cloud where the application originated.

For example, Kik, a communications application that originated as a text messaging service, allows users to download the application and then begin to send messages to other users. A user may create a specific user name and send individual messages or group messages. In addition, Kik allows the user to add emojis to a message.[86] Kik also allows users to send image and movie files. In 2016, Kik added a search engine to its capabilities, so a user does not have to open a separate web browser to conduct a search on the web.[87]

Search and Seizure in the Digital Age:
Securing Evidence from Cyberspace

Information stored in cyberspace is controlled by the Fourth Amendment and several specific federal statutes and some state statutes.[88] This also applies to data in the cloud. It is difficult to go an entire day without seeing some type of advertisement for the cloud, whether it is communication service or data storage.[89] While there are several different types of clouds, for purposes of law enforcement attempting to gain access to the information, the specific functionality of the cloud type is irrelevant.[90]

The question of whether content stored in the cloud is protected under the Fourth Amendment was answered in large part by the United States Supreme Court's decision in the *Riley* and *Wurie* cases.[91] Also of note was the Court's discussion of cloud computing and privacy implications.In dicta, the Court pointed out that a police officer's access of information remotely, i.e., stored in the cloud, through a cell phone would certainly not be permissible pursuant to a search incident to arrest. The Court mentioned the government's acknowledgment that a search of a mobile device that triggered access to cloud-based storage would require a second warrant.[92] The Court noted that the determination of where the data was being accessed, either on the mobile digital device or in the cloud, might be difficult to ascertain.[93] Thus any officer encountering cloud-based data or access to

[81]For example, Irfanview is a common Firefox toolbar add-on that enables users to view EXIF data associated with a particular digital image; see www.irfanview.com. Another common EXIF tool for videos is ExifTool; see http://www.sno.phy.queensu.ca/~phil/Exiftool/. [82]For example, Facebook removes all EXIF data for images and movies posted by users before they are accessible to other users on the site. [83]See http://www.theglobeandmail.com/globe-drive/how-cars-have-become-rolling-computers/article29008154/ [84]In 2014, the National Highway Traffic Safety Administration proposed making EDRs mandatory in all automobiles. See https://fas.org/sgp/crs/misc/R43651.pdf [85]See http://www.theglobeandmail.com/globe-drive/how-cars-have-become-rolling-computers/article29008154/ [86]An emoji is a small digital image or icon used to express an idea, emotion, etc., in electronic communication. [87]See www.kik.com for the different type of communications available through the Kik application. Each different method of communication or process through an application is sometimes called a "platform." When applications add different or multiple platforms, they are considered a multi-functionality application. The evolution of the applications often occurs within social media or communication applications. So as Kik is configured, it is considered a multi-functionality application. [88]These include the Electronic Communications Act (ECPA), Privacy Protection Act (PPA), and state analogues of ECPA, of which the California Electronic Privacy Protection Act (CalECPA) is the one that least comports with the federal statute. [89]Often the banner ads across the top and sides of web based searches contain advertisements for different cloud-based services. They range from data backup to communication applications or online multiplayer games. [90]Generally, there are four different types of cloud based platforms, including Public, Private, Hybrid, and Community. Within the four platforms, there are generally three types of services offered: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). For additional information on cloud structure, see: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf and http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-293.pdf [91]See Riley v. California and United States v. Wurie, 578 U.S. ___, 134 S.Ct. 2473 (2014). [92]Id. at 2491. [93]Id.

cloud-based data is on notice that unless specifically covered in an existing warrant, a new warrant must be secured to access the data.

In addition, data in the cloud, held by most service providers enjoys protections under the Electronic Communications Privacy Act (ECPA). The ECPA covers both communications that are moving (18 USC 2510 et seq and 18 USC 3121 et seq) and data at rest in ECPA's subsection the Stored Wire and Electronic Communications Act (SCA)(18 USC 2701 et seq).

