A Methodology for the Forensic Acquisition of the TomTom One Satellite Navigation System – A Research in Progress

Peter Hannay
Edith Cowan University
phannay@student.ecu.edu.au

Abstract

The use of Satellite Navigation Systems (SNS) has become increasingly common in recent years. The wide scale adoption of this technology has the potential to provide a valuable resource in forensic investigations. The potential of this resource is based on the ability to retrieve historical location data from the device in question while maintaining forensic integrity. This paper presents a methodology to acquire forensic images of the TomTom One satellite navigation unit. This methodology aims to be comprehensive and straightforward, while maintaining forensic integrity of the original evidence. However, in consideration of the aforementioned methodology it should be noted that the defined method may not extract all potential evidence and the viability of collected evidence is dependent on future research into the analysis of said evidence. In order to address this consideration, research into this area is currently ongoing.

Keywords

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

INTRODUCTION

The NAVSTAR Global Positioning System (GPS) was declared fully operational in 1995. At this time however the civilian GPS signal was artificially degraded in order to limit the threat that it posed if used by those who opposed the United States. The non-degraded signal known as 'M-CODE' was reserved for military use only. On May 2nd 2000 this artificial degradation, known as 'selective availability' was disabled and the fully functional signal became available to civilians worldwide (Braunschvig, Garwin, & Marwell, 2003). With the full GPS signal available to the civilian population commercial applications of the GPS network began to increase rapidly. This increase would eventually lead to the wide scale availability of Satellite Navigation Systems (SNS) (Theiss, Yen, & Ku, 2005).

Automotive satellite navigation systems such as the TomTom One (TomTom, 2007), aim to provide navigational assistance to its' users. Often the user will provide a destination point then based on this the device will provide a map and verbal turn-by-turn directions to the specified destination. Such devices are becoming more common and are decreasing in price. It should also be noted that many new cars now come with SNS as standard.

The ability to acquire forensic images from satellite navigation devices is becoming increasingly relevant with the aforementioned increase in availability of these devices. Satellite Navigation units have the potential to provide valuable historical locational data to investigators.

In the application of forensic procedure to satellite navigation systems and indeed any digital evidence as a whole there are a number of issues that must be understood. The primary issue faced by digital forensics is the intangibility of the evidence being collected. As the evidence only exists in digital form the method of acquisition heavily depends on the nature of the storage media on which the target information is located. An example is that data stored in volatile memory can often be erased if power to the device is lost (Noblett, Pollitt, & Presley, 2000). In addition to this the contents of volatile often changes constantly as data is re-arranged. In such cases special methods may needed to forensically preserve evidence that is located in volatile memory.

Digital forensics procedure is focused on preserving the integrity of the original evidence and allowing this integrity to be verified at a later stage (HB171, 2003, pp. 17-18). This verification is normally performed by the use of hashing algorithms and careful documentation.

In order for the evidence to be useful a copy must be acquired, this copy can then be used as part of an investigation without the possibility of compromising the original in the process. In order for this copy to be useful it must be what is known as a 1:1 or bit stream copy of the original (ACPO, pp. 20-21). A bit stream copy is a complete duplicate of the original data, instead of copying the files or other logical structures of the original device the raw data that comprises these structures is read piece by piece and copied to a specified location or

device. This method allows for an analysis to be performed on data that has been deleted or otherwise exists in unallocated space.

ACQUISITION SOURCE

This paper focuses on the forensic acquisition of the digital evidence located on the SD card required for the operation of the device. The aforementioned SD card must be inserted into the device at all times in order for the device to function as its core operating system resides on the card. Initial research suggests the data on the SD card is comprised of at least the following:

- x86 boot sector
- Mapping data
- Operating system files
- Configuration files
- Swap space

The SD card has been chosen as the source of information to be acquired for a number of reasons. Firstly it is easily accessible in a non-invasive manner. It is also possible to acquire the SD card with a minimum of equipment and experience. In addition to this it is possible to acquire an image of the SD card in a covert fashion, in many cases it is not possible to determine that the device has been tampered with.

A number of alternate sources for potential evidence exist, however access to these would likely require some access to the internals of the device. For example internal flash chips and the GPS receiver chip itself could serve as a potential source of information. The acquisition of these components will not be covered in this document, as further research is required into the viability of these. However it is recommended that the satellite navigation unit itself is stored in an EM shielded area and connected to an appropriate power source, the device however should not be turned on. In the event that further research leads to the discovery of new evidence sources this may assist in ensuring that volatile memory is not erased and that forensic information is not overwritten as a result of GPS signals being received.

METHODOLOGY

As the media to be acquired is a standard SD card the procedure for acquiring a forensic image of this media involves attaching the device to a system in read only mode and acquiring a bit stream copy of the SD card. As with any forensic procedure the media should be hashed before and after acquisition, the resulting copy of the data should also be hashed in order to verify its integrity. The methodology and technical explanation of hash computation is however out of scope of this document, as such these procedures will not form part of the outlined methodology.

