Chapter 16
GPS Forensics

Learning Objectives
The objectives of this chapter are to:

- Understand the principles of GPS
- Understand fundamentals of GPS Forensics
- Know how to use GPS data analysis techniques and mapping technology
- Know how to recover track logs from GPS devices
- Become familiar with the tools necessary to examine GPS devices

The law enforcement community has seen an increasing use of Global Positioning System (GPS) device as an instrument of crime, or as a "witness device", due to a feature that autonomously collects and logs positional data during the crime. GPS devices are becoming an integral part of many investigations.

In CSI: Miami (Crime Scene Investigation: Miami)—'Time Bomb', the detective is able to assemble a GPS device using a GPS chip that was discovered on a murder victim's body. The device was then used to backtrack along the path of the victim's vehicle, successfully discovering where this vehicle came from. This information proves to be crucial in identifying the murderer. While this particular story is fake, it is not difficult to imagine such an event occurring in the real world. GPS devices aren't just useful for digital investigation; however, they can provide incriminating evidence too. Being able to prove that a device was at a specific location at a specific date and time could be just as valuable to an investigation as a smoking gun.

GPS device forensics can provide crucial evidence in criminal and civil cases. Some of our modern day GPS devices include portable GPS devices as well as auto, aviation and marine devices.

X. Lin, *Introductory Computer Forensics*,
https://doi.org/10.1007/978-3-030-00581-8_16

In this chapter we will introduce the fundamental basics and techniques of GPS forensics. The techniques we introduce have a wide application in GPS data analysis, even though we will only be discussing them using Garmin GPS device as an example. Finally, we will introduce the tools used for forensic analysis of GPS devices and applications.

16.1 The GPS System

The GPS is a worldwide radio-navigation system formed from a constellation of 27 satellites (24 in operation and three extras in case one fails) and their ground stations that manage the satellites. There are a number of applications of GPS; two of the most popular applications are **GPS Tracking** and **GPS Navigation**. Both operate on the principle of trilateration using satellites. The GPS device communicates with a satellite using high-frequency, low-power radio signals that travel from the satellite to the device. By precisely measuring the travel time of the signal, the device can precisely calculate how far away it is from the satellite; RADAR uses this same principle to detect distant objects.

The theory behind it is very simple. For simplicity, assume that we have precise clocks for both satellites and GPS devices. A satellite constantly broadcasts signals to GPS devices, and the information in a signal contains the identifiable information of the satellite, the current location, and the current date and time (or the time the signal is sent). Upon receipt of a signal, the GPS device calculates the difference between the time the signal is sent and the time it is received. Then it knows how long the signal takes to reach the receiver from the satellite. Since we know a radio signal travels at the speed of light (186,000 miles/s), we can obtain the distance between the satellite and the GPS device by multiplying the signal travel time by the speed of light (Fig. 16.1).

The GPS works based on *trilateration* from satellites, as shown in Fig. 16.2. When a GPS device performs this distance calculation with one satellite, it can only

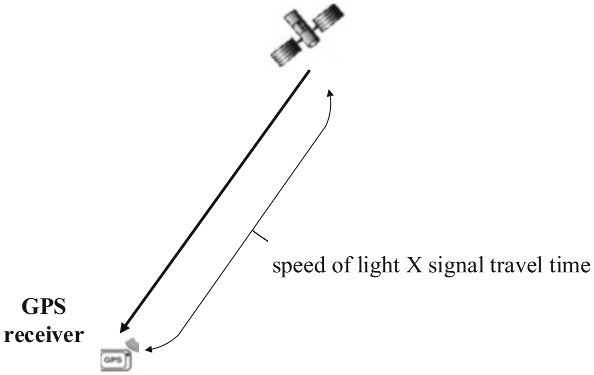


Fig. 16.1 Calculate distance from a satellite using signal travel time distance = speed of light × signal travel time

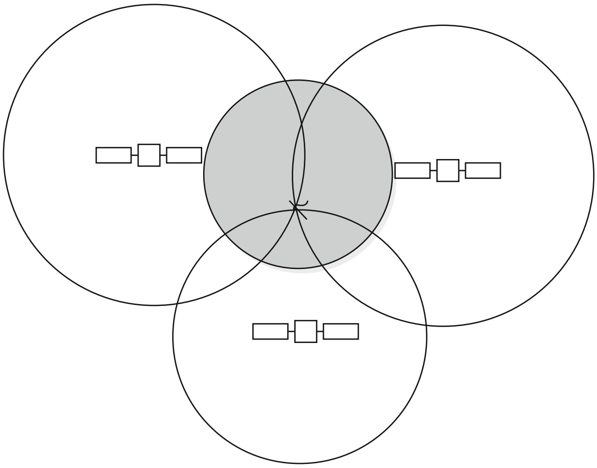


Fig. 16.2 GPS trilateration

conclude that it is somewhere on the surface of an imaginary sphere around the satellite, such that the sphere's radius is the calculated distance. Although very little of this sphere intersects with Earth's surface, the possibilities are still far too great. By performing the calculation with a second satellite, however, a second sphere can be created, and the device lies somewhere on the circle of intersection between the two spheres. A third satellite measurement will narrow the possibilities down to just two points where all three spheres intersect. In most instances, one of these points will not lie on the Earth's surface. As a result, GPS devices typically search for four or more satellites in order to improve the accuracy. For a variety of reasons, GPS devices could fail. For example, while driving through a tunnel or in indoor underground parking lots, GPS devices do not work properly because the satellite signals cannot penetrate walls or other obstacles. It requires a direct line to GPS receivers [1].

Global Positioning System, or GPS for short, device forensics can provide crucial evidence in criminal and civil cases. Some of our modern GPS devices include personal GPS devices as well as auto, aviation and marine devices. Also, GPS applications such as Google Maps become prevalent in today's smartphone. As shown in Fig. 16.3, a typical GPS device today has the following logical structure and consists of:

- GPS receiver: It is an electronic unit that is able to determine the user's current position through analyzing the radio waves sent by GPS satellites.
- Built-in map: It provides map view to the user by mapping the position calculated according to the signals broadcasted by the satellites to a physical location in the world. Also, it can determine the velocity of the user according to its motion. Further, it can derive the driving behavior of drivers.
- Network connectivity: Nowadays GPS devices are equipped with various wireless technologies. For example, Bluetooth becomes very popular in today's smartphone. It allows GPS devices to be paired with the user's phone. As a

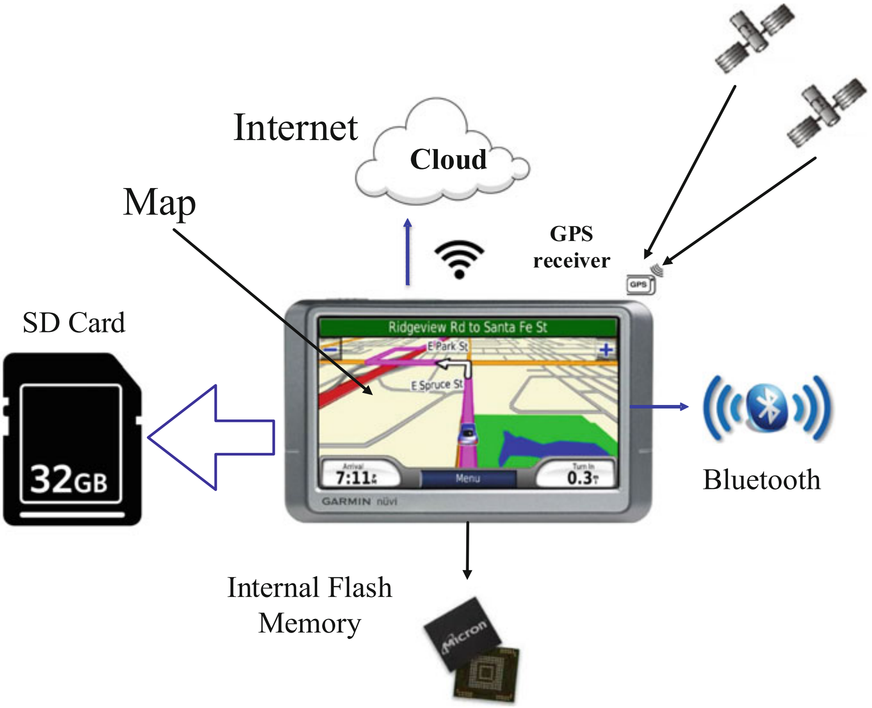


Fig. 16.3 GPS device structure

result, GPS devices can be connected to the Internet, using a wide variety of cloud services, for example, automated map updating. However, it is optional to have it.

There have been plenty of portable GPS devices, but Garmin and TomTom units are by far the most popular ones used by the public. Similarly, with the popularity of smartphones, we have witnessed an increase in the installation of GPS Navigation Apps on smartphones. However, many in-vehicle communications and entertainment system such as Ford Sync (stylized Ford SYNC) also contains built-in GPS navigation functionality, offering drivers' satellite navigation. Nevertheless, the wide variety of available GPS devices create many challenges for investigators; with so many different models available, it becomes difficult to acquire and analyze the evidence in them, as each one must be treated differently. Furthermore, modern GPS devices contain much more than navigational information. They may contain data commonly found in cell phones. Investigators may also find audio, video, and text based files like MS Word or PDF documents. The focus of this chapter will be on Garmin nüvi devices, Garmin nüvi 1350 in particular, but the general process is also applicable for other device types and models.

Some important concepts and definitions that will be used throughout this chapter are presented in Table 16.1 for reference.

