

TomTom **GPS Device Forensics**

Introduction: The sales of portable navigation devices are at an all time high. Last year, more than forty million portable GPS devices like TomTom's GO series or Garmin's Nuvi series were sold worldwide. These devices can be a good source of evidence. With the entrance of hybrid devices into the marketplace, GPS devices now contain much more than navigational information and may contain data commonly found in cell phones as well as audio, video, and text based files like MS Word or PDF documents.

The law enforcement community has seen a dramatic increase in the use of GPS devices as an instrument of a crime or as a "witness device" autonomously collecting and logging positional data while the crime is being carried out. TomTom and Garmin units are by far the most popular devices law enforcement have been encountering. The focus of this article will be on TomTom devices but the general process can be extended to other device types.

TomTom Specifics: TomTom provides a range of devices for navigation. Depending on the capabilities of the model, several different kinds of information can be acquired. Most models have an SD card slot or an internal memory and allow pictures, documents, audio and video files to be stored and accessed thru the device. Standard TomTom files found on a device may include:

- Location Information
- Device Info
- Called list
- Callers list
- Text Message Inbox
- Text Message Outbox
- Contacts
- Bluetooth Name and MAC ID
- User Information

	Recent Destination	BIF File	Setting File	Called File	Calls File	Inbox File	Outbox File
TomTom One Regional	Y	Y	N	N	N	N	N
TomTom One Europe	Y	Y	N	N	N	N	N
TomTom Go 510	Y	Y	Y	Y	Y	Y	Y
TomTom Go 710/720/730/750/790	Y	Y	Y	Y	Y	Y	Y
TomTom Go 910/920/930	Y	Y	Y	Y	Y	Y	Y
TomTom Navigator 6	Y	Y	N	N	N	N	N

All TomTom models will have a locations file which may contain the location the user set as home, a list of any recent destinations and possibly last journey data. It will also have a device information file which contains the device serial number, model number, software version and other general information about the device. Higher end TomTom models like the GO series can act as a hands free device for mobile phones and may contain call data, text messages, contacts and a list of paired phones by their MAC address.

Data Acquisition: Data acquisition can be achieved thru different methods depending on the TomTom model. This is specifically related to whether the device has internal memory or stores its data on a removable SD card.

In the cases of devices that use SD cards, the card can be removed and processed like any other removable media. A forensically sound copy of the SD cards should be made and used to analyze the data. *An important note*, TomTom devices do not support the write protection option built into SD cards and regardless of the write protection tab setting (located on the left of the SD card if looking at the top) will write data to the card.

In the cases of devices that have internal memory, the devices will appear in Windows under "My Computer" when plugged in via USB as a removable storage device with the label "TomTom". Once visible in 'My Computer', it is possible to open the TomTom directory and copy the contents. A more sound approach, than 'clicking and dragging' the files to the desktop, would be to acquire an image of the device and work from that disk image. AccessData's FTK Imager is available from their [support website](#) and will acquire devices without a license. FTK 1.80 will parse up to five thousand files without a license

dongle and is sufficient for devices with 2gb hard drives or less. FTK or Encase will make it easier to decode and view the files.

Note, when powering on the unit to acquire data, if the device establishes a lock from the GPS satellites the device will overwrite the Last GPS Fix information in the CurrentLocation.dat file with its present location. A faraday bag can be used to prevent this from happening or examining the device inside a building away from windows can accomplish the same thing.

Target Files: Once the data has been acquired the following files are good sources of information.

- ***.cfg** - contains locations. The file name depends on the model but is generally 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) and any user information.
- **Called.txt** - Name called (if in phonebook), Number called
- **Callers.txt** - Name of caller (if in phonebook), Number of caller
- **Inbox.txt** – Name, Number, Message, Date & time
- **Outbox.txt** – Name, Number, Message
- **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.

Data Analysis: TomTom devices can store information relate to the owner's home address and a list of their 'Favorite' locations. If a user selects to navigate to either their Home, a Favorite or an address entered as a destination then this information is stored in the 'recent destination' file that ends with a .cfg extension.

.cfg files contain:

- Home location
- Favorites
- Manually entered addresses
- Details of Last Journey (if entered)
- Last GPS Fix of the device

For each of the locations a Latitude and Longitude is stored along with both an automatically assigned name and a user editable name and a house number. It also stores how the user chose to navigate to the address (entering the latitude and longitude, selecting it from the favorites list, etc...).

TomTom devices can be paired to a mobile phone and used as a handsfree device. If this has happened it is possible to recover information that would normally be found in a mobile phone. These files are text files and can be viewed with any text editor.

