eForensics Magazine

MAGAZINE

OSINT in Forensics

Using OSINT to locate missing persons

Honeypotting Threats

Leveraging OSINT for DFIR

Autopsy 4.x, the GUI forensic analysis suite

VOL.08 NO.02
ISSUE 02/2019, (87) FEBRUARY
ISSN 2300 6986

TEAM

Editor-in-Chief
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Managing Editor:

Dominika Zdrodowska
dominika.zdrodowska@eforensicsmag.com

Editors:

Marta Sienicka
sienicka.marta@haking.com

Marta Strzelec
marta.strzelec@eforensicsmag.com

Bartek Adach
bartek.adach@pentestmag.com

Senior Consultant/Publisher:
Paweł Marciniak

CEO:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Marketing Director:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

DTP
Dominika Zdrodowska
dominika.zdrodowska@eforensicsmag.com

Cover Design
Hiep Nguyen Duc

Publisher
Haking Media Sp. z o.o.
02-676 Warszawa
ul. Postępu 17D
Phone: 1 917 338 3631

www.eforensicsmag.com

word from the team

Dear Readers,

We're happy to share with you the newest issue of eForensics Magazine - OSINT in Forensics.

Open source intelligence has a lot to do with digital forensics, and we're going to show you how true that is in this edition. Inside you can find articles on How to find missing persons using OSINT, Leveraging Open Source Intelligence for Digital Forensics and Incident Response, and Adopting a Hacker Mindset and Enhancing a Penetration Test through OSINT.

Also, you'll read about Honeypotting Threats for Security Research and Defense Improvement, learn something about Geolocation Forensics, and come into possession of Autopsy 4.x guide.

That's not everything, of course, but you should see for yourselves!

As always - we want to thank all authors, reviewers, and proofreaders for participating in this project.

Have a nice read!

Regards,

Dominika Zdrodowska

TABLE OF CONTENTS

Enjoy!

Geolocation Forensics

by Brett Shavers

Everything in this article addresses methods and techniques to place a person (or a device) at an exact physical location, anywhere on the planet. Varying methods have varying degrees of accuracy and varying degrees of reliability. When there is only one source of geolocation data, the reliability may not be as accurate or reliable when there are several sources of corroborating data sources. With that, how close can we get in narrowing down a person or device to a specific physical location?

One of the most important aspects of placing a suspect at the scene of a crime is that of geolocation forensics. This is a major point of any investigation. Electronic crimes, that is, crimes facilitated by technology, are no different than other crimes in that a successful case requires placing a person at a device, and most times placing that device at a physical location.

Geolocation forensics involves using the data that places a person or object at a physical location, coupled with that information to be used in a legal matter, either civil or criminal ("forensics" being the legal aspect). The principles are the same in geolocating a civil defendant as they are in geolocating a kidnapping suspect.

With today's Internet connectivity with various consumer devices, geolocation has been turning out to be the most effective method of tracking not only the historical locations of a suspect, but even the future locations based on predictive behavior.

Geolocation as defined in this article relies on more than electronic data and forensic artifacts as it includes the non-technical aspects and non-Internet connected artifacts of a suspect's historical locations. For example, a witness can testify to observing a person at a specific date at a specific time, which goes toward geolocation. Although witness testimony can be flawed, a witness can still provide reliable geolocation evidence, especially when corroborated by independent information.

How close can you get?

Everything in this article addresses methods and techniques to place a person (or a device) at an exact physical location, anywhere on the planet. Varying methods have varying degrees of accuracy and varying degrees of reliability. When there is only one source of geolocation data, the reliability may not be as accurate or reliable when there are several sources of corroborating data sources. With that, how close can we get in narrowing down a person or device to a specific physical location? The listed distances are estimates that can range in varying degrees depending on the situation. Table 1 lists many of the geolocation sources that can be obtained.