Table 16.1 Definitions and common concepts

Coordinate	The coordinates are numbers representing geographic locations on the earth, where one number (e.g., elevation) represents vertical position and two or three of the numbers (e.g., Latitude and longitude) represent horizontal position [2]
Waypoint	Waypoints are geographic locations defined by a GPS device user using their coordinates or addresses, or some other Point of Interest (POI) so that they will be travelled through
Destination	A destination is a geographic location defined by a GPS device user using their coordinates or addresses. It is a location the user wants to arrive at
Track	A history of where and when GPS device users have been. A track consists of many track points or geographic locations where GPS device users have been travelling through
Route	A route is a path from the starting point (by default, the current location) of a trip to the destination defined by the user

16.2 GPS Evidentiary Data

Today's GPS devices contain plenty of data which are of interest to forensic investigators. There are many types of valuable evidentiary data which may be recovered from GPS devices depending on the manufacturer and model [3].

- Track Logs
- Trackpoints
- Waypoints
- Routes
- Stored location, including Home and Favourite locations
- Recent destinations: The addresses of the trips that GPS device users have made.
- Paired device history: History of all devices (e.g., mobile phone) connected to GPS devices via Bluetooth.
- Videos, Photos, Audio
- Call history, contact phone numbers and SMS messages: Call history, contact phone numbers and SMS messages from the connected phone.

16.3 Case Study

Next, we will use a case study as an example of how to conduct a GPS device forensic investigation. Specifically, we will show how to extract track logs from Garmin nüvi 1350.

Fig. 16.4 Garmin nüvi 1350

16.3.1 Experiment Setup

GPS device:

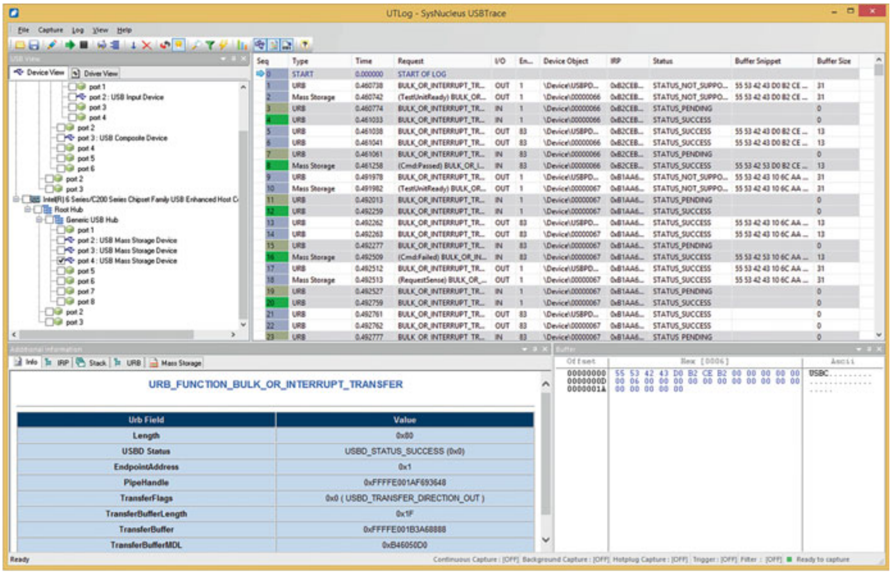
- Garmin nüvi 1350 (Fig. 16.4)

Software:

- FTK imager (version 3.4.2.2) [4]
- USBtrace (version 5.9) [5]
- Google Earth [6]

16.3.2 Basic Precautions and Procedures

Care should be taken when handling an evidence, like the GPS device obtained from the suspect. It is essential to make sure that the data doesn't get tampered in any way when the device is connected to the investigator's computer. Garmin nüvi 1350 provides USB port for computer connection. While Garmin nüvi 1350 is connected to your computer, Windows will recognize it as a "Mass storage device". Because any data that is written into the device by the external unit (in this case the investigator's computer) will only complicate the matter when it comes to the validity of the evidence. So, it is essential that the computer used by the investigator doesn't have any drivers meant for the GPS device and that the computer is not connected to the Internet, in order to prevent the computer OS from automatically downloading the drivers. It may also be imperative to use USB traffic sniffer software to monitor the traffic between the GPS device. Here, the computer is required. It will be required to keep a log of the traffic between the computer and the GPS device that is being investigated. One such example of a USB traffic sniffer software is USBtrace [5] from SysNucleus, as shown in Fig. 16.5. It is quintessential


UTLog - SysNucleus USBTrace
File Capture Log View Help
USB View
Device View
Driver View
port 1
port 2 : USB Input Device
port 3
port 4
port 2
port 3 : USB Composite Device
port 4
port 5
port 6
port 2
port 3
Intel(R) 6 Series/C200 Series Chipset Family USB Enhanced Host C
Root Hub
Generic USB Hub
port 1
port 2 : USB Mass Storage Device
port 3 : USB Mass Storage Device
port 4 : USB Mass Storage Device
port 5
port 6
port 7
port 8
port 2
port 3
Additional Information
Info
IRP
Stack
URB
Mass Storage
Buffer

Seq	Type	Time	Request	I/O	En...	Device Object	IRP	Status	Buffer Snippet	Buffer Size
0	START	0.000000	START OF LOG							
1	URB	0.460738	BULK_OR_INTERRUPT_TR...	OUT	1	\Device\USBPD...	0xB2CEB...	STATUS_NOT_SUPPO...	55 53 42 43 D0 B2 CE ...	31
2	Mass Storage	0.460742	(TestUnitReady) BULK_OR...	OUT	1	\Device\00000066	0xB2CEB...	STATUS_NOT_SUPPO...	55 53 42 43 D0 B2 CE ...	31
3	URB	0.460774	BULK_OR_INTERRUPT_TR...	IN	1	\Device\00000066	0xB2CEB...	STATUS_PENDING		0
4	URB	0.461033	BULK_OR_INTERRUPT_TR...	IN	1	\Device\00000066	0xB2CEB...	STATUS_SUCCESS		0
5	URB	0.461038	BULK_OR_INTERRUPT_TR...	OUT	83	\Device\USBPD...	0xB2CEB...	STATUS_SUCCESS	55 53 42 43 D0 B2 CE ...	13
6	URB	0.461041	BULK_OR_INTERRUPT_TR...	OUT	83	\Device\00000066	0xB2CEB...	STATUS_SUCCESS	55 53 42 43 D0 B2 CE ...	13
7	URB	0.461061	BULK_OR_INTERRUPT_TR...	IN	83	\Device\00000066	0xB2CEB...	STATUS_PENDING		0
8	Mass Storage	0.461258	(Cmd:Passed) BULK_OR_I...	IN	83	\Device\00000066	0xB2CEB...	STATUS_SUCCESS	55 53 42 53 D0 B2 CE ...	13
9	URB	0.491978	BULK_OR_INTERRUPT_TR...	OUT	1	\Device\USBPD...	0xB1AA6...	STATUS_NOT_SUPPO...	55 53 42 43 10 6C AA ...	31
10	Mass Storage	0.491982	(TestUnitReady) BULK_OR...	OUT	1	\Device\00000067	0xB1AA6...	STATUS_NOT_SUPPO...	55 53 42 43 10 6C AA ...	31
11	URB	0.492013	BULK_OR_INTERRUPT_TR...	IN	1	\Device\00000067	0xB1AA6...	STATUS_PENDING		0
12	URB	0.492259	BULK_OR_INTERRUPT_TR...	IN	1	\Device\00000067	0xB1AA6...	STATUS_SUCCESS		0
13	URB	0.492262	BULK_OR_INTERRUPT_TR...	OUT	83	\Device\USBPD...	0xB1AA6...	STATUS_SUCCESS	55 53 42 43 10 6C AA ...	13
14	URB	0.492263	BULK_OR_INTERRUPT_TR...	OUT	83	\Device\00000067	0xB1AA6...	STATUS_SUCCESS	55 53 42 43 10 6C AA ...	13
15	URB	0.492277	BULK_OR_INTERRUPT_TR...	IN	83	\Device\00000067	0xB1AA6...	STATUS_PENDING		0
16	Mass Storage	0.492509	(Cmd:Failed) BULK_OR_IN...	IN	83	\Device\00000067	0xB1AA6...	STATUS_SUCCESS	55 53 42 53 10 6C AA ...	13
17	URB	0.492512	BULK_OR_INTERRUPT_TR...	OUT	1	\Device\USBPD...	0xB1AA6...	STATUS_SUCCESS	55 53 42 43 10 6C AA ...	31
18	Mass Storage	0.492513	(RequestSense) BULK_OR_...	OUT	1	\Device\00000067	0xB1AA6...	STATUS_SUCCESS	55 53 42 43 10 6C AA ...	31
19	URB	0.492527	BULK_OR_INTERRUPT_TR...	IN	1	\Device\00000067	0xB1AA6...	STATUS_PENDING		0
20	URB	0.492759	BULK_OR_INTERRUPT_TR...	IN	1	\Device\00000067	0xB1AA6...	STATUS_SUCCESS		0
21	URB	0.492761	BULK_OR_INTERRUPT_TR...	OUT	83	\Device\USBPD...	0xB1AA6...	STATUS_SUCCESS		0
22	URB	0.492762	BULK_OR_INTERRUPT_TR...	OUT	83	\Device\00000067	0xB1AA6...	STATUS_SUCCESS		0
23	URB	0.492777	BULK OR INTERRUPT TR...	IN	83	\Device\00000067	0xB1AA6...	STATUS PENDING		0

