

Forensic Acquisition and Analysis of the TomTom One Satellite Navigation Unit

Peter Hannay
SEC.AU, Edith Cowan University
p.hannay@ecu.edu.au

Abstract

Global Positioning Systems are becoming increasingly pervasive. The forensic acquisition and analysis of these units is of great interest as it has the potential to yield historic locational data for these units. Analysis of the TomTom one satellite navigation unit has resulted in a method to reliably extract historic data from these devices in a forensically sound manner.

Keywords

Global Positioning System, GPS, forensic methodology, digital forensics, GPS forensics, satellite navigation system, satnav, satnav forensics, TomTom, TomTom forensics.

INTRODUCTION

The first satellite navigation network became active in 1960. The network was known as TRANSIT and was used by US Navy Polaris submarines as a means of determining their current location (Parkinson, 1997). Since 1960 there have been a number of advances in satellite navigation technology as new networks are brought online and others shut down (Theiss, Yen, & Ku, 2005). The most commonly used satellite navigation systems at the moment are NAVSTAR and Glonass, operated by the United States and Russian governments respectively (Polischuk & Kozlov, 2002). Each new satellite navigation network has allowed for increased accuracy, the technology is now at the level where it can be used for automotive navigational assistance, these satellite navigation devices are becoming increasingly common, as such the need for a method of forensically analysing these devices is becoming more critical.

A method for the analysis of the TomTom range of satellite navigation devices has been developed. This method allows for historic locational data to be retrieved from a TomTom device, in a way that does not alter the contents of the device or internal storage and allows for historic locations to be retrieved and presented in a reliable manner. It is important that this information be able to be retrieved as it has the prospective to provide information about the location of vehicles at a given time, this historic locational information has great potential in assisting with criminal investigations.

DEVELOPMENT & METHODOLOGY

When developing a methodology for the forensic analysis of these devices, a number of needs were considered, firstly the need to determine what information could be recovered, the need to recover this information in a repeatable manner and the need to recover this information without altering any of the data on the device being analysed (HB171, 2003). In order to do this a method to acquire the device had to be developed, following this a method to analyse the acquired data was needed.

Acquisition

In order to determine how to properly acquire the device, the device was analysed in terms of its components to establish where the relevant data is likely to be located. In this case there were several storage components, including flash memory, a GPS receiver module and an SD card. One of the goals of acquisition was to be able to acquire the device in a non-invasive manner, however the device does not provide a way to read the internal flash memory or GPS module without opening the case, as such the SD card was the only option that remained.

Once the SD card had been selected it was quite trivial to determine a way to read this media without impacting on the forensic integrity of the device by changing any of the data contained within. An SD card reader/writer was modified in order to render it unable to write to the SD card (Hannay, 2007). This modification was accomplished by simply bending a strip of metal located within the reader that detected the read/write state of the card, the result of which is that it would always detect the card as having been set to read only, this modification is shown in Figure 1 below.

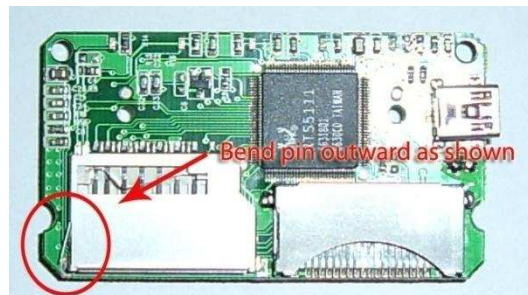


Figure 1. SD Card Reader with Read Only Modification

With the read only device constructed and tested, a procedure to perform the acquisition was developed based on the same method often used to forensically acquire hard disks. In this case the SD card was inserted into the reader and the device copied with a Linux utility known as 'dd'. The method used to acquire the device is shown in Figure 2 below, commands entered have been bolded, whilst output has been made italic. The process (as shown in Figure 2) involves calculating the hash of the SD card, making a bit-stream copy via the 'dd' utility and then calculating the hash of the acquired data to ensure it matches the original exactly (ACPO, 2003).

```
$ md5deep /dev/disk2  
f2452e9b6a984bef855c2b31aff099dc /dev/disk2  
$ dd if=/dev/disk2 of=test.dump  
246016+0 records in  
246016+0 records out  
125960192 bytes transferred in 69.951924 secs (1800668 bytes/sec)  
$ md5deep -l test.dump  
f2452e9b6a984bef855c2b31aff099dc test.dump
```

Figure 2. Method used to Acquire SD Card

The aforementioned method of acquisition was evaluated in order to ensure that it is not possible to alter the original copy of the data. In order to perform this evaluation acquisitions were performed several times, the device was connected to windows and linux systems and several attempts were made to directly write to the SD card. In each case it was not possible to contaminate the data on the SD card in any way. It should be noted however that the SD card reader modification may not work on all SD card readers, and as such, those wishing to make use of this procedure should ensure that they thoroughly evaluate any hardware used for forensic acquisition.