Source	Distance (*best possible*)	Notes
Fingerprints	1 meter	Lifting a fingerprint from a crime scene or from an electronic device ties that item and location directly to the suspect.
RFID	1 meter	RFID (radio frequency identification) transmits a low frequency RF signal to a reader, such as the RFID tags in retails stores to reduce shoplifting. Products can be tagged with RFID chips and tracked via readers along a predetermined route.
Eyewitness	1 meter	Witnesses who can affirmatively identify a suspect can give reliable testimony to the location, date, and time.
Video	1 meter	Security cameras can place a person at a specific place at an exact date/time, and if the video quality can identify the suspect, is one of the better means of geolocation of suspects.
Browser	3-10 meters	Internet browsers that allow the HTML 5 Geolocation API access draws upon GPS, the mobile network location, the Wi-Fi positioning system, and/or the IP address location to deliver the geolocation, depending upon which of these services are available at the time to the device.
GPS	5 meters	GPS (Global Positioning System) uses a constellation of satellites that transmit one-way signals to receivers to determine the position on Earth. Accuracy of the GPS location depends upon several factors such as weather conditions and environmental obstacles.
Assisted GPS	5-50 meters	Assisted GPS (Hybrid) supplements GPS by using cellular network data (cell towers). Assisted GPS is faster than GPS and can obtain location information when there is not a GPS signal.
Wi-Fi	5-15 meters	Wi-Fi Positioning System (WPS) works through the aggregation of wireless access point information (BSSID, MAC address) that is publicly accessible by scanning networks. Once the networks are discovered, they are recorded along with the location into public Wi-Fi location databases that are used for subsequent geolocation uses and as a supplement to GPS geolocation.
IP address	Physical address	The IP address, *if accurate*, can tie a device to a physical location. "Accurate" in that the IP address has not been spoofed or obfuscated through virtual private networks, or accessed via long distance means such as targeted antennas or war-driving.
Mobile (cellular)	500-1500 meters	Cellular positioning systems work off of cell towers as the mobile device connects to (typically) the closest cell tower. With triangulation of cell towers, the coordinates of the device can be found. The accuracy depends upon many factors such as urban areas compared to rural areas, the number and distance of each cell tower, and environmental factors.

Table 1: List of geolocation sources

Each of these sources listed show the '**best'** possible accuracy, which implies that the accuracy can be extremely inaccurate depending upon the source and external factors. For example, an IP address can be very accurate to a physical address, but can be spoofed or hidden via a VPN or Tor (The Onion Browser) and there is no accuracy at all. GPS, which is also very accurate, may not be available due to environment conditions. Cell towers are affected by environment obstacles such as buildings and land features, and so forth. But in combination, using as many of the sources possible, geolocation is highly accurate! Figure 1 is an illustration of geolocation accuracy by distance, which is helpful to visualize when collating data points of geolocation.

