Garmin satnavs forensic methods and artefacts: An exploratory study

Alexandre Arbelet

Submitted in partial fulfilment of
the requirements of Edinburgh Napier University
for the Degree of
Master of Science in Advanced Security and Digital Forensics

School of Computing

August 2014

Supervisor: Richard Macfarlane
Second Marker: Adrian Smales

Authorship Declaration

I, Alexandre Arbelet, confirm that this dissertation and the work presented in it are my own achievement.

Where I have consulted the published work of others this is always clearly attributed;

Where I have quoted from the work of others the source is always given. With the exception of such quotations this dissertation is entirely my own work;

I have acknowledged all main sources of help;

If my research follows on from previous work or is part of a larger collaborative research project I have made clear exactly what was done by others and what I have contributed myself;

I have read and understand the penalties associated with Academic Misconduct.

I also confirm that I have obtained **informed consent** from all people I have involved in the work in this dissertation following the School's ethical guidelines

Signed:

Date: Monday, 18 August 2014

Matriculation no: 40112000

Data Protection Declaration

Under the 1998 Data Protection Act, The University cannot disclose your grade to an unauthorised person. However, other students benefit from studying dissertations that have their grades attached.

Please sign your name below *one* of the options below to state your preference.

The University may make this dissertation, with indicative grade, available to others.

The University may make this dissertation available to others, but the grade may not be disclosed.

The University may not make this dissertation available to others.

Abstract

Over ten years ago, major changes in the Global Positioning System (GPS) technology led to its explosion in popularity. GPS devices are now ubiquitous, escorting their users everywhere they go, and potentially recording the entirety of their whereabouts. As such, they represent invaluable assets to forensic practitioners. Amongst the different brands, Garmin and Tom-Tom are by far the most widespread, and are regularly encountered as part of investigations.

GPS forensics is a relatively new field of study, in which tools and methodologies are very reliant upon the device itself. Whereas several tools and methodologies have been developed to address Tom-Tom devices, the lack of knowledge concerning Garmin devices may lead to investigators missing evidence.

This thesis aims to explore forensic methods applicable to Garmin devices, and highlight locational artefacts located on them, which may be of use in a digital investigation. To do so, three series of experiments have been designed and performed, intending to document the behaviour of the device, the methods to acquire and analyse its content efficiently, and the reliability of the data recovered.

This thesis shows successful acquisition of data from a range of Garmin devices. It also demonstrates that various forensic artefacts can be recovered from Garmin devices, with the results compared to similar research into Tom-Tom GPS devices. This highlights that Garmin devices potentially have a greater forensic potential than Tom-Tom devices, as it was found they typically hold up to 6 month of their user's daily locations, regardless of whether the navigation was in use or not. Using carving techniques and file signatures discovered through the project, this thesis shows how to recover further location tracking data from unallocated clusters. However, it also highlights that such information should be considered carefully, since the work also demonstrates that the data can be manipulated using anti-forensic techniques.

Contents

List of Tables

List of Figures

List of Acronyms

AFSCN	Air Force Satellite Control Network
CS	Galileo Commercial Services
DB	Database
DoD	Department of Defence
DoT	Department of Transport
EEPROM	Electrically Erasable Programmable Read-Only Memory
GLONASS	Global'naya Navigatsionnaya Sputnikovaya Sistema
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GPX	GPS eXchange format
HMI	Human-Machine Interaction
IGEB	Inter-agency GPS Executive Board
MEO	Middle Earth Orbit
MSC	Mass Storage Class
MSD	Mass Storage Device
MTP	Media Transfer Protocol
NGA	National Geospatial-Intelligence Agency
NHTCUS	National Hi-Tech Crime Unit in Scotland
OS	Galileo Open Service
OS	Operating System
POI	Point Of Interest
PPS	Precise Positioning System
PRS	Galileo Public Regulated Services
RQ	Research Problem
SoL	Galileo Safety of Life
SPS	Standard Positioning System
SSD	Solid State Drive

Acknowledgements

My first thanks goes to my supervisor, Richard Macfarlane, for his thoughtful advices and the patient guidance he provided throughout this project.

Additional thanks go to Adrian Smales, for being my second marker.

I am also particularly grateful for the assistance given by Mick Dickson, who accepted to answer my questions and provided a practitioner viewpoint on this work.

I would also like to thanks Delphine Tirole, for her moral support and her patience throughout the duration of this project.

Finally, I wish to thank my parents for their support and encouragement throughout my study.

Chapter 1 Introduction

1.1 Context

In the early morning of May 2nd, 2000, a silent but huge step was taken concerning the Global Positioning System (GPS). "Every civilian GPS receiver around the globe went from errors the size of a football field to errors the size of small room" (Humphreys, 2012). This change led the explosion of GPS devices in popularity. As GPS chips become smaller and cheaper, they are used for an ever-growing number of applications (For instance running, navigation systems, or smartphones), making them almost ubiquitous in today's world. Because of their popularity, they provide a further potential source of data for forensic investigators.

Locational artefacts are of great value to investigators, as they can place a suspect on a crime scene within and timeframe (Ball, 2008), or be used for digital profiling and build the behavioural profile of a suspect based on his whereabouts (C. M. Colombini, Colella, Castiglione, & Scognamiglio, 2012). However, along with the variety of embedded devices comes different technologies, needing appropriate forensic techniques to be investigated (S. L. Garfinkel, 2010).

So far, researchers have published papers on how to forensically investigate GPS devices, but it either addresses GPS broadly (Cusack & Simms, 2011; Last, 2009; Strawn, 2009) or focuses on only TomTom devices (C. Colombini, 2009; Hannay, 2008; Nutter, 2008; van Eijk & Roeloffs, 2010). Despite having an important part of the GPS market share, Garmin has received little attention from the forensic research community.

This lack of documentation induces a lack of knowledge regarding Garmin devices, which may lead to evidence being routinely missed (S. L. Garfinkel, 2010). To help forensic analysts better handle those devices and being able to retrieve the essential information quickly, it is important to explore Garmin GPS forensics, to document where to find such information, and which methods may be used to access it.

1.2 Aims and objectives

Tom-tom and Garmin are the current global leaders for GPS devices (cargpsrating.com, 2014). Whilst Tom-tom has been the subject of numerous studies, few investigations on Garmin GPS devices have been documented (Jones, Sutherland, & Tryfonas, 2008). Regardless of the

brand, forensic investigators must understand what data can be recovered, and how they could be recovered without damaging the physical nor the logical integrity of the device (Carrier, 2005). As the data is likely to be used in front of a court of law, it is therefore paramount to assess its reliability, and whether or not it could have been modified in any way that the investigator would not be able to detect (Lallie & Benford, 2011; Strawn, 2009).

This project aims to explore forensic methods applicable to Garmin devices, and document locational artefacts located on them. To support it, four objectives have been defined:

1. From the literature, review the principles and limitations of the Global Positioning System, and how this technology is used nowadays. Investigate how GPS forensic investigations are performed, regarding to a specific brand such as Tom-Tom or Garmin.

2. Based on the findings of the literature review, design a set of experiments aiming to assess forensic acquisition and analysis of Garmin systems, and challenge the reliability of the evidence retrieved.

3. Implement the experiments and document the main steps in order to make them reproducible. Collect the raw results.

4. Discuss and evaluate the results, by comparing them to similar studies conducted by the community.

1.3 Thesis layout

This thesis is divided into six chapters. The remaining is organized as follows:

- **Chapter 2 - Literature review**: This chapter presents the overall principles of Global Navigation Satellite Systems (GNSS). It also reviews the studies conducted on GPS forensics, anti-forensics, and Garmin forensics. The aim of this chapter is to provide the reader a background understanding, and present the state of the art regarding geo-forensics.
- **Chapter 3 - Experimental design**: This chapter divides the objectives of this thesis into Research Questions, and designs a set of experiments aiming to address them.

- **Chapter 4 - Experimentation**: This chapter describes how the experiments have been conducted and presents the results obtained through them.
- **Chapter 5 - Discussions**: This chapter discusses the results obtained during the experimentation, and compares them to other studies that have been performed on the same subject. It also evaluates the experimentation procedure.
- **Chapter 6 - Conclusions**: This chapter summarizes the main findings of this project, and provides a critical evaluation of the work that has been done. It also provides directions for future work.

Chapter 2 Literature review

2.1 Introduction

The aim of this chapter is to critically review a literature corpus related to the research area. It is divided into four main sections, related to GNSS principles, forensics/Anti-forensics applied to Global Positioning Systems (GPS) and Garmin devices respectively.

The first section provides a background knowledge of navigation systems to the neophyte. The section first presents the different existing systems, before addressing the well-known Global Positioning System, how it operates, how it is used in the modern society and what are the limitations of the technology.

The second section is related to GPS forensics. The section first describes the GPS devices, their structures, the technology they commonly use, where they store the data they collect and so on. In a second part, a state of the art concerning GPS forensics is provided, primarily focused on forensic acquisition and analysis techniques. This section also explores the legal and ethical issues of using GPS data for law enforcement.

The third section is dedicated to Anti-forensics and reviews the techniques already investigated by the forensic community. Two areas are tackled in this section. The first is about how someone could use the internal memory properties of a device to hide data inside it, whereas the second is more about manipulating locational data on the device, in an attempt to mislead an investigator.

The last section is a critical review of the literature related to Garmin forensics specifically. This part describes mainly the techniques that have been used to investigate such devices, the main outcomes and findings of these papers, as well as the challenge commonly encountered when dealing with Garmin systems.

2.2 Global Navigation Satellite System

From the early 1960s to now, the GPS (i.e. Global Positioning System) has come a long way, becoming more prevalent with the passing of time, even being ubiquitous since the 2000s (Humphreys, 2012). The antonomasia is now the most established GNSS (i.e. Global Navigation Satellite System) provider around the world and enables much more than the navigational

purpose for which it was designed. As GPS chips become accessible, the range of applications grows wider, sometime using them in ways that were not intended for (Strawn, 2009).

This chapter discusses the different GNSSs with a special dedication given to the U.S. provider “Navstar GPS” (i.e. NAVigation Satellites by Timing And Ranging Global Navigation System). It will be divided into five sections. The first one remains general and enumerates the different GNSS providers, their status and the services they provide. Then the paper focuses on the U.S. provider, and gives its historical background, following by the applications it enables. A fourth section explains how Navstar GPS operates and what its limitations are. The last section will review jammers and spoofing systems as well as their current usage.

2.2.1 GNSS Providers

A GNSS is a satellite navigation system that provides global coverage. Currently, the U.S. Navstar GPS (National Coordination Office for Space-Based Positioning Navigation and Timing, 2014) and the Russian GLONASS (i.e. Global'naya Navigatsionnaya Sputnikovaya Sistema) (Federal space agency, 2014; Hofmann-Wellenhof, Lichtenegger, & Wasle, 2007) share the market. They will probably be joined soon by the European Galileo (European GNSS Agency, 2014) and the Chinese Beidou, formerly called "Compass" (China National Space Administration, 2014). GPS has been developed in the early ‘60s as a mean to locate U.S. submarines, before being used as a valuable asset during the cold war. As a response, the Soviet Union developed GLONASS. Although both GPS and GLONASS were first designed for military purposes, they opened their services to civilians and foreigners (Larsen, 2001). As reported by Larsen, the coexistence between both the military and the civilian users seems to work, although this dual use of the technology poses a problem. Indeed, despite the assurance of the US government, no international law prevents the USA to stop the GPS service for national security reasons (Larsen, 2001). As GLONASS belongs as well to the military, the same issue must be envisaged.

This situation stressed Europe and China to start their own project (Larsen, 2001), "Galileo" and "Beidou" respectively. The "Galileo" project aims to respond to this "Need for a European controlled GNSS" (European GNSS Agency, 2014). Some services such as air transport or rescue cannot afford any downtime from the GNSS provider, nor a degradation of the service. This is precisely why "Galileo" provides different services, each related to a specific kind of applications (European GNSS Agency, 2014). The following Table 1 summarizes these services and the applications they will be using for.

Table 1 Galileo Services Summary

Service	Scope of application
Open Service (**OS**)	Free of charge, the service aims to offer an accuracy to one metre. It is intended for navigation devices and mobile phones (European GNSS Agency, 2014).
Safety of Life (**SoL**)	The SoL is a guaranteed service dedicated to critical applications with rigorous requirements in terms of availability, continuity and accuracy. It includes a hashing function providing information on the integrity of the signal transmission. The service will be used in sectors such as navigation or aviation (European Commission, 2011).
Commercial Services (**CS**)	This service is an enhanced-encrypted version of the open service aiming to provide an accuracy to the centimetre, to commercial application (European Commission, 2011). According to the European GNSS Agency, (2014), the service will be charged.
Public Regulated Services (**PRS**)	This encrypted service will be restricted to government bodies for sensitive applications. The service provides anti-jamming and spoofing detection mechanisms (European Commission, 2011).

The European constellation is announced to reach full operational capability in 2020, and will consist of 30 satellites positioned in three orbit planes (European Union, 2010). Its Chinese equivalent claims it will be fully deployed by 2017 (Gibbons, 2014).

Each of these providers possesses their own constellation of satellites, at a standardised altitude. The following Figure 1 shows the altitude of the constellations, regarding the GNSS providers. As shown in the figure, each provider has its own standardised altitude. GPS satellites fly at 20200 km above the sea level (National Coordination Office for Space-Based Positioning Navigation and Timing, 2014). GLONASS satellites are located 1000 km behind (19100 km) (Federal space agency, 2014) whereas the Galileo constellation flies at an altitude of 23222 km (European GNSS Agency, 2014).

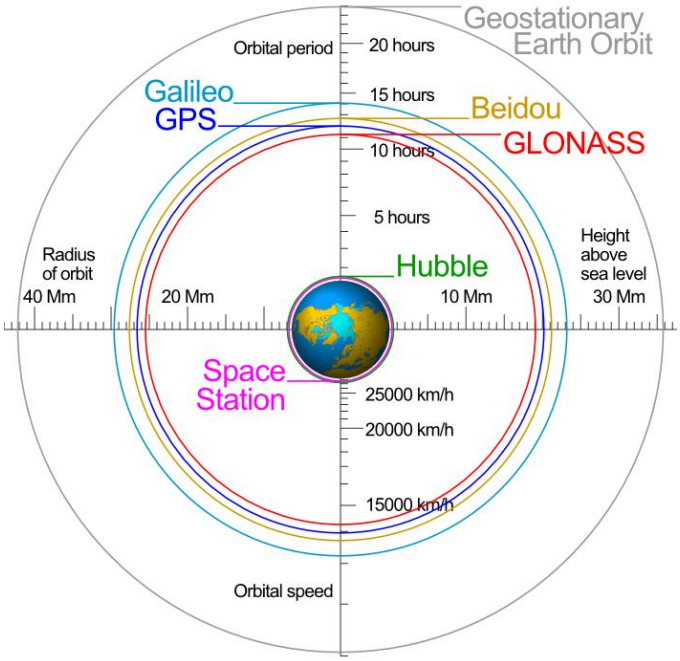


Figure 1 GNSS providers satellite altitude (credit: GPS Spotlight)

2.2.2 Navstar GPS History

In 1957, the launch of "Sputnik 1" by the soviet space program was a success that astonished the whole world. As a result, the US program started to investigate the radio signal emitted by Sputnik (Kahveci & Can, 2013), trying to determine the exact orbit of the Russian Satellite using Doppler measurements. One thing leading to another, they realised that the inverted process, given the satellite's orbit, could accurately determine a receiver position (Parkinson, 1997). This discovery led the NAVY to start the "Transit" project in 1960, providing them a mean to locate their submarines (Hannay, 2008). The developed system was however too slow, leading to the development of "Timation" in 1967, which used range measurements instead of Doppler measurements. Meanwhile, the US Air Force developed a parallel project, called "621B", which added altitude to the information provided. In 1973, they brought together Timation and 621B projects and created the "Navstar Global Positioning System" project. Navstar introduced the use of atomic clocks into satellites, hence providing very accurate timing (Theiss, Yen, & Ku, 2005).

The US government opened GPS services to civilian and internationals in 1993, however using different channels. The two channels have different caretakers, although the general usage is managed by the Inter-agency GPS Executive Board (IGEB) (Larsen, 2001). The civilian grade service, called Standard Positioning System (SPS), is under the responsibility of the US Department of Transport (DoT) whilst the military grade service, the

Precise Positioning System (PPS), belongs to the US Department of Defence (DoD). An agreement between the two agencies defines the responsibilities of each regarding the overall system (Barrett & England, 2008).

Civilian grade GPS was, at its start, purposely degraded by a process called "Selective Availability" (SA) (Doherty, 2013). This service was to prevent the enemy to use the service against the USA. On the 2nd of May 2000, selective availability was turned off, in order to “make GPS more responsive to civil and commercial users worldwide” (National Coordination Office for Space-Based Positioning Navigation and Timing, 2014): "Every civilian GPS receiver around the globe went from errors the size of a football field, to errors the size of a small room" (Humphreys, 2012). This change led to the explosion of GPS devices in popularity. The fear that this function could be again turned on led the European to invest on Galileo. But in 2007, a press release from the DoD claimed that SA would be permanently discontinued and the new satellites will not be equipped with the feature (U.S. Department of Defense, 2007).

Whether it is used for military, civilian or humanitarian purposes, Navstar GPS is now prevalent in today's world, and numerous applications rely upon it.

2.2.3 GPS Usage and controversy

2.2.3.1 Applications

The GPS provides the chip with its location at a known time. Using this valuable piece of information, the chip is able to supply the end user with three features; Positioning, timing, and point-to-point distance (Theiss et al., 2005). These features provide a wide range of applications, which are used in a great variety of businesses. As pointed out by Parkinson, (1997), most obvious is the navigation uses, regardless the type of motion. Since the end of the SA in 2000, the civilian navigation devices market has exploded (Humphreys, 2012).

More recent is the use of GPS for sport purposes. Companies such as Garmin propose GPS solution for all kinds of sports such as running, swimming, golfing, biking… (Garmin, 2014a). These products act like tracking systems, and collect information on the user’s practice. The raw data are then uploaded onto a specific website where the user has an account. The web application processes this information and gives a feedback to the user on his performances. Users can then share a summary of their activities on the common social networks, and challenge other users possessing similar devices (Garmin Connect, n.d.). Personal training is not the only usage of GPS related to sport. For instance, football managers and coaches use GPS

as a mean to analyse the motion of their players (Bekraoui, Cazorla, & Léger, 2010). In their study, Bekraoui et al., (2010) noticed GPS is a cheaper and better solution for quantitative analysis on football players, than video analysis. They argue that the technology could become in a near future, a valuable tool to optimize the preparation of the players.

With the enhance precision offered by augmentation systems such as DGPS, WAAS or EGNOS, farmers can rely upon the technology to automatically drive their machines, whilst focusing on other tasks like fertilizer spreading (Theiss et al., 2005; Trimble.com, 2014).

The positioning feature also led to the creation of tracking systems, which are becoming more and more common within companies as part of their logistic process (Theiss et al., 2005). Tracking systems allow numerous applications to companies willing to optimize their process. For instance, the enterprise "Digital Dispatch" (Digital Dispatch, 2014) proposes an application for taxi dispatching. The solution would benefit to both the user and the company using the application, as taxis are faster to pick up the client, and only the closer available taxi has to be contacted for the course. Tracking systems are also used as security features. The "Triton" form Starcom Systems(2014) allows container tracking for security and management purposes. These trackers allow companies to optimize their logistic process a great deal, and is also used as a mean to look over drivers and be sure their trips remain strictly professional (Spencer & Weber, 2013). The company TrackYour.co.uk provides "peace of mind for those who care" by tracking their children, pets, elderly and so on (TrackYour, 2014). Several car rental companies use their GPS appliances to record the customer driving behaviour. With this piece of information, the company is then able to refuse a customer judged unsafe (Theiss et al., 2005). Trackers can also be used by Police, as an investigative tool. In his article, Ball (2008) said: "Reliable data puts the suspect there between 9:42 and 10:17 p.m. and reveals where she came from and went next". This clearly underlines the impact GPS data on law enforcement. GPS Trackers are now commonly placed on suspects' car, thus allowing the investigators to track their movements (David Lee Vs Commonwealth, 2012; Hubbard, 2008). Tracking systems however raise concerns about ethic and privacy, which will be addressed in the next sub-section.

Closely related to positioning as it involves the actual position of the chip, the point-to-point distance can help to measure things. For instance, the water system of Modesto in California has been mapped using GPS chips, thus completing the project below budget (Theiss et al., 2005).

GPS chips synchronize with the satellites, which have atomic clocks. Hence, the time on GPS chips is always close from satellites' times, which make them very accurate and valuable for application when accuracy of time is paramount. For example, banks use GPS time to synchronize their agencies around the world, using this time as a reference for transactions. Other applications can be imagined, where two actions must be done simultaneously (Theiss et al., 2005). The US Department of Commerce report (U.S. Department of Commerce, 2000) the time accuracy being within 40 billionths of a second.

At the time of writing, one cannot but notice that GPS chips have been embedded in almost every Smartphones on the market, making the technology ubiquitous in today's daily routine (Humphreys, 2012). The technology has been widely exploited by the different social networks, which access the data legally by providing so-called "features" and use the information gathered for target advertisement (Agarwal, D'Angelo, & Jin, 2008; Baker, 2003), activity yet very lucrative. In a survey conducted by Krumm, (2009), it has been shown that people are generally not concerned about the privacy of their location, and therefore give the information easily, a behaviour that could be described as a "privacy paradox" (Barnes, 2006). However, the use of the GPS chips embedded in smartphones might help to resolve societal problems, such as traffic jam. Work & Bayen, (2008) published a paper where the researcher investigated the possibility of traffic monitoring through customers' devices. The information could be gathered directly from the smartphones and therefore ease traffic monitoring. This would allow seeing the whole traffic in real-time, and help to prevent traffic jams.

