Expanding the Potential for GPS Evidence Acquisition

Chad Strawn

Abstract- **This paper looks at the use of Global Positioning System (GPS) data for evidence collection and investigation purposes. The number of devices carrying GPS capabilities has increased over the years, investigators can find these to be helpful in deducing the elements of a crime, and criminals may attempt to thwart investigators by manipulating the data found on a GPS device in an effort to gain an advantage to support their activities. This paper discusses the Global Positioning System network, what type of devices and software is related to GPS, and the information that may be collected during an investigation involving GPS receivers.**

Index Terms – **GPS, forensics, navigation, multipathing, WAAS, AGPS, LBS, geotagging, waypoints, POIs.**

I. Introduction

TECHNOLOGY has greatly changed the way criminals and investigators conduct business over the years. Criminals try to stay one step ahead of the law by adopting technology and using it as a means to conduct business quickly and quietly. Investigators are constantly pursuing offenders in an attempt to thwart their activities and it has turned into a game with both sides trying to learn the inner workings of new technology to work in their favor. In the past few years the market for Global Positioning Devices (GPS) has grown immensely and has become quite affordable to the average citizen. GPS units have diminished in size from the large clunky models first introduced to the public and now the technology is often a standard option on many other electronic devices. This paper will look at the current offerings of devices that contain GPS technology and what that means to an investigator. The technology extends beyond that of devices carrying GPS capabilities, but also includes software that is used in conjunction with GPS information for encoding or decoding data. It is important for an examiner to understand the capabilities accessible by the offenders and to law enforcement personnel to achieve the best outcome of an investigation. While GPS technology has remained fairly unchanged the devices that house the technology have made vast changes in their ability to use GPS data, which has created a new avenue for investigators to collect evidence. It is imperative to realize that a constant evolution of devices will manipulate the ways that both criminals and investigators can use GPS to their advantage.

II. Global Positioning System

To understand the capabilities and potential for evidence on devices utilizing GPS it is necessary for one to have an understanding of the Global Positioning System network and how it functions. It is not necessary to have a thorough understanding of the algorithms and computations required to diagnose the location of a device, but one should be able to understand the principles and limitations of the design. The GPS system was developed by the United States Department of Defense as a tool for the military that could help soldiers navigate foreign territory and deliver munitions precisely on target. The satellite-based system was first employed in 1978 and now consists of a total of 24 satellites that continuously orbit the earth [1]. The system was strictly used for military operations initially, but the United States government opened up the service for civilian use in the 1980s. The signal supplied to the civilian sector suffered from Selective Availability (SA), which was an intentional degradation of the signal accuracy to make sure that adversaries of the country did not have the ability to mount attacks with the same precision as the United States. Selective Availability was turned off in 2000 by the United States and civilian receivers have gained a greater rate of accuracy since.

The satellite system is supported by a number of ground stations that monitor the data sent by the satellites and transmit corrective data back to the satellites [2]. As the satellites orbit the earth they send out two different radio signals designated L1 and L2. L1 is set aside for civilian use and transmits data that can be read by civilian receivers to determine location. These signals contain three pieces of information called ephemeris data, almanac data, and pseudorandom code. Ephemeris data contains the precise location of the satellite as well as the locations of all other satellites in the system. Almanac data includes the time and date of signal transmission, as well as the operational status of the satellite at the time of transmission. The last piece of information sent is the pseudorandom code, which is simply an identification code for the particular satellite that is transmitting the data signal. All of this data is used by the GPS receiver to decipher the position of the receiver in relation to the satellites.

The GPS receiver collects the signals from the satellites and interprets them to give the user a fixed location. That accuracy of the reported location is dependent on the number of satellites the GPS receiver is tracking as well as variables that introduce errors in the data. In order to accurately evaluate data a GPS receiver needs to have either a two dimensional (2-D) or three dimensional (3-D) fix on orbiting satellites. A 2-D fix means that three satellites are being tracked and the GPS receiver can calculate latitude and longitude of the receiver as well as the user's movement. Having a fix on four or more satellites is considered a 3-D lock and adds the additional capability of calculating altitude. This system is based on line of sight and therefore some errors and coverage issues exist. The signals are able to pass through clouds and enter cars and buildings through glass, but certain environmental and structural conditions can impair the accuracy of the satellite's broadcast signal [3]. As the radio signal passes through the earth's atmosphere it is somewhat impeded by the ionosphere and troposphere which slows down the signal. This known effect is partially corrected by accounting for it prior to satellite transmission, so that the data received by the GPS receiver is already partially corrected. An error called Signal Multipathing is created when the satellite signal is reflected off objects, such as foliage, buildings, and exposed rocks. With Multipathing issues it is possible that a GPS receiver is analyzing a signal that is incorrect and the corresponding location given on the receiver may be incorrect. The accuracy of the data is also affected by errors and limitations of the satellites, and includes incorrect data transmissions that contain minor inaccuracies of the reported position. Also, the clocks on the satellites are not as accurate as an atomic clock so some time drift does occur, and accuracy is also dependent on the location of the satellites that the GPS receiver is using to determine position. A receiver that is locked onto satellites that are spaced further apart will have a more accurate reported position than a receiver that is using satellites that are directly overhead or in a straight line of one another.

To help correct some of these issues the Federal Aviation Administration (FAA) and Department of Transportation (DOT) implemented a program in order to provide better reported data so that aircraft could safely use GPS for navigation while maintaining safe distances from other aircraft. If two aircraft were flying one thousand feet apart but both had a reported position that was in error of five hundred feet there is the potential that the aircraft could wind up in the same position even though the reported data places them one thousand feet apart. The system that has been created to enhance GPS technology for air navigation in North America is called the Wide Area Augmentation System, or WAAS [4]. The WAAS system consists of a series of ground stations and satellites that are used to send corrective data accounting for the errors consistent with atmospheric delays, inaccurate position reports, and time drift in order to create a more precise data stream for aircraft. Although this system was developed for the aviation industry it is available for all sectors, including civilian, to gain more accurate reporting capabilities.

An investigator needs to be familiar with the reporting accuracies being used by the GPS receiver. Modern GPS usage is not impaired by the Selective Availability that was implemented by the United States military, but knowing whether the receiver was utilizing data in a 2-D, 3-D, or WAAS capacity, and the location of the satellites being used for the fix can have a significant impact on the precision of the data log. The accuracy of the data is relevant to the hardware in the GPS receiver as well. Some GPS devices utilize antennas that are more sensitive, or have faster processors, and are capable of getting a satellite lock under thick foliage or inside buildings. It is possible that the GPS receiver was at a specific point in time yet is unreported on the data log because it was unable to lock onto satellites. A general rule of accuracy can be assumed, as shown in Fig. 1 that shows the expected potential for deviation when using a GPS receiver that has, or does not have, a lock on WAAS.