URB_FUNCTION_BULK_OR_INTERRUPT_TRANSFER

Urb Field	Value
Length	0x80
USBD Status	USBD_STATUS_SUCCESS (0x0)
EndpointAddress	0x1
PipeHandle	0xFFFFE001AF693648
TransferFlags	0x0 (USBD_TRANSFER_DIRECTION_OUT)
TransferBufferLength	0x1F
TransferBuffer	0xFFFFE001B3A68888
TransferBufferMDL	0xB46050D0

```
Offset     Hex [0006]                                 Ascii
00000000   55 53 42 43 D0 B2 CE B2 00 00 00 00 00     USBC.........
0000000D   00 06 00 00 00 00 00 00 00 00 00 00 00     .............
0000001A   00 00 00 00 00                             .....
```

Ready   Continuous Capture : [OFF] Background Capture : [OFF] Hotplug Capture : [OFF] Trigger : [OFF] Filter : [OFF] ■ Ready to capture

Fig. 16.5 A screenshot of SysNucleus USBTrace which is used for monitoring the traffic between the Garmin nuvi 1350 and the desktop computer running Win 8.1. The Garmin device is connected to the USB port of the desktop computer

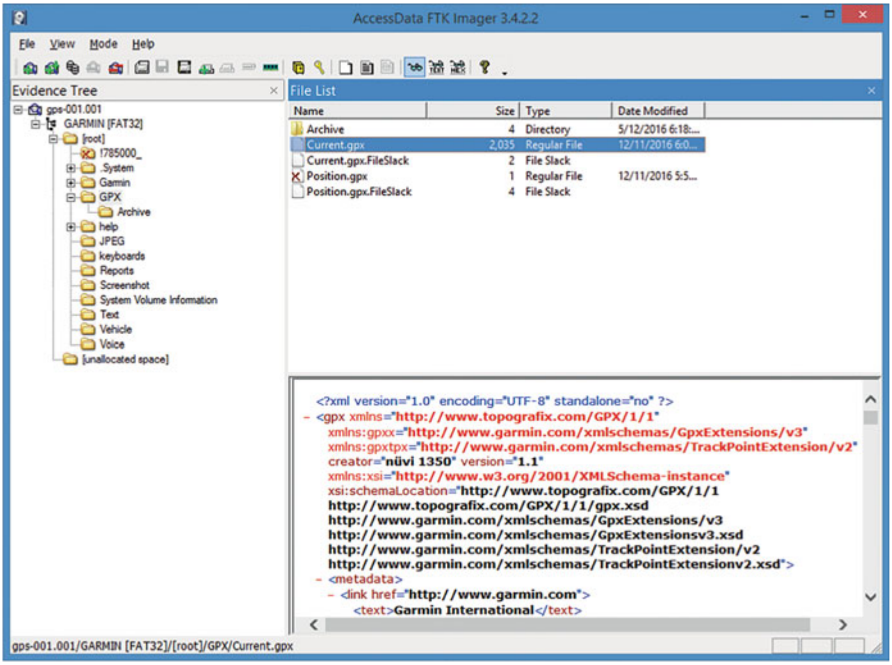
to have a write blocker in place to be doubly sure that the computer doesn't write anything on to the GPS device under investigation.

It is absolutely essential to make a backup copy of the GPS device in question, which is the evidence obtained from the suspect. One such tool that can be used for backing up the device is FTK imager [4] from AccessData, as shown in Fig. 16.6.

All the forensics associated with GPS should be conducted in a place where the GPS device won't be able to contact the satellites, for example, a closed basement or the unit must be in Faraday bag. If not, it leads to a situation where there may be new entries/records on the device after it is confiscated from the suspect. This scenario can be detrimental in accepting the device as an evidence. The information that is most valuable to an investigator who looks for evidence, are files that carry time stamped information about the locations that the GPS unit was at.

16.3.3 GPS Exchange Format (GPX)

The GPS exchange format (GPX) is a light-weight XML data format for the interchange of GPS data (waypoints, routes, and tracks) between applications and web services on the Internet [7]. GPX is designed to be the standard XML format for recording GPS data and exchanging GPS data between applications (and GPS



Name	Size	Type	Date Modified
Archive	4	Directory	5/12/2016 6:18:...
Current.gpx	2,035	Regular File	12/11/2016 6:0...
Current.gpx.FileSlack	2	File Slack	
Position.gpx	1	Regular File	12/11/2016 5:5...
Position.gpx.FileSlack	4	File Slack	

```
  <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <gpx xmlns="http://www.topografix.com/GPX/1/1"
    xmlns:gpxx="http://www.garmin.com/xmlschemas/GpxExtensions/v3"
    xmlns:gpxtpx="http://www.garmin.com/xmlschemas/TrackPointExtension/v2"
    creator="nüvi 1350" version="1.1"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.topografix.com/GPX/1/1
    http://www.topografix.com/GPX/1/1/gpx.xsd
    http://www.garmin.com/xmlschemas/GpxExtensions/v3
    http://www.garmin.com/xmlschemas/GpxExtensionsv3.xsd
    http://www.garmin.com/xmlschemas/TrackPointExtension/v2
    http://www.garmin.com/xmlschemas/TrackPointExtensionv2.xsd">
  - <metadata>
    - <link href="http://www.garmin.com">
        <text>Garmin International</text>
```

gps-001.001/GARMIN [FAT32]/[root]/GPX/Current.gpx

Fig. 16.6 A screenshot of AccessData FTK Imager ver 3.4.2.2. An image of the original Garmin nuvi 1350 is created and the image is opened in AccessData FTK to do the analysis. It has features to view or export a file from the image

devices). It can describe even complex objects that are geographic in nature. It is designed to grow overtime. As GPX is an open standard, no fee or licensing is involved.

Some of the significance used items in Garmin GPX files are Waypoint, Route, Track Point and Track log. The ones that the user can interact with are Waypoint and Route. On the system level, there are Track Point and Track log.

16.3.3.1 Waypoint

The user can store information in Garmin nüvi 1350, for example, by defining waypoints. A waypoint in this case is a location on earth the user stored in the GPS. Mostly, waypoints contain address book as entries. Existence of waypoint alone doesn’t mean that the user was at that particular location. Waypoint could be a location that the user entered that he/she wanted to navigate to, in future. It could also be a location stored by the user where he/she was physically present.

Example for a Waypoint may look as follows:

```
<wpt lat="33.762918" lon="-118.196241">

        <ele>-0.11</ele>
        <name>Long Beach Aquarium of the Pcf</name>
        <desc>100 Aquarium Way Long Beach, CA 9080</desc>
        <sym>Waypoint</sym>
        <extensions>

                <gpxx:WaypointExtension>

                        <gpxx:Categories>

                                <gpxx:Category>Attractions</gpxx:Category>

                        </gpxx:Categories>
                        <gpxx:Address>

                               <gpxx:StreetAddress>100 Aquarium Way</gpxx:
                               StreetAddress>
                               <gpxx:City>Long Beach</gpxx:City>
                               <gpxx:State>CA</gpxx:State>
                               <gpxx:PostalCode>90802</gpxx:PostalCode>

                        </gpxx:Address>
                       <gpxx:PhoneNumber>1 5621253400</gpxx:PhoneNumber>

                </gpxx:WaypointExtension>

        </extensions>

</wpt>
```

As Waypoints are user entries, it may not be consistent. For example, see the waypoint entry above and the one given below:

```
<wpt lat="41.991357" lon="-72.584978">

        <ele>53.72</ele>
        <name>Red Roof Inn</name>
        <sym>Waypoint</sym>
        <extensions>

               <gpxx:WaypointExtension>

                        <gpxx:Categories>

                                 <gpxx:Category>Map Points and Coordinates</
                                 gpxx:Category>

                        </gpxx:Categories>
                        <gpxx:Address>
                        <gpxx:StreetAddress>N 41°59.481' W072°35.099'</
                        gpxx:StreetAddress>

                    </gpxx:Address>

            </gpxx:WaypointExtension>

      </extensions>

</wpt>
```

16.3.3.2 Route

If a user wants to navigate a series of waypoints in a specific order, then it is a route. In other words, a route is defined by the user. After reaching a waypoint, the unit guides the user to the next waypoint.

16.3.3.3 Track Point

The track point shows the location recorded by the GPS regarding where it was, provided the unit was turned on and it had established satellite links. This record carries the timestamp, latitude, longitude, and elevation. The track point extension carries information about the speed as well. The track points are generated automatically by the GPS unit and the user cannot define or change what gets generated. Again, the applications within the GPS decide on the generation frequency of these track point records.

Note that there are no settings in Garmin nüvi 1350 which can dictate the terms of the generated frequency of track points or to turn the recording off. This doesn’t mean that such features are non-existent for other models.