2.2.3.2 Controversy

Nevertheless, some of these applications raise ethical and privacy concerns. The omnipresence of smartphones made GPS even more pervasive than it was supposed to be (Humphreys, 2012), thus "invading all walks of life" (Iqbal & Lim, 2008). GPS applications that went beyond what was imaginable few years ago, and people are using these applications at their full potential, sometimes to the detriment of privacy (Iqbal & Lim, 2008; Kahveci & Can, 2013; Karim, 2004; Spencer & Weber, 2013).

Law enforcement in the US is a great instance of this phenomenon, whilst tracking suspects can help investigators to resolve a case, the fourth amendment prevents them to use the data in court (Hand, 1958). Despite the amendment, the data gathered is generally admitted in court (David Lee Vs Commonwealth, 2012; Gershman, 2009; Iqbal & Lim, 2008; Karim, 2004; Koppel, 2009; Spencer & Weber, 2013). The technology eases the investigation and, in the urge of catching the "bad guy", police forces tend

to avoid fundamental principles. “Professional ethic” requires a “sharp separation between personal and professional morality” (Postema, 1983), a separation which seems to fade away when using tracking systems.

2.2.4 GPS Principles and limitations

Navstar GPS is made of three elements called "control", "space" and "user" segment (Jones et al., 2008). The "control segment" is in charge to control the satellites, which represent the "space segment". The "user segment" represents the end-user devices, such as our common navigational systems. The Figure 2 below illustrates the interactions between the different segments.

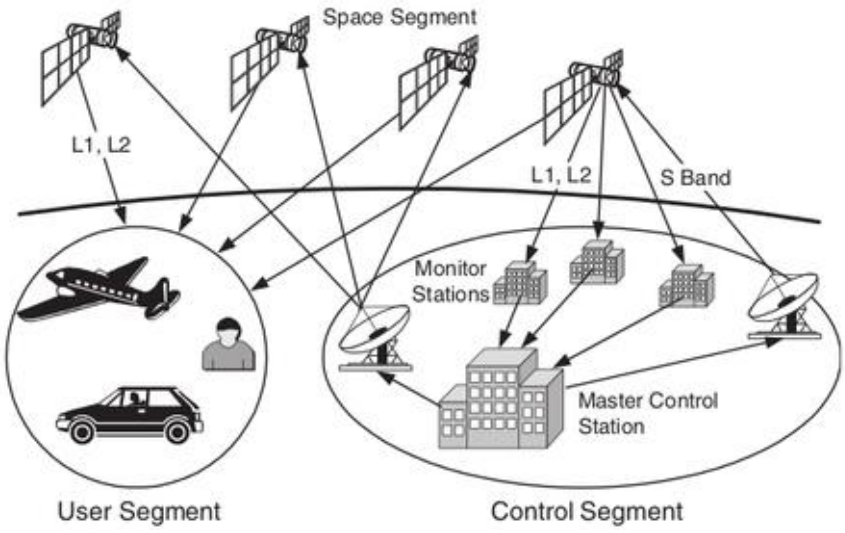


Figure 2 GPS segments (credit: ipgfy)

2.2.4.1 The space segment

The space segment contains, at the time of writing, 32 satellites (US Department for Homeland Security, 2014) currently orbiting the earth , see Figure 3. Twenty four of them are in use, and the remaining eights act as backups. These satellites broadcast their orbital position along with a timestamp when the signal has been emitted. As a matter of fact, the satellites broadcast on two different frequencies, respectively at 1575.42MHz (L1, civilian) and 1227.6MHz (L2, military), L2 being encrypted (Warner & Johnston, 2003).

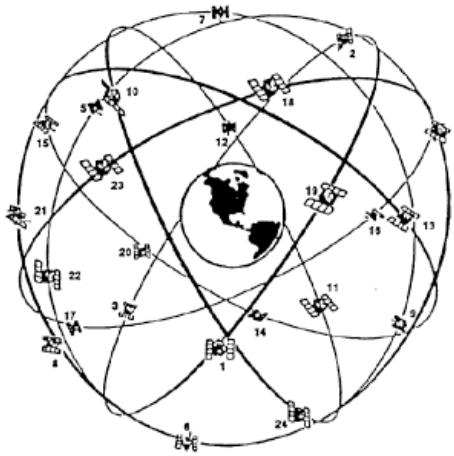


Figure 3 GPS Constellation (credit: gpswien.at)

Due to the share of a reference time by the space and the user segment, the receiver can extract the position from which the signals have been emitted, as well as the time at which it has been emitted and the time of propagation between the satellite and the device. The calculation is as follows:

$$T_{propagation} = T_{reception} - T_{emission}$$

Given the time of propagation, and given that every electro-magnetic waves travel at the speed of light (C), it is possible to calculate the distance (D) between the two entities:

$$D = T_{propagation} * C$$

In order to locate accurately a chip on earth, GPS uses trilateration (C. M. Colombini et al., 2012; Jones et al., 2008), which is similar to triangulation, but using distances instead of angles, as illustrated by the Figure 4.

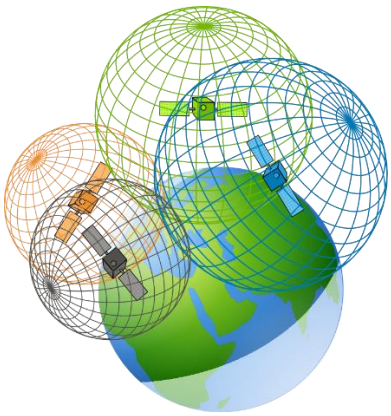


Figure 4 Trilateration principle (credit: openclipart)

In order to illustrate this principle of trilateration, the following is a simplified example of how a receiver can determine its position with four satellites in view.

At `15:03:25.67868765`, A GPS receiver has four satellites in view, respectively called "`A`", "`B`", "`C`" and "`D`". All the satellites broadcast a timestamp, along with their name.

Satellites	Emission Timestamp
A	`15:03:25.67362982`
B	`15:03:25.67445559`
C	`15:03:25.67032675`
D	`15:03:25.67156540`

The receiver extracts the timestamps and determines the time delay between its clock and those timestamps with the following formula:

$$T_{propagation} = T_{reception} - T_{emission}$$

And determines the distance with each of these satellites by multiplying the time delay with the speed of light (given that the speed of light `C= 299792458 m/s`)

$$D = T_{propagation} * C$$

Satellites	Time (s)	Distance (m)
A	`.00505783`	`1516299.2878461`
	`.00423206`	`1268739.66980348`
C	`.00836090`	`2506534.7620922`
D	`.00712225`	`2135196.8339905`

The receiver therefore knows its distance, called range, from different known satellites, as illustrated by the Figure 5. Three satellites allows a receiver a 3D location on earth, and a fourth satellite would allow the receiver to synchronize its clock (McWilliam, Teeuw, Whiteside, & Zukowskyj, 2005).

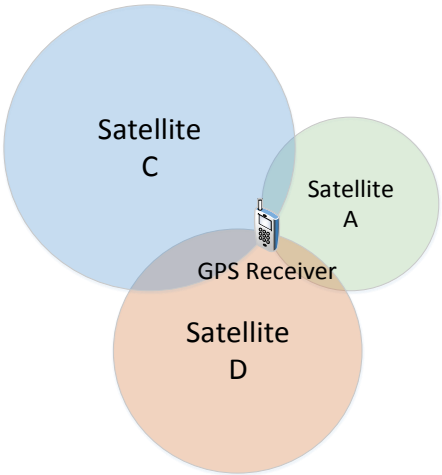


Figure 5 Trilateration example

The satellites positions are known and can be expressed, in an earth-fixed frame of reference, by set of coordinates (X_S, Y_S, Z_S). Given the distance D_i to the satellites i, and their respective coordinates (X_i, Y_i, Z_i), one can determine the coordinates of the receiver, (X_r, Y_r, Z_r), with the following equation:

$$\begin{cases} D_A = \sqrt{(X_A - X_r)^2 + (Y_A - Y_r)^2 + (Z_A - Z_r)^2} \\ D_B = \sqrt{(X_B - X_r)^2 + (Y_B - Y_r)^2 + (Z_B - Z_r)^2} \\ D_C = \sqrt{(X_C - X_r)^2 + (Y_C - Y_r)^2 + (Z_C - Z_r)^2} \end{cases}$$

According to Parkinson, former GPS Program Director, 4 satellites in view are enough to update the time whilst providing longitude, latitude and altitude to the chip (Parkinson, 1997). As shown in the Figure 6 below, the geodetic latitude is a signed angle comprised between -90° (South) and 90° (North) using the equator as plane of reference. The geocentric longitude is a signed angle, comprised between -180° (West) and 180°(East), using the prime meridian as plane of reference (National Geospacial-Intelligence Agency, 1984).

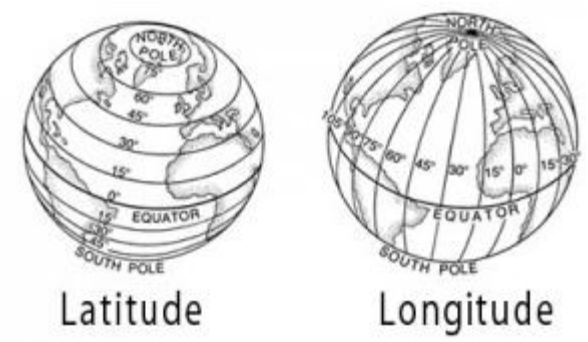


Figure 6 Latitude and Longitude (credit: wikimedia)

2.2.4.2 The control segment

The GPS control segment is the segment in charge for the monitoring and the control of the satellites (National Coordination Office for Space-Based Positioning Navigation and Timing, 2014). It is mainly responsible for time synchronization between the satellites, monitors their "health" and does manoeuvres if need be. There are several stations that are part of this control segment, located across the world. The following Figure 7 shows their location.

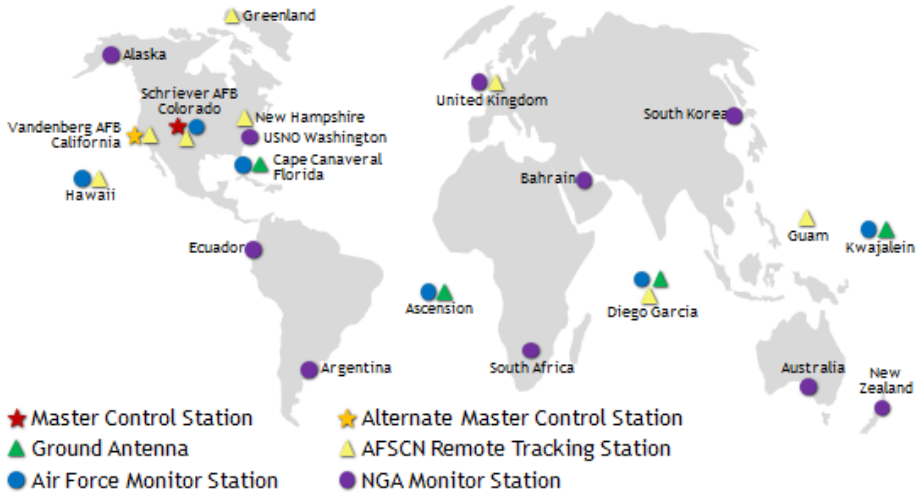


Figure 7 GPS Control segment (credit: gps.gov)

As it can be seen in the Figure 7, there are different types of stations. The "Master control station" is the only station allowed to control and manipulate the satellites. If for some reason the master station is unavailable, an alternate master station can be used instead. Monitor stations are in charge of collecting data coming from the satellites (such as navigation signals, atmospheric data…) and tracking the satellites. There are currently 16 monitor stations, belonging to the Air Force and the National Geospatial-Intelligence Agency (NGA). Ground antennas are used to communicate with the satellites, whilst Air Force Satellite Control Network (AFSCN) remote tracking stations offer to the control segment an increased visibility over the satellites (McWilliam et al., 2005; National Coordination Office for Space-Based Positioning Navigation and Timing, 2014; Parkinson, 1997; Theiss et al., 2005).

2.2.4.3 The user segment

The user segment represents the end user devices. Every device that has an embedded GPS chip in it is therefore considered as being part of the user-segment. Examples of devices from the user-segment can be GPS navigation systems, smartphones, GPS jammers, GPS based timing systems and so on (Parkinson, 1997).

2.2.4.4 Limitations

On its way from the space to the user device, the radio signal might be somehow disturbed, which can affect the accuracy of the location calculated. These effects can be divided into two categories, "local" and "atmospheric" effects (McWilliam et al., 2005).

Atmospheric effects are disturbance occurring in the different layers constituting the atmosphere. These perturbations occur as the wave goes from an environment to another, with a different optical density,

which slightly infers on its speed, thus causing refraction, as illustrated in Figure 8.

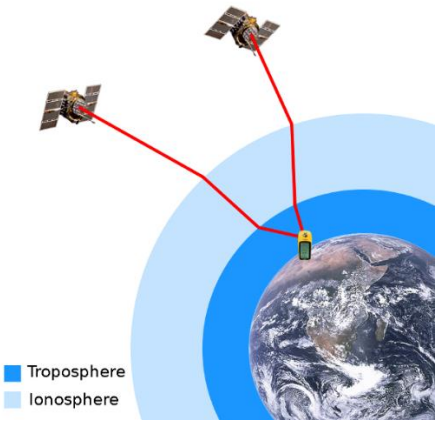


Figure 8 Atmospheric effects on GPS accuracy (credit: wikimedia)

Figure 8 illustrates the phenomenon. The satellite emits a signal at the speed of light. As the different layers of the atmosphere have different optical densities, the speed of the signal will be slightly different from a layer to another, hence explaining a small delay (Dubey, Wahi, & Gwal, 2006; Klobuchar, 1996). According to McWilliam et al., (2005), the disturbance caused by the ionosphere results in a loss of accuracy of 5 to 10 metres, although this effect may produce errors up to 30 metres. Tropospheric effects, however, have a smaller impact. Indeed, the potential error related to this kind of effects is inferior to 5 metres, and generally does not go above 2 metres of inaccuracy.

In order to correct the inaccuracies due to refraction, augmentation systems have been developed (Jones et al., 2008). An Augmentation system can be ground-based such as the Differential GPS (DGPS), or Satellite-based such as Wide Area Augmentation System (WAAS) for the US or European Geostationary Navigation Overlay Service (EGNOS) for the Europe. Both systems works with reference stations positioned at known location, which will analyse the radio signal and send a calibration signal to the end user, through a different canal (Parkinson, 1997). As shown in Figure 9, ground and satellites based systems differ in that ground based-systems will send the correction directly to the user, whereas satellites based (illustrated by Figure 10) will first transmit to a geosynchronous satellite which will relay the correction to the user.

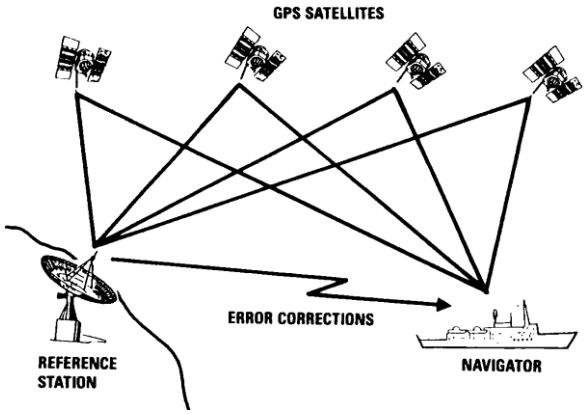


Figure 9 DGPS (credit: gpswien.at)

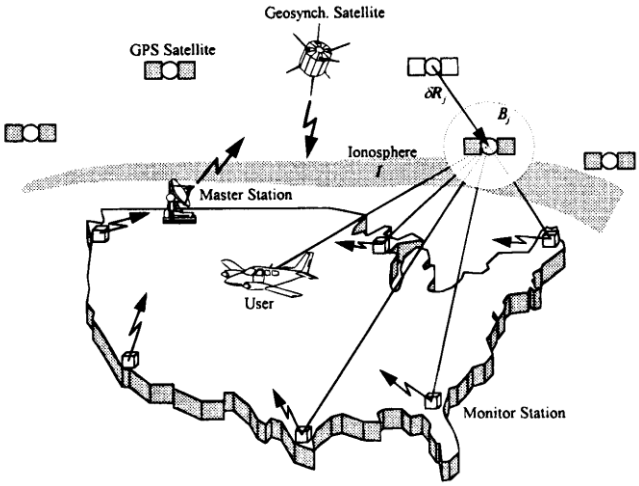


Figure 10 WAAS/EGNOS (credit: gpswien.at)

The advantage of Satellite-based Augmentation Systems (SBAS) is that they cover a wider area. The Figure 11 presents the areas covered by the different SBAS existing currently.

Figure 11 SBAS Coverage (credit: Egnos portal)

According to Strawn (2009) the GPS accuracy can be as good as 3 meter when using some sort of augmentation, such as DGPS, WAAS or EGNOS. Figure 12 below summarizes the GPS system accuracy.

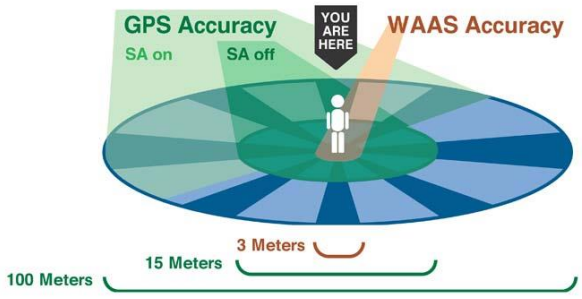


Figure 12 GPS Accuracy w/ WAAS w/o SA (credit: Utah State University)

Local effects can also affect GPS devices a great deal. McWilliam et al., (2005) reported inaccuracies up to 10000 metres due to errors in the receiver's clock. These errors are thankfully very rare, as devices tend to synchronize their time with the satellites as soon as they can (they must have four satellites or more in view to do so). Conversely, the environment surrounding the receiver affects the system accuracy. As with every electro-magnetic wave, GPS signals can be reflected by some environment, and blocked in others. Therefore, the reliability of the device inside a thick forest is not guaranteed. It is possible to loss the signal or have inaccuracies up to 100 metres. In urban environment, it has been shown that buildings tend to reflect the signals, hence creating a so-called "multi-path" effect that confuses the receiver. The Figure 13 below illustrates this phenomenon. The receiver will catch both reflected and standard signal, and will calculate different distances from the same satellite, phenomenon that can infer inaccuracies up to 10 metres.

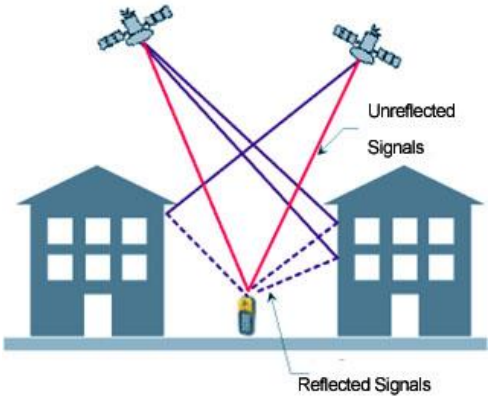


Figure 13 Multi-path effect (credit: precision tracking)

Multi-path effect is currently counterbalanced by calculating the covariance on the received locational-data, which reduces every types of local inaccuracies, as these later are distributed following a Gaussian distribution (McWilliam et al., 2005).

Although it has not been evocated in the literature, another option to prevent multi-path effect would be to use anti-spoofing strategies such as the ones reported by Key, (1995). Indeed, reflected signals arrive to the receiver with a different angle than genuine (non-reflected) signals. As the satellites position is known, it is possible to differentiate the two signals, and therefore reject reflected signals.

These inaccuracies are well known. Unfortunately, they still affect GPS devices. Although it does not impact our standard navigation devices a lot, but to a certain extent, GPS cannot be relied upon as an evidence, nor be used in critical applications such as the self-driving car from Google (Guizzo, 2011). There is currently no solutions to fix these inaccuracies, however, research is currently ongoing, notably (Otero, Otero, & Sánchez, 2009) who propose to use fuzzy techniques for bounding the tolerance of GPS measurements.

2.2.5 Jamming and GPS Spoofing

Tracking applications are becoming more and more popular, especially for security or logistic reasons. However, as these applications grow, means to avoid GPS tracking do likewise. Just like GNSSs, GPS Jammers come from the military. According to (Doherty, 2013), some of these devices have been used during the war between The US Army and the Iraqis. Civilian-grade GPS jammers are used by criminals to steal vehicles whilst blocking the tracker (Last, 2009) or by narco-terrorists to prevent drones to identify the location of marijuana fields (Doherty, 2013). Jammers, see Figure 14, evolve as fast as GPS devices, they have become quite small and can be low powered (Strawn, 2009).

Figure 14 GPS Jammer (credit: lelong.com)

In order to test GPS devices, GPS signal generators can be used (Iqbal & Lim, 2008), however, these devices can be misused and constitute a threat to GPS applications. As jammers cause GPS devices to be ineffective, GPS Spoofing devices trick GPS devices, feeding them with false information (Doherty, 2013). Let us consider a container carried by a truck, with a high value content. Jamming the GPS tracker of the truck would trigger alarms, and appropriate incident-response would stop the attack. Whereas spoofing the signal would go unnoticed and would allow the criminal to hijack the truck, waiting the good moment for an ambush, or to kidnap the driver (Warner & Johnston, 2003).

In order to prevent spoofing, the receiver must be able to differentiate genuine and forged signals. Warner & Johnston (2003) provide a solution to trigger an alarm when the receiver detects suspicious activity. This can be achieved through some kind of authentication coming from the GPS constellation (Pozzobon, Wullems, & Kubik, 2004), or discrimination techniques, as reported by the Volpe report (Volpe, 2001). According to Key (1995), the best anti-spoofing technique is to use antennas that measure the angle-of-arrival of received signals. Since it is merely impossible for the attacker to match the angle-of-arrival from the spoofed signals with the satellites, the spoofed signals can be easily ignored.