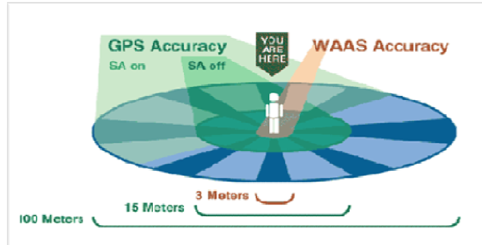

Fig. 1: Average accuracy using GPS receivers with or without WAAS lock. SA (Selective Availability) no longer applies and most current day receivers will achieve 15 meters of accuracy or better [5].

Current day civilian GPS devices using some of the newer antennas commonly achieve better than 15 meter accuracy and a 3-D lock will often have an accuracy of roughly 5 meters.

The implementation of GPS in devices such as the cell phone, which are typically used in urban areas that may not have a clear view of the sky due to buildings and other structures, has created a hurdle in maintaining good signal strength within the GPS network. Location Based Services (LBS) are used to coordinate information transfers between the ground network or a cellular service provider and the cell phone user [6]. LBS networks collect data in order to approximate the position of a user, such as which cellular tower is being used by the cell phone on the network. This gives an approximate position that places the user somewhere within the range of the specific tower. The accuracy of this report leaves something to be desired since the range of a tower can expand in all directions and distances vary depending on terrain and power output [7]. While effective in triangulating a general position it is not entirely effective for emergency services such as the cellular service E911 (Enhanced 911) in North America, where an exact location may be required to get help in a timely manner.

With the addition of GPS many of today's cell phones have the use of assisted GPS (AGPS) which has helped solve this issue [8]. Cell phones are low powered units that do not necessarily have the power to compute the complexities of GPS data, and the errors that are produced from being in a dense urban area make it more difficult to obtain an accurate location utilizing the phone alone. A cell phone that has the duty of computing all GPS data may have readings that are inaccurate and require substantial time to process all the data and gain a satellite lock. The Multipathing errors caused by satellite signals being reflected off buildings creates multiple signals that the GPS must read and attempt to distinguish which signal should be used for position reporting. This can lead to an incorrect location that is recorded to a GPS log and shows the cell phone owner at a position other than where they had been. AGPS helps negate this factor by relaying information to the cell phone and performing the GPS computations within the network as shown in Fig. 2.

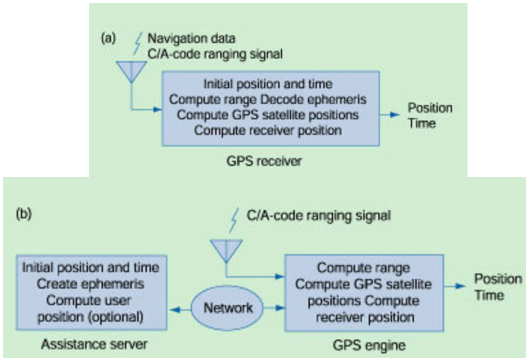

Fig. 2: A standalone GPS receiver processes all the data in (a), while the service provider can assume much of the workload in (b) when using AGPS providing results much more quickly [8]

In an AGPS system the LBS maintains data on the network regarding the current location of satellites as well as estimates of future range and position of these satellites. This behavior of estimating satellite position is called “predictive ephemeris” and allows for a quicker initial 2-D, or 3-D, fix and more accurate position reporting. Since the network already knows which cellular tower the phone is operating from, it has a general idea where the user is located and can substantially decrease the requirement for processing data by using predictive ephemeris that will reveal an accurate location. Not all cell phones or service providers offer standalone GPS capabilities and the GPS functions of the cell phone might only operate with the aid of AGPS, this means the user must be within the provider’s coverage area to gain any GPS data. The cell phone that includes standalone GPS onboard is still capable of computing the GPS data without the aid for LBS and AGPS should the user be out of the service provider’s network area, but it may take longer to do so since all data is being handled locally on the device.

III. GPS DEVICES

The technological innovations in just a few short years have created a wide range of devices that utilize GPS and devices now come in all sorts of sizes and flavors. Keeping up with what devices are utilizing GPS can seem a bit cumbersome with the continual growth of manufacturers adopting it into their devices to attract consumers. There are really only two main categories of GPS devices, built-in and mobile. The built-in devices are typically referenced as those that are permanently placed in a specific area for operation and the primary use of the GPS technology is focused on a specific task. Built-in units such as those seen in Fig. 3, 4, and 5, are

Fig. 3: Magellan Maestro 4370 automobile device [9].

Fig. 4: Garmin GNS 530W aviation device [10].

Fig. 5: Lowrance HDS-10m marine device [11].

commonly found in cars, aircraft, and marine vessels and mounted in an area near the primary controls. These are often built into a dashboard and consist of an LCD (Liquid Crystal Display) screen that allows users to input specific requests of the GPS software and displays output information. Years ago these would be considered an optional piece of equipment that was quite expensive and would only be found in luxury vehicles. Now they are commonly found as a standard option in vehicle packages and can be found in vehicles of all price ranges. Since they are built-in models, they are difficult to remove and one can be fairly certain that the GPS device has gone wherever the vehicle has travelled. As a result, the amount of potential evidence has dramatically increased and can provide a wealth of information to investigators seeking the previous whereabouts of a vehicle [12].

While it is possible to reveal the travel of a mobile device it can be more difficult to place a specific person or object with the GPS device during the duration of travel. Mobile devices can fall into a variety of categories, which include those of the built-in models and are used in automobiles, aircraft, and marine vessels. Just like the desktop computer, the design of mobile GPS devices over the years has yields a smaller footprint to house the technology while increasing the effectiveness and capabilities of the devices. These mobile units are designed for use in these vehicles and are typically equipped with navigation software that contains street, air, or marine data for routing capabilities. Many of them have the ability to fit in a shirt pocket and are easily moved from one vehicle to another. There has been a surge in these devices over the years because the price of the technology has dropped, but also the ability to move it from one vehicle to another is extremely appealing and means that a single device can be purchased instead of a built-in unit dedicated to a particular vehicle.

Laptop computers have become a viable option for GPS navigation as well. With many laptops available for a fairly low price an individual can have a tool that includes all the computer functions they want and have the addition of GPS navigation. These can be a good device for someone who wants to augment their GPS travels with specific software that cannot be used on a smaller device, or for someone who simply wants a larger display in which to read and interact with the GPS data. The only additional piece of hardware required is a GPS receiver that will connect through a USB (Universal Serial Bus) port to the laptop, like the one shown in Fig. 6.