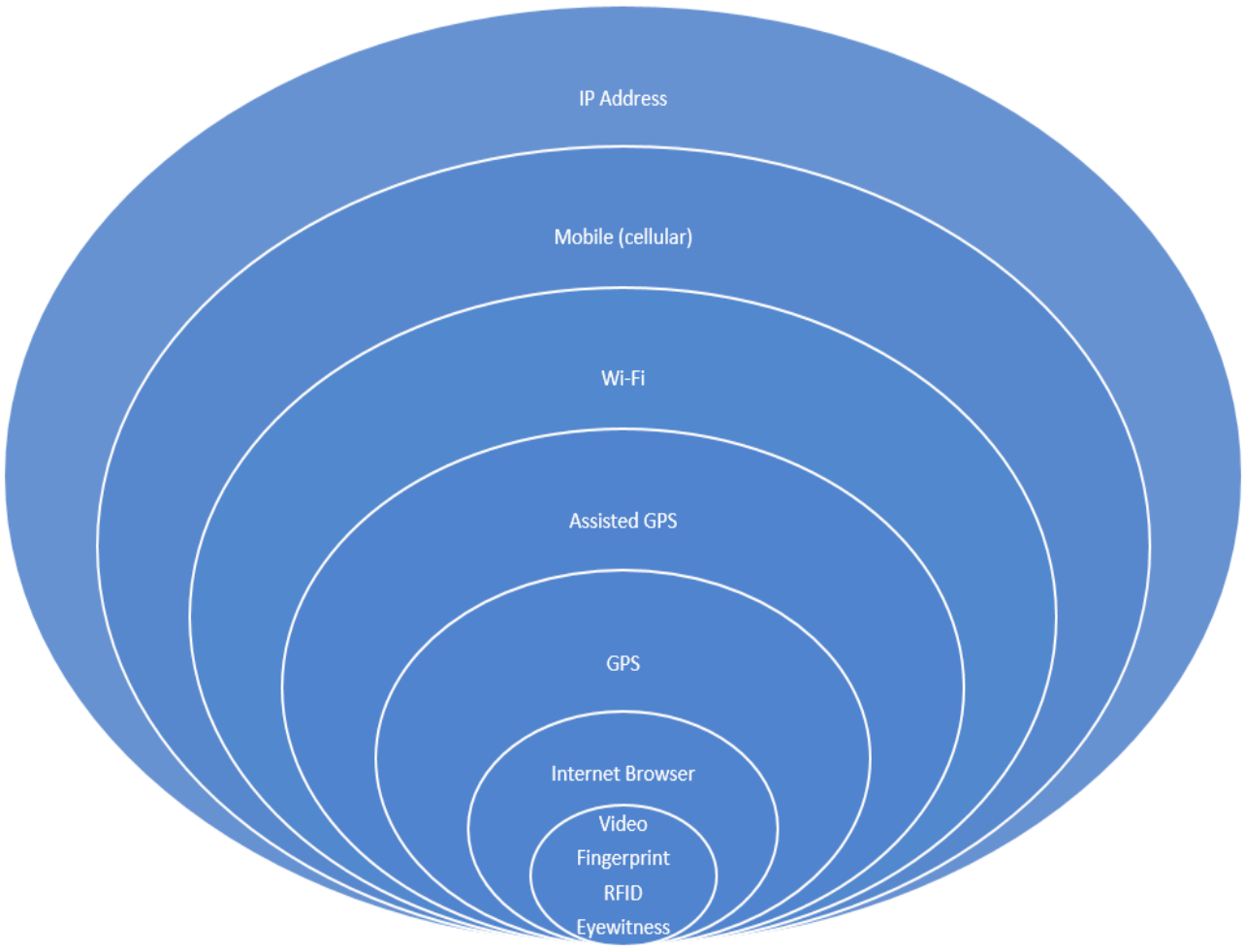

Figure 1 Rings of geolocation

Put on your detective fedora!

Given an incident, whether it be a crime scene or a computer-facilitated crime, one of the first questions asked is "who did it?" You may have geolocation evidence of an unknown suspect, or you may have a suspect in which you need to find geolocation. As an example, if an e-mail was sent to a victim, tracking the e-mail to obtain a physical address is important. Or, if a person is of interest, determining historical geolocation of that person will be important. Both examples require acquiring the physical locations.

Let's start with the desktop computer.

Most personal desktop computers are fixed in one location. They are placed on a desk, plugged in, and may not move for years, if ever until the end-of-life of the machine. It is easy to overlook the desktop computer as a source for multiple geolocation points since it simply stays in one spot. But it is also ripe for pulling geolocation data of the user, even when the user is no where near the computer. Also, user activity tied to a desktop computer, coupled with geolocation data from that computer, can prove or disprove an alibi. Table 2 shows an overview of the geolocation data that can be obtained from a desktop computer (a laptop will typically have more due to being "mobile").

Type	Details	Local geolocation	Non-local geolocation
Computer activity	**Internet activity**: downloads, uploads, URLs visited, URLs typed, cached files **User activity**: user documents created or otherwise accessed, e-mails sent or opened, other applications accessed (games, etc.)	X	
Operating System (registry, logs)	Network connections Logins Event logs	X	
Sync applications	Cloud storage, mobile device syncing, file sharing	X	X

Table 2: Personal computer geolocation sources

The computer activity geolocation data is generally going to be the local geolocation of the computer, in that all the data should point to same location (in the home, as an example). Do not discount the importance of this. If activity on the suspect's computer is at the same time that the crime occurred in a different location, the suspect may have a potential alibi of using the computer. More investigation is needed to corroborate the computer activity with the suspect's possibility of being the user as compared to a different person using the computer.

Even though a desktop computer is not typically used as a mobile computing device, the system still needs to be placed at a location using stored geolocation data. For example, on a Windows operating system, the registry maintains the network connections, which should be compared to the locally available networks. The registry key is shown below that provides a list of past or recent network

