

# EXPERIMENTAL TESTING OF A FORENSIC ANALYSIS METHOD ON THE TOMTOM GPS NAVIGATION DEVICE

Clara Maria Colombini



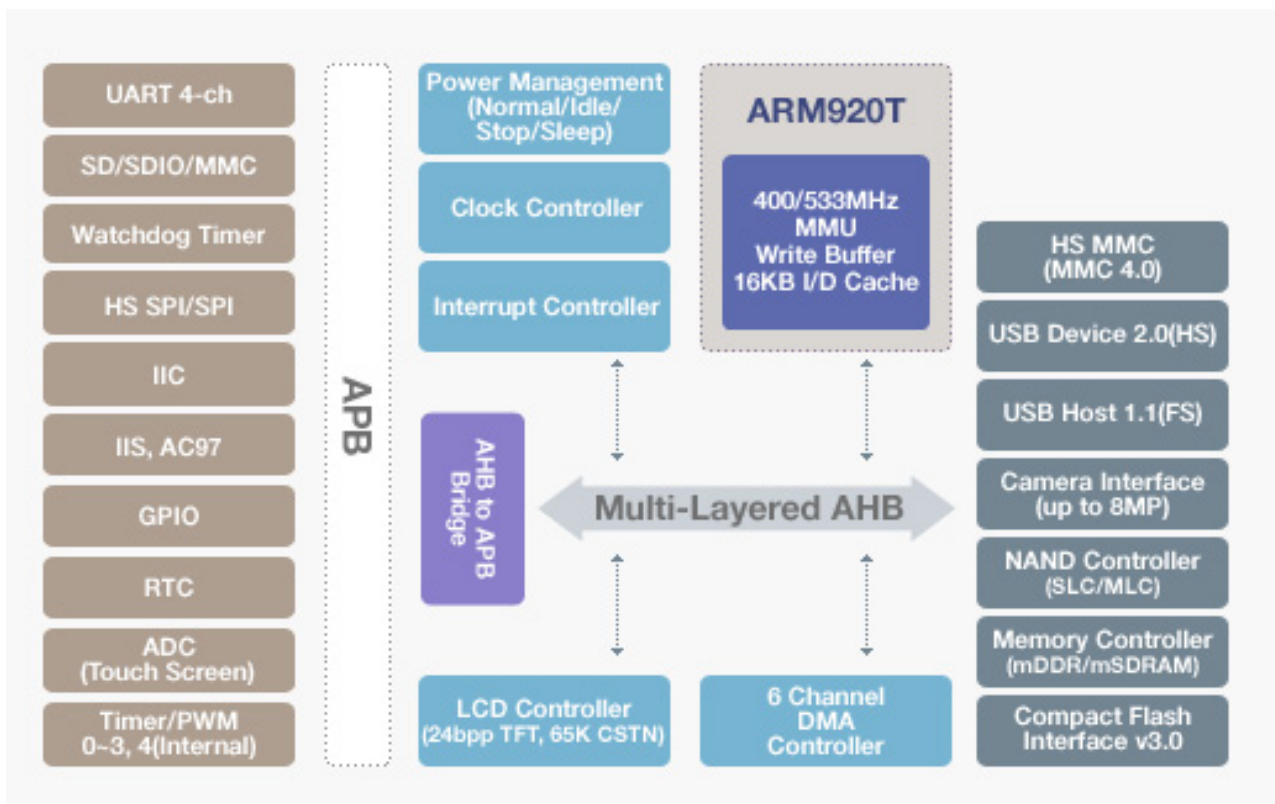
## INTRODUCTION

The earliest Satellite Navigation Systems were designed for the U.S. military, to locate the position of Polaris submarines. Over the years, satellite detection technology has become extremely widespread, and today most automotive vehicles are fitted with such systems.

TomTom, the in-car satellite navigation device, is connected with the U.S. NAVSTAR Global Positioning System (GPS), which utilises 32 satellites in Mid-Earth Orbit (MEO) positioned in six different orbital planes.

The TomTom device itself contains an ARM processor made by Samsung, using Linux to manage the software which – depending on the device – can read either an SD card or the internal memory. A bootloader in the computer searches the hard disk or SD card for the software and map data. It then transfers the software to the 64MB internal RAM memory and starts the software.

The hardware itself starts the GPS and the navigation application. The navigation application then reads whatever settings have been installed, such as the preferred voice and last chosen route.