Analysis

In order to decipher any data that is acquired it was necessary to determine how historical location data was stored, and in the process, determine how to decode this data. The analysis process was developed in a series of stages, the first of which was data collection. Data collection involved establishing a baseline and acquiring this baseline, the baseline image was acquired from a TomTom One unit that had no favourite, home or any other locations set. A number of SD cards then had this baseline copied to them so that there was a point for comparison for each test.

The test procedure for data collection involved driving a series of predefined routes, each time the device was placed into a different mode of operation. It should be noted that each SD card was used for a single test and then acquired, this way it was possible to determine the impact each individual test had on the data acquired.

The data once acquired was compared to the original baseline in order to determine which files had been modified and what exactly had changed. In each case a single file was modified, the contents of this file were

examined in order to determine what data could be recovered. A binary analysis was then conducted in order to determine the exact contents of this file and how it could be decoded.

RESULTS

Each location was presented within the file as a distinct record, each contained four coordinates and an ASCII representation of the location. It should be noted however that the information available depends heavily on the mode of operation that the TomTom One device was in at the time of use, a summary of these modes and the data recoverable in each instance is shown in Table 1 below. When examining these coordinates the first three sets form a triangle, this indicates the area which the device was in at the time the record was created. The fourth coordinate is used internally by the device so that it can navigate to that location again, this fourth coordinate is normally a point on a road nearby and can indicate the direction from which the location was reached.

Table 1 - Operational Modes of TomTom device and recoverable information

Operational Mode	Coordinants retrieved	Coordinants consistant with destination	Textual Description Accurate	Known if destination coordinants reached	Path of movement known
Display current location only	No	N/A	N/A	N/A	N/A
Nav without reaching destination	Yes	Yes	Yes	No	No
Nav and reach destination	Yes	Yes	Yes	No	No
Nav and move in opposite direction	Yes	Yes	Yes	No	No
Search without enabling nav	Yes	Yes	Yes	No	No
Create favourite location	Yes	Yes	N/A	No	No

In order to validate the data recovered from the TomTom device, a second GPS unit was used during testing, this unit logged the vehicles precise coordinates throughout the testing process. These coordinates were compared to those recovered from the TomTom device, a sample comparison can be seen in Figure 3 below. It can be seen that there is a slight margin of error as the exact location (indicated by the green arrows) is slightly outside the area marked by the coordinates retrieved from the TomTom device (indicated by the surrounding crosshairs). The fourth navigational coordinate can also be seen to the lower right.