For example, given below is an example for a track point.

```
<trkpt lat="43.658288" lon="-79.352451">

      <ele>78.48</ele>
      <time>2015-01-15T23:35:46Z</time>
      <extensions>

            <gpxtpx:TrackPointExtension>

                  <gpxtpx:speed>8.24</gpxtpx:speed>
                  <gpxtpx:course>254.12</gpxtpx:course>

            </gpxtpx:TrackPointExtension>

      </extensions>

</trkpt>
```

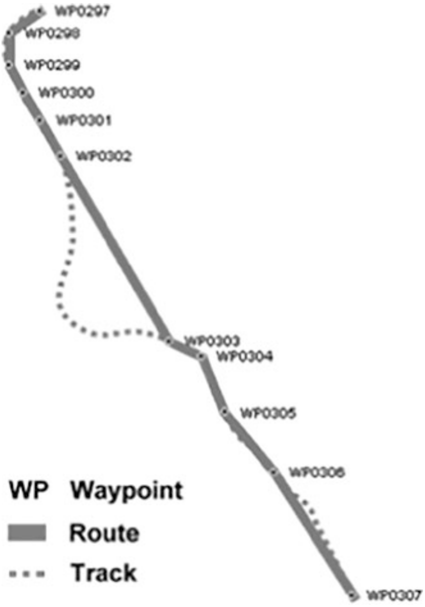


Fig. 16.7 The difference between route and track

16.3.3.4 Track Log

This is the complete list of track points that is created and stored by the unit when the GPS device is locked onto a satellite signal and moving. It is the electronic equivalent of laying down a "breadcrumb trail" to mark the path that has been traveled. This helps the user to retrace the steps. In other words, it allows the user to perform a track back.

The difference between track and route is that route is a suggestion on where the user may go in future. Track, on the other hand, is a record of where the user has been. Track has a good number of track points to generate the fine details of the path. As shown in Fig. 16.7 [8]. Each track point may have a timestamp as a location and time is being recorded. On the other hand the route points are unlikely to have timestamps. Moreover the distance between two track points are on an average 50 meters or less. Nevertheless, the route points may be apart by a kilometer or more.

16.3.3.5 Track Segment

Track is a collection of track points, listed in the order they are generated. This list can be broken down or divided into two or more track segments that are listed in sequential order. Following is an example of a track segment constituted of multiple track points.

```
<trkseg>
        <trkpt>          . . .          </trkpt>
        <trkpt>          . . .          </trkpt>
        <trkpt> . . . </trkpt>
</trkseg>
```

The track points and tracks are a treasure mine for the investigator. It doesn't mean we should limit ourselves to just that. Instead, we should explore more to see what else may be there.

16.3.4 GPX Files

The GPX files which carry the track point information are found in folder \GPX and the archived files are found in \GPX\Archive folder. The latest one is in \GPX folder and it is called "Current.gpx". It contains most recent tracks and carries favorites as well. The archived ones have numeric file names such as "19.gpx" to "38.gpx". The files that are in "\GPX\Archive" folder have past information regarding the track, time, location etc. (Table 16.2).

Table 16.2 Example list of 'gpx' files found in Garmin nüvi 1350

Filename	Full path	File size (Bytes)	Created	Modified
Current.gpx	\GPX\Current.gpx	2,083,450	07/30/2011 15:06	12/11/2016 13:00
19.gpx	\GPX\Archive\19.gpx	2,879,238	07/8/2012 14:00	07/15/2012 17:41
20.gpx	\GPX\Archive\20.gpx	2,949,422	07/15/2012 17:41	08/10/2012 24:17
21.gpx	\GPX\Archive\21.gpx	2,333,630	08/10/2012 24:17	08/10/2012 24:18
22.gpx	\GPX\Archive\22.gpx	3,129,413	08/10/2012 24:18	10/08/2012 13:27
23.gpx	\GPX\Archive\23.gpx	958,394	10/08/2012 13:27	03/14/2013 10:41
24.gpx	\GPX\Archive\24.gpx	1,053,696	03/14/2013 10:41	08/22/2013 20:45
25.gpx	\GPX\Archive\25.gpx	2,166,664	08/22/2013 20:45	08/22/2013 20:47
26.gpx	\GPX\Archive\26.gpx	2,712,169	08/22/2013 20:47	08/24/2013 24:44
27.gpx	\GPX\Archive\27.gpx	2,742,380	08/24/2013 24:44	08/25/2013 05:17
28.gpx	\GPX\Archive\28.gpx	1,107,530	08/25/2013 05:17	09/01/2013 06:42
29.gpx	\GPX\Archive\29.gpx	2,095,540	11/17/2015 13:48	11/17/2015 11:49
30.gpx	\GPX\Archive\30.gpx	3,015,182	11/17/2015 11:49	12/02/2015 14:55
31.gpx	\GPX\Archive\31.gpx	2,073,189	12/02/2015 14:55	12/02/2015 14:55
32.gpx	\GPX\Archive\32.gpx	1,886,340	12/02/2015 14:55	12/02/2015 14:56
33.gpx	\GPX\Archive\33.gpx	1,888,595	12/02/2015 14:56	12/02/2015 15:58
34.gpx	\GPX\Archive\34.gpx	1,859,629	12/02/2015 15:58	12/02/2015 14:59
35.gpx	\GPX\Archive\35.gpx	2,188,914	05/12/2016 14:11	05/12/2016 14:14
36.gpx	\GPX\Archive\36.gpx	2,123,463	05/12/2016 14:14	05/12/2016 14:16
37.gpx	\GPX\Archive\37.gpx	1,995,567	05/12/2016 14:16	05/12/2016 14:18
38.gpx	\GPX\Archive\38.gpx	53,875	05/12/2016 14:18	05/12/2016 14:18

16.3.5 Extraction of Waypoints and Trackpoints

As mentioned earlier the Garmin nüvi’s current waypoints, tracks, and routes are stored in the file “Current.gpx” which is created by the unit. It’s worthy pointing out that Garmin calls waypoints as Favorites. To view them, press “Where To?” on the home screen of the GPS (Fig. 16.8).

In the next screen, press on “Favorites” (Fig. 16.9).

Then, press on “All Favorites” (Fig. 16.10).

And, it will display the favorites as follows (Fig. 16.11).

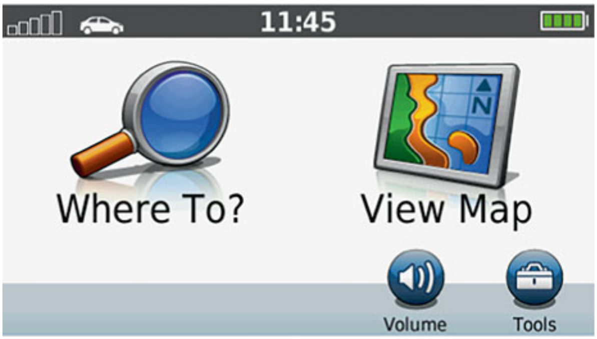


Fig. 16.8 Home screen

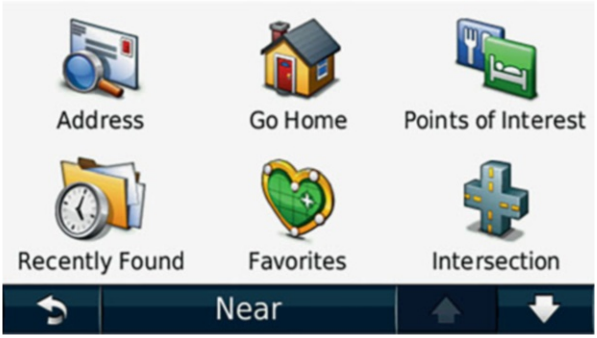


Fig. 16.9 The ‘Where to?’

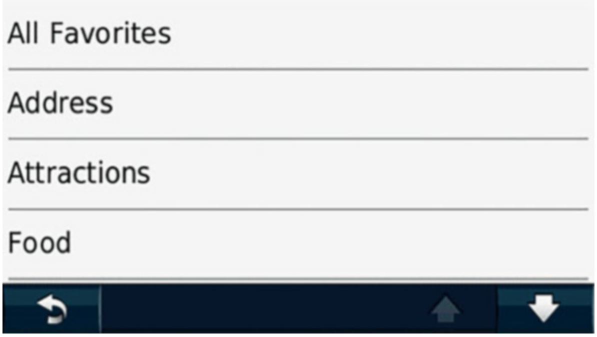
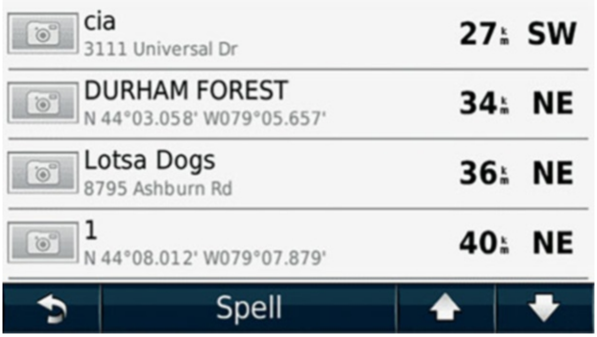


Fig. 16.10 Favorites

Fig. 16.11 All favorites



cia 3111 Universal Dr	27 km	SW
DURHAM FOREST N 44°03.058' W079°05.657'	34 km	NE
Lotsa Dogs 8795 Ashburn Rd	36 km	NE
1 N 44°08.012' W079°07.879'	40 km	NE

16.3.6 How to Display the Tracks on a Map

Getting the favorites, address stored, etc. is great. But from a crime stand point of view, it is essential to prove that the device actually went to a location on the day/time where the actual crime was committed.

So, it is essential to display the data on a map, with all the other parameters. There are a lot of applications and websites that are capable of displaying the track. We use Google Earth [6]. It can be downloaded from http://www.google.com/earth/download/ge/agree.html

Once the application is installed, run it. The opening screen will look as follows (Fig. 16.12):

Let us make an assumption that there was some crime committed in Durham Forest, Uxbridge, Ontario on 21 May 2012 during the day time. Say the GPS device obtained from the suspect still carries the data. After going through the whole archives, say that the relevant data is in file “17.gpx”.

On Google Earth, from the horizontal menu bar, select “File” and click on “Open”. Make sure the selection is for GPS (*.gpx. . .). Browse the folder in which the “17.gpx” file is located (Fig. 16.13).