connections. Most forensic software suites can easily pull network information from the Windows registry, as can smaller forensic tools such as RegRipper.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList
\Profiles
```

If it appears that the desktop has remained connected to only local connections, then the activity on the desktop shows that someone was at that location during the times of activity. However, this does not prove that a specific person was at the computer! Any activity could have been made by anyone with access to the computer. Event logs may also detail wireless connectivity diagnosis information that includes the MAC address of Wi-Fi connections, which further investigation may lead to an IP address and location.

Much of the geolocation data from a desktop is generally going to come back to the physical location of the desktop, which is good if the computer was used to facilitate a crime. However, there is the potential goldmine of geolocation data on a desktop that points to other locations (non-local geolocation). As seen in Figure 2, syncing applications can have both local and non-local geolocation data. Connected devices, such as mobile devices, and applications that use cloud storage syncing provide for a wealth of geolocation data on a desktop computer simply because the non-local geolocation data is placed onto the desktop computer, many times without the knowledge of the user.

Other geolocation data on a desktop/laptop is that of user-created, geolocation content. This exists in the form of chats or e-mails, in which suspects will communicate past, current, or future geolocation information in the form of planning crimes or talking about past crimes. When a live (running) computer is approached, consider acquiring RAM (memory), as many chats will not create a log of the communications, but will be temporarily stored in RAM. On missing persons cases, RAM can hold important chats such as detailing where a person intended to meet another, such as “I will meet you at 7pm at the corner store” in a RAM stored chat that is not stored in any chat program log files.

Dropbox as one example of cloud storage

Dropbox is a cloud storage service in which all your files saved in Dropbox are automatically synced with all the devices that you choose to sync with Dropbox. This can include personal computers and mobile devices. Dropbox (as practically any cloud storage service) provides several methods of obtaining geolocation data, both local and non-local.

One login/connection geolocation on the desktop is tracked and recorded by Dropbox. A Dropbox user has access to this information via their account login, and more detailed information is available from Dropbox via a court order. Figure 1 is an example the information accessible to the Dropbox account owner.

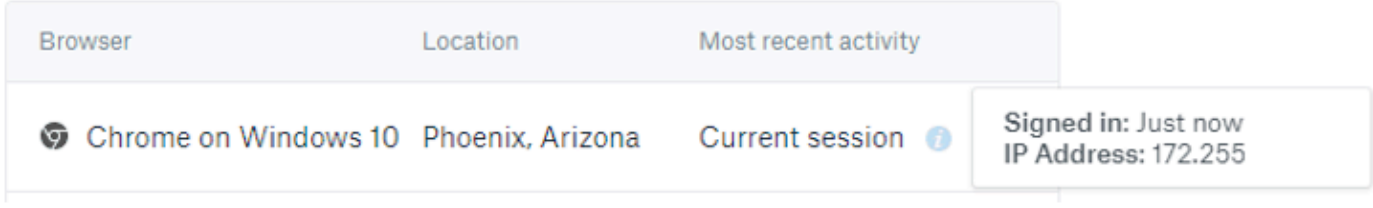

Figure 2: Dropbox connection with location, time of connection, and IP address

An important aspect is that of VPN (virtual private network) usage. Figure 3 shows the same account information as in Figure 1, however, a VPN was subsequently connected, thereby changing the IP address of the connection to appear as if it were in Oakland, California. Any forensic analysis of practically any workstation or laptop should include looking for VPN applications, and any anonymous Internet connection software to prevent false conclusions, such as assuming that a computer was in California (Figure 3) when it was actually in Arizona (Figure 2).

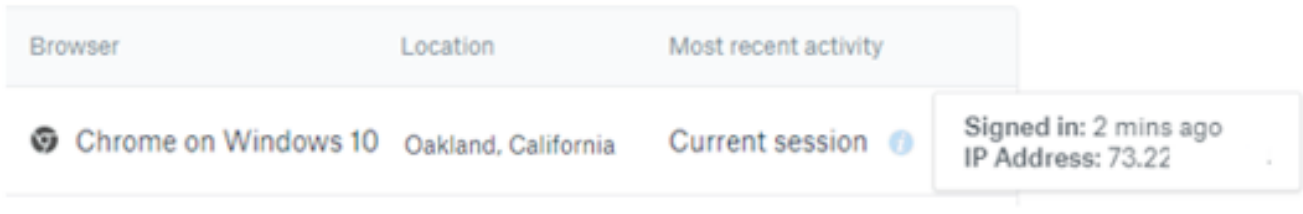

Figure 3: Dropbox connection with location, time of connection, and IP address

Both Figure 2 and Figure 3 give local geolocation data (considering the VPN IP address as local at this point). However, as an investigative goldmine of geolocation data, other connected devices to the Dropbox account will be available in the Dropbox connection history! Figure 4 shows a mobile device, connected to the same Dropbox account with an IP address in Japan. This gives us multiple investigative pieces. We now know of a mobile device with more potential evidence and a treasure trove of more geolocation data. We also have another non-local geolocation data from a desktop computer (or via court order from a cloud service provider).

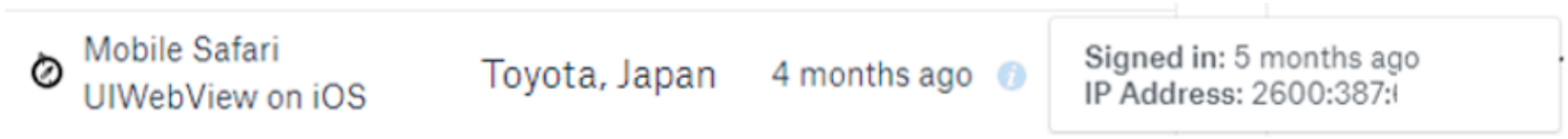

Figure 4: Dropbox mobile device connection with location, time of connection, and IP address

Photos (digital and non-digital)