2.3 GPS Forensics

In a paper on the future of digital forensics, (S. L. Garfinkel, 2010) has foreseen a problem with the coming prevalence of embedded systems, as these can be much harder to image and investigate. In 2009, N. Beebe noted that because of non-standardised interfaces and structures, embedded systems would represent a list of technical challenges for the forensic investigator (Beebe, 2009). Garfinkel supports Beebe's opinion and points out another challenge, the "increasing prevalence of embedded flash storage". This type of storage can be much more difficult to investigate than traditional hard drives. Garfinkel also reports that multiple devices typically must now be investigated for a single case, which was unusual only a few years ago, where the scope of the forensic investigation was limited to a single computer with a small amount of memory (S. L. Garfinkel, 2010).

GPS navigation systems fall under this category, as a large majority of them use internal flash memory. Moreover, these devices act as mass storage devices, allowing the user to store multiple types of data on it, such as pictures, video and documents, thus making the forensic analysis more complex. Just as multiple types of files can be stored inside navigation devices, GPS data can be found in a wide range of situations, such as pictures or applications on smart-phones. Van Eijk & Roeloffs (2010) states that

being able to link a position with a picture or a timestamp can be invaluable in an investigation.

In 2012, an article published in a UK national newspaper illustrated van Eijk & Roeloffs (2010) words. According to the article (Daily Mail, 2012), an Anonymous affiliated hacker calling himself "w0rmer", broke into four US law enforcement websites. In order to claim his victory, w0rmer published a picture of his girlfriend, holding a message for the authorities, shown in Figure 15.

Figure 15 Incriminating picture (credit: troyhunt.com)

Along with the picture, w0rmer had transmitted his GPS coordinates, which subsequently allowed the authorities to locate and arrest him.

GPS navigation devices are now in common use and are allowing extensive location tracking. The data yield by these devices could help when investigating a range of crimes, from common burglary and theft, to grooming, kidnap and murder by providing a history of a suspect's movements through the tracking of his vehicle or phone (Last, 2009). Furthermore, these data can also be used for digital profiling as remarked by Colombini et al. (2012), who compared GPS satnav devices to "digital diaries". Although this field is fast becoming of great importance, current literature does not address it thoroughly, and investigators often lack of procedures and methodologies to retrieve evidence in a forensically sound manner. This lack of procedure can lead to evidence, inculpatory or exculpatory, being missed (S. L. Garfinkel, 2010).

2.3.1 Structure and Operating of satellite navigation systems

The structure of satellite navigation systems (satnav) is specific to each manufacturer and must be known from the forensic investigator in order to properly investigate the device (Doherty, 2013). Despite minor changes, the overall structure of these devices remains the same (Jones et al., 2008) and is basically composed of a radio equipment (receiver), a CPU to compute the data, along with Random Access and Storage Memory. The device is

operated by an operating system, and interact with the user through an output display, generally tactile. In order to extract the data, or charge the devices, a USB port is generally included, and more and more devices have a Bluetooth interface, allowing them to connect smartphones.

Some of these components can hold valuable data, or at least give to the investigator a good clue on where to search. For instance, the Bluetooth connectivity may not be investigated itself, but it provides information on what could possibly be found on the device, as this connectivity is usually used to connect phones to it and provide some kind of hands free features.

2.3.1.1 Operating system

In his book, Doherty (2013) discusses windows CE as being the operating system typically used by most devices. However, his review is limited to a small amount of devices, thus restraining his view of the area. When investigating TomTom Go 500 and 720, van Eijk & Roeloffs (2010) reported the operating system as typically being a variety of Linux, a view shared by Colombini et al. (2012) who investigated TomTom devices as well. Similarly, most of Garmin systems are Linux based, which can be a great advantage for forensic analysis, as they are open-source.

First, Linux-based operating systems are open-source, which mean that the manufacturer must publish their source-code, as well as the modification they have done in order to adapt the OS for the purpose of the device. Being able to analyse the code behind a device can highlight its structure and some of its hidden features. In their study, van Eijk & Roeloffs (2010) used the open source code to reverse engineer the device and locate where the data is stored in the internal memory. They noticed part of the memory was denied access by the operating system itself. He therefore modified the source code, thus allowing a full analysis of the memory.

Additionally, a study has shown that Linux-based OSs do not use the “Trim” command, used to call the garbage collection process in Solid State Drives (SSDs) which is addressed in the next section. This results in higher probability of data reminiscence within devices running Linux-based OSs (King & Vidas, 2011a).

2.3.1.2 Embedded memory

According to Harrill & Mislan, (2007), Satellites navigation systems are considered as small scale devices. As such, they use volatile and non-volatile memory, and process the data through a CPU. The Random Access Memory (RAM) constitutes the volatile memory, which loses its content when not powered. As such, it is harder to investigate and the acquisition process becomes a critical process that needs to be done before the device run out of battery.

Although it needs a different procedure than for standard non-volatile memory analysis and might be more challenging for the investigator, the data held in this part of the device can be paramount. Indeed, just like in TomTom devices, RAM may contain data of forensic interest such as timestamps, which are never stored in the persistent memory, as reported by the experiment conducted by van Eijk & Roeloffs (2010). At the time of writing, no study addressing RAM forensics has been conducted on Garmin devices.

Conversely, the non-volatile memory represents the most important component of the device, at least from a forensics point of view. It is used to store where the user has been since he bought the device. Several studies have been published on it, but they usually access the memory through the device, which may sometimes update timestamps and therefore impact the integrity of the device (Nutter, 2008). In 2008, (Nutter, 2008) divided GPS devices into three categories:

- With SD cards
- With internal hard drives
- With internal flash memory

However, devices with internal hard drives tend to be rare, as manufacturer tend to prefer internal flash drives. Colombini (2009) also divides the devices into three categories, which seems to be more realistic:

- With internal memory only
- With SD card only
- With SD card and internal memory

2.3.1.3 Flash storage

Over the past few years, flash memory has gained in popularity because of its resistance to shock, power consumption (Sansurooah, 2009), performance and reliability (Huang, Chang, Kuo, Hsieh, & Lin, 2008). Flash memory is also called "solid state memory" and is a type of electrically erasable programmable read-only memory (EEPROM) (Sansurooah, 2009) which can be available in two types; NAND-based or NOR-based. Both these types share a common chip architecture, illustrated by the Figure 16.

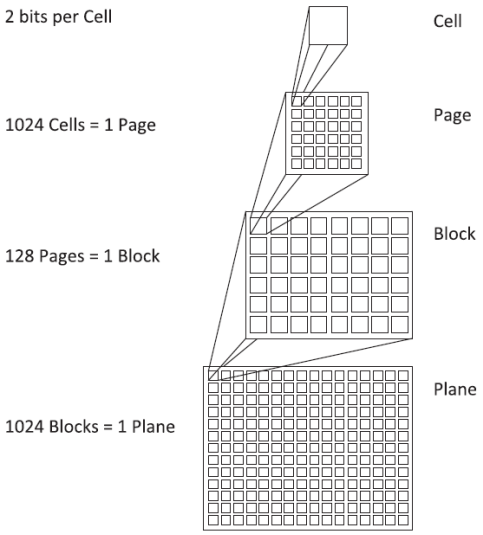


Figure 16 Flash chip architecture (credit: KING & VIDAS, 2011)

As shown in the Figure 16, a flash memory chip is composed of planes. Each plane is composed of blocks, each block is composed of pages which are composed of cells (King & Vidas, 2011a). NAND and NOR memories differ in the way cells are interconnected (Fiorillo, 2009; King & Vidas, 2011a), and by their access patterns (Sansurooah, 2009). Whilst NOR-based memory uses random access and can retrieve information at a byte level (Harrill & Mislan, 2007), NAND memory read and write data on a page basis (Fiorillo, 2009; Huang et al., 2008). This feature makes NAND-flash reliant on an external RAM, as illustrated by the following Figure 17.

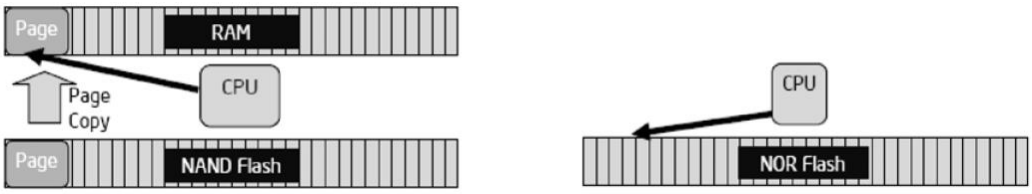


Figure 17 Access pattern of NAND and NOR memories (credit: FIORILLO, 2009)

The figure points out the need for NAND-based memory, to have an external RAM to operate properly. These characteristics have a strong impact on the usage of these types of memory. In 2011, the blog Embedded Domain published a comparative study on NAND and NOR memory. The following Figure 18 reports their findings and gives a highlight on the possible usage of these memories.

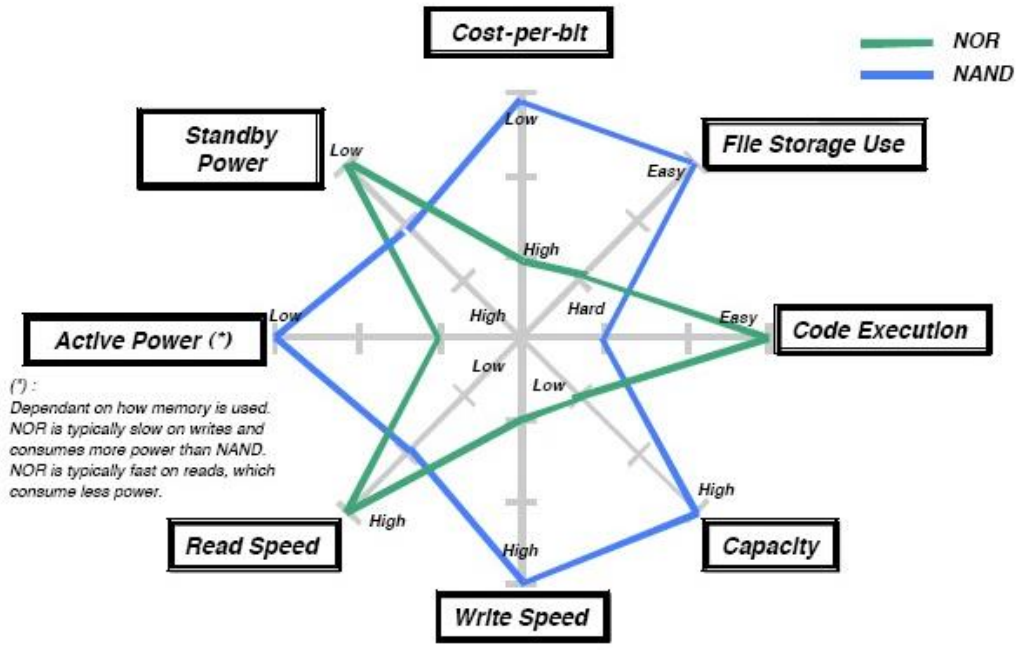


Figure 18 Usage of NAND and NOR memories (credit: Embedded Domain)

Additionally, according to Fiorillo (2009) NAND-based memory tend to be cheaper than NOR whilst offering a similar performance. However, it is less stable and needs a supporting RAM to work. As a matter of fact, NOR-based memory is generally used to store the operating system, whereas and NAND-based memory would be privileged for the storage capabilities of the device (Harrill & Mislan, 2007).

Another important characteristic of flash memory is its inability to program a value from "0" to "1"(Fiorillo, 2009; Sansurooah, 2009). In fact, the initial state of the memory is all 1s. Writing the memory consists in program the value from "1" to "0". If an update is needed, the information will be rewrite somewhere else inside the memory, and the former location will be marked as invalid (Fiorillo, 2009). When the numbers of invalid blocks reach a certain threshold, a background process, called "Garbage Collection", reclaims the blocks invalidated and erases them properly (setting them to all 1s). From a forensic point of view, "garbage collection" makes data retrieval a lot harder than with standard non-volatile memory (M. Breeuwsma & Jongh, 2007; Fiorillo, 2009; Huang et al., 2008; King & Vidas, 2011a; Sansurooah, 2009).

However, King & Vidas, (2011) published a study in which they claim that solid state disk data retention relied on the Operating System in use. They conducted an experiment in which they compared data retention under the different OSs, with different Solid State Drives, and with different type of usage. Their results are resumed in the following Figure 19.

Test	Control	Imation1	Corsair1 (TRIM)	Crucial1 (TRIM)	PQI1	RiData1	OCZ1 (TRIM)
Large File, Low Usage, Win7	100.00%	100.00%	0.00%	0.00%	71.23%	100.00%	0.00%
Large File, Low Usage, WinXP	99.99%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Large File, Low Usage, Linux	99.99%	99.98%	100.00%	99.99%	99.98%	100.00%	100.00%
Large File, High Usage, Win7	100.00%	100.00%	0.00%	0.00%	88.60%	100.00%	0.00%
Large File, High Usage, WinXP	99.99%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Large File, High Usage, Linux	100.00%	99.98%	100.00%	100.00%	99.98%	99.98%	100.00%
Large File, Format, Win7	100.00%	100.00%	0.00%	0.00%	100.00%	100.00%	0.00%
Large File, Format, WinXP	99.99%	100.00%	0.00%	0.00%	0.00%	99.67%	100.00%
Large File, Format, Linux	99.86%	100.00%	0.00%	77.88%	0.00%	3.83%	99.87%
Small File, Low Usage, Win7	99.98%	0.00%	25.53%	27.54%	0.00%	99.98%	25.53%
Small File, Low Usage, WinXP	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%
Small File, Low Usage, Linux	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%
Small File, High Usage, Win7	99.98%	99.98%	27.54%	26.28%	99.98%	99.98%	25.53%
Small File, High Usage, WinXP	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%
Small File, High Usage, Linux	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%
Small File, Format, Win7	0.00%	26.96%	24.46%	0.00%	0.00%	24.63%	0.00%
Small File, Format, WinXP	96.57%	57.21%	24.69%	0.00%	0.00%	54.27%	49.03%
Small File, Format, Linux	99.98%	99.98%	0.00%	99.98%	99.98%	0.00%	99.98%
Average	93.86%	87.62%	49.74%	56.93%	69.60%	81.97%	66.28%

Figure 19 Percent blocks recovered by test and OS type (credit: KING & VIDAS, 2011)

The results show that the recovery percentage is first related to the type of controller. Indeed, data recovery seems harder in storage using controller allowing the ATA/SCSI TRIM command, which allows to the OS to call the garbage collection on a certain block (King & Vidas, 2011a). The second interesting result is that even when TRIM was enabled, the recovery process reached a high success level. King explains this result by reporting that Ubuntu has a lack of TRIM support, and uses quick format procedure.

The OS and the type of controller used by the flash storage are therefore crucial factors to consider when investigating embedded devices such as Satnavs.

2.3.2 Forensic acquisition of satellite navigation systems

Forensic acquisition of a device is typically a delicate process that aims to acquire digital evidence in a way that "ensures its authenticity and integrity" (Casey, 2011). Part of the preservation process, considered as a key concept by the DFRWS (Palmer, 2001), the device must conserve its origin state after the procedure. The following section reviews the different techniques used to acquire satellite navigation devices among the dedicated literature. About the categories introduced earlier, this section will first cover SD card acquisition, then flash memory and finally RAM.

2.3.2.1 SD Card

As reported by Colombini (2009), some navigation systems use SD cards for principal persistent storage, or as an extent of memory. This memory is likely to hold user related data and may include potential evidence that is not related the GPS usage, for example the uploading of non GPS data such

as pirated movies (Strawn, 2009). SD card is easily removable from the device, therefore, best practices would be not to power on the device, and take a copy of it through a write blocker.

In 2008, Hannay published a paper dedicated to SD Card forensic acquisition. The methodology he designed consists of a sequence of simple steps, aiming to acquire the non-volatile memory contained on the device SD card in a non-invasive way, and verify its integrity through hashing algorithms. A bit-stream acquisition is then performed, following the designed methodology, using the Linux "dd" command and a SD card reader converted in a write blocker for the occasion. The Figure 20 shows the SD card reader converted in write-blocker by Hannay. To do so, he bended the pin dedicated to the data input of the SD card, hence making it physically unable to write on the SD Card. Hannay did not analyse the content of the memory he acquired, but his study showed that powering on the device involves data being written on the SD card, even though this latter has its write protect tab set. In 2008, he wrote another article, aiming to analyse the data that could be found on a TomTom one and performed the same process to acquire it.

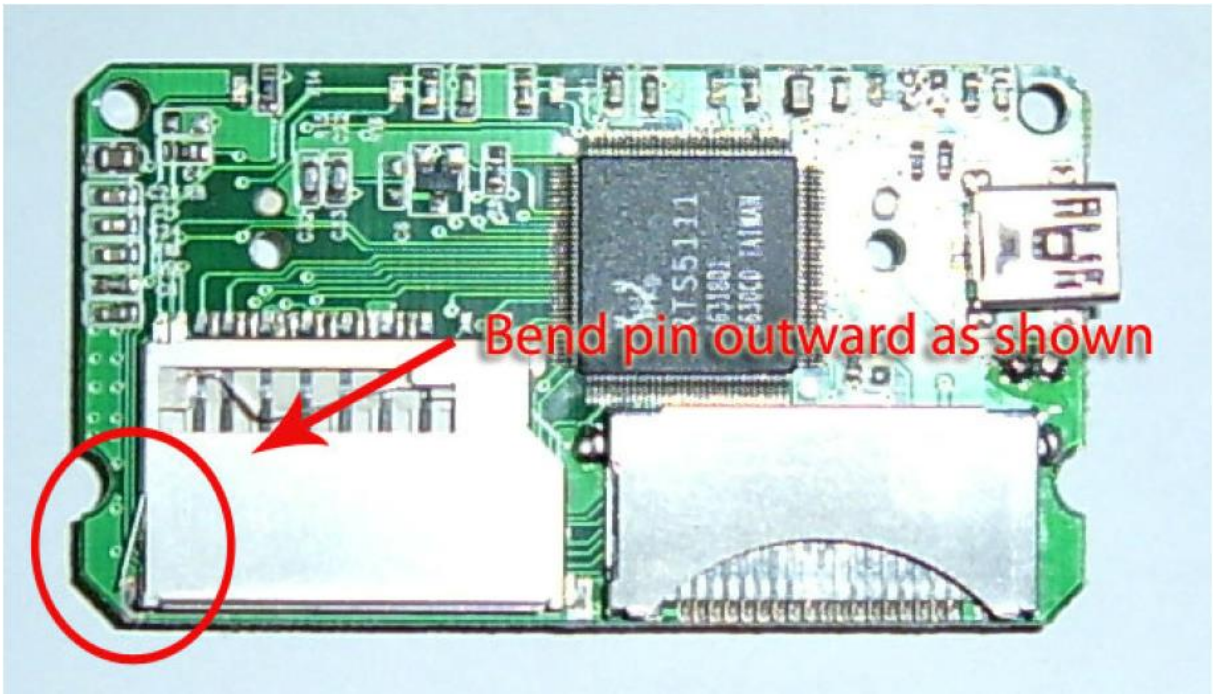


Figure 20 Modified SD card reader (credit: HANNAY, 2008)

(Lemere & Sayers, 2009) recommend using a dedicated write blocker as shown in Figure 21, it will have the same result as Hannay's approach, although more expensive.

Figure 21 UltraBlock USB 3.0 Forensic Card Reader (credit: digital intelligence)

(Lim, Lee, Park, & Lee, 2012) report the use of FTK imager to acquire the SD card, however, unlike (Hannay, 2008; Lemere & Sayers, 2009), Lim did not use any specific device to acquire the memory, and used the device itself (an XROAD navigation v7) to do so. Doing so present a huge risk to compromise the integrity of the system, as simply powering on the device will induce access to the memory. Moreover, Lim did not use any Faraday cage of any sort, therefore, the device, once on, might have acquire a GPS fix, hence altering the memory. Colombini (2009) did the same mistake and acquired the data through the device. It has to be noted that once a GPS device is powered on, its first process will be to get a GPS fix for its position. The obtaining of this fixes results in the alteration of the memory, hence the device integrity. Therefore, a Faraday cage must be used to prevent GPS signal to reach the device (Jones et al., 2008; Lemere & Sayers, 2009; Nutter, 2008; Willassen, 2005).

2.3.2.2 Flash Memory

Acquiring flash memory tends to be a much harder process than the SD card, as it cannot be removed from the device. This problem does not only concern satnav forensics, but advantages brought by flash memories make them ubiquitous in embedded systems. Furthermore, it seems there is no documented standard procedure to acquire internal memory (Willassen, 2005). Fiorillo (2009) divides flash memory acquisition into two categories: physical and logical acquisition [Figure 22]. Concerning satnav devices, logical acquisition consists in mounting the device as a mass storage device, and retrieves, with a basic drag and drop, the files that may contain information. Mounting the device may influence the logical integrity of the system, and therefore shall not be used without a write-blocker. Logical acquisition is a fast and easy way to extract information from a device. If the information the investigator seeks is located inside a known file, this might be the best approach to consider. However, as pointed out by Nutter (2008), significant amounts of data can be retrieved in unallocated clusters, which cannot be accessed without a bit-per-bit copy of the memory. Since retrieving deleted files within the memory can be paramount to

investigators, it is better to consider a physical acquisition, which will allow this bit-per-bit procedure.