Under GPS devices, expand “Tracks”, as shown in Fig. 16.14.

Expanded track will look like Fig. 16.15.

As we are specifically only interested in the details pertaining to 21 May 2012, we can deselect all the others. By selecting the module we want and clicking on “Play Tour” button (indicated in red circle in Fig. 16.16), we can get an overview of the movements.

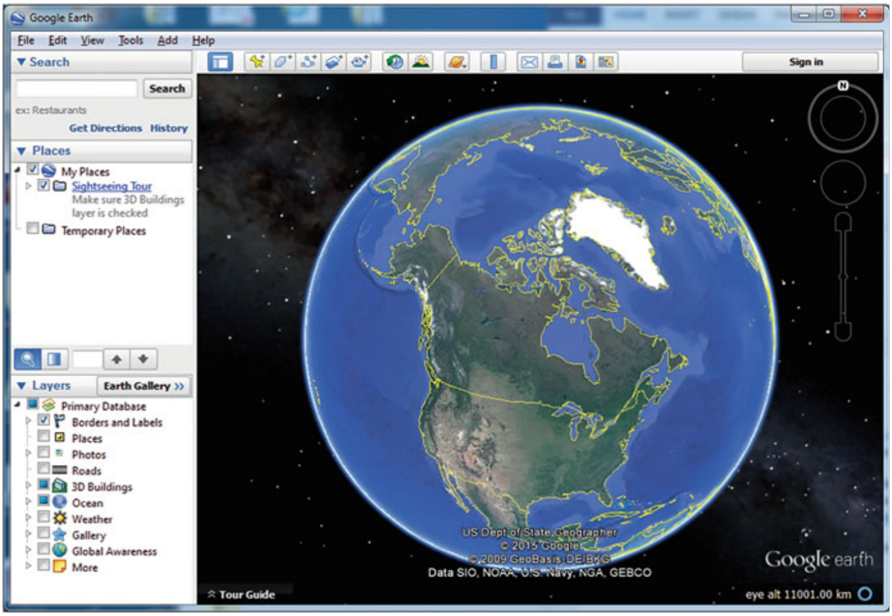
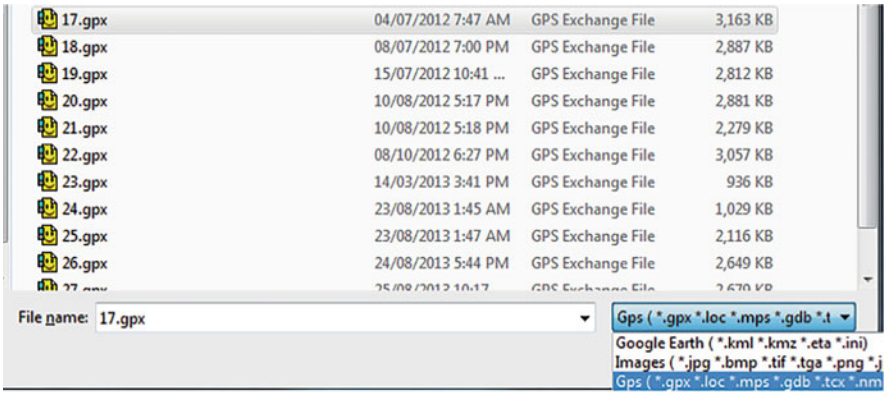


Fig. 16.12 Google earth



17.gpx	04/07/2012 7:47 AM	GPS Exchange File	3,163 KB
18.gpx	08/07/2012 7:00 PM	GPS Exchange File	2,887 KB
19.gpx	15/07/2012 10:41 ...	GPS Exchange File	2,812 KB
20.gpx	10/08/2012 5:17 PM	GPS Exchange File	2,881 KB
21.gpx	10/08/2012 5:18 PM	GPS Exchange File	2,279 KB
22.gpx	08/10/2012 6:27 PM	GPS Exchange File	3,057 KB
23.gpx	14/03/2013 3:41 PM	GPS Exchange File	936 KB
24.gpx	23/08/2013 1:45 AM	GPS Exchange File	1,029 KB
25.gpx	23/08/2013 1:47 AM	GPS Exchange File	2,116 KB
26.gpx	24/08/2013 5:44 PM	GPS Exchange File	2,649 KB
27.gpx	25/08/2013 10:17	GPS Exchange File	2,670 KB

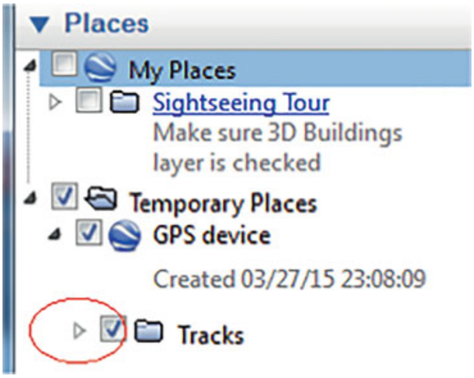
File name: 17.gpx

Gps (*.gpx *.loc *.mps *.gdb *.t

Google Earth (*.kml *.kmz *.eta *.ini)
Images (*.jpg *.bmp *.tif *.tga *.png *.j
Gps (*.gpx *.loc *.mps *.gdb *.tcx *.nm

Fig. 16.13 Select file type

Fig. 16.14 Click on the triangle to expand tracks



▼ Places

□ My Places

▷ □ Sightseeing Tour

Make sure 3D Buildings layer is checked

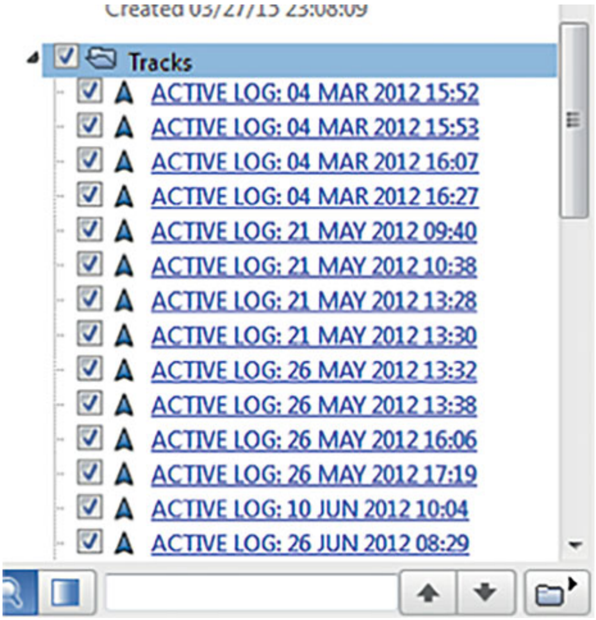
☑ Temporary Places

☑ GPS device

Created 03/27/15 23:08:09

▷ ☑ Tracks

Fig. 16.15 Tracks



Created 03/27/15 23:08:09

☑ Tracks

☑ ACTIVE LOG: 04 MAR 2012 15:52

☑ ACTIVE LOG: 04 MAR 2012 15:53

☑ ACTIVE LOG: 04 MAR 2012 16:07

☑ ACTIVE LOG: 04 MAR 2012 16:27

☑ ACTIVE LOG: 21 MAY 2012 09:40

☑ ACTIVE LOG: 21 MAY 2012 10:38

☑ ACTIVE LOG: 21 MAY 2012 13:28

☑ ACTIVE LOG: 21 MAY 2012 13:30

☑ ACTIVE LOG: 26 MAY 2012 13:32

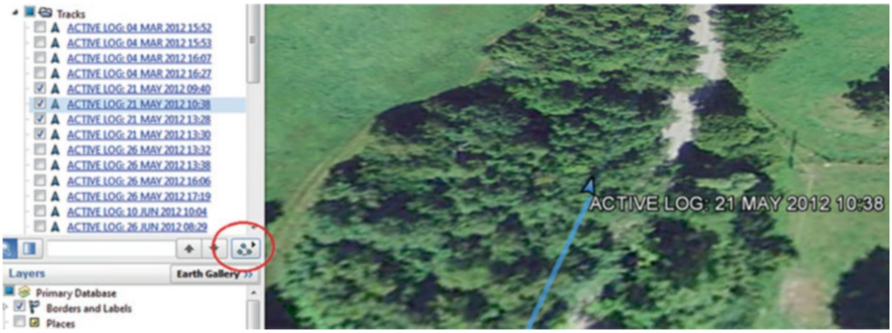
☑ ACTIVE LOG: 26 MAY 2012 13:38

☑ ACTIVE LOG: 26 MAY 2012 16:06

☑ ACTIVE LOG: 26 MAY 2012 17:19

☑ ACTIVE LOG: 10 JUN 2012 10:04

☑ ACTIVE LOG: 26 JUN 2012 08:29



Tracks

□ ACTIVE LOG: 04 MAR 2012 15:52

□ ACTIVE LOG: 04 MAR 2012 15:53

□ ACTIVE LOG: 04 MAR 2012 16:07

□ ACTIVE LOG: 04 MAR 2012 16:27

☑ ACTIVE LOG: 21 MAY 2012 09:40

☑ ACTIVE LOG: 21 MAY 2012 10:38

☑ ACTIVE LOG: 21 MAY 2012 13:28

☑ ACTIVE LOG: 21 MAY 2012 13:30

□ ACTIVE LOG: 26 MAY 2012 13:32

□ ACTIVE LOG: 26 MAY 2012 13:38

□ ACTIVE LOG: 26 MAY 2012 16:06

□ ACTIVE LOG: 26 MAY 2012 17:19

□ ACTIVE LOG: 10 JUN 2012 10:04

□ ACTIVE LOG: 26 JUN 2012 08:29

Fig. 16.16 Overview of movements

Review Questions

1. What are the two most popular applications for GPS?
2. What are the two most popular brands of GPS systems for the public?
3. List four types of evidence that may be found within a GPS device.
4. In GPS navigation terms, what are the differences between Route and Track?
5. What GPS tools do you use regularly, and when has GPS not worked for you? Tell us in the comments.

