Forensic Analysis of the TomTom Navigation Application

Nhien-An Le-Khac, Mark Roeloffs, Tahar Kechadi

Chapter 18

FORENSIC ANALYSIS OF THE TOMTOM NAVIGATION APPLICATION

Nhien-An Le-Khac, Mark Roeloffs and Tahar Kechadi

Abstract Exactly where an individual has been is important when attempting to forensically reconstruct an incident. With the advent of portable navigation systems and mobile phones, information about where a person has been is recorded more comprehensively than ever before. This paper focuses on the data recorded by the Android TomTom Navigation Application. It also describes how mobile device usage data can assist a digital forensic practitioner in determining where the device has been.

Keywords: Forensic acquisition, TomTom, GPS devices, smartphones

1. Introduction

Devices equipped with Global Positioning System (GPS) navigation capabilities assist motorists, pilots and sailors in determining their geographical locations and provide information such as maps, directions, alternative routes and their status, and the locations of amenities (e.g., food and fuel). Because these devices store historic navigation data, the acquisition and analysis of forensic evidence from the devices is of great interest. One of the market leaders in the domain of personal GPS navigation systems is the TomTom Portable Navigation Device (TomTom PND).

Smartphones are used for all kinds of activities, from placing calls to browsing on the Internet and playing games. But more important is the fact that users carry their smartphones wherever they go [2]. Smartphones often incorporate an embedded GPS chip. From a forensic perspective, this feature is very important because it is possible to know the geographical location of the device at any given time. However, a large number of diverse mobile device applications are available, each of which stores relevant data in proprietary formats. The primary chal-

lenge in mobile device forensics is to extract and analyze data from these applications.

Android is currently the most widely used smartphone platform in the United States [4]. One of the most popular navigation applications on Android devices is the TomTom Navigation Application (TomTom NA). It was launched in October 2012 and has been downloaded thousands of times. The application stores multiple geographical points and time-stamps during navigation, making any device that uses the application very valuable in an investigation.

This paper focuses on the forensic acquisition and analysis of navigation data from the TomTom NA. A step-by-step procedure for retrieving forensic data from TomTom NA is described. Multiple driving tests with a Samsung Galaxy S3 (GT-i9300) mobile phone were conducted to locate and decode the significant files. These files contain information about favorite locations, addresses and routes. The paper also compares the data that is available in a TomTom PND and a TomTom NA.

2. Related Work

The vast majority of TomTom device research has focused on the TomTom PND. Analysis of a TomTom PND requires the device to be rooted in order to copy the data [6]. The process described by Nutter [8] extracts a physical image to retrieve the most important files, which are subsequently decoded. The retrieved files include a settings file and data residing in unallocated clusters [8]. The commercial tool TomTology [5] can decode images extracted from the first generation of TomTom PNDs, but not later generations of the device.

Research related to Android mobile phone forensics (see, e.g., [1, 7]) has not considered the TomTom NA. To our knowledge, this is the first effort to focus on the TomTom NA used in Android smartphones.

3. Methodology

Documenting the navigation data available from the TomTom NA involves three steps: (i) physical image extraction; (ii) file identification; and (iii) file decoding and analysis.

Most of the data collection was performed by planning routes, entering favorites, changing the home location, etc. in the town of Gouda, The Netherlands. Two routes in the vicinity of Gouda, approximately 3 km each, were driven while using the TomTom NA.

Physical image extraction used the UFED Physical Analyzer [3]. This tool was chosen over manual bootloader methods because of their complexity and the fact that different devices require different methods.

3.1 Identifying Important Files

The files found in a mobile device are not all forensically useful, so the crucial task is to identify the files of interest. The favorite location data, address and location files were identified by comparing the images before and after entering the test data for altered files; the important files identified by the comparison procedure were designated for extraction using a forensic tool. Because many changes occur throughout the system, it was easiest to perform the comparison of mobile phone filesystems. The process of searching for important files involved three steps: (i) loading the physical image into software (e.g., UFED Physical Analyzer) that decodes the filesystem; (ii) searching for the TomTom folder using the string "tomtom;" and (iii) examining the files in the TomTom folder to identify the altered files.

3.2 File Decoding

The identified files were decoded and analyzed to determine how the data is stored within the files. Because the information is stored in the XML format, useful metadata is also present [10]. Scripts were written to decode the files and extract the relevant information. The outputs of the scripts were presented in the form of tables to help interpret the recovered data.

4. Results

The TomTom NA stores most of the relevant data in base64 strings in XML files. Because of the base64 encoding, each of the strings must be decoded to become readable.