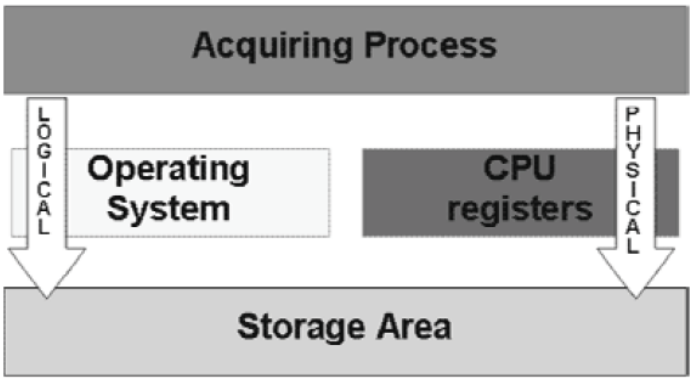


Figure 22 Logical Vs Physical Acquisition (credit: FIORILLO, 2009)

In a study on flash data recovery, (M. Breeuwsma & Jongh, 2007) identified Flasher tools as certainly the less invasive technique to extract flash memory of a device. These tools are devices that will upload what is known as "flash loader" software into the RAM and execute it to get a low-level access to the memory. It has to be considered that the RAM will be damaged. As such, extracting the RAM first would be essential. Flasher tools however seem to be more common for cell-phone forensics rather than for GPS forensics. Similar tools such as Device seizure from Paraben (Paraben, 2014) can also be used, therefore allowing investigators to acquire GPS devices without impacting the logical integrity of the system.

JTAG ports are test access ports that are generally used to debug embedded systems (Greenberger & Homayoon, 1994). However, it can access flash memory and therefore being used to image flash storage (I. M. F. Breeuwsma, 2006; Fiorillo, 2009; King & Vidas, 2011a; Sansurooah, 2009; Willassen, 2005) or RAM memory (van Eijk & Roeloffs, 2010). The copy can be a long process, Van Eijk reported 40 minutes to image a 32MB RAM; at a constant pace, the process will need 21.3 hours to image 1 GB. As the technique might affect the physical integrity of the device as well, the technique should not be used unless there is no other choice.

Another way to extract the memory is to de-solder flash memory chips with the appropriate equipment and read them with a memory chip reader (M. Breeuwsma & Jongh, 2007; Willassen, 2005). The advantage of this technique is that it bypasses the OS, thus avoiding possible logging mechanisms likely to influence the memory. However, as remarked by Dickson, (2014), such techniques are rather expensive and often cannot be used for investigations on a daily basis.

(Fiorillo, 2009) also reports that it is possible to get data from the flash memory of a system using infrared and Bluetooth interfaces using the OBEX protocol. This approach however can only retrieve small part of information, and therefore could not be used to acquire the entire memory.

The techniques formerly presented are however rarely used in practical situations, where investigators acquire those devices generally by connected them to a computer with a USB cable. With regards to "physical acquisition", investigators do not mount the device, and turn it on, then they are able to image the flash memory through commands like "dd", or software like FTK Imager (AccessData, 2014; C. Colombini, 2009; Iqbal & Lim, 2008; Jones et al., 2008; Lemere & Sayers, 2009; Nutter, 2008). Investigators must however be aware that turning on the device might alter the data on the memory. In his study, Nutter (2008) reported that turning on his TomTom device had updated four different files timestamps.

2.3.2.3 RAM

Despite Random Access Memory can hold as much valuable data as persistent storage, few researches have been done on the subject. (van Eijk & Roeloffs, 2010) investigated TomTom Go Series RAM and found timestamps that could be linked to positions, hence providing information that could be essential in case of an investigation. Their study first investigated the different scenarios that could lead to a power loss. Then they used JTAG ports to acquire the memory, following the procedure exposed in (I. M. F. Breeuwsma, 2006). Additionally the study reports that if a bootable system image were to be loaded on the SD Card of the device, the navigation system would boot on that image in priority. The author then loaded a small-modified Linux distribution on the system, allowing him to extract the RAM. Note that this technique could also be used with persistent storage.

Another study conducted by (Rabaiotti & Hargreaves, 2010), proposes a software exploit approach to extract the RAM of an embedded system. Indeed, the study proves that it is possible to exploit a buffer overflow vulnerability to extract the entire RAM out of an XBOX console. Although the scope of its experiment is limited to gaming consoles, Rabaiotti believes that the process would work with GPS devices as well.

2.3.3 Forensic analysis and files of interest

Memory embedded on portable systems such as GPS keeps growing in size, making difficult forensics investigations. Forensic analysis is a time-consuming process, which cannot afford to take every file into consideration (S. L. Garfinkel, 2010). Optimising this process is possible by documenting the inner file structure of the device, and knowing where the information of

interest might be hold. However, as reported by Jones et al., (2008) since GPS devices act as mass storage devices, they are likely to hold all types of data, and not only locational data. Investigators might come across data related to conventional cyber-crime, such as pirated movies, and should keep in mind this eventuality.

With regards to the common files that can be found on such systems, the current literature regularly mentions POIs (i.e. points of interests) and typed destinations as potential evidence (C. Colombini, 2009; Last, 2009; Lemere & Sayers, 2009). Hannay, (2008) published a study in which he listed the recoverable information on Tom-Tom devices, depending on their operational mode. These experiments showed Tom-Tom devices were storing the routes computed by the device, as well as the favourite locations stored by the user. However, this information has its limitations, as there is no way to tell where the user has actually been. Another study conducted by C. M. Colombini et al. (2012) permitted to recover where the user has actually been, by installing a "logging enabler" on the device.

Since they can put someone on the crime scene within a time frame, timestamps are also of great value to investigators (Ball, 2008).Tom-Tom devices use this information but does not store it (Nutter, 2008), however, it is possible to recover some of them by inspecting the RAM of the device (van Eijk & Roeloffs, 2010).

As the devices evolve, they bring new features that may come along its lot of information. Bluetooth capability for instance, makes the device storing information about contacts, emitted and received calls or text messages (Ball, 2008; C. M. Colombini et al., 2012). Additionally, as pointed out by C. M. Colombini et al., (2012), configuration files may contain information useful to establish a behavioural profile of the user, such as the language he speaks, his common whereabouts and so on.

2.3.4 Legal issues for GPS data

The use of GPS data for investigative purpose has become widespread, as it provides valuable information on a subject's movements (C. M. Colombini et al., 2012). This information can be used for a variety of purposes, such as studying the modus operandi of a criminal, or help to resolve crimes related to paedophilia, theft, robbery and so on... Recently, GPS data has been used in courts to verify alibis, or charge suspects. This usage raises questions over the reliability and accuracy of GPS data (Iqbal & Lim, 2008; Lallie & Benford, 2011), and the ethics in making tracking systems admissible in court (Hubbard, 2008).

2.3.4.1 Reliability and admissibility of GPS Data

In 2012, GPS data has been used as compelling evidence to charge sex offender David Lee (David Lee Vs Commonwealth, 2012), and Hubbard (2008), witnessed more than 70 cases using GPS data in court of law within a period of three years. Cases involving GPS data are becoming more frequent (Hubbard, 2008). However, as pointed out by Iqbal & Lim (2008), the legal literature does not question the accuracy nor the authenticity of GPS signals. Drivers are acquitted of speeding charges based on their satnavs (Williams, 2008), whilst devices reporting speeds of 3000000 mph are also admitted in court (Iqbal & Lim, 2008).

"DNA just puts the accused at the scene. Reliable GPS data puts the suspect there between 9:42 and 10:17 p.m." Ball said (Ball, 2008). However, non-reliable GPS data can lead to injustice, with people wrongly charged and suspects exonerated due to false alibis. This report presented situations where GPS data could not be trusted, nor be considered as accurate (Parkinson, 1997; Theiss et al., 2005). It also has presented situations where people were able to modify the data held inside their devices, thus impacting the investigation outcomes (Iqbal & Lim, 2008; Lallie & Benford, 2011). Even though this information can mislead intentionally or unintentionally a case, legal discussions seem to ignore the problem and rather focus on ethical concerns aroused by GPS tracking, influencing the fourth amendment (David Lee Vs Commonwealth, 2012; Koppel, 2009; McGrath, 2011).

2.4 GPS Anti-forensics

"The criminal genius is a creature of comic books and movies." (Ball, 2008). The lack of accuracy of GPS data, and its vulnerability to anti-forensic techniques raise concerns about whether or not such data should be admissible in court. Whilst the research community tries to warn about the impact of anti-forensic techniques (Harrill & Mislan, 2007; King & Vidas, 2011b; Lallie & Benford, 2011; Strawn, 2009), practitioners, based on their in-the-field experience, believe that criminals typically would not have the knowledge to use such techniques.

However, anti-forensics techniques exist, and, according to Nolan et al. (2005), criminals are aware of the residential data that may reside on electronic devices. Solutions can be envisaged, and must be, in order to prevent criminals to create their evidences as their will. Concerning GPS devices, anti-forensics can be considered at two different levels. First, there is the internal memory, where evidence can be hidden or destroyed, then the GPS data, which can be modified, or forged.

2.4.1.1 Internal memory

Operating Systems use memory, regardless the underlying technology. To do so, these technologies must provide a way for the OS to interface with the memory. Solid state memories use a feature called "Flash Translation Layer" (FTL) for this purpose (Huang et al., 2008). According to King & Vidas (2011), Solid State Drives (SSDs) may relocate data, without the OS reporting it. This feature could be misused in an attempt to hide data. Furthermore, their study demonstrated that manipulating the TRIM command might trigger the garbage collection and therefore, wipe a whole disk. Although TRIM is a command related to the ATA interfacing scheme, equivalents of the TRIM command are commonly found among the other types of interface (SCSI, SD). These characteristics can be used for anti-forensics, allowing a criminal to hide data inside his device, or to wipe its whole memory within seconds (King & Vidas, 2011a).

2.4.1.2 Geo-positional anti-forensics

As stated by Nolan et al. (2005), there is no doubt that criminals are now aware of the evidence an investigator is able to recover from the devices they carry. If Ball, (2008) is wrong, that would mean that these criminals are able to manipulate these devices in a way they provide alibis instead of exculpatory evidences when investigated. In 2008, Iqbal & Lim investigated GPS tracking systems, in order to see if it was possible to edit the data stored inside them. The study concludes that there is no method to validate the data, or verify the authenticity of the data recovered.

Another study leaded by Lallie & Benford (2011) obtained the same results, by extracting data out of an IPhone, editing it, and then put back the modified data in lieu of the genuine data. Both studies question the reliability and therefore the liability of these evidences, which could have been somehow compromised before being considered in a trial.

The concerns raised by the forensics community regarding anti-forensics techniques are not shared by the practitioners. Ball, (2008) considers the criminal genius as utopic and does not consider anti-forensics as a threat. An interview conducted with NHTCUS (i.e. National Hi-Tech Crime Unit in Scotland) representative Mike Dickson outlined the same conclusions. According to M. Dickson, criminals are more likely to send someone driving around with their GPS device than manipulating the data inside it. However, it is important to know what is possible on this type of devices, in order not to be surprised if such event were to happen.

2.5 Garmin satellite navigation systems

Among the GPS forensic literature, only a very small section considers the firm Garmin, and yet it is considered the market leader in some areas. Studies tend to be focused on TomTom devices which are predominately used for vehicle navigation (Dickson, 2014). This section investigates the state of the art of Garmin forensics; the research that has been performed compared to other devices; considers the results from current research; and looks at the challenges related to this area of navigation devices forensics. The study conducted by (Jones et al., 2008) in 2008 seems to be the first to tackle Garmin devices. Three Garmin models have been investigated, a Nüvi 200W, a Nüvi 310 and a StreetPilot 510c. A TomTom GO 710 was also part of the study. The results of the study report the discovery of one GPS artefact in particular in Garmin devices: the "Current.gpx file", whereas Tom-tom contained several GPS data files. The analysis of this file showed that it contained the favourite locations entered by the user in a XML format. (Jones et al., 2008) concluded that further research was needed on these types of devices.

In 2012, in a study on digital profiling through GPS based evidences, (C. M. Colombini et al., 2012) investigated a Garmin device, but unfortunately did not analyse the findings. The files and folders found on the device are however listed, and the same Current.gpx was found, along with a folder called "archive". Both were found in a folder "gpx", located at the root of the device.

Blog articles were found, providing further information on Garmin devices. In 2008, Electronics360 disassembles a Garmin Nüvi 200W, hence revealing the internal components [Figure 23 and Figure 24].

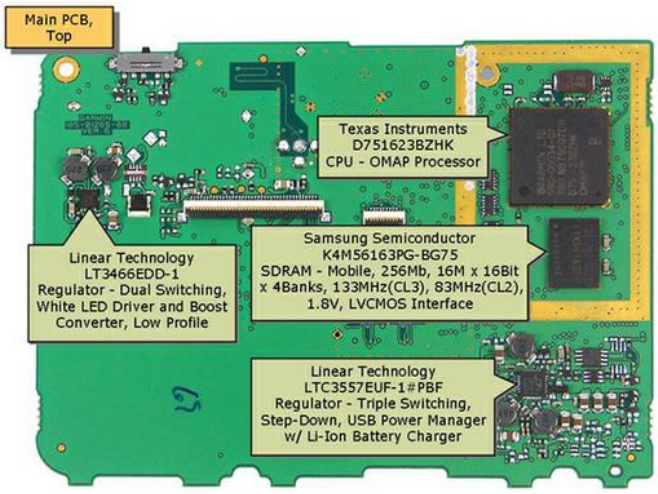


Figure 23 Nüvi 200W: PCB, Top side (credit: electronic360)

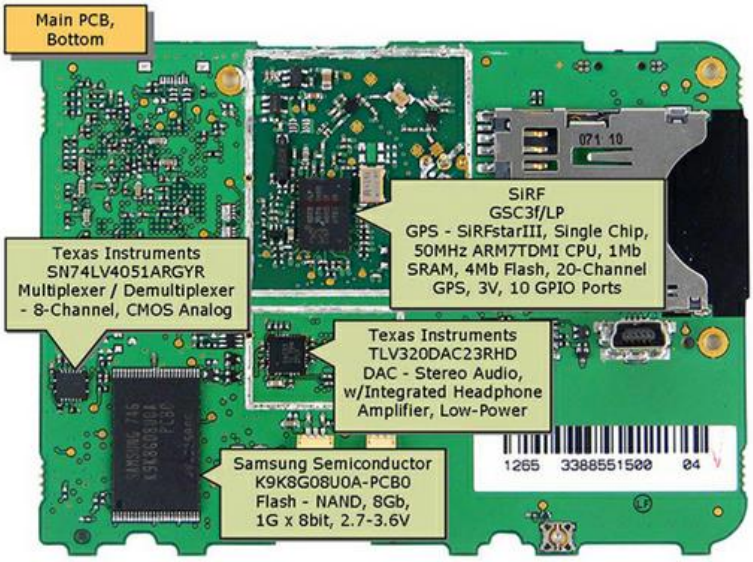


Figure 24 Nüvi 200W: PCB, Bottom side (credit: electronic360)

As shown in Figure 24, the Garmin Nüvi 200W uses a NAND flash memory, which, as stated in section 2.3.1, can be subject to alteration due to the garbage collector and wear-levelling mechanism.

Then the blog “Forensics from the sausage factory” posted an article about Garmin forensics. It presents the outcomes of an investigation on a Nüvi 200, and the same "Current.gpx" file, introduced earlier by Jones’s study. According to the author, "Recently found location" did not appeared to be saved within the user accessible memory (Forensics from the sausage factory, 2009).

As the literature and the blogs seem to suggest, Garmin typically did not store much data that easily could be of use to an investigator. However, since 2010, things seem to have changed. In his blog, (Lehr, 2010) reports on a tracking feature, enabled by-default on most Garmin devices. According to him, there is no need for the user to enter a destination. The device starts logging its position as soon as it is turned on. Garmin called this feature the “Triplog”, and defines it as being the “electronic equivalent of laying down a breadcrumb trail to mark the path that has been travelled” (Garmin, 2014b).

From a forensics point-of-view, such feature has a paramount importance. Actually, Garmin devices are rarely turned off, a short pressure on the power button will only turn off the screen (like a smartphone). Moreover, the battery expectancy in sleep mode can be quite long. Therefore, it can be inferred that people, using regularly their Garmin device for navigation purpose, are tracked by the feature at all times, and that all their trips have been logged inside the navigation system. Lehr reports having seen devices with 6 months of history. Garmin, however, reports that 10000 points can

be stored within a Triplog file, and up to 20 files can be archived on the device (Garmin, 2014b). What is interesting is that the file containing that information is still called "Current.gpx". Lehr suggests that the file contains the most recent log, and the folder "archive" contains older logs renamed "1.gpx", "2.gpx" and so on.

Another article on forensicsblog.com confirms this behaviour on recent Garmin devices. Additionally, files with an extension ".db" have been found, suggesting the use of SQLite databases (DBs). As far as the author is concerned, those files do not have forensic value as they are sparsely populated, but further research is needed in order to see exactly how these files are used by the system (fork(), 2013). The author extracted the data and plotted them on a map using Google earth [Figure 25].

Figure 25 Data retrieved from a Garmin device on Google earth (credit: fork())

2.6 Conclusion

The first part of this literature review provided background information on the origin of GPS, its initial purpose and how prevalent it has become. By reviewing GNSS principles and limitations, it also showed that GPS data might not be as reliable as it seems to be, due to inaccuracies and systems used to disrupt GPS signals (Iqbal & Lim, 2008; Theiss et al., 2005).

Conversely, the data contained inside Satnavs can be of crucial value, and mature methodologies aiming to investigate these devices have not been yet well defined (Harrill & Mislan, 2007). The literature surrounding GPS forensics remains focused on Tom-Tom devices, disregarding other brands such as Garmin. The section 2.3 investigated the current techniques and challenges related to Satnav forensics, regardless of the brand. Studies

related to forensic acquisition of GPS devices highlighted that the successfulness of the imaging process rely on the device itself. As underlined by Nutter (2008), small interactions between the user and the device may compromise its integrity. Other techniques are conceivable, but they are mainly based upon peculiar characteristics of GPS devices and might not be reproducible (Rabaiotti & Hargreaves, 2010; van Eijk & Roeloffs, 2010).

The section 2.4 investigated the literature related to anti-forensics. Even-though anti-forensics have not been yet performed on Garmin nor Tom-Tom devices, their inner-structure makes them potentially vulnerable to it. Studies showed that locational artefacts of other device such as smartphones were vulnerable to anti-forensic techniques. Further research should therefore be conducted on GPS devices, to evaluate the risk of locational data being manipulated.

The last focused on the brand Garmin, which seems to be neglected by both forensic community and investigators. Peer reviewed studies related to these devices are rare, and yet only a couple of forensic specialized blogs discussed this topic. The lack of knowledge concerning these devices may lead to mistakes that could make evidence ineligible in a court of law (S. L. Garfinkel, 2010). Based on similar studies on Tom-Tom devices, experiments should be conducted on Garmin devices, in an attempt to highlight how they operate and store location-tracking data. The structure of Garmin devices must be clearly defined, and the behaviour well understood in order to avoid altering the device memory and being able to recover the most from it.

Chapter 3 Experimental design

3.1 Introduction

As highlighted by the literature review, there is a lack of understanding and research concerning Garmin GPS devices. How they operate and manage their data has not been yet documented by the research community. Additionally, acquisition and analysis techniques formerly used for TomTom devices might be inappropriate or inefficient for Garmin GPS. In an attempt to optimize the overall forensic investigation procedure, experiments have been designed and divided into three main categories; "Acquisition", "Analysis" and "Anti-forensics". Each of these categories contains a certain amount of "research questions" (RQs), which are used to define the scope of the experiments.

Forensic acquisition can be performed with different techniques (van Eijk & Roeloffs, 2010), which will have a different impact on the logical or physical integrity of the devices (Nutter, 2008). To highlight these consequences, the first category investigates the different methods and tools that can be used to image the memory of Garmin devices.

As stated by S. L. Garfinkel (2010), the lack of knowledge concerning a device might lead to evidence being routinely missed by investigators. The second category aims therefore to document how Garmin devices operate and store their data. This category also aims to evaluate how likely a data is to remain inside the memory with the passing of time.

The last category addresses the question of anti-forensic techniques within Garmin devices. Although the study was conducted on IPhones, Lallie & Benford (2011) showed how locational data can be manipulated without leaving traces. This last category's purpose is therefore to study the achievability of anti-forensic techniques on Garmin devices, with a focus on data modification.

This chapter is divided into four sections. The first one introduces the devices that will be used throughout the experiments, whereas the second, third and fourth sections are dedicated to the aforementioned categories, "Acquisition", "Analysis" and "Anti-forensics" respectively.

3.2 Devices considered

The experiment designed in this chapter is conducted on a set of three Garmin navigation devices, all of them from the Nüvi range. Additionally, a fourth device may be used in some experiment, acting as a reference. The devices are a Nüvi 1340, a Nüvi 2515 and a Nüvi 2595. The reference device is a Nüvi 2595 as well. The characteristics of these devices are described below.

3.2.1 Nüvi 1340

Release date	: 2009
Data cards	: Micro SD
Battery life	: 4 hours
Memory type	: Solid State (Flash)
Memory size	: ≈4 GB
Bluetooth	: No
Waypoints	: 1000
Triplog feature	: NC
Park position	: NC

Figure 26 Nüvi 1340 (front)

Figure 27 Nüvi 1340 (back)

3.2.2 Nüvi 2515

Release date	: 2011
Data cards	: Micro SD
Battery life	: 2.5 hours
Memory type	: Solid State (Flash)
Memory size	: ≈2 GB
Bluetooth	: yes
Waypoints	: 1000
Triplog feature	: yes
Park position	: yes

Figure 28 Nüvi 2515 (front)

Figure 29 Nüvi 2515 (back)

3.2.3 Nüvi 2595

Release date	: 2011
Data cards	: Micro SD
Battery life	: 2.5 hours
Memory type	: Solid State (Flash)
Memory size	: ≈8 GB
Bluetooth	: yes
Waypoints	: 1000
Triplog feature	: yes
Park position	: yes

Figure 30 Nüvi 2595 (front)

Figure 31 Nüvi 2595 (back)

3.3 Acquisition

Although the analysis can be conducted on the device itself, it is more common to acquire a copy of the memory for further analysis. As data can be lost, or altered and therefore not recognized as evidence, the "Acquisition process" is a paramount phase in a digital forensic investigation (Carrier, 2005). With regards to Garmin devices, the literature reviewed did not addressed the acquisition procedure itself in depth, and usually relies on well-known acquisition software such as FTK Imager (AccessData, 2014).