TomTom internal architecture

The integrated GPS module ensures that the satellite signal translates into coordinates pinpointing the user's exact position on the map. After start-up, the GPS module calculates the user's position from the nearest satellite signals it receives; the module works out its position by calculating its distance from at least four different satellites, which send out information such as identity, altitude, position in relation to other satellites, etc.

The latest models feature RDS-TMC technology. The "Radio Data System-Traffic Message Channel" is a service providing real-time traffic information integrated in the device via a special receiver. The service provider encodes the message and sends it to FM radio transmitters which transmit it as a Radio Data System (RDS) signal alongside regular FM radio broadcasts. The TMC decoder inside the TomTom decodes the RDS signal into visual and/or spoken message on the device.

Bluetooth enabled models allow TomTom to communicate with other electronic devices like mobile phones, operate as a hands-free speakerphone, or receive information sent to a mobile phone via a wireless connection such as GPRS (General Packet Radio Service) or UMTS (Universal Mobile Telecommunications System).

This work presents research into a forensic analysis procedure on TomTom satellite navigation devices, which are able to detect extremely useful information for investigative purposes. Information such as stored addresses, itineraries, home, points of interest, etc. enable the device user's travels, favourite itineraries and most frequent destinations to be reconstructed.

The main focus of the experiment was to develop a procedure for creating a "repeatable" forensic image of the internal memory, so that an identical forensic image can be produced at any time and can be used for analysis or as exhibits.

## **DEVICES ANALYSED**

The following models were analysed:

1. TomTom One with 1GB internal memory only – 2006 model;
2. TomTom One with 2GB internal memory only – 2008 model;
3. TomTom One with external SD memory card only – 2006 model;
4. TomTom One XL Italy with 512MB internal memory + SD Card – 2008 model;
5. TomTom Go 730 with 1GB internal memory + SD Card – 2008 model.

## **CREATION OF THE FORENSIC IMAGE**

It should be noted that regarding the PC connection, the experiment did not consider the procedure for generating a forensic image of the SD memory card which can be removed from the device and can be treated like any other mass storage unit as per Computer Forensics rules.

The term “forensic image” as used herein refers to the result of a special copying procedure known as “bit by bit”, i.e. a system that scans the entire surface of the master hard drive one bit at a time, producing a clone, i.e. an identical copy, on a destination drive whose contents will be analysed.

Whenever possible, forensic analysis is not conducted on the original device but rather on its “clone”, or bitstream image, so as to preserve the integrity of the original evidence for any future analyses. Three forensic images were produced for each of the four models examined (one for each PC), for the following aims:

1. since there was no “original” image available, i.e. one that was “definitely unaltered” against which to compare the images produced using this experimental method, which would have required an invasive procedure physically parallel to the memory chip, the first image generated was used as the starting point, and any changes observed during the tests were checked against the other two;
2. three different PCs were used to simulate different scenarios (e.g. counter-reports, analyses at a later time, etc.).

In order to provide a sufficiently broad overview, forensic images were created using:

- Personal Computer running Windows OS;
- Personal Computer running Linux OS.

## PROCEDURE IN WINDOWS ENVIRONMENT

The procedure for creating the three forensic images was carried out on three different PCs:

1. PC workstation running Microsoft Windows XP PRO SP3;
2. PC notebook running Microsoft Windows Vista Home Edition;
3. Eee PC running Microsoft Windows XP Home Edition.

### Software:

Accessdata FTK Imager 2.55 (free download).

Please note that it was not possible to use the hardware write blocker provided (Tableau T8) since when connected the PC does not recognise the device ( TomTom → T8 → PC).

## PREPARING THE PC

The first step was to ensure that TomTomHOME software was not installed on the PC (for automatically updating TomTom data), or that the registry file did not contain keys or voice files from previous TomTom installations:

SOFTWARE registry file;

SYSTEM registry file: no entries relating to previous installations of TomTom USB drivers must be present in the CONTROL SET sub-key.....\ENUM\USBSTOR.

It is essential to carry out these checks because as soon as TomTom is connected to the PC it will try to update its data, searching for the software and registry keys signalled on the PC, and this will alter its files. Since no hardware write blockers can be used, the USB ports have been configured as read-only, creating a special registry entry to disable the write option command on the peripherals connected to the PC via the USB ports. The PC was disconnected from the Internet so as to prevent accidental attempts to update the device.