The TomTom NA also uses a consistent location data structure to identify the places of interest to a user. The location data structure includes the following components:

- **Location_UserName:** The name given (by a user) to a location (not applicable if it is an address).
- **Location_UserPos:** The position of the location in a specified coordinate system (usually decimal degrees). This is the point that the user enters into the device.
- **Location_LocName:** In the case of a street address, the street name is saved in this field. If the location is a city, the city name is stored in this field.
- **Location_LocType:** The type of the location. The following types have been identified:

  - LOCTYP_MAPTICK: Navigated to a "Point on Map" or to a "Latitude-Longitude."
  - LOCTYP_ADDRESS: Navigated to an "Address" or "Contact."
  - LOCTYP_HOME: Navigated to "Home."
  - LOCTYP_POI: Navigated to a "Point of Interest."
  - LOCTYP_undefined: No defined location.
  - LOCTYP_FAVOURITE: Navigated to a "Favorite."
  - LOCTYP_GPS: The current GPS location. If this is in a route stream, it is also the last known position. The current GPS position may be incorrect if there was no GPS coverage (in which case, the last known GPS location is stored).

- **Location_CityName:** The city associated with the location.
- **HouseNumber_Number:** The house number associated with the address.

There is no option to see if a location was visited, unless the Location_LocType is LOCTYP_GPS, in which case, the location was visited at some point in time. The relevant files and data identified include settings, favorite locations and searches, and recent destinations.

4.1 NavkitSettings.xml

The `NavkitSettings.xml` file contains the home locations and a range of settings.

- **UP_HomeLocations:** This item stores the home locations. The TomTom application can store multiple numbered home locations. The location with the highest number is the current home location.
- **TTPlusManager:** This item contains all the paid subscriptions activated in the TomTom application. Some of these subscriptions are for Mobile HD traffic, TomTom Places, Free POIs, Free Maps and Free Voices. The start and end times are stored with each subscription. The TTPlusManager data type has entries for the username, password, ConnectionData_LastValidTime, ConnectionData _LastConnectionTime and AccountInfo_DatelastUpdate. The times for ConnectionData_LastValidTime, ConnectionData _LastConnectionTime and AccountInfo_DatelastUpdate are off by one month and one day. Repeated observations indicated that the

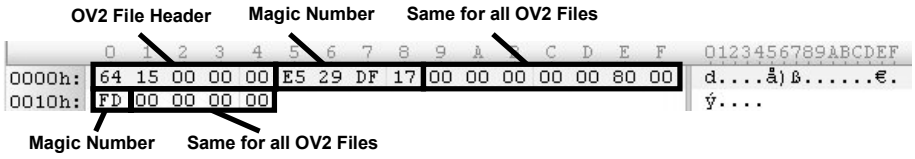

Figure 1. OV2 file header.

date on the TomTom servers is off by one month. The time is correct and is in Greenwich Mean Time (GMT).

- **LastDockedPositionX, LastDockedPositionY, LastDocked Time:** These three items reference the last docked location. LastDockedPositionX and LastDockedPositionY contain the longitude and latitude of the last docked position in the location format. The time is stored differently from the other time records (i.e., minutes instead of seconds). Therefore, decoding requires the time to be multiplied by 60 to convert it to the time format used elsewhere in the application.

- **MapUpdateLastReminderDate,LastMapShareConnection Reminder, LMGDisplayDate, LastMapShareSubscription Reminder, LastTimeTempBTEnabled:** These items correspond to static dates and times. We were unable to alter the values.

- **UserTimeOffset:** This item stores the offset (in seconds) of the clock in the mobile device. For example, when the time offset is GMT +2 (summer time in The Netherlands), the value of the variable is 7,259. Dividing the value by 3,600 results in a value of approximately 2, which corresponds to the GMT offset.

- **ArrivalTime:** During testing, it was not possible to change the value of this item, which remained fixed at 86,401. We concluded that the value is not changed by the application.

- **LocalSearchService:** This item contains the local search history. A search term that is used multiple times is stored only once.

4.2 Favorites

The favorites are stored in the `Favorites.ov2` file. The OV2 file also appears in TomTom PNDs and the format is documented in the TomTom API [9]. Figure 1 shows the header of an OV2 file. The first five bytes are the OV2 file header. The next four bytes at offset `0x10`

are magic numbers specific to OV2 files, which are different for different Android devices. The bytes located between `0x09` and `0x0F` are the same for all OV2 files.