A mount can be installed in the vehicle for the laptop so that it is easily accessible and the GPS antenna is usually just placed onto the dashboard. Even though the footprint of the laptop has become smaller it is a bit more cumbersome to move than the small units made specifically for vehicle use. A laptop used as a GPS navigator will fit the needs of some people, but the other models manufactured specifically for vehicle use are generally more popular.

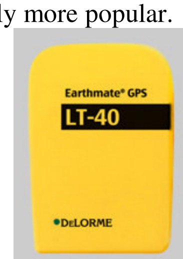

Fig. 6: DeLorme Earthmate LT-40 USB device [13].

Growing in popularity is the market of devices that are even smaller than the mobile vehicle devices. The use of cell phones and smart phones for GPS navigation has become a handy tool incorporated inside a device that many people have with them at all times, see Fig. 7.

Fig. 7: Apple iPhone [14]

Most cellular vendors are now offering phones and data plans that support the use of GPS and they work very similar to the smaller vehicle units. They can be used to obtain routing information and input desired addresses or points of interest. Being capable of conducting GPS routing using a cell phone is extremely convenient for many people as it alleviates the need to carry another device devoted to GPS navigation. A lot of people always have their cell phone on hand and being able to pull up GPS information when needed means there does not have to be a necessary plan to haul along another device with GPS capabilities. Due to the extremely small size of cell phones they cannot house a lot of extra hardware, and the antennas used for GPS service may not be of the highest quality since GPS is a secondary function. This may mean that satellite reception might not be as good as found on a device devoted solely to GPS functions, although most of these shortcomings are offset by LBS and AGPS.

Fig. 8: Garmin Oregon 300 [15].

There are a multitude of handheld GPS devices on the market and the number of these continues to grow as manufacturers work to apply GPS technology to a variety of activities. The most common type would be the device that is created with the outdoor hiking/hunting enthusiast in mind, shown in Fig. 8. These devices tend to offer rugged durability and can include a number of different functions that include tracking and routing capabilities, topographic maps, and electronic compasses and altimeters. The range of devices varies greatly from the low end models for individuals on a tight budget, or not desiring a lot of extra functions, and high end models that include a lot of bells and whistles with a hefty price tag to match. The type of chipset and antenna will vary within these models as well, so some may be better at acquiring a satellite lock under heavy tree cover or in deep canyons.

The market for outdoor devices has expanded to include a number of other sports and seems to expand every year. There are a number of units available that allow GPS functionality built into a small unit that fits on the wrist, and other small models are only about three inches in diameter and can be hung around the neck on a lanyard. These devices are often marketed with running enthusiasts in mind, but the features and simple design can be appealing to a lot of different people. There are models of GPS units built specifically with bicycling in mind and they often contain map data like other trail designed units. One of the newer devices launched to the public is designed for individuals to use while golfing. This device allows users to upload course data and keep track of all their shots during a round of golf, and can keep score for the round as well.

The technology has also jumped over to digital cameras by way of built-in technology on the camera, or as shown in Fig. 9 through the use of an additional piece of hardware that can connect to the camera. This ability embeds GPS information inside the picture data to give latitude and longitude coordinates. The appeal for users is that it is easy to identify the location where the picture was taken and there is no need to guess the location when reminiscing about travels taken years prior. Additionally, users can submit their pictures to Internet sites that offer photo storage

Fig. 9: Jobo digital camera add-on [16].

and link the GPS data to an interactive map. These online albums can be shared with others to provide a detail of the route and coordinates should they wish to visit the location as well.

There are certain devices manufactured specifically for tracking and logging purposes that can be monitored live from a distance or analyzed later once it has been retrieved. Potential uses include devices placed by law enforcement that have probable cause to track suspect vehicles [17], or a parent who uses a device to keep tabs on their child, Fig. 10.

Fig. 10: Amber Alert GPS 2G [18].

Of course the market has created a device to hinder the possibility of GPS tracking by offering devices that can be used to jam GPS signals, like the unit shown in Fig. 11.

Fig. 11: Tayx Pocket GPS Jammer [19].

Some of these jamming devices are quite small and are able to operate off a vehicle 12v plug in an attempt to thwart any GPS tracking devices that may be located on the vehicle.

IV. Software and Services

Keeping current with all of the GPS devices available can be quite a chore for investigators and there is the potential of GPS information available on a device, or stored elsewhere that is not apparent upon first inspection. Manufacturers continue to launch a bunch of new models each year that incorporate new, or enhanced, sets of features and are tailored for different sports or interests. In addition to new hardware models being available there are new software packages being released by manufacturers and third-party developers. Some of these software applications are distributed to update, or increase, the data sets and capabilities of devices, while others are created with the specific intent of being used for examination of GPS devices.

There are a number of applications offered by vendors that are created for use by investigators to examine and retrieve forensic evidence from GPS devices. Two such companies that offer applications are Paraben Corporation and Berla Corporation. Paraben [20,21] offers two titles called Device Seizure and Point 2 Point. Device Seizure is an all-in-one application that can be used to examine data on multiple handheld devices, like cell phones, PDAs, and GPS units. This application will pull device settings, maps, waypoints, tracks, and routes from the GPS. In addition to saving this data it can create a *.GPS file that will incorporate all of the point data from the waypoints, tracks, and routes which can be used with Paraben's Point 2 Point. Point 2 Point is a software package that can be used in conjunction with the *.GPS file to display all recorded points in Google Earth to gain a map perspective of the locations where the GPS device had been taken.

Berla Corporation [22] offers software applications by the name of Blackthorn and TomTology [23]. Blackthorn is specific to GPS analysis and will pull all relevant data pertaining to the data logs that include waypoints, tracks, and routes. The data can then be exported into Microsoft Excel so that it can be easily manipulated and placed into other applications. It also works in conjunction with Microsoft MapPoint and can plot all data points onto a map in a similar fashion as Paraben's Point 2 Point, in order to visualize the travels of the GPS device. Another title from Berla is TomTology that is specific to the analysis of GPS units made by TomTom. TomTology essentially does what the other software packages do in that it records all of the pertinent data. These data sets can be viewed in Google Earth just as can be done with Paraben's Point 2 Point. These applications are created for the use of GPS forensic investigations, but there are other applications available that can be used to view stored GPS data, or to manipulate data in other applications or on the GPS.