The intent of this section is therefore to design a set of experiments aiming to evaluate the tools and techniques that can be used to image Garmin devices in a forensically sound manner, with regard to the behaviour of the device. The experimentation design is driven by a core question, and aims to address a set of RQs. This section is therefore divided accordingly into two sub-sections, the first describing the main objective of this set of experiments and its related RQs, the second describing the experiment themselves.

3.3.1 Research questions

In order to address the needs of this study, the experiments must be designed following a main objective, which is driven by the overall aim of the research; acquire the data held by Garmin navigation systems whilst preserving their integrity. This objective is supported by a set of RQs, which are inspired by the literature reviewed. As highlighted by the blog fork() (2013) on Garmin systems and a study published by Nutter (2008) on Tom-Tom, even minor interactions with devices can have an impact on their memory, hence altering the evidence. The RQs listed in Table 2, therefore

aim to identify those interactions through the experimentation, in an attempt to raise the awareness of forensic investigators. They address two different subjects, RQ1 to RQ6 are related to the behaviour of the device, whereas RQ7 and RQ8 are more focused on the tools and techniques used to perform the acquisition.

Core objective: *"Acquire the data held by Garmin navigation systems in a forensically sound manner"*

Table 2 RQs related to the Acquisition process

Codes	*Research questions and hypothesis*
Acq-RQ1 *Acq-RQ2*	*"Does turning on (RQ1)/off (RQ2) a Garmin device has an impact on its integrity?"* As it has been pointed out by the literature, some devices may log the time at which they have been turned on/off (fork(), 2013). This behaviour has been observed on a Garmin Nüvi 1490, but the hypothesis is that this behaviour is likely to be present in other model of the brand.
Acq-RQ3	*"Does connecting the device to another entity via USB has an impact on its integrity?"* Likewise, a study conducted by Nutter (2008) on Tom-Tom navigation systems showed that timestamps were updated when the device were connected to a computer. With regard to Garmin devices, no document confirms nor disproves such behaviour.
Acq-RQ4 *Acq-RQ5* *Acq-RQ6*	*"Does leaving the device turned on has an impact on its integrity?" (RQ4)* When turned on, GPS devices keep trying to obtain a GPX fix, in order to synchronize their clock and be ready to navigate. This information can be stored in its RAM or its internal memory. This behaviour has been noticed on Tom-Tom devices, and reported by several studies (C. Colombini, 2009; LeMere & Sayers, 2009; Nutter, 2008), it is assumed that such behaviour may be found on Garmin devices as well. *"Does leaving the device turned on away from GPS signals has an impact on its integrity?" (RQ5)* LeMere reports that using a faraday bag or cage can prevent this kind of behaviour, as the GPS fix is never obtained, thus preventing the device from updating the data (LeMere & Sayers, 2009). This should be similar in Garmin devices. *"Does leaving the device turned on connected to a computer has an impact on its integrity?" (RQ6)* Nutter reports another way to prevent a Tom-Tom device from trying to get a GPS fix, by connecting the aforementioned device

	to a computer. The device will use "mass storage mode" in which it does not use its locational features. The hypothesis is that Garmin devices may act the same.
Acq-RQ7	*"What forensic imaging tools can be used to efficiently acquire Garmin devices?"* Apart from the device's behaviour, another key component to consider is the acquisition tool itself. Most of the literature investigating Tom-Tom devices use FTK Imager, or the "dd" command (C. Colombini, 2009; Jones et al., 2008; LeMere & Sayers, 2009; Nutter, 2008). However, no evaluation has been done specifically for GPS devices.
Acq-RQ8	*"Is there a way to image the device, without making a USB connection?"* As pointed out by the RQ3 defined earlier on, connecting the device through USB might have an impact on its integrity. In order to prevent any alteration, it is important to evaluate other possibilities to image the device.

3.3.2 Experiments

The core objective previously defined is a guiding thread to the design of the experiments. The RQs divide this objective into smaller questions, ensuring the test set is as exhaustive as possible. The result of this design is a set of three experiments, addressing the eight RQs formerly introduced. Each of these experiments will be carried out on the "Garmin set", the devices described in Section 3.2.

3.3.2.1 Experiment n°1: Evaluation of forensic imagers

RQs related: Acq-RQ7

This first experiment aims to evaluate the most popular imaging tools when dealing with Garmin devices. Each tool has to image the Garmin set, and will be evaluated on the successfulness of its copy and its execution speed. The tools considered for this experiments are as below:

- FTK Imager v 3.1.4.6 – AccessData
- EnCase Forensic Imager v 7.09.00.111 – Guidance Software
- GUYMAGER v 0.7.1-1 – Caine 5.0 Live CD
- "dd" command – Caine 5.0 Live CD

The experiments will be carried out on the following computer:

Table 3 Computer used for experiment n°1

PC Notebook

Model	Lenovo T420s
OS	Windows 7 SP1 32bits
RAM	4.00 GB
CPU	Intel(R) Core(TM) i7-2620 @ 2.70GHz
Storage	SSD 160 GB

The following metrics are taken into account for the evaluation of the tools:

- Successfulness of the copy (cryptographically verifiable)
- Execution speed

3.3.2.2 Experiment n°2: Boot with another OS

RQs related: Acq-RQ8

As it has been remarked by Nutter (2008), connecting a GPS device to a computer may result in a timestamp being updated somewhere in the memory. This behaviour is due to the operating system present inside the device. To prevent this, van Eijk & Roeloffs (2010) made a Tom-Tom device boot with another operating system, specifically crafted to access and copy the RAM. This is possible because Tom-Tom devices boot in priority on the SD Card, and then on their internal memory. The present experiment aims to assess whether or not such technique is possible on Garmin devices. To do so, a similar experiment to the one conducted by van Eijk & Roeloffs (2010) is designed, involving the following steps:

1. Select a lightweight Linux distribution.
2. Create a bootable SD card.
3. Copy the Linux distribution onto the SD card.
4. Assess whether or not the device try to boot from the SD card.

This experiment differs a bit of the original experiment in that the distribution does not aim to copy any of the data. Nevertheless, making the device avoiding its original bootloader, even if the experiment results in an error, represents a proof of concept that could be the subject of further research.

3.3.2.3 Experiment n°3: Timestamps analysis

RQs related: Acq-RQ1, Acq-RQ2, Acq-RQ3, Acq-RQ4, Acq-RQ5, and Acq-RQ6

As mentioned earlier, manipulating GPS devices may result in timestamps being written somewhere in the memory. Knowing the consequences of an action carried out on a device is paramount for a digital investigator. This experiment has for goal to pinpoint the timestamps being written for a given action. The experiment will use a PC Notebook running Kali Linux and the SleuthKit (TheSleuthKit, 2014).

Table 4 Computer used for experiment n°4

PC Notebook	
Model	Lenovo T420
OS	Kali Linux
RAM	4.00 GB
CPU	Intel(R) Core(TM) i7-2620 @ 2.70GHz
Storage	HDD 500GB

The experiment consists in performing a set of actions at a known time, and then looks for timestamps updates. The procedure is as follow, at least 5 minutes should separate each steps of the procedure:

1. Turn on the device – note the time (t_1).
2. Connect the device to the computer – note the time (t_2).
3. Using the SleuthKit, look for timestamps updates at times T_1 and T_2.
4. Disconnect the device – note the time (t_3)
5. Power off the device – note the time (t_4)
6. Connect the device (still turned off), the device should turned on by itself once connected – note the time (t_5)
7. Using the SleuthKit, look for timestamps updates at times T_3, T_4 and T_5.
8. Disconnect the device and restart it – note the time (t_6)
9. Wait 20 minutes with the device close to a window
10. Connect the device – note the time (t_7)
11. Using the SleuthKit, look for timestamps update between t_6 and t_7.
12. Redo steps 8 to 11, with the device protected from GPS signals.
13. Wait 20 minutes with the device connected
14. Note the time (t_8) – Using the SleuthKit look for timestamps updates between t_7 and t_8.

3.4 Analysis

When investigating a device, the "Analysis" stage is far less critical than the "Acquisition", as the work is mainly done on copies. However, it remains nevertheless the core stage where evidence is found and carved out of the memory. As memory can nowadays reach huge proportions, even in small scale embedded systems such as GPS devices, one must be aware of its internal structure and what eventual data can be found, in order to search in the right direction (Harrill & Mislan, 2007; Strawn, 2009). As highlighted by the literature review, few studies document the internal structure of Garmin devices.

The aim of this section is to investigate the file system architecture of Garmin devices, locate where the valuable information is held and evaluate

the different means to carve it out of the memory. Just as standard computer forensics, the recovery of deleted files must also be taken into account. The section is divided into two sub-sections, the first defines a set of research questions to be addresses, and the second one the experiments assessing those latter.

3.4.1 Research problems

As for the acquisition, the research problems related to analysis are driven by a main objective being the optimization of the analysis process. The architecture of the file system will be investigated, and the tools performing the analysis evaluated. Additionally, some specific features present in Garmin devices can very valuable data for an investigator. For instance, the "Triplog" feature, per default in the majority of recent Garmin devices, allows the device to track the user, even though he is not using it consciously. The RQs are defined to monitor that the experiments stay on track regarding the main objective. These RQs are related to three main subjects of investigation; the location of the file of interests within the device, the reminiscence of this data on the device, and the traces left by the Triplog feature. The Table 5 below details these RQs.

Core objective: *"Optimize the analysis process on Garmin navigation systems, to retrieve as much evidence as it is possible, within a short lapse of time"*.

Table 5 RQs related to the Analysis process

Code	*Research problems*
Ana-RQ1 *Ana-RQ2* *Ana-RQ3* *Ana-RQ4* *Ana-RQ5* *Ana-RQ6* *Ana-RQ7*	*"Where does the device store:* • *The home address of the user? (RQ1)* • *The route he has taken? (RQ2)* • *The favourite locations he stored (waypoints)? (RQ3)* • *The previous searches done on the device? (RQ4)* • *The itineraries computed by the device? (RQ5)* • *The information produced by the Triplog (RQ7)"* This first RQ aims at pinpointing the valuable information within the device. In their study, C. M. Colombini et al., (2012) listed the information stored on GPS devices that may be of interest for an investigator. This list has been used in conjunction with another study published by Hannay (2008), in which he pin-pointed the location records on a Tom-Tom device. The hypothesis is that Garmin devices hold similar information in a similar structure.
Ana-RQ8 *Ana-RQ9*	*"What is the structure of these files (RQ8) and what tools can be used to make them readable by humans (RQ9)?"* Once the location of the information within the files known, it is important to consider how the data can be easily read by an

	investigator. The structure known can also help recover deleted data, which is the objective of the next RQ.
Ana-RQ10	*"How volatile is the information held by Garmin devices?"* Alike other devices, the data held in GPS devices can be lost, deleted by the system to free some space. Being able to recover these files can be of paramount importance, as remarked by a representative of the National Hi-Tech Crime Unit in Scotland (NHTCUS), in an interview conducted on the 14 July 2014. This RQ aims to assess the data reminiscence on Garmin devices, and the efficiency of well-known forensic tools in performing this task.

3.4.2 Experiments

The two experiments described below have been designed accordingly to the eleven RQs formerly introduced. The RQs help to define the scope of the experimentation. Experiments are carried out on the Garmin set described in Section 3.2.

3.4.2.1 Experiment n°4: Locating forensic artefacts

RQs related: Ana -RQ1, Ana -RQ2, Ana -RQ3, Ana -RQ4, Ana -RQ5, Ana -RQ6, and Ana-RQ7.

This first experiment aims to pinpoint where the data of interest might be located on the device. As each piece of information listed above in the RQs is the result of an interaction between the user and the device, it is possible to interact in a way making the information easier to locate (e.g. Home address somewhere in China).

Concerning the experiment, it has to be noted that the three devices will follow the same steps, with different configurations:

- Nüvi 1340
- Nüvi 2515 – Triplog feature disabled
- Nüvi 2595 – Triplog feature enabled

The first part of the procedure follows the same steps than Hannay's study (2008):

1. Display current location, and note the coordinates with the reference device.
2. Navigate without reaching the destination.
3. Navigate and reach destination.
4. Navigate and move in opposite direction.
5. Navigate with the device in sleep mode.
6. Search without enabling navigation.
7. Create favourite location.

In order to address all the RQs, additional steps will also be carried out:

8. Search for POIs
9. Save a favourite destination
10. Set the home address.

The second phase then intend to recover the data with the SleuthKit and Autopsy. Once recovered, the details and the structure of the files containing valuable information will be documented In order to validate the data acquired, a Nüvi 2595 will be used as reference.

3.4.2.2 Experiment n°5: Deleted files recovery

RQs related: Ana -RQ11

Devices are likely to hold more information than they seem to, deleted files may hold very valuable information and can sometimes be recovered, depending on the underlying technology. As no metadata entry exists for these files, one must know the inner-structure of a file to recover it. The previous experiment defined the headers and trailers of the file of interests, information that can be used to carve eventual deleted files out of the memory. This experiment aims to assess the data reminiscence on Garmin devices and the tools that can be used to extract the information. The scope of this experiment is limited the locational data.

The tools evaluated as part of this experiment are:

- Windows explorer (acting as a reference)
- Autopsy
- EnCase
- Scalpel
- Foremost

The procedure is as follow:

1. Attempt to extract deleted files from the memory.
2. Calculate a hash of these files and compare them to the files discovered using the windows explorer.
3. Document the older file (containing locational data) found on the device.

3.5 Anti-forensics

Anti-forensics is a controversial topic amongst the forensics community. Whereas academics such as Lallie & Benford, (2011) and Strawn, (2009) tend to warn the community about the risks of anti-forensics on locational data, practitioners argue that this menace is highly unlikely to happened, as

criminals do not have the technical background to perform such manipulations (Ball, 2008). This opinion seems to be shared by several professional working in the field, as observed by a NHTCUS representative, interviewed the 15 July 2014. According to him, criminals will more likely send someone with their GPS whilst they are committing a crime rather than travel with the device and then manipulate the data to justify their alibi.

Despite this difference of opinion, anti-forensics are on the rise, and must be consider as a potential threat (Sartin, 2006). It is important to understand what action can be done on these devices in order not to be caught by surprise if anti-forensics were to grow wider in GPS devices in a near future.

3.5.1 Research problems

Anti-forensics is a broad subject, defined by Garfinkel as "a growing collection of tools and techniques that frustrate forensic tools, investigations and investigators" (S. Garfinkel, 2007). Inside GPS devices, it can be found under multiple form, from stenographic data embedded into files, to data simply wiped out of the memory (Sartin, 2006). Concerning the present study, the scope of the research problems is narrowed to the modification of locational data only. These problems are defined following a core objective:

"Assessing the ways in which an attacker could modify the data held in Garmin devices in a way it could mislead an investigator"

This induces three RQs, aiming to address the main objective, described in the Table 6 below. These RQs have been inspired from a study published by Lallie & Benford, (2011), in which they modified the locational data inside pictures, before uploading the pictures back in the IPhone they were belonging to.

Table 6 RQs related to Anti-forensics

Code	*Research problems*
Ant-RQ1	*"Can the content of a file be modified on a device, without having an impact on the timestamps?"* As pointed out by Ball, (2008), a location associated with a timestamp can be of crucial importance in an investigation. Inversely, being able to modify this data to mislead an investigator to a false alibi can be paramount for a criminal, and lead to an injustice.
Ant-RQ2	*"Can the timestamp of a file be modified without leaving any traces?"* When accessing a device with a computer, timestamps may be updated in the process (Nutter, 2008), a criminal might be able

> to revert these using anti-forensic techniques, in order to cover his tracks.

3.5.2 Experiments

This subsection presents the experimentation related to anti-forensics. A set of three experiments, designed accordingly to the related RQs has been designed. These experiments do not rely upon the model of the device. Therefore, only one device from the Garmin set will be considered, the Garmin Nüvi 2515LM.

3.5.2.1 Experiment n°6: File's content alteration

RQs related: Ant-RQ2

This experiment aims to modify the content of the device memory without updating any timestamps. The hypothesis is that if the file is modified at a byte level, not at a file system level, timestamps will not be updated. To verify this assumption, the following experiment has been designed, composed of the following steps:

1. With the SleuthKit, localize the geolocation of the favourite "Garmin Scotland".
2. Modify the data in a way the new coordinates points to Edinburgh.
3. Verify the information on the device has been correctly updated.

3.5.2.2 Experiment n°7: Timestamp alteration

RQs related: Ant-RQ3

Although the aim of this experiment is different, the procedure is similar to the experiment n°9. As mentioned earlier, connecting the device to a computer, or simply turning it on might have a repercussion on certain timestamps. This experiment aims to show it is possible to revert these changes. The procedure is as follow:

1. With the SleuthKit, localize where the updated timestamp is stored.
2. Modify the data in a way it shows a data a week before the original.
3. With the SleuthKit, verify the timestamp has correctly been updated.

3.6 Conclusion

This chapter described the experiments that have been designed to investigate Garmin devices' based on the literature reviewed in the previous chapter, highlighting the lack of work in the area. Three types of tests have been designed, aiming to investigate the acquisition, analysis and anti-forensic techniques respectively. Conducting these experiments should address a range of research questions, which would provide a better

understanding of the devices' structure and behaviour, and help investigators to handle them.

The first set of experiments, related to forensic acquisition, aims to evaluate the well-known imaging tools when dealing with Garmin devices, and provide a better understanding on the device specific behaviours that could have an impact on the investigation.

The second set aims to investigate the file structure and the data reminiscence of Garmin devices. As this kind of experimentation has been regularly used in studies addressing Tom-Tom devices (C. Colombini, 2009; Hannay, 2008; Nutter, 2008), the results gathered in these experiments will have a point of comparison on Tom-Tom devices.

The third and last set aims to assess the possibility for one to mislead an investigator by manipulating the data held on a device. The three experiments target the content as well as the timestamps, hence investigating the possibility for someone to create compelling evidence or alibis for themselves.

Chapter 4 Experimentation

4.1 Introduction

This chapter documents how the experiments previously designed have been conducted, and summarizes the results obtained. Just like the previous chapter, it is divided into three sections, dedicated to the categories the experiments belong to, respectively “Acquisition”, “Analysis”, and “Anti-forensics”. Each experiment has its own sub-section, in which a summary of the procedure carried out is explained, along with the processed results. Full procedures are detailed in the Appendices when relevant.

4.2 Acquisition

4.2.1 Experiment n°1: Evaluation of forensic imagers.

The experiment intended to evaluate the performance of well-known forensic imagers when dealing with Garmin devices. To do so, the three devices from the Garmin set have been imaged on PCA, using four different tools; FTK Imager, EnCase Forensic Imager, Guymager and the Linux “dd” command. About the acquisition procedure itself, it has proven to be easier on Linux than Windows.

When handling the experiment with Linux, every devices have been imaged simply by connecting the device to the computer, and then selecting the device amongst a list (for Guymager) or in the “*/dev/*” folder (for the dd command). Full acquisition procedures under Linux are detailed in Appendix E (Guymager) and Appendix F (dd).

Inversely, using windows-based tools FTK and EnCase, only the Garmin Nüvi 1340 could have been acquired at a first time. Garmin Nüvi 2515 and 2595 were detected by the computer, but did not appeared in the device list of the tools. After some research, it appears that this difference is due to the use of different protocol to communicate with the device (Garmin, 2014c). In fact, the Nüvi 1340 uses “USB mass storage device class” (USB MSC) to communicate with the computer (Sandisk, 2013). The device will therefore be seen as a “Mass storage device” by the OS, see Figure 32. Conversely, more recent Garmin devices such as the Nüvi 2515 and the Nüvi 2595 tested tend to use Media Transfer Protocol (MTP), which makes the device being recognized as a “Portable Device” (c.f. Figure 33). MTP is a protocol designed by Microsoft to facilitate media synchronization between Windows and portable devices such as MP3 players (Sandisk, 2013). When

using MTP, Windows does not mount the device, and it is therefore impossible to access it with the forensic tools considered for this experiment.

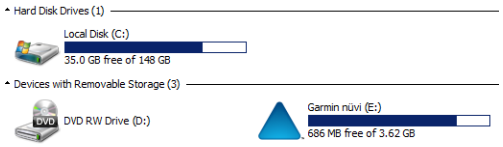


Figure 32 Garmin Nüvi 1340 in windows

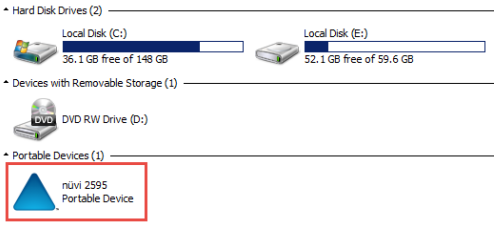


Figure 33 Garmin Nüvi 2595 in windows

It has been possible to image successfully the devices by updating the driver software, thus making them being recognized as mass storage devices. The procedure has been inspired by a similar procedure done on MP3 players (Taylor, 2011), and is described in Appendix G.

The procedure also showed that EnCase were able to acquire the RAM of the device, whereas FTK, dd, and Guymager could not access it.

Whilst acquiring the devices, the execution times have been measured. As shown in Figure 34 below, the measurements show equivalent performance between the tools. The choice of the tool therefore does not have an impact on the performance of the acquisition.