'Contacts' folder contains: (earlier versions have these files in the root folder)

- The contacts list from the mobile phone previously connected
- A list of numbers called
- A list of calls received
- Sent/Received SMS messages

Unallocated Space - Useful information can be found in the deleted space on a TomTom. If the user has 'reset' their device then no live information will be available but the unallocated space will contain the information that was present before the reset. Also in the deleted space will be records of previous journeys plotted and potentially the actual GPS position of the device when the journey was plotted and its last GPS fix for that journey.

Last Journey - When a journey is plotted using a TomTom it takes the current GPS position of the device as the start point of the journey. Until the destination is reached the TomTom stores both the Origin and the Destination. If a wrong turn is taken in the journey the TomTom will initially attempt to make the user turn around or will try to steer the user back on to the route. If this fails then the TomTom will be forced to re-plan the journey. If this happens then the TomTom will again take the current GPS position as the origin, leaving the destination the same. When examined, the Last Journey Origin will be a place where the TomTom has been but it may not be the place the entire journey started from.

Last GPS Fix – A TomTom device always records where it is when it has a GPS fix, this is the 'Last GPS Fix' It may be in mid journey if the TomTom was turned off mid journey or it may be a place where the TomTom has been turned on since. Like the 'Last Journey Origin', this is a place where the TomTom has been. The last GPS fix can be found in the *CurrentLocation.dat* file and is only available on newer TomTom device. Older models may store the information in the .cfg file.

Triplog Files - TomTom devices collect anonymous usage data from users who allow it. If a user enables this function while setting up the device, in the device file system there will be a folder titled 'statdata' containing files titled 'triplog-yyyy-mm-dd.dat'. These files are encrypted and there are no known tools that can read the contents.

Recommended Seizure Techniques: Like any other GPS device, TomTom devices are continuously collecting information and writing data to memory whenever they are powered on. When you seize a device, power the unit off and do not turn it on until you are ready to examine it. When you are ready to examine the device you should be inside away from windows so the device does not have a clear view of the sky. A faraday bag can be used to ensure that the TomTom cannot establish a lock from the GPS satellites. If it establishes a satellite lock, the device will overwrite the Last GPS Fix information in the *CurrentLocation.dat* file.

Until the latest software update, App 8.0.10, released in the July/August 2008 timeframe, turning a TomTom device off that is protected by a pin code would not prevent you from accessing the device with a computer. App 8.0.10 has "fixed" that issue and requires the pin code to be entered before the device will go into disk mode.

Tools Available: Currently the best tool available for examining TomTom devices is TomTology. It was developed by two computer crimes investigators from the UK. It is a forensic tool used exclusively for examining TomTom devices and provides users with the capability to; Decode live data (Home Location, Favorites, Recent Destinations, Last Journey Start and End Point, Stored Phonebook, Called Phone Numbers, and Received Phone Numbers), automatically retrieve deleted journeys from unallocated

space, locate deleted phone numbers, export all or selected locations to Google Earth, and produce detailed HTML reports. TomTology will automatically perform a full analysis of a TomTom including unallocated space and can extract data from a disk image created by FTK or EnCase.

There is also a separate EnCase Enscript available to parse files from an image file using EnCase. Email us for information and to request a copy at info@gpsforensics.org.

Definitions:

ENTERED LOCATIONS - These locations have been entered into the TomTom, either as a Home, a Favorite, a Destination or a Point of Interest. They appear at the top of the list when a user chooses to navigate to a new address.

FAVORITES - It is possible for a user to enter a number of addresses or places into their TomTom and save them as a Favorite. It is then possible for a user to quickly access these places to navigate to them.

HOME LOCATION - The Home Location is the address or place that has been entered by a user into the TomTom as the location of their home.

LAST GPS FIX - The TomTom keeps track of where it is. It may be along a journey if one is in progress or just where the device was when it was last turned on.

LAST JOURNEY INFORMATION - TomTom devices can save the details of the last journey. The last journey Origin is the actual position of the TomTom unit. It does not always mean that this is the start of the journey. If the user takes a wrong turn and the TomTom has to recalculate the route it places this point as the Origin of the last journey. It can be said that the TomTom device has physically been at this location.

NAVIGATED BY - How the user selected the location is stored in the TomTom. When a user selects to navigate to a destination they can do so by selecting to navigate to:

- Home
- Favorite
- Recent Destination
- Postal Code
- Entering the address manually
- Selecting the point off a map
- Point of Interest
- Entering the Latitude and Longitude
- Selecting to go to a city centre

ORPHANED LOCATIONS – Orphaned Locations are those addresses found in the deleted space that are no longer part of a file or the header of the file has been overwritten. Because they are no longer part of a file all of the information may not be available. It may not be possible to say what type of entry they are, only that they are present upon the device.

RECENT DESTINATIONS - Recent Destinations are places that the user of the TomTom has selected to navigate to. It does not mean that they have been there, only that the address has been entered.