Some applications support "geotagging" which is a term for linking GPS data to digital photos. This is done by way of pairing up a GPS track log with the timestamps found on digital pictures. A couple of applications that support this ability are Early Innovations GPS Photo Linker [24] and Francois Schnell's [25] free GPicSync. With these applications a user can encode the GPS data into the EXIF header of digital photos so a user can refer back to the location at a later date, or to link the images to a map program such as Google Earth. There are different ways a user can associate the pictures with the GPS data, some methods can perform the task automatically while other require manual manipulation by the user. An application can compare the timestamps on both the GPS and digital images and automatically link the pictures to the GPS track log, or a user can simply lay down the GPS track on a map and manually associate the pictures with a particular location on the map.

Another application that supports image modification is DeLorme's XMap [26], which includes some unique capabilities to reference GPS data with an image. XMap is a geographic information system (GIS) tool that allows users to capture, manage, and manipulate geographic data. In this case a user can easily upload or download specific data points, such as waypoints, routes, and tracks, to or from the GPS device. A user can manipulate the data in XMap, like changing the location of a waypoint or moving a track, and upload it back to the GPS with the newly created positions. Another feature of XMap is the ability to link an image to latitude and longitude coordinates. All a user needs to do is import the image and set certain reference points on the image to correspond with those on a map and the image will be associated with those coordinates. An example of this method will be presented later to show how applications can be used to alter GPS data.

Like the GPS devices that are specifically made to track and log the movement of a desired object, there are a number of services associated with tracking and logging. A couple of companies that offer such services are LandAirSea [27] and LiveViewGPS [28]. With these services an individual can deploy GPS tracking units on a fleet of vehicles, parents can track their children, or valuable assets can be tracked for security purposes. Some options with these services are simply logging devices that can be purchased by a user and attached to the item they wish to have tracked. The device utilizes battery power and can be easily transferred from one item to another, and the data tracks can be downloaded to a computer for examination. Other devices offer the capability to hardwire a tracking device into a vehicle's power system in order to have sustained power to continuously log and track the vehicle position.

Both of these companies also offer live tracking services where GPS data is transmitted and accessible by the user via the Internet. The user can log in to the service to see the location of a tagged item, such as a vehicle. There are certain available options when dealing with vehicles that can allow the user to initiate commands, such as lock the doors or disable the engine. Alerts can be sent to a user if the GPS device moves beyond an area that has been established as an inappropriate area of operation. A parent who wishes to have a GPS travel in their child's backpack can establish parameters that will set off alerts should the GPS move outside the allowed area. For example, a maximum speed can be set that the GPS is allowed to travel or a "geo-fence" can be established designating safe areas for the GPS to identify. Should the GPS travel at a rate of speed faster than allowed, or travel outside the established fence an alert will be sent to the parent notifying them the GPS, presumably with child, is moving outside the designated limits.

V. Investigating GPS

At one time gathering GPS data meant an investigator needed only to focus on finding a device whose sole capability was that of a GPS receiver. These units were fairly specialized and often marketed to selective clientele, such as the built-in models for luxury cars. Nowadays the GPS capabilities have migrated from these specialized devices and have found their way into other types of devices. The reverse is happening as well where dedicated GPS receivers are gaining new capabilities and can handle other types of data as well. This opens up the field of GPS forensics and means that evidence of value may be found in many different devices that are being used for a number of different tasks [29]. This means that more of the crimes that are being committed have the potential of containing GPS information.

Many GPS devices, especially the mobile automobile units, now allow Bluetooth connectivity, an image viewer, mp3 player, and video capabilities. Also, many of the GPS units intended for outdoor recreation use have stepped up the capabilities by including image viewers and allowing manipulation of the mapping data being displayed. This means that there is much more to examine and the potential evidence is more than just data plots representing GPS readings. The incorporation of GPS capabilities in cell phones have now created additional data values that can help tie the other activities on the cell phone to a specific location [30]. The wave of popularity that seems to be growing with "geotagging" means that the majority of digital cameras in the future will contain GPS capabilities.

With all these devices that have recently adopted GPS capabilities, or the GPS units that now offer other types of abilities, the forensic examiner needs to be aware of the potential data that may be located on the device in question. Being able to interpret multiple types of data can help an examiner piece together a scenario that may been unattainable using only a single point of data, or it may create leads that an examiner can follow to turn up more evidence. It becomes very important that examiners are able to keep up to date on all the devices, and software applications, that are able to utilize GPS technology. While the majority of people may use these devices and software packages in the manner for which they were intended, there are going to be individuals who are continually looking for exploits that may alter data to their advantage [31].

There are a number of areas where an investigator can look for clues when dealing with cases that may involve GPS data. First, the physical search can be extremely revealing in the potential evidence that may have been hidden or removed from the scene. With the rise in popularity of mobile GPS units, car and handheld, may people are installing mounts to hold their devices. Inspecting the glass on the windshield can reveal suction cup marks from an attached mount, or some distinguishing marks may be left behind from a mount that had been used on a dashboard. More permanent mounts may be placed that could reveal the use of a laptop or other GPS device in a vehicle.

Most devices nowadays include additional memory expansion options beyond that of the internal memory installed on the device. These memory modules come in the form of SD (Secure Digital), or micro-SD, cards that may be inserted, or removed, easily in a unit. The SD card found in a unit may include potential evidence, or other cards may be located on the premises being searched. These SD cards can hold as much as 32GB of data, can be viewed on the computer as a removable drive, and may contain content that is not native to the device being examined. An SD card found on a GPS unit marketed for backpacking use could very easily be hiding 32GB worth of pirated movies or music.

There are other signs that may not actually reveal any further evidence, but should be pursued in order to verify whether or not such data may exist. A unit purchased to jam GPS signals may be found in the area of the search and while this is not proof that an individual was actually jamming GPS signals, it provides a good reason to suspect that they are attempting to hide something. Finding one of these devices should tell the investigator that other equipment could very well be located nearby that contains GPS capability that was intentionally blocked for a particular reason. Finding Bluetooth devices at the site of the search can possibly be linked to a GPS unit that includes hands free Bluetooth capability that can reveal whether the device had been paired with the GPS unit at some point. Also, finding such items as a digital camera may mean that the device was used in conjunction with another piece of hardware or software to insert GPS location data into the digital image headers.

Even if there are no devices found in the area a search of any computers may lead examiners to believe that such devices do exist and should be sought after. A computer may have software installed that is dedicated to a GPS unit, such as a mapping program, or other applications could reveal a history of uploaded photos that contain geotagging references. Like all investigations, GPS forensics must be approached with a willingness to view a broad picture and the skill to decipher the small details in order to rebuild the occurrence of the crime. Being able to look at a number of physical attributes of the scene can increase the likelihood of revealing GPS units that have been hidden from the investigator.