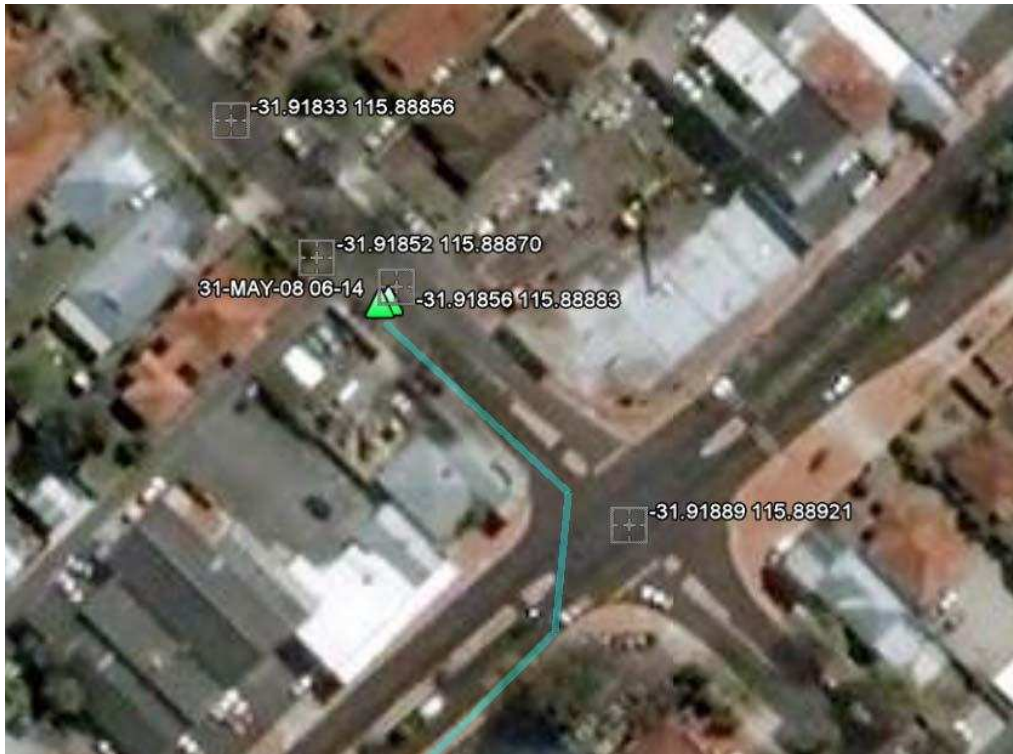


Figure 3 - Image overlaying locations retrieved from TomTom with those taken from a secondary GPS unit

The acquired results are of significance as they demonstrate the data which can be recovered from a TomTom GPS unit, this information is of value as it allows forensic investigators to understand the scope of what can be determined by a forensic analysis of these devices. In this case the understanding that whilst a historic location may be present in the records of the TomTom device that does not mean that the device has actually been to that location, this type of understanding is critical when undertaking investigations involving satellite navigation based evidence.

ONGOING RESEARCH

Research into TomTom devices is currently ongoing, there are a number of alternate sources of information within the device, including onboard flash memory and the GPS receiver module itself. These sources of information will be examined in order to discover what further information may be discovered from the device. In addition to the research being conducted on the TomTom devices, a wide range of other devices is also being explored, these include automotive satellite navigation units as well as phones and other location aware devices.

CONCLUSION

Satellite navigation systems are becoming of increased forensic interest as their usage becomes increasingly widespread. There are a number of devices on the market currently, however these devices often use proprietary methods of encoding historic locational data and as such there is the need to understand specific file formats and encoding methods in order for forensic analysis to take place. In order to address this need research into the methodology for the acquisition and subsequent analysis of these devices has been conducted.

This research has led to understanding of the file formats used by the TomTom One device. As such it is now possible to decode the historic locational data stored within these devices in a forensically sound and non invasive manner. It should be noted however that the data that can be recovered depends heavily on the mode of operation the TomTom One device was in at the time of use, with some modes leaving little to no trace of locational data and others providing a full set of coordinates.

Research into satellite navigation forensics is being continued, with focus towards on-board flash storage and GPS receiver modules. The aforementioned research is being conducted on TomTom devices, other automotive satellite navigation units as well as phones and other location aware devices.

REFERENCES

ACPO (2003). Good Practice Guide for Computer based Electronic Evidence 3.0. Retrieved 16 Oct, 2007, from http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf

Hannay, P. (2007, 3rd December). *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.

HB171 (2003). *HB171: Guidelines for the management of IT evidence : handbook*. Sydney: Standards Australia.

Parkinson, B. W. (1997). Origins, evolution, and future of satellite navigation. *Journal of Guidance, Control, and Dynamics*, 20(1), 11-25.

Polischuk, G. M., & Kozlov, V. I. (2002). THE GLOBAL NAVIGATION SATELLITE SYSTEM GLONASS: DEVELOPMENT AND USAGE IN THE 21ST CENTURY. *34th Annual Precise Time and Time Interval Meeting*, 151-160.

Theiss, A. K., Yen, D. C., & Ku, C.-Y. (2005). Global Positioning Systems: an analysis of applications, current development and future implementations. *Computer Standards & Interfaces*, 27(2), 89-100.

COPYRIGHT

Peter Hannay © 2008. The author/s assign Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. The authors also grant a non-exclusive license to ECU to publish this document in full in the Conference Proceedings. Any other usage is prohibited without the express permission of the authors.