It should be noted that powering the satellite navigation unit on whilst the SD card is inserted will result in data being written to the SD card and the hash changing. In this case the position of the write protect tab on the SD card is irrelevant as the TomTom One does not discriminate if writing should be permitted based on the tab's position. Instead the SD card is treated as writable regardless of the tab's position.

Equipment

In order to perform the acquisition of the SD card it is necessary to have a number of items.

Write blocking SD card reader

Initial examination of commercially available SD card readers has shown that it is possible to modify these devices so that they will not perform write operations. This modification can be performed as shown in the diagram below.

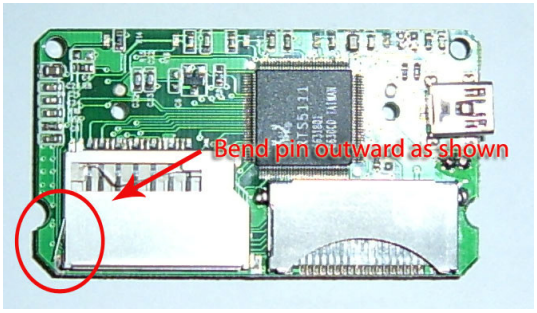

Figure 1. SD Card Reader with Read Only Modification

A movable tab on the side of SD cards is commonly used to set the media to operate in 'read only' mode. This tab is similar to that on 3¼ inch floppy drives, in that the accessing device detects the tab's position rather than the read only logic existing on the media itself. As such the aforementioned modification works by manually bending the pin that detects the position of this tab so that the device will always detect the tab as being in the 'read only' position. The result of this is that all media will be treated as read only, regardless of the position of the tab.

Forensic Workstation

The forensic workstation is typically a standard PC with USB capabilities and a storage device with adequate free space to store the acquired image. In this case it is assumed that the workstation in question is running a Linux operating system with access to a terminal or other standard Linux command line interface (CLI).

'dd' Software

The dd software is capable of performing low-level data operations such as performing a bit stream copy of the data to be acquired.

Process

1. Attach write blocked USB SD card reader
2. Insert a non-critical SD card for testing purposes
3. Perform a hash of the SD card
4. Ensure the file system (if any) present on the SD card has not been mounted
5. Attempt to write to the SD card
6. Perform an additional hash of the SD card
7. Ensure that the hash matches the original
8. Remove the SD card
9. Insert the SD card to be acquired
10. Perform a hash of the SD card
11. Ensure the file system (if any) present on the SD card has not been mounted
12. Acquire a copy of the SD card using dd
13. Perform a hash of the SD card
14. Perform a hash of the acquired file
15. Ensure that the hashes match the original
16. Remove the SD card from the reader

LIMITATIONS OF THE RESEARCH

A number of limitations are inherent in the methods outlined in this paper. These limitations are primarily due to the focus on a single satellite navigation unit. It is due to this focus that the methods outlined here may have limited use in the field, as research has yet to be performed into the application of the aforementioned methods

with other satellite navigation units. Additional there is a limitation to the data which is acquired through the means outlined within this paper, for example location data may be present in the flash memory of the devices internal GPS module. This particular source of information is not acquired through this method.

An additional factor limiting the usefulness of data acquired through these means is the lack of an established method to extract meaningful data from the acquired images. Currently the author is perusing further research into this area with the aim of evaluating the feasibility of analysing and extracting historical locational data from the acquired images. Indeed it is possible that the acquired images may have limited use, as the extent of data present in these images is currently unknown. It should however be noted that preliminary research into this issue suggests that at least some historical location data can be gained from these images.

CURRENTLY ONGOING RESEARCH

Research is currently being conducted in order to determine the significance of evidence located on areas of the device other than the SD card. In addition to this an analysis of the contents of the SD cards utilised by the TomTom One device . Furthermore a number of other satellite navigation units are currently being examined in order to determine the forensic value of data contained within and viable methods for acquiring that data.

CONCLUSION

In conclusion satellite navigation is a field of increasing importance to law enforcement and other investigative agencies. The methodologies outlined within this paper should allow someone with adequate forensic training to acquire an image from the SD card of the TomTom One satellite navigation system. It should however be noted that the forensic value of this image is dependant on future research into the significance of the data stored within the image, however initial research suggests that historical location data is present. Significant evidence may exist in other parts of the TomTom One satellite navigation system, however this has yet to be determined. Research is currently ongoing in this area.

REFERENCES:

ACPO. Good Pracice 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

Braunschvig, D., Garwin, R. L., & Marwell, J. C. (2003). Space Diplomacy. *Foreign Affairs, 82*(4), 156.

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

Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and Examining Computer Forensic Evidence. *Forensic Science Communications, 2*(4).

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.

TomTom. (2007). TomTom, portable GPS car navigation systems - TomTom One Australia. Retrieved 31st October, 2007, from http://www.tomtom.com/products/product.php?ID=399&Category=0&Lid=8