The forensics analysis of a cell phone and GPS unit are very similar with the addition of so many related features. An investigation on a GPS unit in a vehicle can very likely reveal a wealth of information that includes phone calls made, contact lists, and paired devices. Likewise the cell phone may reveal GPS data and offer up a track created by the individual. Previously searched addresses or followed tracks can be apparent in the history of the device. The devices used today contain a lot more than a single specialized function that can be extremely revealing when thoroughly searched.

An examiner who is comfortable in dealing with GPS data and understands the errors that can occur in datasets is in a good position to piece together the travels of a specific device. An examiner will want to look at the GPS log to reveal any tracks, routes, or other information that may be stored on the device [32]. The log files with vary in how the data is saved and managed depending on the manufacturer of the device. In most cases an examiner will be able to find "breadcrumb" trails, which are data points that denote the track created during the travels of the device [29]. The settings used to record tracks will vary upon the device and the settings selected by the user. Typically a data point is recorded after the device has moved a predetermined distance such as every ten feet, or points will be logged based upon time intervals. Looking at Fig. 12, the image shows the data points of a recorded GPS track.

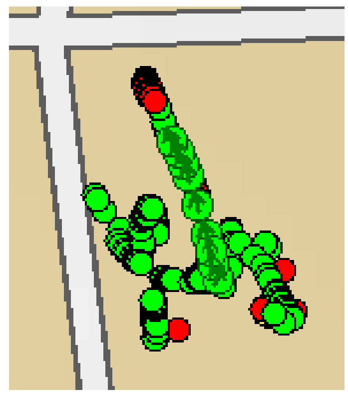

Fig. 12: DeLorme Topo USA track log with visual recorded intervals.

The green points are recordings that occurred when the GPS had a lock on the satellites giving a good position and show movement along a path by placing arrows pointing in the direction of travel. The red data points are recorded positions that occurred during a set time interval even though the GPS device was unable to identify a specific location due to a loss of satellite reception. The accompanying image in Fig. 13 shows that data points were being recorded every second by the device and whether the recorded point was based off of an established lock with satellites.

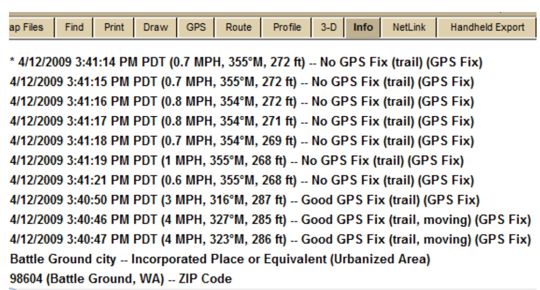

Fig. 13: DeLorme Topo USA track log showing GPS fix and recording interval.

Being able to review these data points can create a link between the location of the device and whether it is relevant to the offense being investigated [33]. Understanding the accuracy of the GPS system and the potential errors that produce variances in the reported location of the device can help paint a usable track that plots the whereabouts of the user. Multipathing errors may create a dataset that has plotted points that appear to jump around the map or inadequate signal reception due to buildings or heavy foliage cover may neglect to properly record a position during travel. Simply reading the track log and taking the plotted points at face value may create an inaccurate representation of the track and cause confusion about the exact whereabouts of the device. Physically retracing the path can help the examiner reveal possible causes for error that led to the displacement of data points along the track, such as passing through a tunnel, and potentially connect the device with a relative degree of accuracy to the offense.

In addition to the plotted tracks there may be saved routes that can be viewed in order to view trips that a user has taken or are planning on taking. Depending on the type of GPS devices routes may consist of turn-by-turn directions along roads or trails, or they can contain data that is a direct route between points. Most devices also allow the creation of custom waypoints and points of interest (POI). Identifying these waypoints or POIs can help an examiner in understanding why the user moved through certain areas and what areas they were planning on visiting in the future. Perhaps the suspect was planning on meeting an accomplice after committing an offense; the GPS could hold valuable information regarding the meeting location.

Many devices allow the custom POI to include comment information regarding the data point, like the custom waypoint shown in Fig. 14 detailing the location of a money exchange and a name that could lead to a person of interest.

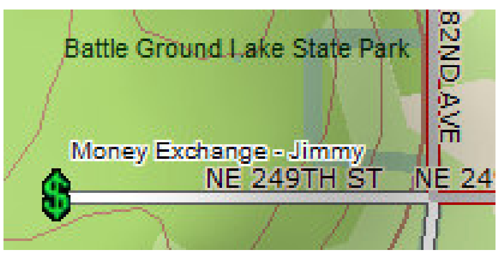

Fig. 14: DeLorme Topo USA custom POI

In most cases it is also possible to identify recent location searches, identify the coordinates of a home location, and possibly find information about the owner of the device such as name and phone number.

The examiner has a good idea of what types of data are available on each device and it may be beneficial to show a couple of examples to increase the familiarity of what a person may find during their investigation. First, a brief example will be presented that looks at TomTom mobile auto units and how the data can be manually checked or automatically mined using the TomTology software. The second example will provide a little more depth involving an outdoor recreational GPS device, DeLorme's Earthmate PN-40. The PN-40 and associated software allow some unique capabilities that are not found on a lot of other trail units in the current market.

The TomTom devices are very similar to the other mobile GPS receivers one might encounter in the field and in many cases an examiner can view data in the same manner as described. Data is stored via internal flash memory and some units allow an increase to the maximum available memory with the use of an SD card [33]. Hooking the GPS device up to a computer via a USB cable allows a person to view the contents of the memory on the computer as though it were a removable drive. Fig. 15 shows a view of a TomTom unit that has been connected to a Windows based computer and has been recognized as removable media.

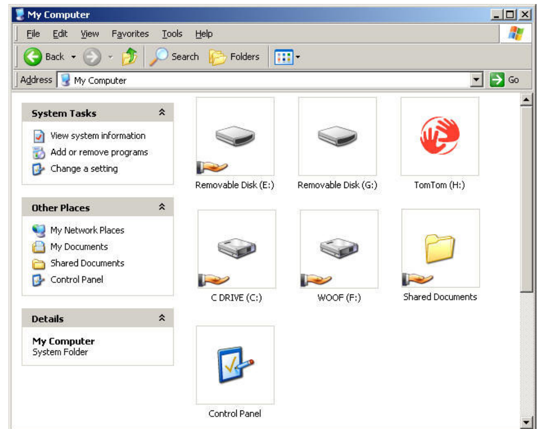

Fig. 15: Viewing TomTom GPS as a removable drive in Microsoft Windows [34].