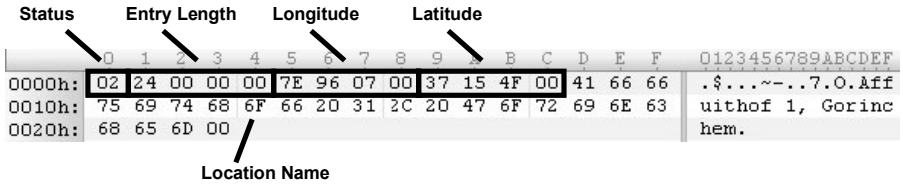

Figure 2. OV2 Favorite entry.

Figure 2 shows an example Favorite entry. The first byte is a status byte, which indicates that the entry is a current favorite. The next four bytes denote the length of the entry (in this case, `0x35`). The next eight bytes hold the longitude and latitude of the location. The user string is the last part on the entry, which is a null-terminated ASCII string. Note that the home location is not stored as a favorite.

4.3 Benelux_XXXXXXXX.xml

The `Benelux_XXXXXXXX.xml` file contains a large number of relevant fields. The `XXXXXXXX` in the Benelux filename is a number that is specific to a particular mobile device model. Each mobile device model is assigned a number (not necessarily unique). For example, a Samsung Galaxy S3 smartphone has the file `Benelux_AF7DE92B.xml`.

The most relevant portion of the `Benelux_XXXXXXXX.xml` file is the data immediately preceding the final `</string>` tag. The XML items in this file include: EngineRecents; AddressRecents; NeverAskedDefaultCountry; SafetyCameraWarnings; LastSelectedPoi; PoiSet; RouteStream; LastSelectedSearchItem; LastKnownTrueGpsPosX; LastKnownTrueGpsPosY; PDKAutoShutdown; PDKDisableiPodMenuIcon; RegularRouteLocHome; RegularRouteLocWork; LastSelectedPoiData; PDKUseDefaultSettingsFromUserFile; TrafficOnMap; SoundVolumeHandsFree; TrafficAutoUpdate; TrafficAutoReplan; TaiwanCenterAvailable; CurrentTrafficRouteType; PoiWarnings; GeoFormat; CurrentSelectedCountryIndex; TrafficUpdateFrequency; UserEnabledTraffic; PoicatHotlistCat; SupportASN; ValidPassword; PoicatHotListValidatedOnce; PoicatHotlistHit; UserMarkerAvailable; TrafficWarnings; EnableBT.

The most relevant items from the forensic point of view are:

- **EngineRecents:** This item stores the recently visited locations in the location format. The locations include addresses, points of interest (POIs) and particular points on a map.
- **AddressRecents:** While EngineRecents stores all the locations, AddressRecents only stores the locations that are addresses.
- **RouteStream:** This item stores the departure location data, the destination location data and the departure time. If the device has a GPS lock, the departure location is the current GPS location. If not, the last known location is stored. The departure time is dependent on the clock of the device, not the GPS time. Therefore, if the time on the device is set incorrectly, the departure time is also incorrect.
- **LastSelectedPoi:** This item stores the last selected location (or POI) in the location format.
- **LastSelectedSearchItem:** The TomTom application has an option to perform a local search. The TomTom local search looks for the closest location of interest near the current location. For example, a user who wishes to find a retail store would enter the name of the store and TomTom would attempt to locate the closest stores using an Internet connection. In the local search screen, the last selected search item can be seen; this item is stored in LastSelectedSearchItem. The sub-data types are the same as for the EngineRecents data type.
- **RegularRouteLocHome/Work:** During the research, this item was observed not to store any data. However, the name suggests that it stores a regular route to help the user plan a trip. The item could, perhaps, be used by the user to see the amount of traffic on a home/work route.
- **LastKnownTrueGpsPosX/PosY:** These items store the last known GPS position. The GPS time is not stored.
- **LastSelectedPoiData:** This item stores the location of the last selected POI. An inconsistency regarding the stored data is that the GPS location must be halved in order to match the GPS location format used elsewhere in the application.

4.4 Voices

The TomTom Android program includes a VoiceProvidersDatabase that contains the locations of the available audio voice files. The audio

voice files, which give directions to the user, are stored in an external micro SD card when available or in the internal storage of the device. If the user storage area is not large enough, the application will not work. The voice files and map chart material are downloaded and stored the first time that the program starts. The voices feature was not investigated further because no changes were observed between routes.

4.5 Times and Dates

The TomTom PND stores little time/date information with GPS coordinates. The most interesting temporal information in a TomTom PND is the triplog data, which contains the routes that were driven, along with their dates and times. It is essentially a breadcrumb trail along which the TomTom PND was driven. The TomTom NA does not contain a triplog; thus, this highly relevant information is not available.