Even just as important with Dropbox geolocation data is that of the files placed in Dropbox folders. Digital cameras and mobile devices can be configured by the user to automatically upload videos and photos to their Dropbox account, which will automatically sync to all devices including a home computer. This is an important aspect since a mobile device might not be recovered and the uploaded photos may be the only evidence that can be seized from the unavailable mobile devices. Even if the mobile device is destroyed, the photos that have been uploaded to cloud storage may contain all the geolocation data needed. Figure 5 shows an example of photos that have been uploaded to a Dropbox folder from a connected mobile device.

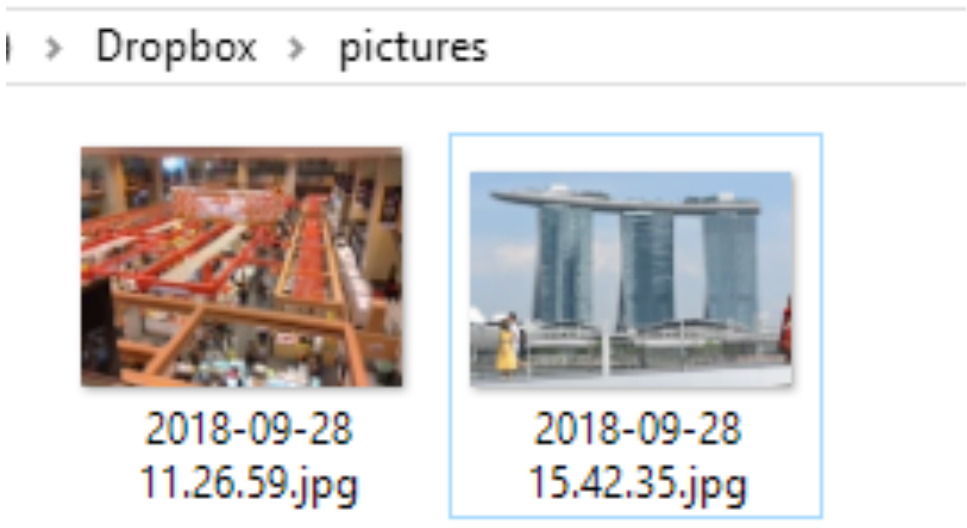

Figure 5: Photos uploaded to Dropbox

The evidence potential with photos that have been uploaded to cloud storage extend to the metadata of the photos, which not only gives you geolocation data from embedded exchangeable image file format (EXIF) metadata, but also the content of the photo which can be geolocation specific. The Figure 5 photos were taken in Singapore (landmarks in the content of photos are great for identification of geolocations!). Plus, the EXIF data seen in Figure 6 show not only the date and time of the photo, but also the geolocation by latitude/longitude/altitude.

GPS timestamp	09/27/2018 20:26:55 -7
GPS error	12759/50
Altitude	41.11 m
Image direction	T 312.54
Latitude	1° 18' 11.29" N
Longitude	103° 50' 5.61" E
Geolocation	1.30313,103.83489

Figure 6: EXIF data

To reiterate an important point about EXIF metadata in a photo, a person took the photo, and was standing in exact spot identified in the geolocation metadata field at the time noted in the metadata field. You just need to identify that person if it is your suspect. An added bonus is when your suspect is in the photo along with the embedded geolocation data.

With non-digital photos, which are increasing becoming rarer, the content may provide geolocation information. Landmarks are one example, but also smaller features such as furniture in a room or business storefronts.

Mobile Devices

The mobile device is king among geolocation sources. There is quite literally nothing that matches a mobile device in tracking its user. In effect, a mobile device that has location services turned on is equivalent to having a GPS tracker attached to a person, without the requirement of a search warrant. For the vast majority of mobile device users, this is a non-issue as the average user isn't committing

crimes. However, for criminals, carrying a mobile device may eventually be in the hands of law enforcement and will have access to years of historical geolocation data.

Much of the geolocation data stored on mobile devices are due to the many applications used by mobile device users, such as mapping applications, search applications, and social media applications. The mobile device itself may also keep a record of geolocations based on Wi-Fi and GPS locations.

The location (path, database, etc.) of mobile device geolocation storage depends on the operating system and version of the operating system. For example, iOS 4 stores cell tower and Wi-Fi geolocation data in Consolidated.db and applications that use this data are stored in Clients.plist (which includes MAC addresses). Later versions of iOS store geolocation data in cache_encrypted.db.

The Facebook application on Android devices store data in threads_db2. So, depending upon the operating system, the version of the operating system, and the applications used, there are many sources of geolocation data stored on mobile devices. Although some databases are encrypted, and some may require "jailbreaking" to access, the amount of easily available geolocation data on a mobile device in and of itself can be overwhelming in a good way.

Other aspects of mobile devices mirror that of a personal computer. Search terms, specifically searches using a mapping application are saved on mobile devices. Text messages and chat services may also contain geolocation content (as opposed to coordinates) by way of the words typed by the suspects, such as "I was at Greg's house last night".

As an investigative matter, mobile devices are more easily tied to a person than any other electronic device for the simple reason that mobile devices are not typically, if ever, shared with other persons. Most everyone, including criminals, have their own mobile device or several devices. To share a mobile device such as a cell phone would mean that someone other than the owner will have access to phone calls, emails, texts, and chats meant for the owner of the device. This is an unreasonable alibi that a mobile device was loaned to another person during the commission of a crime.