Additionally a unit that has a removable SD card may have the data viewed in a computer that has a built-in card reader, or via an appropriate adapter that can be used to access the data. A user who can peruse the file contents will find the structure contains a number of folders that include configuration files as well as datasets that will hold the information of such items as user requested routes, waypoints, phonebook information; and may contain storage areas for additional file types like images and music files.

Fig. 16: TomTom One automobile unit [35].

TomTom has a number of different GPS models, an example is shown in Fig. 16, available for purchase with several different features existing on the various models [36]. An examiner who is familiar with the devices or at least able to do a short bit of research on the device collected for evidence, can determine what features are present on the specific model. The list shown in Fig. 17 provides some detail on what information can be extracted from the files that are accessible when viewing the device as a removable drive on a computer. It is of course recommended to perform these actions on an imaged copy of the data.

- ***.cfg** - Holds Locations. File name depends on version and is found in a folder with the name of the map. The file name is either 'Mapsettings.cfg' or <name_of_map>.cfg. There may be more than one map installed on the TomTom. The map currently in use can be found by looking at the 'currentmap.dat' file.
- **ttgo.bif or ttnavigator.bif** – general device information, model number, serial number, user password (encrypted)
- **Settings.dat** - Paired phone ID and MAC address (max 5). Any other user information like phone nickname, etc... if entered
- **Called.txt** - Name called (if in phonebook), Number called
- **Callers.txt** - Name of caller (if in phonebook), Number of caller
- **Contacts.txt** - Name of contact, Number of contact. This file only exists if the user has chosen to import their address book from their phone.
- **Inbox.txt** – Name, Number, Message, Date & time
- **Outbox.txt** – Name, Number, Message

Fig. 14: Common file types found on TomTom GPS devices [36].

Most devices contain an owner's information screen where the owner can input personal contact details in case the device becomes lost. Reviewing this screen may reveal name, phone number, and address of an individual. The vendor also offers online registration for a GPS receiver, which an investigator may be able to acquire the user's registration information using the serial number on the device and the proper legal procedures. If the data found on the device is not producing any usable results the ability to retrieve the information from the vendor may turn out to be extremely helpful. In general these devices can be examined in the same method as your typical hard drive.

TomTology simplifies the search of TomTom devices a bit by presenting data in a friendly looking user interface and can automatically mine the device's memory to collect relevant data on the device. To search for data all one needs to do is start a new case and select the "Find Evidence" button, then the software will automatically scan all attached drives on the computer and locate the one that contains the TomTom.

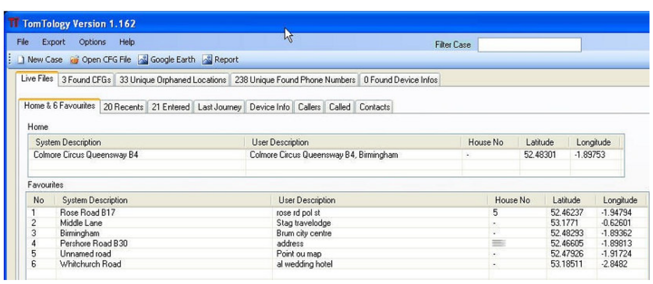

Fig. 15: Sample examination data from TomTology software [37].

The image in Fig. 18 shows the data that has been extrapolated from a TomTom unit and TomTology has sorted the data into tabs that can be viewed to determine the value of the evidence. The "Live Files" show all current data on the device that is usable by the owner; TomTology also scans the deleted space for artifacts and will place old configuration files in the "Found CFGs" tab for analysis as well.

Data can be exported and viewed in Google Earth so an investigator can gain a nice visual representation of the path traveled. Another nice feature of the program is that it can be added to EnCase as a viewer in order to access .cfg files directly from within EnCase [36]. TomTology is a nice tool for the examiner as a means to collect data in a consistent and usable manner. The only downfall is that it only works on TomTom GPS devices and in the past number of years there have been a number of other companies that have gained a good portion of the market of mobile GPS devices. An investigator may find the software being used sparingly as devices from other manufacturers are being seen more during the collection of evidence [29].

In essence the GPS receiver is the same device regardless of the form factor. Some offer specialized functions, but in the end they are all devices that present information to the examiner and can be inspected as though it were any hard drive. As the technology progresses and the processing power increases while maintaining the same size footprint, these devices are now capable of carrying out more specialized functions. DeLorme has released their handheld model called the Earthmate PN-40, shown in Fig. 19.

Fig. 16: DeLorme Earthmate PN-10 [38].

The PN-40 by itself is much like any other GPS receiver marketed for the outdoor enthusiast and contains the usual data that would be collected from similar devices, such as tracks, routes, waypoints, and points of interest. The device is capable of being loaded with map types other than the typical vector map data this is commonly found on the GPS receiver. This ability alone does not make it more complex to examine, but it becomes a bit more unique against the competition when paired with DeLorme's Topo USA or XMap software. The following example looks at the potential of the software applications and what the data looks like if an investigator were to perform a live examination on the PN-40.

Topo USA is an in depth application that allows users to make additions to the data sets and save them to transparent draw layers. This draw layer can then be imported into the PN-40 seamlessly making the data set look as though it is part of the original data set on the GPS receiver. The Topo software includes the major streets and hiking trails found in the United States, all of which can be transferred to the PN-40. An individual can create a trail that looks like any other, import it to the device, and just looking at the GPS receiver one would assume that the trail was valid. This trail may actually carry a hidden meaning that is only known to the creator of the trail, or select individuals. The following screenshots show a hiking trail that was created around Champlain College. The first is the view in the Topo USA software after the trail has been created (Fig. 20), it appears with a multi-colored line that would look the same as any hiking trail found on the map traversing the landscape.

Fig. 20: DeLorme Topo USA software showing a user created trail.

The remaining images are screenshots from the PN-40 unit that show details about the map data, which shows a draw layer existing in the map "Champlain Test" (Fig. 21), and that particular map is being displayed on the unit (Fig. 22). The use of a transparent draw layer in the map data makes it so the trail does not look out of place against the

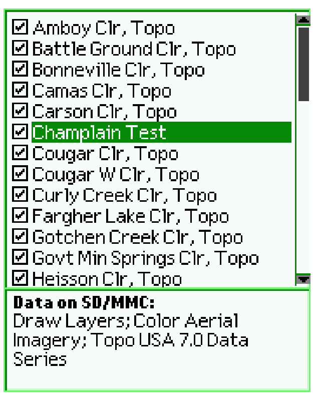

Fig. 21: Screenshot of PN-40 showing data layers in map set.