Regarding storage of the forensic images obtained, a new 50GB firewall was created on each of the three PCs, then wiped<sup>1</sup> and formatted in Fat32.

---

<sup>1</sup> Procedure for permanent deletion of files from memory card by overwriting with spurious data until all traces are eliminated.

## **CONNECTING THE DEVICE TO THE PC**

Material used: mini USB cable for TomTom

Environment: the analysis was conducted in a closed room to prevent the TomTom device from locating the satellite.

The most sensitive part of the whole experiment was connecting the device to the PC so that the operating system “recognises” the TomTom’s internal memory without modifying the data stored within the memory, including the relevant “metadata”, i.e. other data describing this information, such as dates of creation, modification and access, as well as size, etc..

The connection procedure varies from model to model: each model behaves differently depending on whether or not there is an SD Card slot.

The direct analysis of the model with the SD Card only was performed according to Computer Forensics rules.

The TomTom device has to be connected to the PC’s USB port and turned on, so in order to detect any changes to the data present when the drivers are installed, communication flows via USB between the TomTom and the PC were monitored throughout the connection procedure. The analysis was carried out using a specific tool, SysNucleus USB Trace v. 2.0.

## **MODELS WITHOUT SD CARD SLOT**

MODELS TESTED:

Tomtom One with 1GB internal memory only – 2006 model;

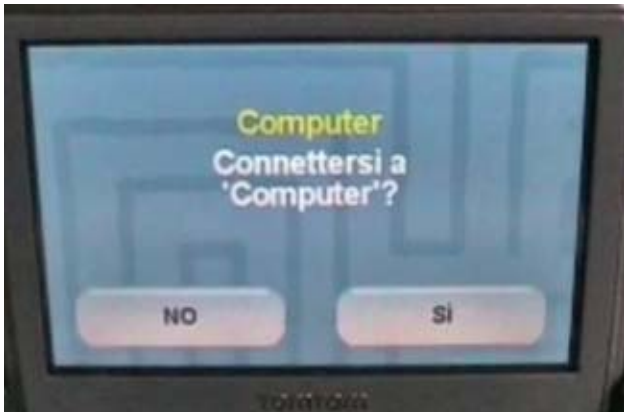
Tomtom One with 2GB internal memory only – 2008 model.

## **CONNECTION**

The PC is turned on and the operating system started up.

Monitoring is started on the data flow via USB on the port chosen for the connection.

Before turning the device on it is connected to the PC using the relevant cable. The TomTom is turned on. The screen illustrated below appears on the device:



Click on "YES". The image below will now appear on the screen, indicating that the connection has started.



Once the connection has started, the screen below appears.



The computer signals that it has found a new USB device, installs the drivers and assigns a disk drive letter to the new peripheral device.

The same procedure was used for the three different PCs used.

The analysis of the data produced by monitoring the communication flows via USB between the TomTom and PC during the connection and installation of the drivers of the devices evidenced that no changes were made to the data contained in the device.

## **CREATION OF THE IMAGE**

The forensic image was made on the three different test PCs using FTK Imager Accessdata v. 2.55, which calculates the Hash<sup>2</sup> MD5 and SHA1 both of the original<sup>3</sup> and the new image created, and verifies that it is an exact copy.

The new UBS peripheral is selected as the source and the DD image format (not processed) is chosen.

Destination unit: the ad hoc partition created on the PC.

The procedure is the same on all three PCs utilised.

## **RESULTS**

An examination of the Hash MD5 and SHA1<sup>4</sup> files, which are identical, confirms that the three images created for each of the 4 devices are exactly the same and there has been no change to the data in the flow that the TomTom generates when connected to a Windows system.

The comparison was made using MD5summer v. 1.2.0.11.

In any case, as noted above, it is always essential to turn on the device since our intention was to conduct a “non-invasive” analysis, without having to open the device and/or remove the internal memory.

---

<sup>2</sup> “Hash” means the hash calculated on a data flow determined after two intelligent systems (with CPU) have joined on a communications protocol.

<sup>3</sup> “Original” means not the original data stored on the device, but the original data flow leaving the device when it connects with a Windows system.

<sup>4</sup> Hash algorithms are a kind of “footprint”, that univocally distinguishes all electronic trace of the forensic analysis so as to comply with data integrity requirements. This “digital watermark” is produced by “one-way hashing” (e.g. MD5 and SHA1) which generates unmistakable reference to the original trace but does not allow it to be reconstructed. These algorithms are utilized internationally and ensure a satisfactory level of security/safety.