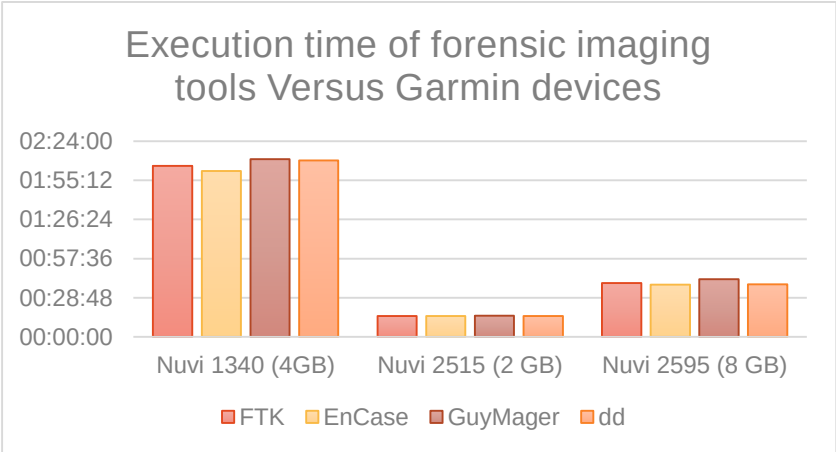


Figure 34 Execution time of forensic imaging tools Versus Garmin devices

However, the generation of the device might have an impact. As shown in the Figure 34, the acquisition of the Garmin Nüvi 1340, took twice the time needed to acquire the Garmin Nüvi 2595, yet two times bigger. This is because the Nüvi 13xx generation uses USB 1.1, whereas Nüvi 25xx generation uses USB 2.0.

4.2.2 Experiment n°2: Boot with another OS.

Tom-Tom devices boot on the SD card in priority (van Eijk & Roeloffs, 2010). Such characteristics can allow an investigator to make the device boot on a custom OS designed to copy the content of the memory, hence bypassing the internal OS and avoiding the USB connection. The present experiment aimed to evaluate the presence of this characteristic within Garmin devices.

All the devices from the Garmin set accept Micro SD card. The first phase of the experiment was therefore to create a bootable SD card, with a lightweight Linux distribution on it. This has been done by using the freeware "*Win 32 Disk Imager*" (see Figure 35 below).

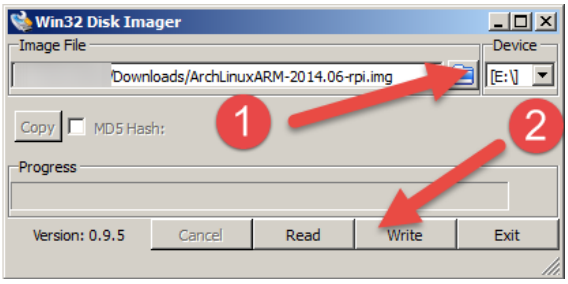


Figure 35 Win 32 Disk Imager

The software allows to image portable devices such as USB drives or SD Cards, and inversely, to write back images on devices. An "Arch Linux" image was written on the SD card. Although there is no documentation on the matter, it has been assumed that Garmin devices were running ARM processor, hence the choice of the image.

The experiment has then been conducted on the devices of the Garmin set. No change has been noticed, and all the devices considered used their original boot sequence. These results can have two significations. First, the device did not consider the presence of the SD card to perform its boot sequence, and therefore followed its casual sequence by booting on its internal memory. Second, the boot from the SD Card was unsuccessful, and because of that, the device did boot on its internal memory instead. Although none of these hypotheses can be invalidated, the boot sequence was performed as usual without additional time (which would have explained a boot failure), hence making the first supposition more likely.

It can therefore be reasonably assumed that Garmin devices do not boot uppermost on their SD card.

4.2.3 Experiment n°3: Timestamps analysis.

This experiment intended to identify actions an investigator is susceptible to make and would result in an alteration of the device. The procedure

designed in the section 0 has been followed and resulted in a better understanding of Garmin devices' behaviour.

Six different case studies were tested, among which four of them were conclusive. The results show that turning off a device, or leaving it on, connected to a computer does not affect its integrity in any way. However, timestamps are updated every time a device is turned on (Table 7), or connected to a computer (Table 9 and Table 10).

Table 7 Timestamps updated when turning on Garmin devices

Path	Type	Modified	Accessed	Created
/Garmin/GarminDevice.xml	file	X		X
/Garmin/GarminDevice.tmp	file (deleted)	X		X

The Table 7 above summarizes the timestamps that have been updated by turning on the device. As shown in the Figure 36 below, a temporary file called "*GarminDevice.tmp*" is created, and helps to the creation of another file called "*GarminDevice.xml*". The temporary file is then deleted. As no traces of any timestamps have been found within those files, another experiment has been conducted, aiming to highlight the differences between two versions of this file by comparing their MD5 hash. This showed these two files do not change, but are re-created every time the device is turned on.

Figure 36 Files created when device is turned on

Table 8 Timestamps updated when turning off Garmin devices

Path	Type	Modified	Accessed	Created
/Garmin/Diag/GarminOS.log	file	X		

When turning the device off, the device logs the event in a file called "*GarminOS.log*", as shown in the Figure 37 below.

```
I[2014/08/04 22:32:24] (DBG:dbg_pwrp_prj.c) {03046038} [dbg_pwrp_prj.c:DBG_pwrdn:72] DBG module power down
I[2014/08/04 22:34:16] (DBG:dbg_pwrp_prj.c) {03046038} [dbg_pwrp_prj.c:DBG_pwrdn:72] DBG module power down
I[2014/08/04 23:00:20] (DBG:dbg_pwrp_prj.c) {03046038} [dbg_pwrp_prj.c:DBG_pwrdn:72] DBG module power down
I[2014/08/06 09:21:16] (DBG:dbg_pwrp_prj.c) {03046038} [dbg_pwrp_prj.c:DBG_pwrdn:72] DBG module power down
```

Figure 37 Content of the file GarminOS.log

Table 9 Timestamps updated when connecting Garmin devices to a computer under Linux

Path	Type	Modified	Accessed	Created
/GPX/Current.gpx	file	X	X	
/GPX/Position.gpx	file (deleted)	X		X

When the device is connected to the computer under Linux (Table 9), two files appear to have been altered. A temporary file, called "*Position.gpx*", and another file called "*Current.gpx*" (see Figure 38).

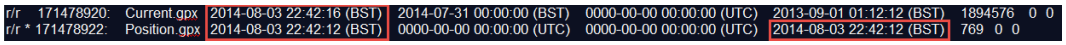


Figure 38 File modified when connecting the device to a computer

The time at which the device is put into USB mode is stored in a temporary file containing (if possible) the Last known position. This file is called "*Position.gpx*"; gpx standing for GPS eXchange format, a lightweight XML format dedicated to the interexchange of GPS data (Topografix, 2004). The file is structured as a XML, and the node "*time*" contains the date at which the device has been into USB mode (see Figure 39).


```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?><gpx xmlns="http://www.topografix.com/GPX/1/1"
xmlns:gpxx="http://www.garmin.com/xmlschemas/GpxExtensions/v3"
xmlns:gpxtpx="http://www.garmin.com/xmlschemas/TrackPointExtension/v2" creator="nüvi 2595" version="1.1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.topografix.com/GPX/1/1
http://www.topografix.com/GPX/1/1/gpx.xsd http://www.garmin.com/xmlschemas/GpxExtensions/v3
http://www.garmin.com/xmlschemas/GpxExtensionsv3.xsd http://www.garmin.com/xmlschemas/TrackPointExtension/v2
http://www.garmin.com/xmlschemas/TrackPointExtensionv2.xsd"><metadata><link href="http://www.garmin.com">
<text>Garmin International</text></link><time>2014-08-03T21:42:13Z</time></metadata>
```


Figure 39 Position.gpx

The file "*Current.gpx*" is updated with the information held by "*Position.gpx*" (see Figure 40), and remains on the device.


```
▼<gpx xmlns="http://www.topografix.com/GPX/1/1" xmlns:gpxx="http://www.garmin.com/xmlschemas/GpxExtensions/v3"
 xmlns:gpxtpx="http://www.garmin.com/xmlschemas/TrackPointExtension/v2" xmlns:xsi="http://www.w3.org/2001/XMLSchema
 instance" creator="nüvi 2595" version="1.1" xsi:schemaLocation="http://www.topografix.com/GPX/1/1
 http://www.topografix.com/GPX/1/1/gpx.xsd http://www.garmin.com/xmlschemas/GpxExtensions/v3
 http://www.garmin.com/xmlschemas/GpxExtensionsv3.xsd http://www.garmin.com/xmlschemas/TrackPointExtension/v2
 http://www.garmin.com/xmlschemas/TrackPointExtensionv2.xsd">
 ▼<metadata>
   ▼<link href="http://www.garmin.com">
      <text>Garmin International</text>
    </link>
    <time>2014-08-03T21:42:13Z</time>
  </metadata>
 ▼<wpt lat="25.061784" lon="121.640268">
    <ele>38.10</ele>
    <name>Garmin Asia</name>
    <link href="Pictures/Garmin_Asia.jpg"/>
   ▼<extensions>
    ▼<gpxx:WaypointExtension>
     ▼<gpxx:Address>
        <gpxx:StreetAddress>No 68, Jangshu 2nd Road</gpxx:StreetAddress>
        <gpxx:City>Shijr, Taipei County</gpxx:City>
        <gpxx:Country>Taiwan</gpxx:Country>
      </gpxx:Address>
     </gpxx:WaypointExtension>
```


Figure 40 Current.gpx

Table 10 Timestamps updated when connecting Garmin devices to a computer under Windows

Path	Type	Modified	Accessed	Created
/GPX/Current.gpx	file	X	X	
/GPX/Position.gpx	file (deleted)	X		X
Every files on the device	file		X	

However, as pointed out by Table 10 above, when connecting the device to Windows systems, if the investigator does not use any write-blocker, the "Accessed Timestamps" of every file present on the device will be updated (see Figure 41 below).

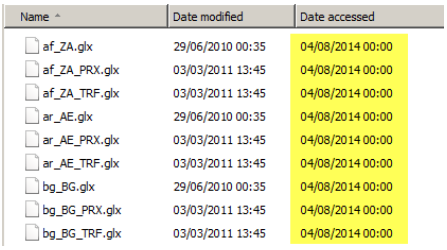


Figure 41 Files accessed under windows systems

In order to prevent this, a manipulation is nevertheless possible for those who do not have a physical write-blocker with them. To do so, one must edit the Windows registry as shown in the Figure 42.

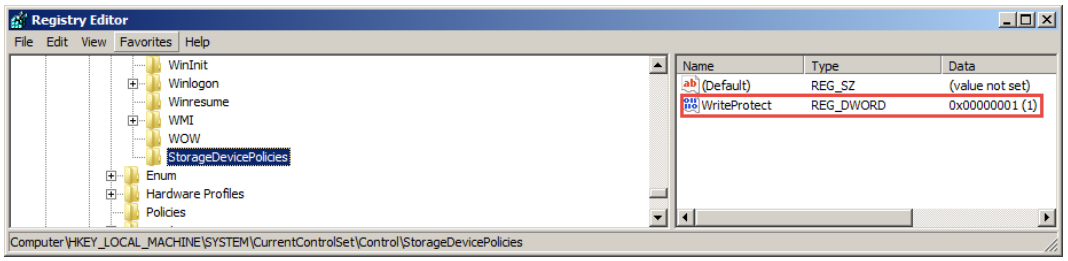


Figure 42 Write-protect policy in windows registry

This manipulation will make windows consider storage devices as read-only, thus preserving the original timestamps.

Two case studies however do not provide enough results to draw any conclusions: Leaving the device on, with and without protection against GPS signals. The experiment was to turn on a device, wait a certain amount of time before connecting it to a computer and look if any timestamps had been updated in between. This experiment had however a limitation; if the information collected during this period of time is stored in the same file as the time at which the device has been connected, the modification would be hidden by the timestamp update related to the USB connection. Further investigation will therefore be needed.

4.3 Analysis

4.3.1 Experiment n°4: Locating forensic artefacts.

Similar to other embedded devices, Garmin GPS systems have their own data hierarchy. This experiment aims to document this by interacting with the device in a way could highlight where the evidence is likely to be found within all the information.

The procedure described in section 3.4.2 highlighted several files holding valuable information. These files are listed in the Table 11 below and will be

documented thereafter. In order to pinpoint these files, the SleuthKit-based software "Autopsy", for windows, has been used. When conducting the experiment, the time has been noted for every step. Then, using autopsy, the files recovered have been sorted regarding their last modification time, hence highlighting the impact of the experiment of the device.

Table 11 Files of interest and information held inside them.

File of interest	Data
/GPX/Current.gpx	Last USB connection. Home address. Favourite locations. Last trips coordinates.
/GPX/Archive/	Folder containing trips archives (.gpx extension).
/.System/GtmData.tmp*	Last connection to the network to get traffic updates.
/.System/Logs/searches.txt*	Searches (POIs)
/.System/SQLite/recent_searches.db*	
/.System/SQLite/quick_search_list.db*	
/.System/SQLite/user_strings.db*	Destinations entered.
/.System/SQLite/RecentStops.db*	Recent stops made by the user.

* Garmin Nüvi 25xx only

4.3.1.1 Current.gpx and the Archive folder

From a forensics point of view, "Current.gpx" is one of the most important files that can be found within Garmin devices, as it holds very useful data to investigators. As showed in the Table 11 above, "Current.gpx" holds the favourite locations of the user, as well as its recent whereabouts if the Triplog feature is enabled. This file is typically found under in the "*/GPX*" folder on Garmin devices except ones from the Nüvi 200, 300, 600 and 700 series (Garmin, 2014b). As mentioned in Table 11, this is where the device stores the favourite locations of the user, its home address, and sometimes records its movements.

This file also uses the GPX format. The simple structure of this file makes it relatively easy to investigate, and humanly understandable. To read it, the easiest way is to drag and drop the file in an internet browser, such as Google Chrome (Google Inc., 2014a) or Firefox (Mozilla, 2014), to access the raw data in a readable way (see Figure 43). Documentation on the gpx structure can be found on the website of the company Topographix, responsible of the format (Topografix, 2004).

```
▼<gpx xmlns="http://www.topografix.com/GPX/1/1"
 xmlns:gpxx="http://www.garmin.com/xmlschemas/GpxExtensions/v3"
 xmlns:gpxtpx="http://www.garmin.com/xmlschemas/TrackPointExtension/v2"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" creator="nüvi 2595" version="1.1"
 xsi:schemaLocation="http://www.topografix.com/GPX/1/1 http://www.topografix.com/GPX/1/1/gpx.xsd
 http://www.garmin.com/xmlschemas/GpxExtensions/v3 http://www.garmin.com/xmlschemas/GpxExtensionsv3.xsd
 http://www.garmin.com/xmlschemas/TrackPointExtension/v2
 http://www.garmin.com/xmlschemas/TrackPointExtensionv2.xsd">
 ▼<metadata>
  ▼<link href="http://www.garmin.com">
    <text>Garmin International</text>
   </link>
   <time>2014-08-04T22:24:55Z</time>
  </metadata>
 ▼<wpt lat="55.937405" lon="-3.226161">
   <ele>-0.11</ele>
   <name>Caley Sample Room</name>
   <desc>58 Angle Park Terrace Eh11, Midlothian</desc>
  ▼<extensions>
   ▼<gpxx:WaypointExtension>
    ▼<gpxx:Categories>
      <gpxx:Category>Bars & Pubs</gpxx:Category>
     </gpxx:Categories>
    ▼<gpxx:Address>
      <gpxx:StreetAddress>58 Angle Park Terrace</gpxx:StreetAddress>
      <gpxx:City>Eh11</gpxx:City>
      <gpxx:State>Midlothian</gpxx:State>
      <gpxx:PostalCode>EH11 2</gpxx:PostalCode>
     </gpxx:Address>
     <gpxx:PhoneNumber>0131 3377204</gpxx:PhoneNumber>
    </gpxx:WaypointExtension>
   </extensions>
  </wpt>
```


Figure 43 Current.gpx within Chrome

The structure of this file, found within every Garmin devices is as the following:

`<gpx>`	Opening tag of the file.
`<metadata>…</metadata>`	**Metadata:** Section containing the time when the device has last been connected to a computer.
`<wpt>…</wpt>` `<wpt>…</wpt>` …	**Waypoints:** Contains home address and favourite locations.
`<trk>…</trk>` `<trk>…</trk>` …	**Tracks:** Contains where the user has been at a given time.
`</gpx>`	Closing tag of the file.

To extract locational data and present them on a map, the gpx file can simply be opened with Google Earth (Google Inc., 2014b). Doing so will make the analysis easier as it will draw the trips done by the user on a map and highlights the POIs (Figure 44).

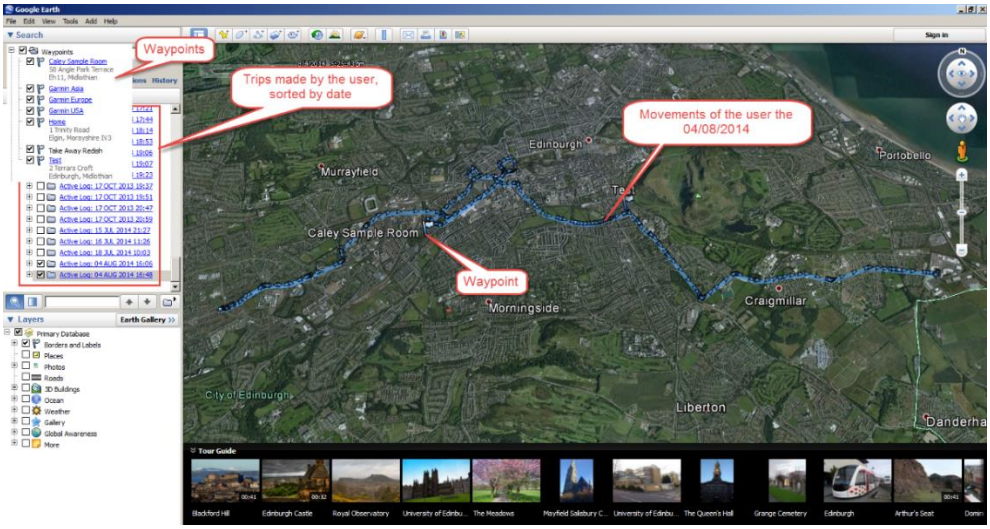


Figure 44 Current.gpx in Google Earth

Additionally, the "*/GPX*" folder holds another folder, called "Archive" in which are stored historic locational data. Through this file, on a device used on a weekly basis, it has been possible to recover trips that have been done a year earlier.

The experiment also highlighted the presence of a DB, in which are stored the recent stops the user has made. As shown in Figure 45, the DB stores the coordinates of the stop, along with a timestamp and a textual description. Although such information can be deduced from the timed-location recovered in "Current.gpx", it nevertheless might be of interest as it could draw the attention of an investigator on a potentially suspicious activity.

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: history — New Record — Delete Record

	time	lat	lon	name
	Filter	Filter	Filter	Filter
37	750976139	637802279	-25964487	Near 13 Bakewell Street
38	774108586	667354199	-38582112	Near Marvid Snack Bar
39	774378393	667186420	-40553898	Unknown Location
40	774390475	667186420	-40553898	Unknown Location
41	774445513	670257606	-52178249	Unknown Location
42	774462955	667071913	-37908034	Near Braid Hills Drive & Liberton Drive & Liberton Tower Lane
43	774614573	665673706	-58094957	Near Morris's Lounge Bar
44	774620368	665763452	-57851594	Unknown Location
45	774650509	663839918	-55980862	Near A78 (E) & Nethermains Road (SE)
46	776103955	667313152	-37052928	Near Fort Kinnaird Retail Park

< 37 - 46 of 46 > — Go to: 1

Figure 45 RecentStops.db content

The experiment also pointed out the presence of a temporary file called "GtmData.tmp". This file, recovered by Autopsy, contains the last time the device has been connected to the radio network to receive traffic updates.

4.3.1.2 Data issued from user interaction (Nüvi 2515 and 2595)

On recent Garmin devices, such as the Nüvi 25xx series, it is possible to recover data that resulted from an interaction with the user, such as the searches he has done, or the keywords he has entered.

The experiment conducted to the discovery of a file called "*searches.txt*" located inside "*/.System /Logs/*". This file contains what the user has been searching, as well as the nearby proposition computed by the device (see Figure 46).

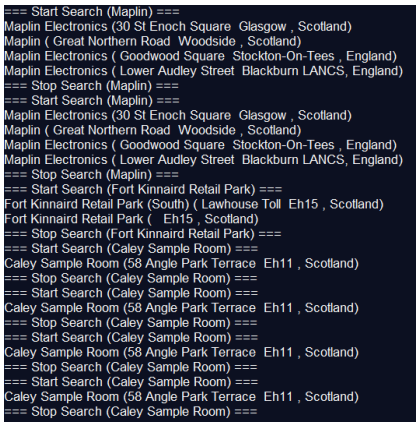


Figure 46 Searches.txt on a Nüvi 2595

Recent Garmin devices use DBs used for internal purposes. These latter can also hold information and therefore potentially cross correlate an evidence. During the experiment, these DBs have been accessed with SQLite Database Browser (Piacentini & Morgan, 2012).

Searching for a POI makes the device update two of these DBs; "*quick_search_list.db*" and "*recent_searches.db*", which are used as a cache to reduce the response time on next similar inquiries (fork(), 2013).

Entering an address also has its repercussions in the DBs, more precisely on "*user_strinb.db*". As its name suggests, this DB contains the strings that have been typed by the user. As shown in Figure 47, this concerns mainly addresses and postcodes. However, phone numbers can also be found amongst the data.

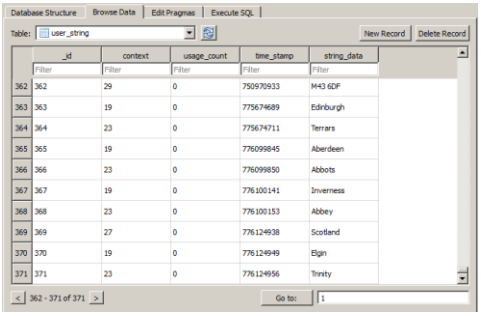


Figure 47 user_strinb.db *content*

4.3.1.3 Information recovered within the devices considered.

This sub-section resumes what information has been recovered on the different devices from the Garmin set. The Garmin set is made of three devices, belonging to two different series (Nüvi 13xx and Nüvi 25xx). On the Nüvi 2515, the Triplog feature has been disabled, in order to see the impact of turning on/off such feature on the data recovery process.