Consider all types of mobile devices when looking for geolocation sources. Not only are cell phones common, but also tablets, fitness watches, vehicle GPS devices, and practically any device that has Internet or cellular connections.

Social media

As previously mentioned, the apps associated with social media accounts track geolocation data. The more apps, the more data tracked, and the more likely multiple apps will corroborate each other in having accurate geolocation data.

Outside the device (mobile or desktop), the service providers can provide even more geolocation data. If a device has five or ten social media apps, then the investigator has five or ten providers from which to seek the information. Not only can the geolocation of everyday usage be obtained, but also the IP address of logins across any device. To clarify this point, if a suspect logs into his social media account at a library, the social media service should (up to a certain point in time) be able to provide the IP address of that login. This can be important when suspects intentionally or unintentionally leave their mobile device elsewhere, but need to communicate via social media or e-mail.

Given the life of any social media account, the originating IP address (and e-mail address!) to create the account, and subsequent logins with the related IP addresses can give a thorough historical record of a person. Although not every location is pertinent to a crime, it is possible that a suspect has visited a crime scene before it was a crime scene in the past, which would tie the suspect to the scene for some reason that needs further investigation.

Google/Other services

Google is well-known to track its users. Unless specifically turned off, tracking services are enabled and recorded perpetually. Given access to a suspect's account (via court order), Google tracking by itself is impressive. Additionally, Google records search history, which means addresses, businesses, or persons that are typed as searches by a suspect also indicate geolocation information. The searches may be for locations to travel to, plan crimes at, or be co-conspirators in crimes.

Internet comments/forums/posts/e-mail

The IP address is one of the most commonly obtained geolocation sources, because it is one of the most common required point of accessing computers. If a suspect is posting comments to a blog, or posting a blog itself, or e-mailing any other person, the IP address is typically logged at the 3rd party

service. The 3rd party service may be a blog hosting company, a webmail provider, or a webhosting company.

Identifying the username of a suspect, and identifying the websites where the suspect has been posting comments online, gives investigators the avenue of obtaining the IP address used for each post via a court order. Potentially, one suspect may post comments and blogs online using various locations via mobile device, personal computer, or public computer. Each of these IP addresses add to the historical location of the suspect.

Security cameras

Today's public spaces are virtually covered with security cameras, traffic cameras, red-light cameras, surveillance cameras, and mobile devices recording life's every moment in public. These types of videos are fantastic geolocation sources as they contain the very likeness of the suspect, typically date and time stamped, and show every moment made. Sometimes, the suspect's vehicle is captured as is any co-conspirator.

Some cities possess so many security cameras, that a suspect's entire driven route through a city can be mapped out camera to camera, down to the stop sign and use of turn signals.

Purchases (credit cards, receipts, etc.)

Historical spending activity of a suspect's use of credit cards (again, via court orders) can place the suspect at a location, to include the amount of money spent. This type of historical geolocation is similar to a mobile device in that a suspect will have a difficult time of claiming to not have been at that location as the credit card was loaned to another. Additionally, many businesses maintain security camera footage, which can confirm the identity of a suspect at a location.

Citations (speeding tickets, etc.)

It is worthwhile to obtain the driving record of suspects in any investigation when historical location is important. Although not always likely, it is possible for any suspect to be given a traffic citation or parking ticket. In the case of a traffic citation, the identity is usually going to be confirmed with the use