## MODELS WITH INTERNAL MEMORY + SD CARD PORT

### MODELS TESTED:

TomTom One XL Italy with 512MB internal memory + SD Card – 2008 model;

TomTom Go 730 with 1GB internal memory + SD Card – 2008 model.

Additional material used: pre-wiped SD memory card<sup>5</sup>.

## CONNECTION

If the TomTom device has an SD memory card slot, a preliminary operation is needed before connecting to create the forensic image, since there are two ways to connect this type of device to a PC.

- without an SD card inserted in the slot:

the device goes into “update” mode and looks for the TomTom Home software on the PC for automatically updating user data on the Internet. When it fails to find the software the device tries to install it (the device software includes a compact self-installing version TomTom Home). The PC recognises it as a navigation device and installs the data update drivers. In this mode, certain files on the device are automatically updated and therefore changed. This is confirmed by analysing the data produced by monitoring communication flows via USB between TomTom and PC, using the SysNucleus USB Trace v. 2.0 tool, during the connection of each device as described here.

- with SD Card inserted:

the device goes into “USB peripheral” mode and as such is recognised by the PC which installs only the USB connection drivers.

No communication is attempted to update the TomTom data and the TomTom Home software is not searched for on the PC, so the files stored within the device are not changed; the machine only reads the contents of the SD Card, which is assigned an external hard drive letter. An analysis of the information generated by monitoring communication flows via a USB between the TomTom and the PC, using SysNucleus USB Trace v. 2.0 during the

---

connection and installation of the device drivers, confirms that the data stored in the device has not been changed.

With the information thus acquired, a connection is made as described below, which turns out to be ideal for enabling the PC to detect the content of the internal memory.

After deleting all traces of the previously installed TomTom drivers from the PC, the device, still off, is connected to the PC via the mini-USB cable.

The new “forensic” SD Card is inserted (see above: additional material used).



The device is then turned on. The image below shows the TomTom screen during connection.



The TomTom screen shows that the device is connecting: the device is in USB mode and the PC views the content only of the SD Card, to which the operating system assigns an external hard drive letter. Once the USB connection drivers are installed, the device is switched off, the SD Card

removed and the device is switched on again. The TomTom screen again shows that the device is connecting.

The computer does not need to recognise the peripheral device again, as it already has the drivers, and views the data contained in the internal memory of the external hard drive previously assigned to the SD Card.

## **IMAGE CREATION**

At this point, the forensic image is created on the three different PCS, using FTK Imager by Accessdata v. 2.55 software.

The physical unit of the new UBS peripheral is selected as the source and the image is chosen in DD format (not processed). The destination drive is the partition created ad hoc on the PC.

The same procedure is run on the three different PCs.

## **RESULTS**

The Hash MD5 and SHA1<sup>6</sup> files are identical, confirming that the three images generated for each of the 4 devices are exactly the same; the data flow generated by the TomTom when connected to one of the Windows systems has remained unchanged.

The comparison was made using MD5summer v. 1.2.0.11.

In any case, as observed, the device always has to be switched on, since the analysis in question is “non invasive”, and as such does not require the device to be opened and or/ the internal memory removed.

---

<sup>6</sup> **Hash** algorithms are a kind of “footprint” univocally distinguishing the electronic trace of the forensic analysis, so as to preserve data integrity. The “digital watermark” is created via a one-way hashing operation, (e.g. MD5 and SHA1), which generates a “footprint” that refers exclusively to the original trace, but does not enable it to be reconstructed. These algorithms are used internationally and ensure a satisfactory level of security.

## RUNNING THE PROCEDURE UNDER LINUX

Again, the procedure was carried out on three different computers.

1. PC workstation with Linux Fedora v. 10 operating system;
2. PC notebook with Linux Helix v. 1.9 operating system, running live<sup>7</sup> from CD;
3. Eee PC with Linux NBCaine v. 0.5. operating system running live from USB device.

## CONNECTION

Under Linux, there was no need to adopt different connection procedures for the various models of the device.

Before switching the device on it is connected to the PC using the mini-USB cable. The device is then switched on.

The Linux operating system recognises the device as a USB memory peripheral.

It is not necessary to “mount”<sup>8</sup> the TomTom, which stays on *read-only*.

Instead, the image destination device is mounted and set to *read-write*.