An example may help explain whether a communication is in transmission. Suppose you have Anne and John. They meet at an event and decide that they like each other and trade emails, Anniesunshine1@msn.com and JohnnyKicks@yahoo.com, with the thought of meeting later to go out. John gets home following the event and sits down at his computer, points his web browser to his email, and composes a message to Anne at her email address. He then hits send. The message is broken up into smaller packets of information and travels from John's computer to the servers at Yahoo! They are then routed across the Internet to MSN, where MSN collects the various packets, re-assembles them, and then places them in Anne's inbox as an unread email. Upon getting notice of the new email on her mobile device, Anne accesses her account and views the message. When is the email no longer in transmission? A common sense answer would probably be when Anne opens the email and reads it. That would be incorrect. The email in question is no longer in transmission when MSN receives the packets of information and configures them into the original email. Once that step is completed for purposes of the federal statute, the email is no longer in transmission. Once the provider has placed the email into Anne's inbox it is considered to be in electronic storage.

You may have just read that paragraph and asked why you might care about something so apparently hyper-technical. The reason is that the ECPA enacted different legal requirements to obtain communications that are in transmission as opposed to those that are in storage. If a communication is still in transmission, in order to obtain its contents or intercept it, law enforcement must use either a Title III (intercept) order or the State Court equivalent. If the communication is no longer in transmission, the SCA dictates the steps law enforcement must take to secure the information.

The SCA creates three levels of privacy for communications:[94]

1. **Subscriber data:** This is enumerated in the statute as the identity of the account holder, address, phone number or email address or user name, type of service, length of service, and original IP address when account was created. If the account is a paid service subscriber data would also include the means and source of payment.[95]
2. **Transactional data:** This includes the date, time, and duration of the communication or access to the Internet, but more broadly encompasses any material that is neither enumerated as subscriber data nor defined as content.
3. **Content:** This is defined in the statute and includes everything pertaining to the substance, meaning or purport of the communication.[96]

For a moment, imagine that our hypothetical scenario with Anne and John occurs using pay phones instead of emails and instead of sending a message, Anne and John have a conversation. The ECPA applies to that conversation. The location of the two pay phones, the number assigned to each call, and who owns those phones would be subscriber data. The date and time, duration of the communication, and the number called would be transactional data. The actual conversation would be the content. The same levels apply to communications over the Internet. So accessing the name under which the email sender signed up for service would be subscriber data. The dates and times the user was connected to the service, including the routing and signaling information as well as header information on the email is transactional data. The actual message within the communication constitutes the content.

In addition to breaking out the parts of communications or an account into the three different groups or buckets as above, the SCA also mandates the legal process required to access each different level of data. The more information that is sought, the higher the level of process required. For subscriber data, all that is required is a subpoena.[97] For transactional data, law enforcement must use a court order.[98] To obtain content, law enforcement has to use a search warrant.[99]

One very important aspect of securing data from cyberspace is the opportunity to delay notice to the subscriber.[100] For any government entity issuing a search warrant, court order, or subpoena pursuant to 18 U.S.C. 2703, an application and order from a court may be sought to delay notification to the subscriber.[101] According to the statute, the government must provide facts supporting one or more of the five enumerated conditions to justify delaying notice.[102] With privacy and government access to data recently taking center stage if an ongoing investigation would be negatively impacted

---

[94]See 18 U.S.C. 2701-2710 et seq., at https://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/html/USCODE-2010-title18-partI-chap121.htm [95]See 18 U.S.C. 2703(c)(2), at https://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/html/USCODE-2010-title18-partI-chap121.htm [96]See 18 U.S.C. 2703(c), at https://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/html/USCODE-2010-title18-partI-chap121.htm [97]See 18 U.S.C. 2703(c)(2), at https://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/html/USCODE-2010-title18-partI-chap121.htm
[98]See 18 U.S.C. 2703(d) at: https://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/html/USCODE-2010-title18-partI-chap121.htm. This is often referred to as a "specific and articulable facts" order or "D" order because the authority for the order is found at 18 USC 2703(d). The order has to contain language that specific and articulable facts that evidence relevant and material to a criminal investigation will be found in a specific location. [99]See 18 U.S.C. 2703(a), at: https://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/html/USCODE-2010-title18-partI-chap121.htm. There is an exception in the SCA for emails that are over 180 days old, but for practical purposes, it probably safer to use a search warrant to obtain any type of content. [100]See 18 U.S.C. 2705, at https://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/html/USCODE-2010-title18-partI-chap121.htm [101]Id.
[102]18 U.S.C. 2705(b)(1)-(b)(5): (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

if the target were to be informed it is critical for an investigator to obtain the requisite order to compel the provider to delay notice.