For each of the devices, the information recovered has been synthetized into two tables, the first one related to information resulting from a Human-Machine Interaction (HMI), and the second one to data produced by the device whilst under experimentations.

Nüvi 13xx:

Unlike more recent devices such as the Nüvi 25xx series, the Nüvi 1340 does not have any log folder or DBs. As underlined by the Table 12 below, the only information related to HIM has been recovered through the "*Current.gpx*" file.

Table 12 HMI information on Nüvi 1340

Operational mode	Coordinates retrieved	Address retrieved	Timestamps retrieved	Textual description accurate
Enter an address and enable navigation	no	no	no	N/A
Search w/o enabling navigation	no	no	no	N/A
Search and enable navigation	no	no	no	N/A
Create favourite location	yes	yes	no	yes
Set home address	yes	yes	no	yes

However, the Triplog feature, present in this model (Garmin, 2014b), provides the investigator with valuable information related to where the user has been, even though he did not follow the navigation. The Table 13 below shows that the use of this feature (enabled by default) makes the user being tracked at all time. However, given that no information related to the destination could have been retrieved within the memory, there is no way to know if the plotted destination has been reached or not.

Table 13 Locational information on Nüvi 1340

Operational mode	Coordinates retrieved	Timestamps retrieved	Path of movement known	Known if destination reached.
"View map" mode	yes	yes	yes	N/A
Nav without reaching destination	yes	yes	yes	no
Nav and reach destination	yes	yes	yes	no
Nav and move in opposite direction	yes	yes	yes	no
Sleep mode	no	no	no	N/A

Nüvi 2515 (25xx Triplog disabled):

In order to assess the impact of turning on/off the Triplog feature on data retrieval, the feature has been disabled on one of the device of the 25xx series, the Nüvi 2515. As previously mentioned, recent Garmin series do have DBs embedded, aiming to reduce the search time and therefore enhance the user experience. The Table 14 below highlights what information valuable to investigators can be retrieved within these DBs. It has to be noted that DBs such as "*quick_search_list.db*" or "*user_strinb.db*" do store timestamps along with the raw information, which can be paramount when investigating a large amount of data.

Table 14 HMI information on Nüvi 2515 (Triplog disabled)

Operational mode	Coordinates retrieved	Address retrieved	Timestamps retrieved	Textual description accurate
Enter an address and enable navigation	no	yes	yes	N/A
Search w/o enabling navigation	no	no	no	N/A
Search and enable navigation	no	yes	yes	N/A
Create favourite location	yes	yes	no	yes
Set home address	yes	yes	no	yes

Table 15 give prominence to the repercussions engendered by disabling the Triplog feature. Once the feature disabled, no information is stored inside the memory. As the scope of this study does not cover the RAM, this latter has not been investigated, but such information is likely to be found in the RAM, which therefore should be further investigated.

Table 15 Locational information on Nüvi 2515 (Triplog disabled)

Operational mode	Coordinates retrieved	Timestamps retrieved	Path of movement known	Known if destination reached.
"View map" mode	no	no	no	no
Nav without reaching destination	no	no	no	no
Nav and reach destination	no	no	no	no
Nav and move in opposite direction	no	no	no	no
Sleep mode	no	no	no	no

Nüvi 2595 (25xx Triplog enabled):

In this experiment, the Nüvi 2595 represents the 25xx series, with the Triplog feature enabled. As it can be seen in TA below, the feature does not have any impact on the databases, in which the same information previously discovered could have been retrieved.

Table 16 HMI information on Nüvi 2595 (Triplog enabled)

Operational mode	Coordinates retrieved	Address retrieved	Timestamps retrieved	Textual description accurate
Enter an address and enable navigation	no	yes	yes	N/A
Search w/o enabling navigation	no	yes	no	N/A
Search and enable navigation	no	yes	yes	N/A
Create favourite location	yes	yes	no	yes
Set home address	yes	yes	no	yes

However, when it comes to locational data, having the Triplog enabled allows investigators to recover a great deal of information (see Table 17). By cross correlating the location where the user has been and the searches he has done, the investigator can easily deduce if the user reached the destination he was aiming towards.

Table 17 Locational information on Nüvi 2595 (Triplog enabled)

Operational mode	Coordinates retrieved	Timestamps retrieved	Path of movement known	Known if destination reached.
"View map" mode	yes	yes	yes	N/A
Nav without reaching destination	yes	yes	yes	yes
Nav and reach destination	yes	yes	yes	yes
Nav and move in opposite direction	yes	yes	yes	yes
Sleep mode	no	no	no	no

An additional experiment has been carried out, aiming to see whether disabling the Triplog whilst driving would have a visible impact or not. The Figure 48 presents the result of this last experiment. The signal acquisition has been represented in red, then the vehicle has been driving using the map display, without any navigation. The Triplog has then been disabled, and no further locational data could have been recovered past this action.

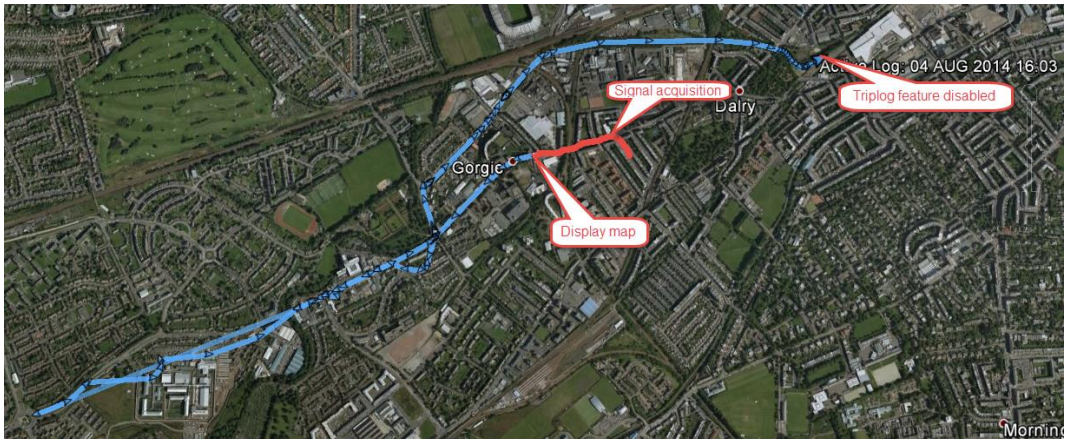


Figure 48 Triplog disabled whilst driving

4.3.2 Experiment n°5: Deleted files recovery.

The last experiment underlined the value of "Current.gpx" for a digital forensic examiner. As stated by Garmin, only a restricted amount of data can be held in the memory. The firm reports up to 10'000 points per file and a maximum of 20 files per devices, stored inside the "*/GPX/Archive*" folder (Garmin, 2014b). This present experiment aimed to investigation the actual data retention of Garmin systems, as it is known that a file deleted at the OS level may remain within the memory for much longer.

".gpx" files contains mainly waypoints – such as the user's home address or favourite locations – and tracks, which are where the user has actually been with the device. The Archive folder contains up to 20 of these files, named with a number, incremented each time. The lower the number is, the older the file. Incidentally, in a folder containing 20 files named 6.gpx to 25.gpx, it can be deduced that five files have already been deleted at the OS level. Whilst it is still possible to recover part of the memory, the usage of flash memory makes the recovery difficult, as underlined in the section 2.3.1. In order to recover the most of the data, the recovery has been attempted at two different levels. The first one is to recover the whole .gpx file, containing waypoints and tracks. The second is to retrieve these data separately. Three different methods have been used to recover the data. The file browser aims to underline what could be retrieved by simply navigating through the folders of the device. The "fls" command represents what a basic forensic investigation might extract, with deleted files recovery. "Scalpel" is a tool used to carve data out of the memory. Given appropriate header and trailer, "Scalpel" can retrieve part of a file that no longer exists in its entirety. The configuration files used for the carving procedure can be found in Appendix H, and the results are detailed in the Table 18 below.

Table 18 Information retrieval depending on the recovery technique.

Data	Device	Archive Files name	File browser	fls	Scalpel
.gpx files	Nüvi 1340	[44.gpx – 63.gpx]	22	23	26
	Nüvi 2515	[7.gpx – 26.gpx]	22	23	26
	Nüvi 2595	[26.gpx – 45.gpx]	21	22	22
Total waypoints	Nüvi 1340	--	11	11	19
	Nüvi 2515	--	5	5	5
	Nüvi 2595	--	7	7	7
Total tracks	Nüvi 1340	--	1965	1965	1992
	Nüvi 2515	--	232	232	294
	Nüvi 2595	--	2107	2107	2192

As shown in the Table 18 above, carving files based on their header and trailers seems to be the more efficient method to extract the most data out of a device. The results will be further discussed in the next chapter.

Once carved, .gpx files can be directly read by software such as Google Earth (Google Inc., 2014b). Regarding the waypoints and tracks, as shown on Figure 49 and Figure 50, the carving process recovers them as GPX entities, and therefore only needs to be encompassed by opening and closing gpx tags "<gpx></gpx>" to be open by the same kind of software.


```
<trk><name>Active Log: 04 OCT 2013 20:11</name><trkseg>
<extensions><gpxtpx:TrackPointExtension><gpxtpx:course>
lat="53.455052" lon="-2.158412"><ele>46.28</ele><time>2
<gpxtpx:course>338.82</gpxtpx:course></gpxtpx:TrackPoin
<time>2013-10-04T19:12:03Z</time><extensions><gpxtpx:Tr
</gpxtpx:TrackPointExtension></extensions></trkpt><trkp
<extensions><gpxtpx:TrackPointExtension><gpxtpx:speed>1
</extensions></trkpt><trkpt lat="53.455182" lon="-2.158
```


Figure 49 Structure of a recovered track


```
<wpt lat="57.650472" lon="-3.317053"><ele>-3.48</ele>
<name>Home</name><desc>1 Trinity Road
Elgin, Morayshire IV3</desc><extensions>
<gpxx:WaypointExtension><gpxx:Address>
<gpxx:StreetAddress>1 Trinity
Road</gpxx:StreetAddress><gpxx:City>Elgin</gpxx:City>
<gpxx:State>Morayshire</gpxx:State>
<gpxx:PostalCode>IV30 1</gpxx:PostalCode>
</gpxx:Address></gpxx:WaypointExtension></extensions>
</wpt>
```


Figure 50 Structure of a recovered waypoint

This process of adding gpx tags to view the data recovered is a process that could be easily automated. Once this manipulation done, the information can be read through Google Earth, as shown in the Figure 51 and Figure 52 below.

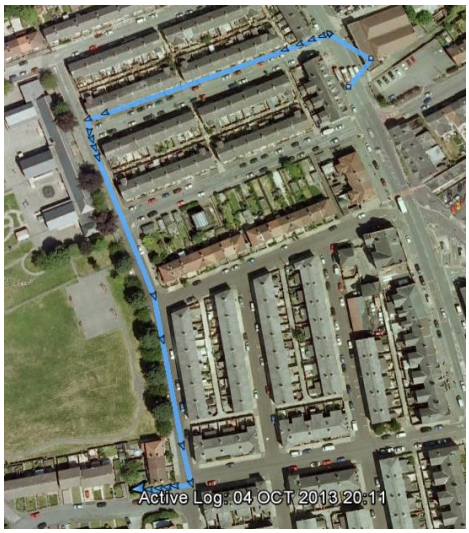


Figure 51 recovered track in Google Earth

Figure 52 recovered waypoint in Google Earth

4.4 Anti-forensics

4.4.1 Experiment n°6: File content alteration.

Be able to retrieve evidence is paramount to digital investigators, however, techniques to counter forensics exists, and could be used by criminals in order to create an alibi or create an inculpatory evidence on someone else's device. This experiment shows how information inside Garmin devices can be manipulated in a way it could mislead an investigator, without leaving any traces on the timestamps. The goal is therefore to modify a location stored on the device, by manipulating its latitude or longitude.

Since there is no results but the procedure itself, this latter will be detailed and explained below. The procedure has been carried out on a Garmin Nüvi 2515, using a computer running Kali Linux and using the SleuthKit to access and manipulate the data. Due to the amount of data the commands can produce, the output has been reduced to the relevant data only. The full procedure with more detailed outputs can be found in Appendix I.

First thing is to pin-point where the data is located on the device, at a byte level. Using the SleuthKit, more precisely the "fls" and the "istat" command, one is able to locate the blocks containing the information.

```
$fls /dev/disk/by-label/GARMIN
[...]
d/d 22: GPX
[...]

$fls /dev/disk/by-label/GARMIN 22
[...]
d/d 32113800: Archive
[...]

$fls /dev/disk/by-label/GARMIN 32113800
[...]
r/r 32139308: 60.gpx

$istat /dev/disk/by-label/GARMIN 32139308
[...]
Name: 60.GPX

Directory Entry Times:
Written: Wed Dec 4 08:07:06 2013
Accessed: Thu Jan 1 01:00:00 1970
Created: Thu Nov 28 19:38:18 2013

Sectors:
2070136 2070137 2070138 2070139 2070140 2070141 2070142 2070143...


$dd if=/dev/disk/by-label/GARMIN bs=512 skip=2070137 count=1 | xxd
[...]
0000130: 3c74 726b 7365 673e 3c74 726b 7074 206c <trkseg><trkpt l
0000140: 6174 3d22 3531 2e33 3834 3136 3422 206c at="51.384164" l
[...]
```

Once the targeted information pin-pointed, it is possible to modify it. Piping the Linux "echo" command into a "dd" command is a way to access the byte without needing any additional tools.

```
$echo -ne "\x34"| dd of=/dev/disk/by-label/GARMIN seek=1059910468
bs=1 count=1 conv=notrunc
1+0 records in
1+0 records out
1 byte (1 B) copied, 0.000260159 s, 3.8 kB/s

$dd if=/dev/disk/by-label/GARMIN bs=512 skip=2070137 count=1 | xxd
[...]
```

```
0000130: 3c74 726b 7365 673e 3c74 726b 7074 206c <trkseg><trkpt l
0000140: 6174 3d22 3431 2e33 3834 3136 3422 206c at="41.384164" l
[...]
```

The command above shows the modification has been applied on the latitude, changing the value from “51” to “41”.

```
$istat /dev/disk/by-label/GARMIN 32139308
[...]
Name: 60.GPX

Directory Entry Times:
Written: Wed Dec 4 08:07:06 2013
Accessed: Thu Jan 1 01:00:00 1970
Created: Thu Nov 28 19:38:18 2013
[...]
```

These commands did not affect nor modify any timestamps. Thus, it is possible to access the device at a byte level and bypass any logging that could take place at an OS level.

Even though the experiment modified only one targeted byte through several commands, such process can be automated and turned into a software dedicated to GPS anti-forensics, thus making the process easier and accessible to non-technical people.

4.4.2 Experiment n°7: Timestamps alteration.

As it has been shown throughout the previous experiments, recent Garmin devices tend to log most of the user interactions with the device. This being, an investigator could rely upon those pieces of information to make its investigation progress. Although it can of precious help, the following experiment try to send a warning to the forensic community, not to rely blindly upon timestamps that might have been reverted or manipulated at some time.

The procedure that has been carried out is very similar to the previous experiment. Instead of altering the data, the metadata are modified, hence making it possible to revert timestamps unwillingly modified at a first time. The procedure has been carried out on a Garmin Nüvi 2595, using a computer running Kali Linux and the SleuthKit to access and manipulate the data. The full procedure with the detailed outcomes can be found in Appendix J.

```
$fls /dev/disk/by-label/GARMIN
[...]
d/d 21: GPX

$fls /dev/disk/by-label/GARMIN 21
d/d 171155846:    Archive
r/r * 171155848:    Position.gpx
```

```
r/r 171155850:    Current.gpx

$istat /dev/disk/by-label/GARMIN 171155850 | head
[...]
Name: CURRENT.GPX

Directory Entry Times:
Written:    Wed Jul 23 12:03:10 2014
Accessed:    Tue May 27 00:00:00 2014
Created:    Sat Sep 28 10:36:32 2013
```

Instead of altering the content of a file, the aim is to modify its metadata. This information can be found in the sectors dedicated to its parent folder.

```
$istat /dev/disk/by-label/GARMIN 21
[...]
Name: GPX

Sectors:
10711992 10711993 10711994 10711995 10711996 10711997 10711998
10711999
```

The modification process is a basic “echo” command piped into the “dd” command.

```
$echo -ne "\xf0" | dd of=/dev/disk/by-label/GARMIN seek=5484540146
bs=1 count=1 conv=notrunc
1+0 records in
1+0 records out
1 byte (1 B) copied, 8.9676e-05 s, 11.2 kB/s

$istat /dev/disk/by-label/GARMIN 171155850 | head
[...]
Name: CURRENT.GPX

Directory Entry Times:
Written:    Wed Jul 16 12:03:10 2014
Accessed:    Wed Jul 16 00:00:00 2014
Created:    Sat Sep 28 10:36:32 2013
```

The command above shows the modification has been done successfully, and assesses therefore the possibility for one to have the complete control of the information present on such devices.

4.5 Conclusion

In this chapter, seven experiments have been successfully carried out on a sample of three Garmin devices from two different generations. Among these experiments, the three firsts were related to the acquisition process. The results collected show that the efficiency of acquisition does not depend of the tool being used to perform such procedure.

On the question of the device's behaviour, the results suggest that turning on/off or connecting the device to a computer does have an impact on its logical integrity. An investigator willing to conduct an investigation involving Garmin devices must be aware of this, otherwise he may leave traces on the evidence. Moreover, it has been discovered that connecting a Garmin device to a computer running Windows, without the use of any write-blocker or write-protect policy, results in all the file's accessed timestamp being updated at the day of connection.

Then, two experiments investigated what could be retrieved on Garmin devices, where it could be stored and how long is it likely to remain in the memory. These experiments permitted to highlight the structure of the file system used by Garmin devices, and assessed how long valuable data may remain on the device before being deleted (at an OS level), or totally erased of the memory. Using the structure of the information discovered, it has been possible to define hexadecimal headers and footers for two artefacts of significant value to investigators: favourite locations (i.e. waypoints) and position of the user over time (tracks). The headers and footers designed have then been used to carve out a significant amount of useful data, which could not be retrieved by the deleted file recovery feature of Autopsy.

The last category of experiment was about purposely manipulating the data without leaving traces on the device. These experiments have been conducted successfully, in which both timestamps and locational data could have been manipulated. The successfulness of such experiment warns not to blindly rely upon such data without the evidence been cross-correlated.

The experiments have been conducted and their results collected. The next chapter discuss these results and assess the experimentation process itself.

Chapter 5 Discussions

5.1 Introduction

This chapter discusses and evaluates the raw results obtained through the experiments conducted in Chapter 4. These results are then compared against those of similar studies. It also takes a global view over the different experiments to answer the objectives of the present thesis. The chapter is divided into three sections, being respectively related to forensic acquisition, analysis and evidence admissibility.

The first sections synthetize the main findings about the behaviour of Garmin devices during the acquisition process. It highlights how the device might log the interactions with the user and gives directions how to acquire the data with minimum impact on the device. It also reports on the effectiveness of the different acquisition tools used to image the memory.

The second section describes the most interesting pieces of information that can be recovered on a Garmin device. The location of these artefacts within the files is documented, and their reminiscence in the memory evaluated. This part also compares the evidence that can be recovered on Garmin and Tom-Tom devices.

The final section concerns anti-forensics and describes what manipulations can be expected on Garmin devices. It first presents the results of the experiments conducted in Chapter 4 and evaluates them against other work. The results are compared to those obtained by Lallie & Benford, (2011), which demonstrates successful alteration of locational data held in pictures of IPhone devices. The implications of anti-forensics are then discussed, taking into account both practitioners and researchers viewpoints.

5.2 Forensic acquisition of the device

As stated before, forensic acquisition is considered as a paramount phase in forensic investigations (Carrier, 2005). Regardless of the brand, studies dealing with GPS devices tend to describe how they performed their procedure, but often do not consider how the device might react to it (C. M. Colombini et al., 2012; C. Colombini, 2009; Hannay, 2008; Jones et al., 2008; Lemere & Sayers, 2009; Strawn, 2009). From the literature reviewed, Nutter (2008) has been the one of the very few to consider how the acquisition procedure might have an impact on the device's memory. Regarding Garmin devices, the research material was extremely limited. A

blog article investigated the timing data contained in the temporary file "Position.gpx", but did not investigate where the timestamp was coming from and simply concluded it was the time the device had been turned on (fork(), 2013). The experiments conducted in Chapter 4 aimed to investigate this behaviour and the method to acquire the device efficiently in a forensically sound manner. These experiments have been carried out successfully and provided several outcomes.

5.2.1 Acquisition performance

The first experiment aimed to assess the different acquisition tools when dealing with Garmin devices. The results showed the acquisition performance depends on the device itself, and not the tool used to perform the acquisition. Indeed, the acquisition time measured was very similar from a tool to another. However, big differences have been noticed when imaging a device belonging to an older generation. This is due to the use of different version of USB from one series to another, whilst Nüvi 25xx devices use USB 2.0, Nüvi 13xx devices are still using USB 1.0, hence making then imaging process longer. Recent devices also use MTP and therefore are not recognized by windows-based forensic software without changing the driver to make them being considered as Mass Storage Device instead.

Concerning the tools, Linux-based tools Guymager and the "dd" command have revealed themselves as being less invasive when used "out of the box". Indeed, without the use of a write blocker, or a write protect policy, connecting the device through USB results in updating the accessed timestamps of every file present of the device. However, if enough measures have been taken, tools are similar, although EnCase remains the only one that can access the RAM, yet outside the scope of this thesis.

5.2.2 Garmin logging system

The second and third experiments aimed to document the behaviour of Garmin devices during the imaging process. The results show that every interaction between the user and the device is being logged or at least has an impact on timestamps. The following Table 19 summarized files impacted when acquiring Garmin devices.