16.4 Practice Exercise

The objective of this exercise is to practice GPS Forensics to reconstruct location, waypoint, and speed data.

16.4.1 Setting Up Practical Exercise Environment

For this exercise, assume a Garmin GPS devices can be found by the reader. Also, USB to Mini-USB Cable is needed to connect the GPS device to the computer. If not, you can use the GPS image provided in the book. In the zipped file which contains all the data files used in the book, you will find a ch16 subfolder that contains all the files for this exercise. Make sure you copy and paste these files into a particular folder on your hard disk.

1. Download the AccessData's FTK Imager from the following website: http://www.accessdata.com/support/product-downloads
2. Run the downloaded installer and follow the on-screen instructions to finish the installation with default settings.
3. Download the Google Earth from the following website: https://earth.google.com/download-earth.html

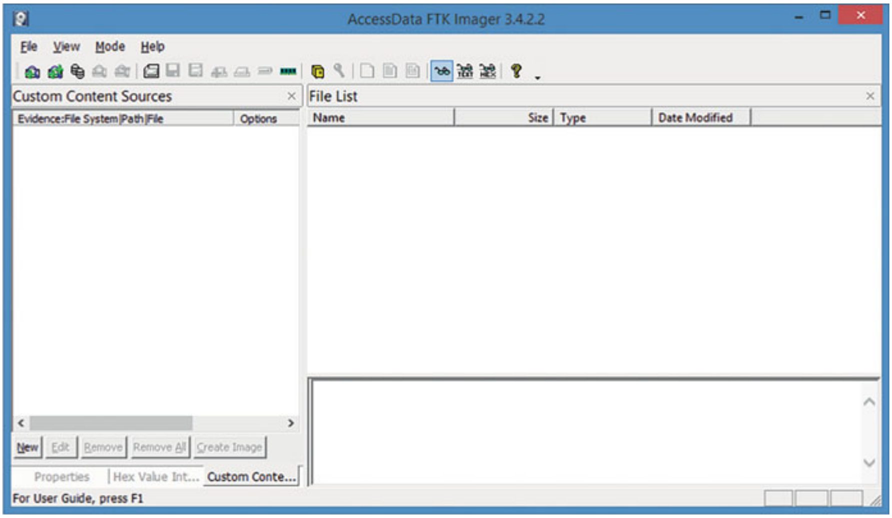
   Note: both of Google Earth and Google Earth Pro are free for public now, so you can download either of them for GPS investigation.
4. Run the downloaded installer and follow the on-screen instructions to finish the installation with default settings.

16.4.2 Exercises

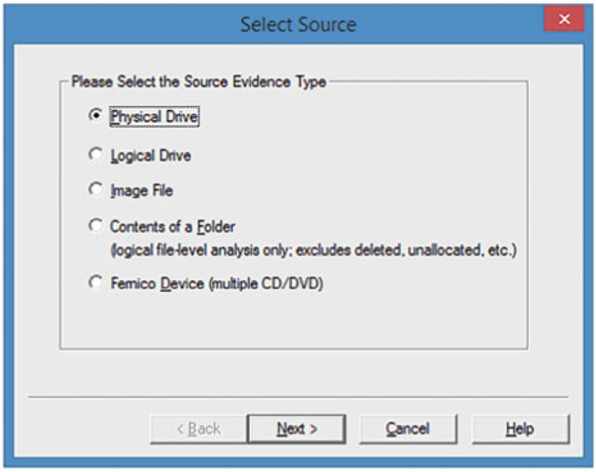
Part A: Acquire a Forensic Image of a Garmin nüvi 1350 Device with FTK Imager

Note that if you don't have any Garmin GPS devices, you can skip this part and proceed to next exercise to analyze Garmin GPS Image provided.

1. Launch the FTK Imager



2. Click **Tools** > **Create Disk Image**.
3. On **Select Source** page, choose the Source Evidence Type you are using. In the present exercise, you will select "**Physical Drive**" since we are creating an image of the internal storage of a GPS device. Then, click on **Next** to continue.



Select Source

Please Select the Source Evidence Type

● Physical Drive

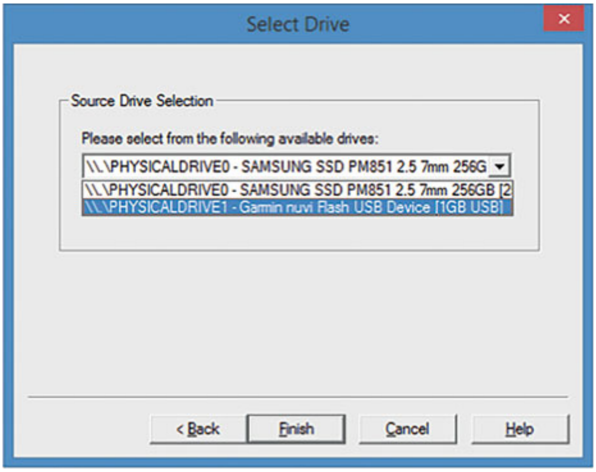
○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)

4. Select the driver to be imaged and click **Finish** to continue. For our scenario example, we will select "**\\cr.\PhysicalDrive1**". Then, click on **Finish** to continue.



Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE0 - SAMSUNG SSD PM851 2.5 7mm 256G

\\.\PHYSICALDRIVE0 - SAMSUNG SSD PM851 2.5 7mm 256GB [2

\\.\PHYSICALDRIVE1 - Garmin nuvi Flash USB Device [1GB USB]

5. On **Create Image** page, click **Add** to select where you want to save the image.

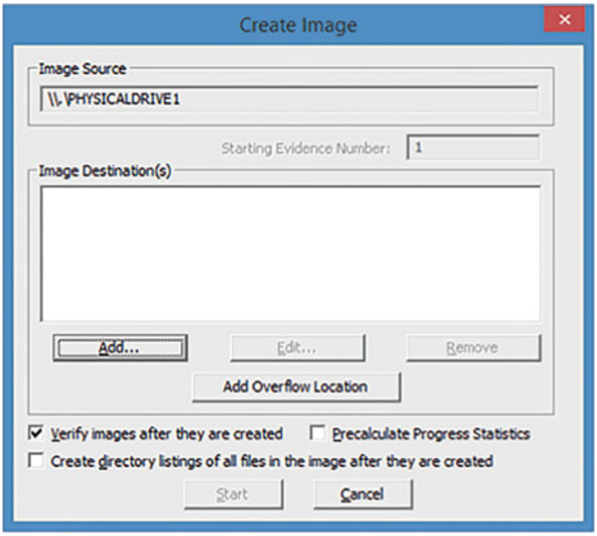


Image Source

\\.\PHYSICALDRIVE1

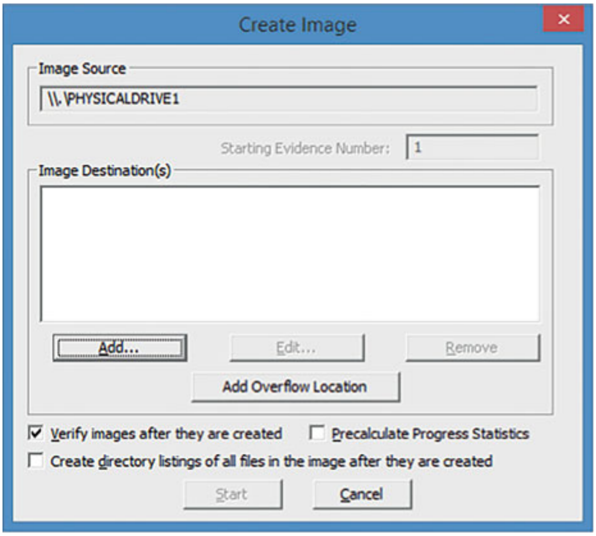
Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created □ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

6. Continue through the prompts and select **Image Type** (for example, **Raw (dd)** which just contains the data from the GPS device). Enter **Evidence Item Information** (Case Number, Evidence Number, Unique Description, Examiner and Notes), and select both the **image destination folder** and the **image filename**.
7. Once the image destination setup is complete, you can either click **Add** to add another destination or click **Start** to begin the acquisition.