## IMAGE CREATION

The forensic images are then created in “DD” format, using the software packages listed below:

1. Linux Fedora v. 10: command line procedure via console<sup>9</sup>;
2. CD Helix Live 3: ADEPTO 2.0;
3. USB NBCaine: AIR 1.2.8.

---

<sup>7</sup> **Live** mode allows an operating system downloaded directly to memory from a CD or USB flash drive to be used, without the need to rely on the hard disk(s) present on the machine.

<sup>8</sup> **Mounting** enables a block peripheral to be initialised to permit read/write access.

<sup>9</sup> **Console** mode is an alternative to graphics mode in which commands are facilitated by a graphical interface with buttons and windows. In consoled mode, commands must be written with no intermediation needed.

## COMMAND LINE PROCEDURE

The *mount* command is used to check that neither of the two drives (the source disk drive, i.e. the TomTom internal memory, or the partition chosen by us to store the image) has been automatically mounted, and then the partition destined to store the forensic image is mounted in *read-write*; the original disk is NOT mounted because the data is read directly from the device with the copy command.

```
# mount -o rw /dev/hdb4 /media/hdb4
```

Before copying, the destination device is wiped to delete any previously stored data. The following command can be used to complete the operation:

```
# wipe /media/hdb4
```

The original is hashed using the DD command, specifying only the input file and sending the output of this command in *pipe*<sup>10</sup> to an *md5sum* (execution of MD5 hash).

```
# dd if=/dev/hda1 | md5sum
```

The image is then created: the simplest form of the DD tool is used for the copy. The command syntax requires an input file and an output file to be specified.

```
# dd if=/dev/sdb1 of=/media/hdb4/tomtom01.img
```

At the end of the operation, the command returns the number of read and written records, with a few statistics on bytes copied, total operation time and average transfer rate of the process.

The image created using the DD command is hashed, specifying only the input file and sending the output of this command in *pipe*<sup>11</sup> to an *md5sum*.

```
# dd if=/media/hdb4/tomtom01.img | md5sum
```

---

<sup>10</sup> In UNIX the **pipe** is a mechanism for controlling information flows. In other words, the pipe is a system for using outgoing information flows from one command as input for another command.

## PROCEDURE VIA AIR (AUTOMATED IMAGE & RESTORE) TOOL

There are obviously pros and cons with using a command line tool; the main advantage is that there is total control over each individual instruction imparted, including the ability to directly specify which options and parameters to use for each device; conversely, the complexity of the commands and the different number of options may easily generate mistakes.

However, the Helix and Caine distributions overcome these difficulties with a series of graphical interface tools allowing the operator to exploit the usability of the window interfaces.

Below is the procedure made for creating forensic images using the AIR (Automated Image & Restore) tool, included in the Caine distribution.

First select the source device on the left hand side of the template, and the destination device on the right.

Next, select no image compression.

Then select the type of hash to use for verifying the identity of the original and the copy.

Here DCFLDD<sup>12</sup> is been selected instead of DD.