One hot topic for investigators and prosecutors is whether it is lawful to secure evidence from the cloud through mobile device extraction tools. There are currently several different software and hardware programs commercially available to extract information from mobile devices. This includes pulling usernames and passwords for third-party applications on the mobile device that access remote servers for functionality. While other mobile extraction devices and software would find the same information, there are some extraction tools that use the recovered forensic artifacts to directly access data on the remote servers through the third-party applications.[103] Once it has connected to the remote servers, the extraction tool uses the authentication information and credentials from the mobile device extraction and pulls all of the available data from the remote servers.[104] The actual data collected from the third-party server depends upon the individual application.

While these tools provide a unique opportunity to expedite the collection of data from third-party servers, there are Fourth Amendment issues that have yet to be tested in the crucible of criminal litigation. As a threshold, it is important to obtain authority in a warrant to access cloud data. If the facts of the case necessitate, it may be possible to do that with an anticipatory warrant, or to have a supplemental search warrant drafted and available to submit to judicial authority in the event circumstances arise.. In addition, there may be implications about extraterritorial searches, on both a state and federal level though more on the state. Certain states refuse to allow state search warrants for companies or information outside of the state.[105] Others allow for access to material outside the state whether held by a service provider or not, and still others only allow for access to material out of state when held by a service provider. A prosecutor familiar with these issues should be consulted prior to obtaining information through embedded credentials, whether on a mobile device or a computer.

Any warrant to obtain cloud-based information with embedded credentials should articulate why it is necessary to obtain the information in such a manner rather than through the more usual process of serving legal process on the cloud provider. Furthermore, anticipatory warrants should include a nexus between that device and the cloud-based material. The statement of probable cause must contain language that demonstrates that the user of the device has access to cloud-based applications and that evidence may be found in those locations.

For example, an offender is using an Android mobile device and downloads various applications through the Google store. For the mobile device to work, the device purchaser must have a Google account. The moment a user signs up for a Google account, he has access to the Google cloud. This is true for two reasons. First, everyone who has an email account technically has "cloud" access. When emails are being sent back and forth, they have to reside somewhere. That somewhere is on the servers of ISPs. Those servers are the "cloud." Second, Google allows a new user 15 gigabytes of cloud storage for free.[106] That means any user can store, share, and even invite others to see or collaborate on files and data in their Google Drive.[107] Including these details is imperative for any search warrant to establish the link between the criminal conduct and where it may be stored.

Securing Evidence from Cell Phone Providers

Similar to securing evidence from ISPs, there are three levels of service for data being stored by cell phone providers. Generally, all that is necessary to secure basic subscriber information and monthly phone records is a subpoena. However, to gain transactional data (CSLI) or "pinging" information, either a court order or search warrant is required. As of the writing of this article, every federal appellate court that has considered the issue has ruled there is no expectation of privacy in CSLI.[108] Currently, however, the Ninth Circuit has yet to have an appellate-level case, but district court decisions in the circuit have held that a person's CSLI does have an expectation of privacy and a search warrant must issue to secure the data.[109] Similarly, several states have also ruled a search warrant is required to obtain CSLI.[110]

Conclusion

There is no question that advances in technology, digital evidence, and digital media far outpace the law's ability to keep pace. However, it is incumbent on investigators and prosecutors to stay current on the latest developments. Some of the best evidence to corroborate cases may be found in digital media.