Create Image

Image Source: \\.\PHYSICALDRIVE1

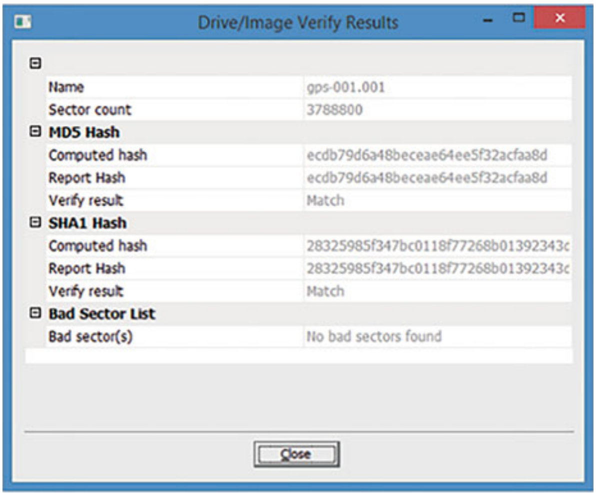
Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created ☐ Precalculate Progress Statistics

☐ Create directory listings of all files in the image after they are created

8. Once completed, the **Drive/Image Verify Results** page will appear.



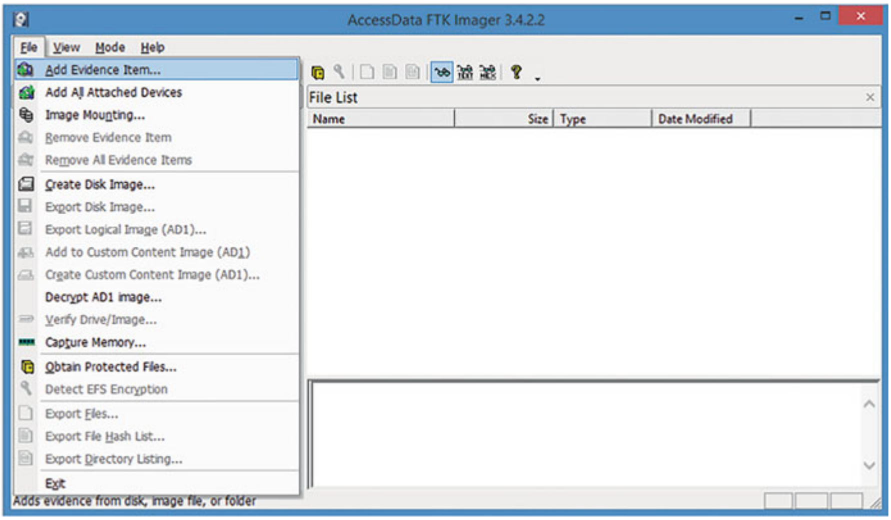
Drive/Image Verify Results

Name	gps-001.001
Sector count	3788800
MD5 Hash	
Computed hash	ecdb79d6a48beceae64ee5f32acfaa8d
Report Hash	ecdb79d6a48beceae64ee5f32acfaa8d
Verify result	Match
SHA1 Hash	
Computed hash	28325985f347bc0118f77268b01392343c
Report Hash	28325985f347bc0118f77268b01392343c
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

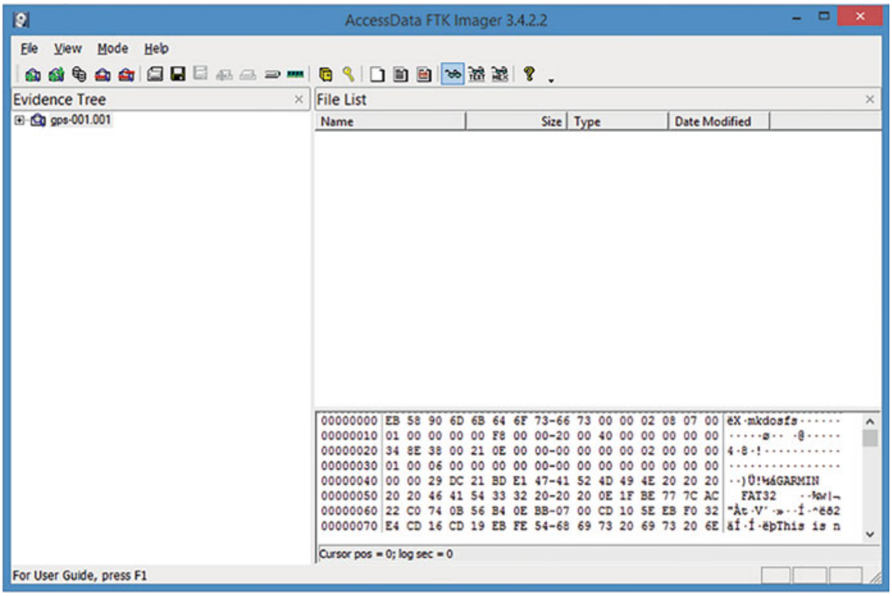
Part B: Extract Track Logs from Garmin nüvi 1350

The next step is to extract track logs from the Garmin nüvi 1350 image we acquire. The ".gpx" file is the key file for navigation in GPS forensics. As mentioned earlier the folder \GPX contains the GPX files which carry the track point information.

1. Launch the FTK Imager and click **File > Add Evidence Item** to add the GPS device image you acquire (or provided in the book) as an evidence item.



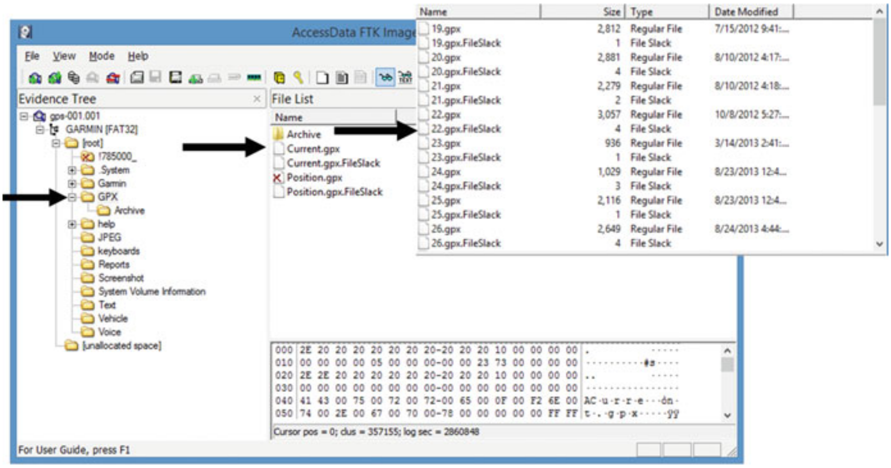
2. Continue through the prompts and select the Source Evidence Type ("Image File"), and select the acquired image file. Then, click **Finish** to add it as an evidence.



```
00000000 EB 58 90 6D 6B 64 6F 73-66 73 00 00 02 08 07 00 ëX·mkdosfs······
00000010 01 00 00 00 00 F8 00 00-20 00 40 00 00 00 00 00 ·····ø·· ·@·····
00000020 34 8E 38 00 21 0E 00 00-00 00 00 00 02 00 00 00 4·8·!···········
00000030 01 00 06 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000040 00 00 29 DC 21 BD E1 47-41 52 4D 49 4E 20 20 20 ··)Ü!½áGARMIN
00000050 20 20 46 41 54 33 32 20-20 20 0E 1F BE 77 7C AC   FAT32    ··¾w|¬
00000060 22 C0 74 0B 56 B4 0E BB-07 00 CD 10 5E EB F0 32 "Àt·V´·»··Í·^ëð2
00000070 E4 CD 16 CD 19 EB FE 54-68 69 73 20 69 73 20 6E äÍ·Í·ëþThis is n
```

Cursor pos = 0; log sec = 0

3. Expand the Evidence Tree and Navigate into the folder \GPX (and its subfolder Archive), and locate the GPX files from GPS devices.

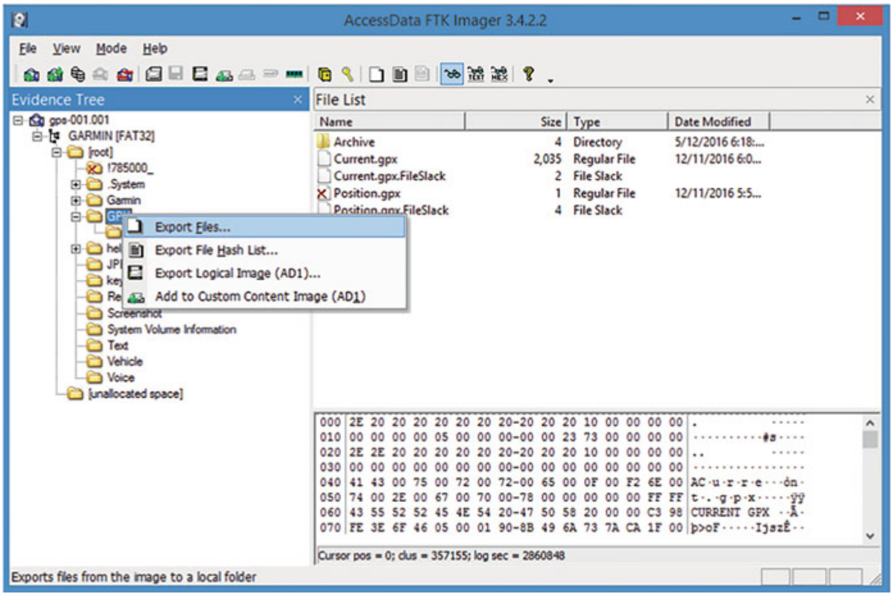


Name	Size	Type	Date Modified
19.gpx	2,812	Regular File	7/15/2012 9:41:...
19.gpx.FileSlack	1	File Slack	
20.gpx	2,881	Regular File	8/10/2012 4:17:...
20.gpx.FileSlack	4	File Slack	
21.gpx	2,279	Regular File	8/10/2012 4:18:...
21.gpx.FileSlack	2	File Slack	
22.gpx	3,057	Regular File	10/8/2012 5:27:...
22.gpx.FileSlack	4	File Slack	
23.gpx	936	Regular File	3/14/2013 2:41:...
23.gpx.FileSlack	1	File Slack	
24.gpx	1,029	Regular File	8/23/2013 12:4...
24.gpx.FileSlack	3	File Slack	
25.gpx	2,116	Regular File	8/23/2013 12:4...
25.gpx.FileSlack	1	File Slack	
26.gpx	2,649	Regular File	8/24/2013 4:44:...
26.gpx.FileSlack	4	File Slack	

```
000  2E 20 20 20 20 20 20 20-20 20 20 10 00 00 00 00  .          -----
010  00 00 00 00 05 00 00 00-00 00 23 73 00 00 00 00  ----------#s----
020  2E 2E 20 20 20 20 20 20-20 20 20 10 00 00 00 00  ..         -----
030  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ----------------
040  41 43 00 75 00 72 00 72-00 65 00 0F 00 F2 6E 00  AC·u·r·r·e···òn·
050  74 00 2E 00 67 00 70 00-78 00 00 00 00 00 FF FF  t·.·g·p·x·····ÿÿ
```

Cursor pos = 0; clus = 357155; log sec = 2860848

4. Transfer GPX files to your computer by right-clicking on the folder GPX, choose **Export Files** from the options in the menu that appears, and select the destination folder. In our example, we saved it under \Garmin.