The only TomTom NA location-specific temporal information that is available is found in the last docked locations time and the departure time. Unfortunately, these time/date items are set by the mobile device and could be incorrect. Also in the case of the departure time, if the data type is LOCTYP_GPS, it could be wrong if there was no GPS lock at that location. In short, limited time/date data is available, making it difficult to identify where a mobile device was at a certain point in time.

5. TomTom PND versus TomTom NA

The TomTom Go 720 and TomTom Via 825 Live devices were chosen for comparison. The Go 720 is a first generation TomTom PND system. The relevant data is stored in the `mapsettings.cfg` file, which can be decoded by the TomTology program.

The Via 825 Live is a second generation TomTom PND. It is no longer possible to get a physical image of this device using a USB connection. Data extraction requires the chip to be removed or a proprietary non-destructive method to be used. The relevant data is stored in the `mapsettings.tlv` file, but other files also store data related to the data found in the first series of TomTom PNDs.

Table 1 shows the corresponding locations in TomTom PND and TomTom NA where user data of interest in forensic investigations is stored.

6. Conclusions

The analysis of the Android TomTom NA on a Samsung Galaxy S3 smartphone provides important details about potential digital evidence. Files that contain location information for the device were identified by comparing filesystem changes between multiple physical captures.

Table 1. Corresponding TomTom PND and TomTom NA data locations.

Items	**First Generation**	**Second Generation**	**Android Application**
Triplogs	*Statdata* folder	*Statdata* folder	N/A
Home Location	`mapsettings.cfg`	`userpatch.dat`	`NavkitSettings.xml`
Favorites	`mapsettings.cfg`	`Favorites.ov2`	`Favorites.ov2`
Recent Destinations	`mapsettings.cfg`	`mapsettings.tlv`	`Benelux` file
Entered locations	`mapsettings.cfg`	`mapsettings.tlv`	`Benelux` file
Journeys	`mapsettings.cfg`	`mapsettings.tlv`	`Benelux` file with departure time
Last Docked	`mapsettings.cfg`	`Userpatch.dat`	`NavkitSettings.xml` with a timestamp
Bluetooth Coupled Devices	`mapsettings.cfg`	`Settings.tlv`	Handled by the Android OS
SIM Card Data	N/A	`mobility.sim`	Handled by the Android OS

Another important contribution is the comparison of the contents of files residing in a TomTom PND and a TomTom NA. A TomTom PND stores data in a binary format while the TomTom NA uses the XML format and the base64 encoding. The TomTom PND and TomTom NA record similar user favorites and search data, which enable digital forensic practitioners to determine where the devices have been.

Future research on the TomTom NA will focus on subscription services. Some of these services, including TomTom HD traffic and the services that provide information about speed cameras and danger zones, can provide detailed information about the geographical locations visited and routes taken, and may also reveal information about user actions (e.g., speeding). Future research will also focus on TomTom NA running on other smartphones models and on recovering deleted data.

References

[1] L. Aouad, T. Kechadi, J. Trentesaux and N. Le-Khac, An open framework for smartphone evidence acquisition, in *Advances in Digital Forensics VIII*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 159–166, 2012.

[2] L. Barkhuus and V. Polichar, Empowerment through seamfulness: Smartphones in everyday life, *Personal and Ubiquitous Computing*, vol. 15(6), pp. 629–639, 2011.

[3] Cellebrite, UFED Touch Ultimate, Petah Tikva, Israel (www.cellebrite.com/mobile-forensics/products/standalone/ufed-touch-ultimate).

[4] comScore, comScore reports March 2013 U.S. smartphone subscriber market share, Reston, Virginia (www.comscore.com/Insights/Press_Releases/2013/5/comScore_Reports_March_2013_US_Smartphone_Subscriber_Market_Share), May 3, 2013.

[5] Forensic Navigation, TomTology2, Bromley, United Kingdom (www.forensicnavigation.com/index.php/products/tomtology2).

[6] P. Hannay, A methodology for the forensic acquisition of the TomTom One Satellite Navigation System – A research in progress, presented at the *Fifth Australian Digital Forensics Conference*, 2007.

[7] J. Harkness, An Investigation of Mobile Phone Forensics, M.Sc. Thesis, School of Computer Science and Informatics, University College Dublin, Dublin, Ireland, 2011.

[8] B. Nutter, Pinpointing TomTom location records: A forensic analysis, *Digital Investigation*, vol. 5(1-2), pp. 10–18, 2008.

[9] TomTom, TomTom Navigator SDK (version 3.0, build 193), Amsterdam, The Netherlands (www.tomtom.com/lib/doc/ttnavsdk3_manual.pdf), 2004.

[10] World Wide Web Consortium, Extensible Markup Language (XML), Massachusetts Institute of Technology, Cambridge, Massachusetts (www.w3.org/XML).