Digital Investigation 16 (2016) 29–37

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Forensic analysis of newer TomTom devices

Jens Elstner [a], Mark Roeloffs [b, *]

[a] Bundeskriminalamt, Thaerstrasse 11, 65193 Wiesbaden, Germany
[b] Netherlands Forensic Institute, Department of Digital Technology and Biometry, P.O. Box 24044, 2490 AA The Hague, Netherlands

ARTICLE INFO

Article history:
Received 30 October 2015
Received in revised form 22 January 2016
Accepted 28 January 2016
Available online 24 February 2016

Keywords:
Forensic
Memory acquisition
Memory analysis
Navigation system
GPS
TomTom
ISP

ABSTRACT

Today many investigations involve TomTom devices due to the wide-spread use of these navigation systems. The process of acquiring a memory dump from the first generation of TomTom devices was relatively easy by utilising the USB-connection and standard forensic tools. Newer devices, however, do not provide this or any other readily available data connection, making the task much more complex. In addition to existing and relatively complex chip-extraction procedures, an easier data acquisition method was developed without the need to de-solder flash memory chips. The presence of new files and the differences in data formats found in these devices meant that new methods of data analysis and decoding also needed to be developed.

Introduction

For the first generation of TomTom devices, the investigation was quite straightforward as described in Nutter (in press). These TomTom navigation systems can be coupled to a PC by connecting a USB cable to the mini USB port. These devices appear as a mass storage device and a memory dump can simply be extracted using forensic software. When the second generation of devices came onto the market, mass storage was no longer offered. Instead these devices incorporated a proprietary connector or a micro USB-connector.

While it is still possible to execute a chip extraction (or chip-off) which is described in Breeuwsma et al. (2007), this method is very time consuming and can lead to damaged devices. Therefore another method had to be developed to extract a memory dump from the second and third generation of TomTom navigation systems.

During the research, three hardware generations could be distinguished. The three hardware versions and their differences are discussed in Section TomTom hardware generations.

Due to the fact that mass storage was no longer an option for acquiring data, another method had to be developed. The different methods are explained in Section Making memory dumps.

Decoding of the extracted memory dumps, together with the analysis of the storage format, are described in Section Decoding.

Previous work

The first generation TomTom devices were thoroughly examined by Nutter (in press), whereby the different file types were identified and decoded. The volatile RAM memory of these devices has also been examined, as described in van Eijk and Roeloffs (2010). Although not a great deal of data was found in the volatile memory, at least there was a general method for the extraction of the contents of the RAM. File system data may also contain relevant information as shown in Minnaard (2014).

* Corresponding author.
E-mail addresses: Jens.Elstner@bka.bund.de (J. Elstner), m.roeloffs@holmes.nl (M. Roeloffs).

http://dx.doi.org/10.1016/j.diin.2016.01.016
1742-2876/© 2016 Elsevier Ltd. All rights reserved.

Breeuwsma et al. (2007) describes a method of achieving a memory dump from an embedded device by executing a chip-off. Methods to analyse embedded systems are described in van der Knijff (2010). The de-soldering method is described as the most generic acquisition method.

Besides the TomTom hand-held devices, there are other embedded systems with built in eMMC flash memory chips, such as Smart-TVs. In the paper Boztas et al. (2015), multiple methods of extracting a memory dump from these Smart-TVs were discussed.

In addition to their hand-held devices, TomTom also provides smart phone applications for Apple and Android (TomTom, 2015). Research on an older version of a TomTom application on Android smart phones has been published in Le-Khac et al. (2014). In this paper, the focus will be solely on the TomTom hand-held systems.

At the present time, there is one commercial company that sells a complete solution for performing a memory dump using an ISP (In System Programming) solution. With an ISP solution there is no need to de-solder a memory chip, as the method works by connecting a memory reader to the PCB (Printed Circuit Board) of the device and reading the memory. The hardware is called CODED (Chip On Data Extraction Device) and is coupled with a password-protected website, where all the relevant ISP points and methods for executing memory dumps are only made available to the customers of Forensic Navigation (2015a). The software TomTology2 (Forensic Navigation, 2015b), developed by the same company, is the first commercial software to decode images from the second and third generation TomTom devices.

TomTom hardware generations

During numerous investigations involving various TomTom navigation systems, three different device families could be distinguished. These three families are characterised in the paragraphs below.

First TomTom generation

According to Wikipedia (2015), the first generation of TomTom hand-held devices was sold from May 2004 with the launch of the Go. The first generation of TomTom devices are discussed by Nutter (in press). TomTom devices of this hardware generation are, for example, the GO series 3xx, 5xx, 630, 7xx, 9xx, ONE, XXL, XL and the first Rider version.

In order to perform a memory dump of these devices, a connection needs to be established with a USB cable to the mini USB port of the device. The PC then detects the device as a so-called mass storage device, and with forensic imaging software a memory dump can easily be extracted.

For these devices, the most interesting artefacts are stored in the following files:

- MapSettings.cfg: contains *home location, entered location, favorite* and *start of last calculated route*
- UserPatch.dat (not available in all first version devices): contains *last GPS fix* and *home location*

The method to process this first hardware version of TomToms has been extensively discussed (Nutter, in press) and needs no further research.

Second TomTom generation

The second generation of TomTom devices was sold from the end of 2010 with the launch of the Go 1000 Live (according to Wikipedia (2015)). TomTom devices of this hardware generation are, for example, the Start, Via, XL, ONE, 10xx, 15xx, Truck and the second Rider edition.

These devices incorporate a micro USB port, however when a connection is made by using a USB cable, the device is not shown as a mass storage device. Instead, it is possible to establish a TCP/IP connection over USB, a SSH server can be reached, and a private key for this server can be found in the TomTom PC software. However, until now no valid password has been ascertained and therefore it is not possible to authorise a connection to gain access.

A method for copying the memory content of these devices is described in Section Making memory dumps. The most interesting artefacts are stored in files in a different format than that of the first TomTom generation. The files are:

- mapsettings.tlv: contains *home location, entered location, entered via favorite* and *start of last calculated route*
- userpatch.dat: contains *home location* and *last GPS fix*
- favorites.ov2: contains *favorite*

Decoding of these files is described in Section Decoding.

Third TomTom generation

According to Wikipedia (2015), the third generation of TomTom devices appeared on the market with the launch of the Go 400. These devices deviate from the second generation in the utilised processor on the PCB, the user interface and the underlying software. TomTom devices of this generation are for example the GO 4x, 5x, 6x, 4xx, the new versions 5xx, 6xx, 5xxx, 6xxx, and the newest models of Truck and Rider.

The method of executing memory dumps of these devices is practically the same as that of the previous version with a small twist, as is described in Section Connecting eMMC interface on PCB.

The files with most interesting artefacts follow the same format as the previous generation, but are stored under a different name and in a different location within the file system:

- _internalstorage_data_ttcontent _common_installed_<Map Name>_.tlv or <Map Name>_MapSettings.tlv: contains *recent locations*, *home location* and *start of last calculated route*
- userpatch.dat: contains *home location* and *last GPS fix*
- favorites.ov2: contains *favorite*