Name	Size	Type	Date Modified
Archive	4	Directory	5/12/2016 6:18:...
Current.gpx	2,035	Regular File	12/11/2016 6:0...
Current.gpx.FileSlack	2	File Slack	
Position.gpx	1	Regular File	12/11/2016 5:5...
Position.gpx.FileSlack	4	File Slack	

```
000  2E 20 20 20 20 20 20 20-20 20 20 10 00 00 00 00  .          -----
010  00 00 00 00 05 00 00 00-00 00 23 73 00 00 00 00  ----------#s----
020  2E 2E 20 20 20 20 20 20-20 20 20 10 00 00 00 00  ..         -----
030  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ----------------
040  41 43 00 75 00 72 00 72-00 65 00 0F 00 F2 6E 00  AC·u·r·r·e···òn·
050  74 00 2E 00 67 00 70 00-78 00 00 00 00 00 FF FF  t·.·g·p·x·····ÿÿ
060  43 55 52 52 45 4E 54 20-47 50 58 20 00 00 C3 98  CURRENT GPX ··Ã·
070  FE 3E 6F 46 05 00 01 90-8B 49 6A 73 7A CA 1F 00  þ>oF·····IjszÊ··
```

Cursor pos = 0; clus = 357155; log sec = 2860848

Exports files from the image to a local folder

Part C: Analyze Track Data from .gpx Files

In the following exercise you will analyze one GPX file, \GPX\Current.gpx, and answer the following questions. In order to answer these questions properly, you will perform statistical analysis of GPX Files. In doing so, you need to parse GPS track data (tracks and waypoints) into a format accepted by a statistical analysis tool such as Excel. You can either develop your own GPX file parser or use an open source tool. There are many online tools for GPX file analysis. For example, you can use the following tool named GPX Editor to analyze track data from GPX files https://sourceforge.net/projects/gpxeditor/

It is strongly recommended that you design and develop your own GPX file parsing and analysis tool for this exercise.

GPX Files Analysis Questions:

Q1. How many track points are stored in the file "Current.gpx"?

Q2. What are the latitude and longitude of the first track point stored in the file "Current.gpx"?

Q3. How many waypoints are defined in the file "Current.gpx"?

Q4. What are the latitude and longitude of the first waypoint stored in the file "Current.gpx"?

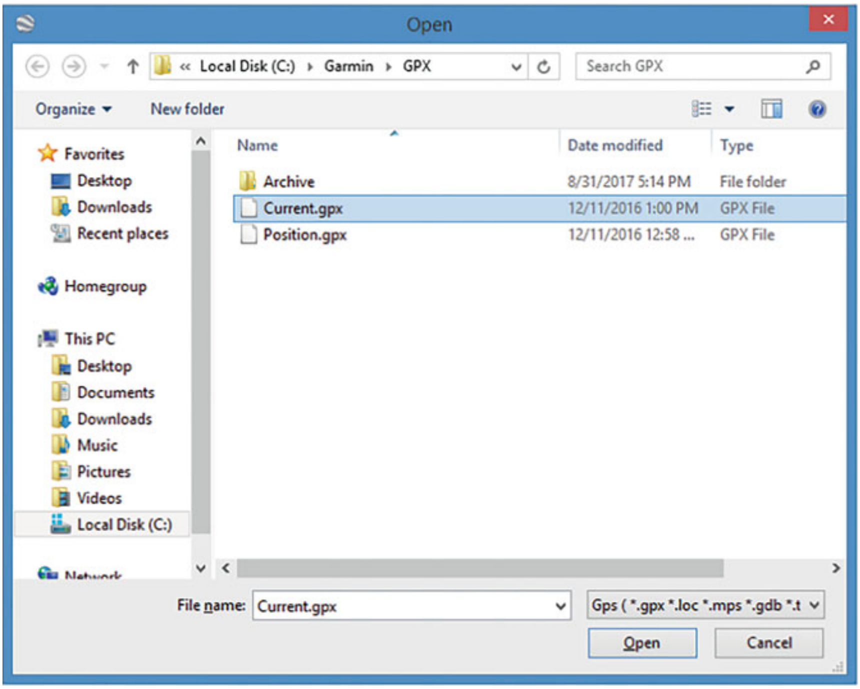
Q5. What is the total distance traveled by the car according to the "Current.gpx"?

Part D: View Track Logs in Google Earth

In the following exercise you will practice how to use Google Earth in your investigations. It is particularly very useful for presentation to investigators, attorneys and in courtrooms.

Note that if your GPS device isn't supported by Google Earth, you will need to import GPS data as a .gpx or .loc file.

5. Launch the Google Earth Pro and Click **File > Open**.
6. Select GPX Files from the Open dialog box by navigating into the folder \Garmin \GPX. Notice that the dialog has a combo box for selecting the file types, and you have to select GPS file types including GPX.



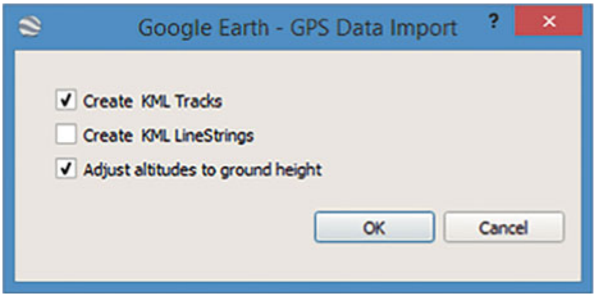
Name	Date modified	Type
Archive	8/31/2017 5:14 PM	File folder
Current.gpx	12/11/2016 1:00 PM	GPX File
Position.gpx	12/11/2016 12:58 ...	GPX File

File name: Current.gpx

Gps (*.gpx *.loc *.mps *.gdb *.t

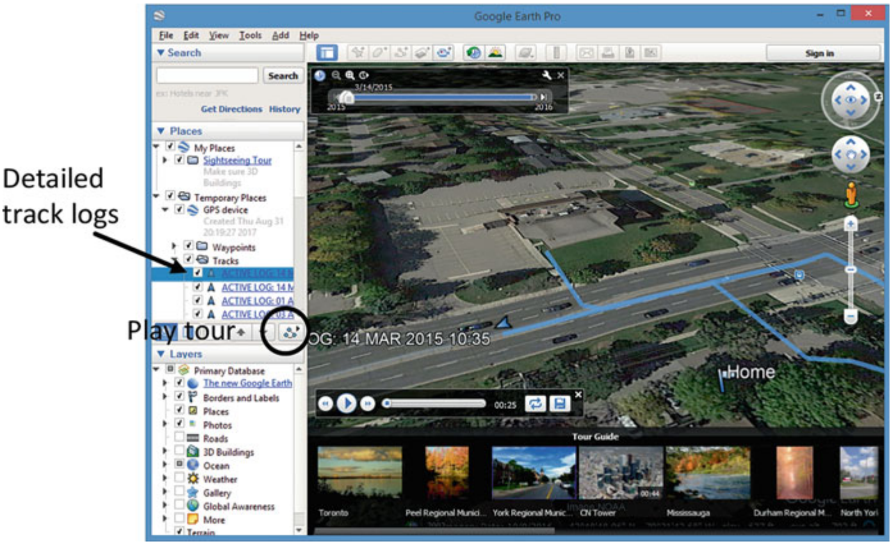
7. On Google Earth—GPS Data Import page, both Create KML Tracks and Adjust altitudes to ground height options are enabled by default. Leave all the default options in place and click on **OK** to continue.

   Note that Keyhole Markup Language (KML) is a file format used to display geographic data in Google Earth and Google Maps.



☑ Create KML Tracks
☐ Create KML LineStrings
☑ Adjust altitudes to ground height

8. Once a GPX file is imported into Google Earth, you can view the routes the suspect has traveled by clicking the **Play Tour** button.



References

1. http://www.trimble.com/gps_tutorial/howgps-triangulating.aspx
2. Geographic coordinate system. http://en.wikipedia.org/wiki/Geographic_coordinate_system
3. TomTom GPS Device Forensics. http://www.forensicfocus.com/tomtom-gps-device-forensics
4. FTK Imager. http://accessdata.com/product-download
5. Usbtrace - USB Analyzer, USB Protocol Analyzer, USB Bus Analyzer/Sniffer For Windows. http://www.sysnucleus.com/
6. Google earth
7. Developing GPX Applications With GPX. http://www.topografix.com/gpx_for_developers.asp
8. Wikipedia. ‘GPS Exchange Format’. http://en.wikipedia.org/wiki/GPS_Exchange_Format