of a government issued identification, in a vehicle they own or lease, and issued a citation with direction of travel, make and model of vehicle, address, phone number, and other relevant information.

Putting it all together

Some investigations are easy in that you only need to place the suspect at one location at one point in time. For these types of investigations, there may be no need for anything other than the geolocation data you obtain for that time period.

Other investigations benefit from more historical geolocation data. Even when only one incident at one location constitutes the crime scene, it is possible, if not highly likely, that the suspect visited the crime scene many times before to plan the crime, and even visited after the fact for a number of reasons. The fact of planning a crime may not only be important in charging decisions and sentencing, but could lead to other victims that are not yet identified, or persons that were being stalked as future victims.

The ease to put together a timeline of historical geolocation data depends on the type of investigation and how much geolocation data is needed for the investigation. As mentioned, it may be a simple task of one location and one date/time. One example can be an employee accused of printing confidential material at a workplace on one day. Placing the employee at work, on that day, using geolocation from a mobile device, desktop computer activity, proxy card access logs, and witness statements can solidify the suspect at the scene. A simple visualization media, such as a poster showing the geolocation data, would suffice in displaying the data.

Conversely, another example could be a long-term investigation where multiple suspects traveling to multiple locations committing multiple crimes requires an immense amount of geolocation data collection and multiple visualization media. This type of investigation usually involves multiple mobile devices, computer systems, and communication methods, which is not to say that the external geolocation sources (security cameras, witnesses, tickets, etc..) won't be needed, but that the organization is that much more labor intensive.

Forged evidence/misleading evidence

Much of the geolocation information discussed can be forged, modified, deleted, erased, or wiped. IP addresses can be hidden or spoofed with VPNs or anonymous browsers like Tor (The Onion Browser).

Automated programs can simulate computer user activity in an attempt to 'fake being home'. Devices can be loaned to others in an attempt to thwart surveillance efforts. Even the EXIF data of a photo can be manipulated!

However, one of the major points of this article is that it is the accumulation of all geolocation data that makes the case. If one part of the data does not fit, then you must prove or disprove its validity. Has it been modified? Is it a malicious fake or planted data? Does any other data corroborate it? If not, there is usually sufficiently enough geolocation data from multiple other sources to rely upon.

The other point to make is that little of this is easy or quick. Mobile device forensics is difficult. Encrypted databases might not be accessible. Mobile devices might not have any applications that track location (if all turned off). Some crimes may have no electronic devices involved at all, and the reliance of traditional geolocation sources have to be relied upon, such as security cameras and witnesses.

But as time goes on, and technology continues to make our lives easier by tracking every location, we can be assured that few persons will be able to commit a crime without creating some geolocation data. So, the next case you get, ask yourself, "what are the geolocation data sources that I can find?"

About the author

Brett is a digital forensics consultant and trainer with 15 years experience in the digital forensics industry as a law enforcement officer and private consultant. Brett's cases have ranged from homicide, kidnapping, human trafficking, and narcotics to class action litigation. He is the author of several digital forensic books including Placing the Suspect Behind the Keyboard, Hiding Behind the Keyboard, and the X-Ways Forensics Practitioner's Guide. Brett also provides a curation of 'all things DFIR' to everyone in the field and those wanting to enter the field of Digital Forensics and Incident Response at http://www.dfir.training.