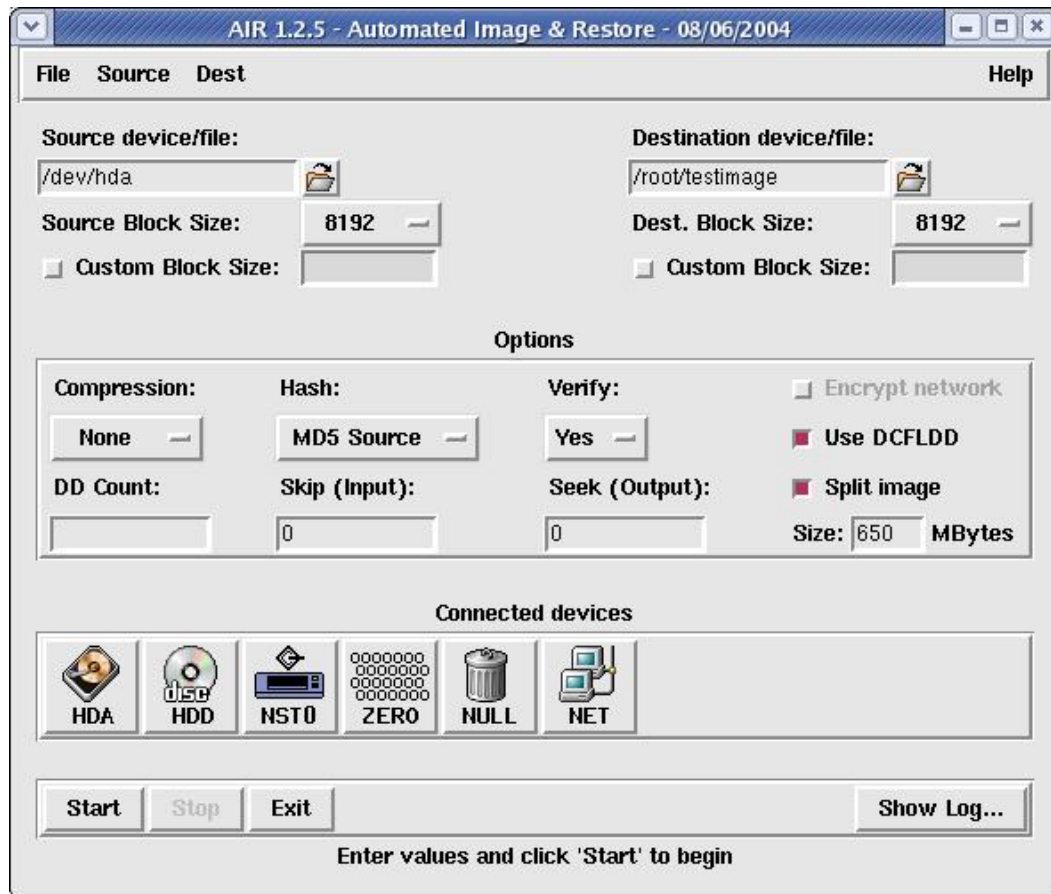
This option does not branch the image into different files and does not encrypt the file with a key.

Then check the *noerror* option on the *conv* parameter, which continues the image creation operation even in the event of read errors.

Before pressing the start button and beginning the copy process, click on the *show status windows* button to see how the operation is progressing.

---

<sup>12</sup> DCFLDD is used to perform certain operations; the advantage is that it calculates hashes concurrently with the creation of the copy, eliminating the extra step needed when using DD.



## RESULTS

An inspection of the Hash files, which are identical, confirms that the three images generated for each of the four devices are exactly the same and that there has been no change to the data they contain.

In any case, as observed, the device always has to be switched on, since the analysis in question is "non invasive", and as such does not require the device to be opened and or/ the internal memory removed.

## ANALYSIS

The memories on TomTom devices (both the internal memory and the SD Card) behave just like any other digital memory insofar as they can store, conceal and delete files of any kind.

The TomTom memory creates forensic images “bit by bit” so that all the data stored can be analysed; even deleted or fragmented data can be carved<sup>13</sup> out with the use of special forensic software.

The tool used to perform the analysis was AccessData FTK 2.2 running Windows; it can view the contents of all files present, including the relative meta-data, and recover deleted or fragmented files. However, for the purposes of an investigation seeking satellite navigation data using the device, only the relevant files are listed below.

<p>TTGO.BIF</p>	<p>Contains information concerning the device, including: model, serial number, language, current map, current base map, voice.</p> <p>Below is an example of file content from which this information can be gleaned.</p> <pre>[TomTomGo] DeviceName=TomTom ONE XL DeviceVersionHW=ONE XL DeviceSerialNumber=L26497J00167 DeviceUniqueID=AK8AG AADSW RamDiskVersion=20080529 BootLoaderVersion=53026 LinuxVersion=190943 ApplicationVersionVersionNumber=8010 ApplicationVersion=9369 UserLanguage=Italiano UserName=L26497J00167 LastConnectionTime=Never GPSFirmwareVersion= BuiltInColorScheme0=Belgica BuiltInColorScheme1=Brittanica BuiltInColorScheme2=America BuiltInColorScheme3=Germanica  BuiltInColorScheme4=Australia BuiltInColorScheme5=Deuteranopia BuiltInColorScheme6=Greys BuiltInColorScheme7=Antarctica BuiltInColorScheme8=Africa BuiltInColorScheme9=Astra CurrentColorSchemeBuiltIn=1 CurrentVoiceInfo=Roberto CurrentMap=Italia CurrentMapVersion=710.1571 CurrentHomeLocation=45.53052,9.03387,Via Francesco Daverio 11, Milano Traffic=N</pre>
-----------------	--

<sup>13</sup> Data **carving** is a technique for recovering deleted or de-allocated files.