Fig. 22: Showing the same trail created in Topo USA on the PN-40.

overlaying vector data that rests on top of the color aerial image. Another example of using these draw layers would be where an individual creates a similar trail that leads to their marijuana grow operation tucked into the dense wilderness and marks the end of the route with a common waypoint symbol. The casual observer would not be able to tell that the data was not originally there, but an examiner could look at the data layers to see data has been imported into the device and a draw layer would give good reason to analyze further.

An examiner can look at the map sets to see what types of data are contained in each set. Deselecting the box next to the map set will turn the data set off and it will not be displayed on the PN-40. The examiner can continue down the list disabling all sets that do not contain draw layers, and then they can go into the Data Layering options on the device to disable all layers except the draw layer, seen in Fig. 23. This will allow the examiner to see only what was created on the draw layer and they can begin to isolate data points to determine whether there may be any evidentiary value.

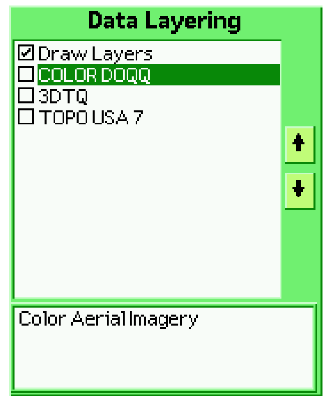

Fig. 23: Individual Data Layers that can be selected to view data installed on the PN-40.

If the examiner is suspicious of the draw file for a particular area they may decide to check the other map data layers out for the particular location shown. In this case the data file that holds the color aerial imagery of Champlain College is embedded with a Microsoft Word file called "GPS Camo.doc". The file was placed there using a utility called Camouflage that can be used to hide data within other files. An investigator who can locate the Word document will find a message that reads, "This is hidden to show that GPS devices can hold more than meets the eye." This ability means that data sets that do not contain draw layers can be just as valuable for evidence collection.

Another interesting ability regarding mapped data comes through the use of XMap. XMap is the GIS software application that was described earlier and can convert collected geographic data into viewable map data. Any data that is collected and turned into the appropriate digital medium can be loaded into XMap and displayed as a map. The example shown here takes a sample .jpg file that happens to be a picture of a bunny. Using XMap data points are assigned to the bunny image and corresponding points are associated with the map. The software creates a data layer that aligns to imported data, in this case the .jpg file, to correspond with the map rotating and resizing the image as necessary. Once the image is associated with the map data it can be loaded onto the GPS receiver as though it is a map layer. The intent of this feature is to allow users to upload map data to improve their information of an area, although nothing restricts users from associating other data with the map. In this case the image has been associated with a location in Idaho and is visible when browsing that area of the map, in Fig. 24. An image that is loaded may not always be immediately visible when viewing the map screen because the PN-40 allows users to establish priority settings for data layers at different zoom levels. It could be that color imagery is set to show at a higher priority level and if it were present it would be visible instead of the bunny image. The only way to tell that external data was loaded in this case is by reviewing the data layers available on the PN-40 in which case the "ImageData Series" layer would be present, and turning off select data layers and reviewing the map will reveal the data present on the GPS receiver.

Fig. 24: Delorme XMap with a .jpg image registered and oriented on the map.

Any of these created map sets can be freely downloaded from the PN-40 to another user's Topo USA software. In this case it is possible to send hidden messages amongst individuals either with embedded files or image registration. It should be noted that in order to exchange data between both Topo USA and XMap the PN-40 must register a partnership with the application. An investigator can find these partnerships in registry files that will contain the serial numbers of the PN-40 devices that have connected to Topo USA. Being able to retrieve this information can tie a particular GPS receiver to any computer that it has been used on and exchanged files with DeLorme's software.

The functionality of GPS units has drastically changed over the years as they have become integrated into a large number of other electronic devices. These units have become particularly valuable to investigators who are trying to piece together the timeline and movement of individuals during commission of an offense. It is important that the focus of the examination does not rely only on the GPS data collected from devices, but incorporates the findings into the other aspects of the investigation. GPS technology is most assuredly not perfect and an investigator must be aware of the deviations that can occur in data recordings due to errors introduced through hardware or environmental issues.

Investigations are often complex due to a number of variables and the GPS device incorporates a number of new variables that increase the complexity of the puzzle being solved by examiners. An examiner who understands how the GPS system works and the inherent errors can produce good results that may show with a level of certainty the location of the device and the owner during a crime. The number of devices containing GPS technology has grown substantially in the past few years and the technology will most certainly be introduced into new devices in the near future simply due to the fact that it can be installed into devices with a small footprint.

GPS technology poses a great opportunity for investigators, as it is a source of data that was not so readily available and affordable to the public only a few years ago. Now that it has become popular and is incorporated into so many devices the data collected can help fill the gaps in information that might plague investigators who are unable to place the whereabouts of an individual [40]. The data pulled from GPS devices, which often incorporate more data types than just GPS information, can be accessed and examined typically in the same manner as one would go about investigating data on a computer. This helps immensely as it means investigators can very easily capture and navigate through the data found without the need for specialized training. It also means that data acquisitions on many GPS receivers capture information in the same manner as performed on a computer hard drive, and are admissible into the courtroom as a recognized and accurate representation of the data that resides on the device.

Criminals will do what they can to hide data in a fashion that makes it look legitimate to casual users and attempt to keep it inconspicuous to investigators. Like other facets of the investigation an examiner must make sure that the data revealed on a GPS unit is not taken at face value and they combine their findings, both digital and physical, to unravel the problem lay out before them. Both law enforcement and criminals who are trying to outdo each other in an attempt gain the upper hand are using the technology. As GPS software applications become more abundant criminals will find new methods of obscuring their tracks, and software will be created for law enforcement that will attempt to seek out these methods and reveal the true nature of such data. GPS devices have been successful in tracking criminals and have been an integral part of obtaining prosecutions against offenders [41]. One can be assured that GPS technology will remain a central part of many devices in the future and it offers advantages to those on both sides of the law; the game of cat and mouse has escalated with technology and the GPS receiver is commonly involved in the chase.

REFERENCES

[1] Garmin (n.d.). What is GPS? (March 4, 2009). Available at http://www8.garmin.com/aboutGPS/

[2] GPS Passion. (n.d.). GPS explained.. Retreived March 2, 2009, from http://www.gpspassion.com/Hardware/explained.htm

[3] Köhne, A. & Wößner, M. (2007, March 4). Sources of errors in GPS. Retreived April 19, 2009, from http://www.kowoma.de/en/gps/errors.htm

[4] Federal Aviation Administration, (2007, June 26). Wide area augmentation system. Retreived April 19, 2009, from http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/waas/

[5] Garmin (n.d.). What is gps? Retrieved March 4, 2009, from http://www8.garmin.com/aboutGPS/

[6] Phifer, L. (2006, December 21). Location-based services for your mobile. Retrieved March 26, 2009, from http://searchmobilecomputing.techtarget.com/tip/0,289483,sid40_gci1236097,00.html

[7] Mellars, B. Forensic examinatin of mobile phones. *Digital Investigation , 1* (4) 266-272. (2004).