Biographies

Lead author Justin Fitzsimmons is Program Manager of High-Tech Crime Training Services for SEARCH, The National Consortium for Justice Information and Statistics. This national nonprofit organization provides training on how to conduct digital evidence investigations and the legal procedures and practices for handling cases involving digital evidence (www.search.org). He presents and teaches at conferences, workshops, webinars, and trainings on

[103]Cloud Analyzer is only one product with this capability, Lantern 5 from Katana has ICloud Extraction and Oxygen Forensics Detective 8.3 Cloud Extractor have similar capabilities. [104]For in-depth discussion, see Cellebrite's white paper on the functionality of the device: http://www.cellebrite.com/Media/Default/Files/Forensics/White-Papers/Extracting-Legally-Defensible-Evidence-From-Cloud_WhitePaper.pdf [105]New Hampshire is one state that has determined that a state warrant may not be used for extraterritorial content. See State v. Mello, 162 N.H. 115 (2011) holding that a state search warrant may not be used to learn subscriber data from an out-of-state service provider. [106]See https://www.google.com/drive/ [107]Id. [108]See U.S. v. Carpenter and Sanders, 14-1572/1805 (6th Circuit, April 13, 2016)(need citation), U.S. v. Chavez, 2016 WL 740246 (D. Conn., Feb. 24, 2016), United States v. Davis, 785 F.3d 498, 506-17 (11th Cir. 2015) (en banc), In re United States for Historical Cell Site Data, 724 F.3d 600, 611-13 (5th Cir. 2013), In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 313 (3d Cir. 2010), In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. 2703(c), 2703(d) Directing AT & T, Sprint/Nextel, T-Mobile, Metro PCS, Verizon Wireless, 42 F. Supp. 3d 511, 517 (S.D.N.Y. 2014) (collecting more cases) [109]See: In re: Application for Telephone Information Needed for a Criminal Investigation, 119 F.Supp.3d 1011 (N.D. Cal., July 7, 2016), United States v. Cooper, No. 13-CR-00693-SI-1, 2015 WL 881578, at *8 (N.D.Cal. Mar. 2, 2015). [110]See: Mass v. Augustine, 467 Mass 230 (Mass. February 18, 2014)

digital evidence collection, computer forensics, crimes against children, cybercrime, and human trafficking. He formerly worked as a Senior Attorney for the National Center for Prosecution of Child Abuse, and as an assistant state's attorney for Kane and DuPage Counties, Illinois. He is a graduate of the Illinois Institute of Technology's Chicago-Kent College of Law. Contributing authors are SEARCH staff Timothy Lott, Lauren Wagner, and Dean Chatfield. As Director of High-Tech Crime Training Services, Mr. Lott oversees a program that provides expert technical assistance and training to local, state, and federal justice and public safety agencies nationwide in electronic crimes investigations, systems security, and computer forensics. He is a former Deputy Probation Officer for Sacramento County, California, and was assigned to the Sacramento Valley Hi-Tech Crimes Task Force, which conducts multijurisdictional investigations involving crime where technology or identity theft is a factor. He earned a master's degree in Forensic Studies (Computer Forensics concentration) from Stevenson University, and is a certified Instructor through the California Commission on Peace Officer Standards and Training (POST). As High-Tech Crime Training Specialists for SEARCH, Ms. Wagner and Mr. Chatfield teach investigative courses, present at national and regional cybercrime conferences, assist justice agencies in active cases, and develop online investigative tools and guides. Ms. Wagner earned a master's degree in Forensic Science and a master's certificate in Forensic Computer Investigation from the University of New Haven. She is a certified Instructor though California POST, and also is certified in the Intermediate and Advanced Instructor Development levels of their Master Instructor program. Mr. Chatfield previously worked for the National White Collar Crime Center (NW3C) as a supervisory computer crime specialist, where he developed cyber and forensic course curriculum, managed development of NW3C software, and was liaison with Microsoft's Digital Crimes Unit on forensic evidence projects. He has 25 years' experience in law enforcement in Arizona and Colorado, as a criminal investigator, police chief, and field training officer. He is a Computer Forensic Expert certified by the International Association of Computer Investigative Specialists (IACIS).

APA Staff

CHILD ABUSE PROSECUTION PROJECT
ASSOCIATION OF PROSECUTING ATTORNEYS
11 DUPONT CIRCLE NW, 2ND FLOOR
WASHINGTON, DC 20036
CHILDABUSEPROSECUTION.APAINC.ORG