	<p>CurrentFuelpricesType=  CurrentFuelpricesTypeString=  CurrentFuelpricesLastFullUpdate=  ValueRatio=BpHDxKhXmBZzHUCpsA==  Features=PlusDownloadDynamic,PlusDownloadGeneral,PlusDownloadMap,PlusDownloadPOI,PlusDownloadScheme,PlusDownloadUpgrade,PlusDownloadVoice,PlusDownloadRingTone,PlusMessageNotification,PlusPushChannel,PlusTraffic,PlusWeather,PlusEphemeris,PlusBuddies,PlusMobileSafetyCameras,PlusRoadConditions,PlusFixedSafetyCameras,PlusFuelPrices,HDTraffic,PlusOnlineCamera,PlusTripReporting,HomeBackup,PhotoJPGViewer,PhotoBMPViewer,Newyork,Newyork1Dot6,Itinerary,Caymann,Durham,PhoneFeatures,CarSymbol,RDSTMC,Prague,Bluetooth,SDSlot,InternalFlash  SupportedPatchTypes=1F  NrSupportedErrorTypes=132  UserPatchDatVersion=102  CompressedPatchVersion=150  MapServerPatchDatVersion=104  DeletedPoiDatVersion=200  ServerLineIndexDatVersion=102  ServerNameIndexDatVersion=102  MapShareSupportedProviders=203  CharacterSet=Latin-1</p>
CURRENTLOCATION.DAT	Contains the latest position of the device
CURRENTMAP.DAT	Contains the current map
GPRSSETTINGS.DAT	Contains the GPRS configuration (if present)
SETTINGS.DAT	Contains the name and MAC Address of any telephone connected, wireless settings, provider data, and user telephone data, if entered (GO models only)
GPRS.CONF	Contains the GPRS PIN number (if entered) (GO models only)
MAPSETTINGS.CFG	Files with a “CFG” extension, such as “mapsettings.cfg” or “name_map.cfg” are all contained in the folders of the relevant maps and contain all the information on “Favourites”, itineraries, addresses , and points of interest stored.
\CONTACTS\ CALLED.TXT	Contains telephone numbers called from the telephone connected to the TomTom (GO models only)
\CONTACTS\ CALLERS.TXT	Contains the telephone numbers that have called the telephone connected to the TomTom (GO models only)
\CONTACTS\ CONTACTS.TXT	Contains the contact list of the telephone connected to the TomTom (GO models only)
\CONTACTS\ INBOX.TXT	Contains text messages received from the telephone connected to the TomTom (GO models only)
\CONTACTS\ OUTBOX.TXT	Contains text messages sent from the telephone connected to the TomTom (GO models only)
NOMEFILE.ITI	Contains stored itineraries
TEMPORARY.ITI	Contains itineraries not stored with a filename

Depending on the model, certain files may be missing from the device.

This table reports some differences among different models.