[8] LaMance, J., Jarvinen, J., & DeSalas, J. Assisted GPS: A low-infrastructure approach. Retreived March 1, 2002, from http://www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=12287

[9] Magellan, (n.d.). Magellan Maestro. Retrieved March 19, 2009, from http://www.magellangps.com/products/product.asp?segID=408&prodID=2158

[10] Garmin, (n.d.). GPS/NAV/Comm. Retrieved March 19, 2009, from https://buy.garmin.com/shop/shop.do?cID=194&pID=8052

[11] Lowrance, (n.d.). Marine. Retrieved March 19, 2009, from http://www.lowrance.com/en/Products/Marine/HDS-High-Definition-System/HDS-10m-Multifunction-GPS-Chartplotter/

[12] Hubbard, B. Police turn to secret weapon: GPS device. Retreived August 13, 2008, from http://www.washingtonpost.com/wp-dyn/content/article/2008/08/12/AR2008081203275_pf.html

[13] DeLorme, (n.d.). Earthmate LT-40. Retrieved March 19, 2009, from http://shop.delorme.com/OA_HTML/DELibeCCtpSctDspRte.jsp?section=10091&minisite=10020

[14] Navigadget, (2007, January 19). iPhone GPS. Retrieved March 19, 2009, from http://www.navigadget.com/index.php/2007/01/19/iphone-gps-part-2

[15] Garmin, (n.d.). Oregon 300. Retrieved March 19, 2009, from https://buy.garmin.com/shop/shop.do?cID=145&pID=14903

[16] Emerick, D. (2008, February 5). Jobo announces GPS digital camera add-on. Retrieved March 19, 2009, from http://emerick.blogspot.com/2008_02_01_archive.html

[17] GPS tracking, 06-2741 (United States Court of Appeals February 2, 2007).

[18] Amber Alert GPS, (n.d.). Amber Alert GPS 2G. Retrieved March 19, 2009, from http://www.amberalertgps.com/

[19] Tayx, (n.d.). Pocket GPS tracker jammer. Retrieved March 19, 2009, from http://www.tayx.co.uk/gmt04-pocket-gps-jammer.html

[20] Paraben Corporation.. Device seizure v3.1. Retreived February 4, 2009, from http://www.paraben-forensics.com/catalog/product_info.php?cPath=25&products_id=405

[21] Paraben Corporation.. Point 2 point v2.0. Retreived February 22, 2009, from http://www.paraben-forensics.com/catalog/product_info.php?products_id=404

[22] Berla Corporation. Blackthorn. Retreived February 21, 2009, from http://www.berlacorp.com/blackthorn.html

[23] Forensic Navigation. TomTology. Retreived March 2, 2009, from http://www.forensicnavigation.com/#/products/4527490520

[24] Early, J. GPSPhotoLinker. Early Innovations Web site. Retreived February 12, 2009, from http://www.earlyinnovations.com/gpsphotolinker/

[25] Schnell, F. GPicSync. Google Code Web site. Retrieved April 13, 2009, from http://code.google.com/p/gpicsync/

[26] DeLorme. XMap 6 GIS software suite. Retreived March 22, 2009, from http://www.delorme.com/xmap/

[27] LandAirSea Systems. How GPS tracking works. Retreived March 1, 2009, from http://www.landairsea.com/about/gps-tracking.html

[28] LiveViewGPS. What will LiveViewGPS do for you? Retreived April 19, 2009 from http://www.liveviewgps.com/

[29] Last, D. Silent witness. *Navigation News* , pp. 10-13. (2009, January/February).

[30] Smith, N. M. GPS gis and position tracking technology privacy and law enforcement. Retreived February 21, 2009, from http://www.computer-forensic-technician.com/wordpress/gps-gis-and-position-tracking-technology-privacy-and-law-enforcement/

[31] Iqbal, M. U., & Samsung, L. Legal and ethical implications of GPS vulnerabilities. *Journal of International Commercial Law and Technology , 3* (3), 178-187. (2008)

[32] Williams, C. J. GPS technology doubles as crime-fighting tool. Retreived November 25, 2008, from http://articles.latimes.com/2008/nov/25/local/me-gps25

[33] Nutter, B. Pinpointing TomTom location records: A forensic analysis. *Digital Investigation. 5*, 10-18. (June 16, 2008)

[34] Landis Media, (n.d.). How to install POIs. Retrieved March 19, 2009, from http://www.tomtomfree.com/Install_POI.htm

[35] Keating, T. (2006, August 17). New TomTom One GPS. Retrieved March 19, 2009, Web site: http://blog.tmcnet.com/blog/tom-keating/gps/new-tomtom-one-gps.asp

[36] LeMere, B., & Sayers, A. (2009, January 14). TomTom gps device forensics. Retrieved March 3, 2009, from http://www.forensicfocus.com/tomtom-gps-device-forensics

[37] Berla Corporation, (n.d.). TomTology - GPS forensics. Retrieved March 19, 2009, from http://www.berlacorp.com/tomtology.html

[38] DeLorme, (n.d.). DeLorme Earthmate PN series. Retrieved April 19, 2009, from http://shop.delorme.com/OA_HTML/DELibeCCtpSctDspRte.jsp?section=10460

[39] Hannay, P. Forensic acquisition and analysis of the TomTom One satellite navigation unit. Retreived December 4, 2007, from http://data.openduck.com/wp-posts/2007/12/04/paper-a-methodology-for-the/20_Hannay%20-%20A%20Methodology%20for%20the%20Forensic%20Acquisition%20of%20the%20TomTom%20One%20Satellite%20Navigation%20System%20-%20A%20Research%20in%20Progress.pdf

[40] Ball, C. GPS evidence might drive your case home. *Law Technology News.* Retreived October 29, 2008, from http://www.law.com/jsp/legaltechnology/PubArticleFriendlyLT.jsp?id=1202425606808

[41] Reuters. GPS data from landairsea tracking device aids murder investigation of 12-year old. Retreived March 31, 2008, from http://www.reuters.com/article/pressRelease/idUS122531+31-Mar-2008+PRN20080331

Chad Strawn is a 2009 graduate of Champlain College receiving his BS in the Computer and Digital Forensics program. He is looking to make a career transition into the field of digital forensics and to pursue further studies in the area of GPS forensics. Chad can be reached at chadstrawn@comcast.net.