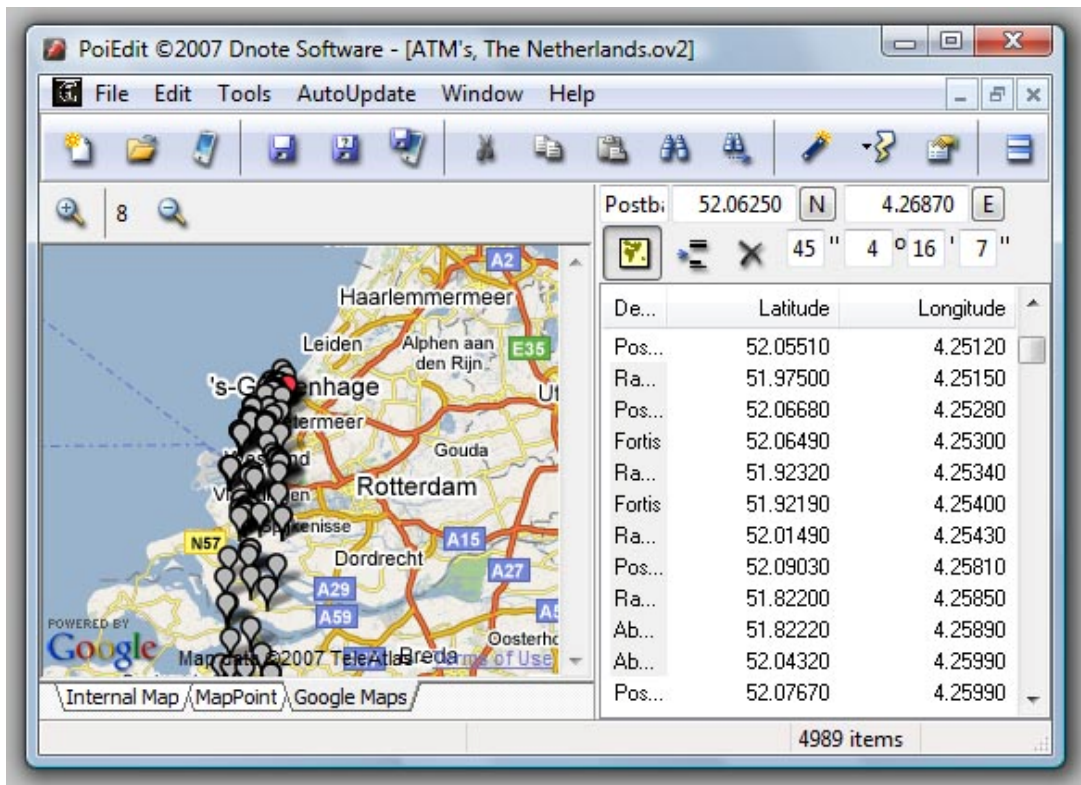
	RECENT DESTINATION	BIF FILE	SETTING FILE	CALLED FILE	CALLS FILE	INBOX FILE	OUTBOX FILE
TOMTOM ONE REGIONAL	YES	YES	NO	NO	NO	NO	NO
TOMTOM ONE EUROPE	YES	YES	NO	NO	NO	NO	NO
TOMTOM GO 510	YES	YES	YES	YES	YES	YES	YES
TOMTOM GO 710/720/730/750/790	YES	YES	YES	YES	YES	YES	YES
TOMTOM GO 910/920/930	YES	YES	YES	YES	YES	YES	YES
TOMTOM NAVIGATOR 6	YES	YES	NO	NO	NO	NO	NO

### SPECIFIC TOMTOM ANALYSIS SOFTWARE

There are various software packages on the market for analysing TomTom navigation files. POIedit is a shareware programme that runs under Windows, for reading DAT files.

It is interesting because it can identify and view the exact locations of addresses stored in the “mapsettings.cfg” file on GoogleMaps (an Internet connection is required).

The figure below pinpoints the geographic location of addresses contained in the “mapsettings.cfg” file.



## BIBLIOGRAPHY

1. C.M. Colombini, Y. Corio, *La corretta gestione di un incidente informatico e alcune ipotesi di linee guida per le operazioni di forensics. La Dead Analysis*. White Paper, Corso di Perfezionamento in Computer Forensics e Investigazioni Digitali, AA 2007/2008.
2. B. Nutter , *Pinpointing TomTom location records: A forensic analysis*. 2008 Elsevier Ltd.
3. Peter Hannay, *A Methodology for the forensic acquisition of the TomTom One satellite navigation System – A research in progress*, Edith Cowan University, 2007.
4. A.K. Theiss, DD.CC. Yen, C.Y. Ku, *Global positioning systems: an analysis of applications, current development and future implementations*. Computer Standards & Interfaces, 2005.
5. SEC.AU, Edith Cowan University
6. ACPO (2003). *Good Practice Guide for Computer based Electronic Evidence 3.0*. Retrieved 16 Oct, 2007.
7. P. Hannay, *A Methodology for the Forensic Acquisition of the TomTom One Satellite Navigation System–A Research in Progress*. Paper presented at the 5th Australian Digital Forensics Conference, 2007.
8. A. K. Theiss, D. C. Yen, & Ku, *Global Positioning Systems: an analysis of applications*. 2005.
9. <http://www.marcomattiucci.it>.
10. <http://ww.tomtom.com>
11. <http://www.GPSforensics.org>
12. <http://www.forensicswiki.org/wiki/GPS>
13. <http://www.symbian.com>
14. [http://www.samsung.com/global/business/semiconductor/productInfo.do?fmly\\_id=229&partnum=S3C2443](http://www.samsung.com/global/business/semiconductor/productInfo.do?fmly_id=229&partnum=S3C2443)
15. <http://www.maerco.it/index.php/2007/01/03/open-tom-tomtom-opensource/>
16. [http://www.opentom.org/Main\\_Page](http://www.opentom.org/Main_Page)

*A special thanks to the Major Marco Mattiucci, Commander of the RTI – Reparto Tecnologie Informatiche - RACIS Roma – Arma dei Carabinieri.*