Table 19 Timestamps updated during the imaging process

Device is turned on	Device is turned off	Device is connected via USB
/Garmin/GarminDevice.xml /Garmin/GarminDevice.tmp	/Garmin/Diag/GarminOS.log	/GPX/Current.gpx /GPX/Position.gpx

These steps however need to be done to image the device. Since the OS of the device is responsible for this logging scheme, a solution could be to bypass it to acquire the memory. In their study on Tom-Tom devices, van

Eijk & Roeloffs (2010) noticed that if a bootable SD Card were present in the device when starting, this latter would boot on the SD card in priority rather than booting on its internal memory. Assumptions were made that Garmin devices would act the same, but the experiment carried out denied this hypothesis. Another way to prevent the OS to alter the data is to physically access the memory, using JTAG test connectors on the CPU (I. M. F. Breeuwsma, 2006; van Eijk & Roeloffs, 2010), however, as the hardware analysis of the devices goes beyond the scope of this study, this path has not been considered. Future studies on the matter should consider this option. Two levels of experimentation are possible; the first one is to dismantle the device and note the CPU used, then look at the CPU specifications to see whether it has such port or not. The second goes further and aims to reproduce the experiment conducted by van Eijk & Roeloffs (2010), in which they successfully imaged the entirety of the memory through this port. Other options exist, such as using software exploits to make the device boot on another OS, as suggested by Rabaiotti & Hargreaves (2010), or through Bluetooth or infrared as mentioned by Fiorillo (2009), however, such techniques can be hard to perform and therefore might not be worth investigating.

The interview conducted with an NHTCUS representative Mike Dickson, and forensic practitioner, highlighted a gap between forensics as considered by the research community, and the "in the field" reality. According to him, techniques such as boundary scanning via JTAG are typically not worth considering as they are hard to carry and therefore too expensive to be used at a large scale. If there is no other means to carry out the imaging process, then the evidence, although it has been altered, is still valid in court. However, investigators must be aware of what can be altered by their manipulations on the device.

5.3 Forensic analysis and file of interests

With the growing size of today's hard drives, having a structured investigation procedure is paramount to recover the relevant information in a short lapse of time. To do so, it is important to be aware of internal structure of the information, where the relevant data is stored, and how it is possible to access the most of it. Most the literature addressing Garmin files of interests reviewed considered "Current.gpx" has being the most important file held within the device (C. M. Colombini et al., 2012; Jones et al., 2008). Although, this might be true, it is yet far of being the only one. A blog article went a bit further and listed some of the file where valuable data could be contained, without going into depth about what exactly could be retrieved (fork(), 2013). The experiments carried out in section 4.3 have

been of great value to pinpoint the location of valuable forensic information, summarized in the Figure 53 below. It has to be noted that only locational data have been taken into consideration for this study, which means other folders might contain valuable information as well, such as call or text messages emitted and received on the device providing Bluetooth pairing. These artefacts can also be of great value to an investigator as they may contain evidence of communication between the suspect and its accomplice (C. M. Colombini et al., 2012; Lemere & Sayers, 2009). Such artefacts should therefore be addressed by further research.

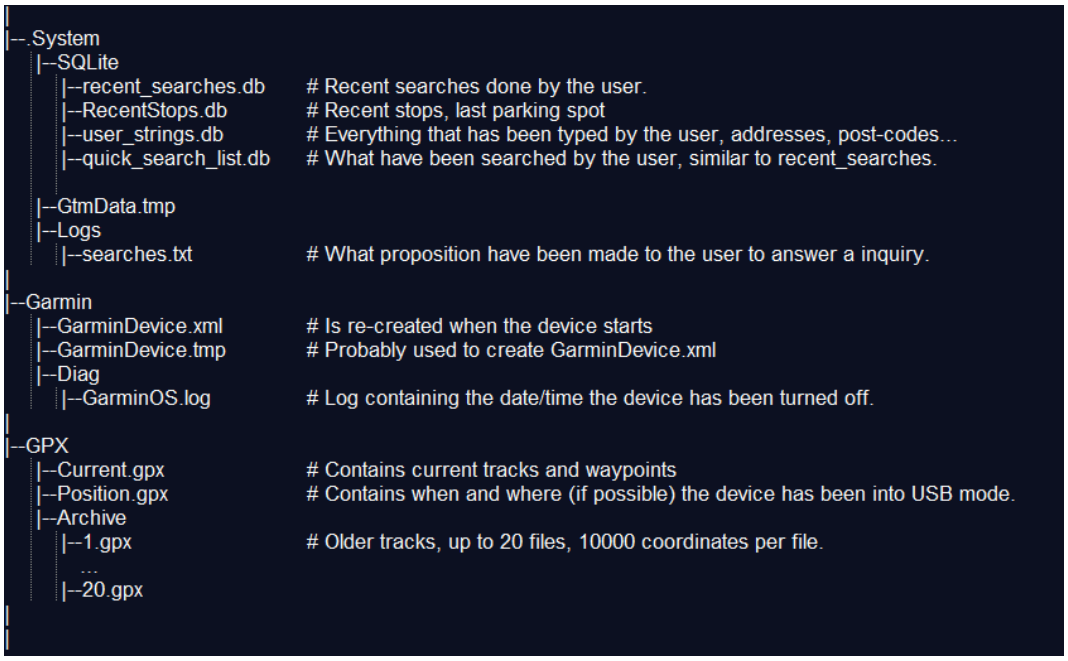


Figure 53 File structure in a Garmin Nüvi 2595

As shown in the figure above, new generations of devices log more information than before. The main difference noticed between the 13xx and the 25xx generations is the presence of databases recording the interactions a user has had with the device. These databases provide investigators with a lot of user-related information, which can be used along with digital profiling techniques to create the behavioural profile of a user.

Moreover, these experiments underlined under which conditions the data was collected by the device. Hannay, (2008) published a study in which he conducted a similar experiment on Tom-Tom devices. Depending of the mode of operation of the device, Hannay has been able to retrieve historic location data (see Figure 54). However, this data is issued by the route computation of the device, not its movement. As no information is stored, indicating whether the destination has been reached or not, it is therefore impossible to know, with certainty, where the user has actually been. Another study conducted by Nutter, (2008) on similar devices showed that no timestamps were stored along with the locational information. Because

Tom-Tom devices do not log the real-time position of the user, no timestamps need to be stored in memory. They are, just as the current location of the user, processed in the RAM, behaviour highlighted by van Eijk & Roeloffs, (2010) study, which discovered those timestamps whilst analysing the data contained by the volatile memory.

Operational Mode	Coordinants retreived	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

Figure 54 Operational Modes of Tom-Tom devices and recoverable information (Hannay, 2008)

Unlike Tom-Tom devices, Garmin devices store the actual position of the device, rather than the route that has been computed. The Table 20 shows the information recovered from a Garmin Nüvi 2595, depending on its operational mode.

Table 20 Locational information on Nüvi 2595 (Triplog enabled)

Operational mode	Coordinates retrieved	Timestamps retrieved	Path of movement known	Known if destination reached.
"View map" mode	yes	yes	yes	N/A
Nav without reaching destination	yes	yes	yes	yes
Nav and reach destination	yes	yes	yes	yes
Nav and move in opposite direction	yes	yes	yes	yes
Sleep mode	no	no	no	no

As highlighted by the results in Table 20, the Triplog feature introduced by Garmin in most of its products allows recovering very accurate and timed information on the position of a user at a given time. Full movement path have been recovered, even though no navigation had been set. This characteristic belonging to Garmin devices makes them real asset for investigations. However, few experiments have been conducted whilst the device was in sleep mode, and it has been noticed that sometimes, even with the device in sleep mode, locational data was still recorded by the feature. This behaviour has been noticed by Lehr, (2010), although his study did not deeply investigate this question either. Based on observations made during the experiments, the hypothesis is that the device will keep logging its position – even in sleep mode – until he has lost the GPS signal. In this particular case, a device in sleep mode will not try to get the signal back, whereas a device navigating or in map mode would. As this behaviour is not

yet fully understood, further research should be conducted, including a wider range of devices.

Regarding data reminiscence on Garmin devices, the experiments conducted showed that an investigator were more likely to recover the most of the information by taking into account the unallocated clusters of the memory as well. Locational data can be carved out of the memory quite easily, given their XML structure. As shown in the Figure 55, Figure 56, and Figure 57, the results suggest that carving smaller pieces of information than entire GPX file have been shown to be more effective, as the bigger the chunk of data, the more likely for it to be corrupt. Data recovery via carving has showed to be more efficient than other techniques.

With regards to the recovery of entire gpx file, the experiment showed that carving the information based on known header and trailer were more efficient than relying on standard forensic tools such as Autopsy (using fls). The Figure 55 below shows the results of this experiment and highlights that more data were extracted with scalpel, than through the "fls" command or the file browser.

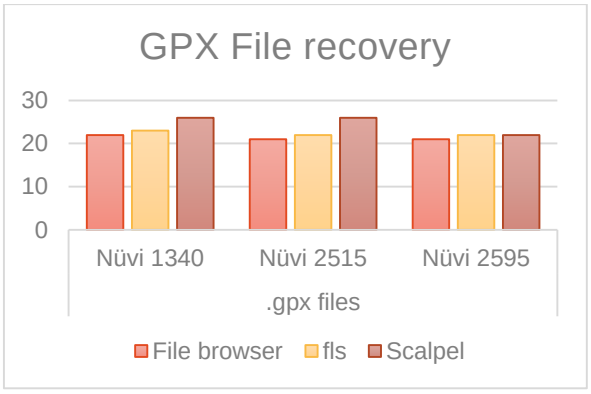


Figure 55 GPX File recovery

When considering waypoints (see Figure 56), substantially more data was recovered on the Nüvi 1340. However, the number of waypoints recovered was the same for each recovery method attempted, on every other device. This might be the result of waypoints being deleted by the user, still held within the unallocated cluster of the Nüvi 1340.

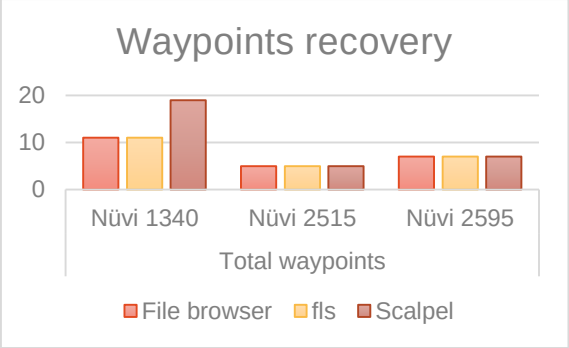


Figure 56 Waypoints recovery

Tracks are ordered lists of locational data forming a path (Topografix, 2004). As they contain the exact location of the device – and by extension its user – has been, tracks are of paramount value to investigators (Nutter, 2008). Figure 57 below shows the tracks retrieved depending of the recovery technique. Again, more data was extracted using carving methods than other techniques.

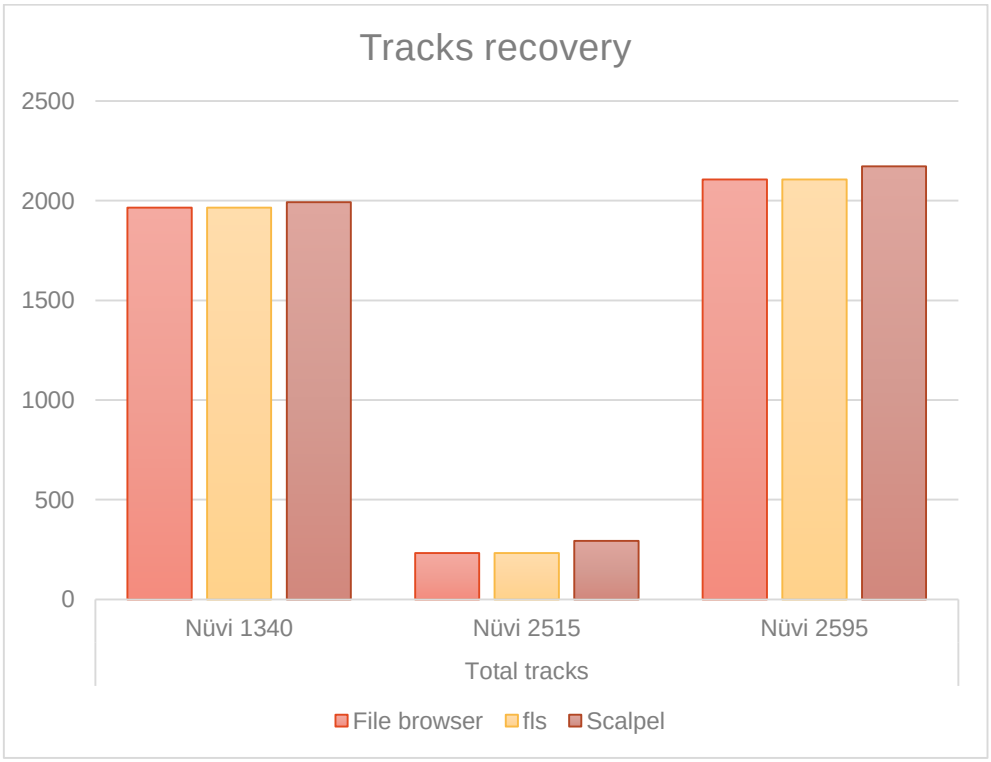


Figure 57 Tracks recovery

Additionally, as mentioned earlier, archive files are named incrementally over time. By correlating this to the results, it can be inferred that the additional .gpx files recovered with Scalpel use to be part of the archive, and has been deleted. For instance, carving files with scalpel permitted the retrieval of three more files than when using the "fls" command on the Nüvi 1340. It can therefore be inferred that those three files are likely to be part of the 44 files that have been deleted on the device. The next Table 21

resumes the number of additional .gpx files that have been recovered with scalpel, and compares these numbers to the mileage of their respective devices (expressed by the archive lowest name).

Table 21 Recovery percentages

Device	Files recovered with scalpel	Files recovered with fls	Archive's lowest name	Percentage of additional file retrieved	Deleted file recovery percentage
Nüvi 1340	26	23	44.gpx	13.0%	6.8%
Nüvi 2515	26	23	7.gpx	13.0%	42.8%
Nüvi 2595	22	22	26.gpx	0%	0%

The percentages above did not provide any further information; however, the same experiment should be conducted on a larger set of devices in order to draw conclusions. Nevertheless, it seems that the amount of data recovered remains around three to four files, regardless of the device's mileage. It has to be noticed that no files could have been recovered on the Nüvi 2595 device. As numerous deleted tracks were recovered on this same device, it is assumed that file corruption at the header and trailer level might be responsible. However, this assumption can only be asserted by conducting the same experiment on a larger set of devices.

5.4 Admissibility of locational evidences

As claimed by Ball, (2008), locational data constitutes an asset of great value for investigations. Despite known inaccuracies, GPS data is still widely used as a lead, or evidence in a court of law (Hubbard, 2008).

Two experiments have been conducted, described in section 4.4, aiming at demonstrating how locational data could easily be manipulated without leaving any traces an investigator could notice. By accessing the memory at a Byte level, one is able to manipulate the memory, without altering any timestamps (See Figure 58).

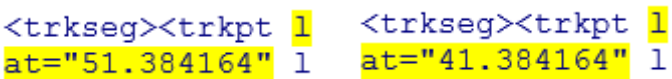


Figure 58 Original locational data versus modified data

Moreover, if any timestamps were to be modified in the process, the same technique could revert the timestamps, thus preventing anyone to discover the manipulation through the timestamps (see Figure 59).

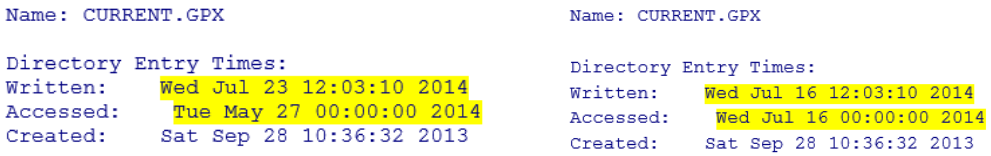


Figure 59 Original timestamp versus modified timestamp

Another experiment conducted by Lallie & Benford, (2011), aimed also at challenging the reliability of locational data contained within pictures on iPhones. As a result, they showed it was possible to modify such data contained within pictures without leaving any traces. This means a criminal could modify the data in a way it could mislead an investigator, or create an alibi for himself.

Typically in the real world, practitioners do not believe the criminals to have the knowledge to perform such manipulations (Dickson, 2014). As claimed by Ball, (2008), "The criminal genius is a creature of comic books and movies", thought which seem to be shared by NHTCUS representative Mike Dickson. In his interview, M. Dickson reported from experience that criminals would behave differently; "They would send someone else driving around with their device rather than manipulating the data inside it". However, M. Dickson acknowledged the need for the forensics community to be aware of the anti-forensics possibility.

Although anti-forensics is a quite controversial subject among the forensic community, it should not be ignored. The fact that criminals do not use these tools does not mean they will not one day.

5.5 Conclusion

This chapter discussed the main findings issued by the experiments, and compared them against other studies, reviewed in Chapter 2. Several outcomes have emerged from these discussions.

On the question of forensic acquisition for Garmin devices, this study showed the importance of considering the device's behaviour in the acquisition process, as it may have an impact on the integrity of the system. These results are similar to those observed by Nutter (2008) which documented timestamps being modified when imaging Tom-Tom devices. To prevent this, investigators must circumvent the OS and its inherent logging system. Several techniques investigated in this study might address this problem, however, as remarked by Dickson (2014), they would be too expensive to be considered on a daily basis.

The experimentation also permitted to locate several files containing timed locational data that could be of interest to investigators. Further research showed that this data was issued by the Triplog feature and the locational

data recovered was in fact the whereabouts of the GPS device's owner. These results were compared against similar studies on Tom-Tom devices, in which the only locational data found was generated by the route computation, not by the movement of the device (Hannay, 2008; Lemere & Sayers, 2009; Nutter, 2008). About locational data, this study shows that Garmin devices have a greater forensic potential than Tom-Tom devices, as the coordinates retrieved assess an actual location where the user has been.

This thesis also evaluates the reminiscence of locational data post-deletion. As stated by Garmin (Garmin, 2014b), only a limited amount of data is kept inside the device. Using specific headers and footers discovered during the experimentation, the data has been carved out of the unallocated clusters. The results were very conclusive, as a large amount of data could have been recovered. With comparison to other techniques such as the deleted file recovery feature of EnCase or Autopsy, the experiment showed that carving was more efficient, although the experiment should be conducted on a larger sample to draw conclusions.

The experiments also highlighted that Garmin devices were prone to anti-forensic techniques. Indeed, it is possible for one to manipulate every bit of information on the memory, without leaving traces nor updating timestamps. Although this raises concerns amongst the research community (Lallie & Benford, 2011; Strawn, 2009), forensic practitioners believe that criminals are typically not skilled enough to use such techniques. This also opens an interesting question, which could be addressed by further research.

Chapter 6 Conclusions

6.1 Overall conclusion

This thesis aimed to explore the forensic potential of Garmin navigation devices, and assess the reliability of the information, which may reside on them. As very few studies about Garmin devices were published at the time of writing, studies about similar devices such as Tom-Tom products have been used as a base of comparison. The project tackles three areas, respectively forensic acquisition, analysis and anti-forensics. For every one of them, both theoretical and practical aspects were considered. Through the literature reviewed and the experiments conducted, several conclusions can be drawn.

The acquisition process of such devices requires knowledge of the device, and its behaviour. Interacting with Garmin devices alters their memory, as the device logs every HMI. For instance, the system logs the time at which the device has been turned on/off, has been connected to a computer through USB or has been connected to the traffic receiver. A way to prevent this happening would be to bypass the OS, but this option is unfortunately too expensive to be used on a regular basis.

Unlike Tom-Tom devices, which store the routes the device has computed, the locational data contained inside Garmin devices can show where the device has actually been. Additionally, it has been discovered that the devices hold timestamps in their non-volatile memory has well, thus allowing an investigator to track where a suspect has been within a given timeframe.

Locational data remains on the device in an archive folder, which, according to Garmin, can contain up to 20 files, each containing up to 10000 coordinates. When this threshold is reached, the device deletes the older files. This thesis however showed that it was possible to carve out in average four to five additional files, regardless of the size of the memory, and regardless of the device's mileage.

New generation Garmin systems have databases embedded inside them, logging HMIs such as searches, text entered and POIs. Although such information does not always have timestamps associated, it can still be used to establish the behavioural profile of a user.

Investigators must remain careful when dealing with such data, and cross correlate every evidence that can be found the device. Indeed, as demonstrated through the experiments of this project, everything on the device can be manipulated without leaving any traces. Although such practices are not common amongst current criminal society, it does not mean it will not be.

6.2 Appraisal of achievements

At the beginning of this project, four objectives have been defined:

1. From the literature, review the principles and limitations of the Global Positioning System, and how this technology is used nowadays. Investigate how GPS forensic investigations are performed, regarding to a specific brand such as Tom-Tom or Garmin.

2. Based on the findings of the literature review, design a set of experiments aiming to assess forensic acquisition and analysis of Garmin systems, and challenge the reliability of the evidence retrieved.

3. Implement the experiments and document the main steps in order to make them reproducible. Collect the raw results.

4. Discuss and evaluate the results, by comparing them to similar studies conducted by the community.

6.2.1 Objective n°1

The first objective has been achieved and reported in Chapter 2. The first aim of the literature review was to provide a background knowledge to the reader. Although most of GPS forensics studies introduces their research by describing GPS principles, it has been found that most of these were vague. In order to remain rigorous in the terms and principles, the very basics of GPS were studied from Parkinson, (1997) who was the original GPS program director.

Concerning GPS forensics, the literature is mainly focused on Tom-Tom devices, and rarely addresses Garmin devices. Amongst the few studies investigating Garmin devices, the devices considered were old devices, not in use at the time of writing. These devices did not provide the investigator with any data of interest. The first hypothesis for this lack of interest towards Garmin devices was therefore that those were not storing any data

of interest, therefore being pointless to investigators. Mike Dickson, a forensic practitioner, remarked that in fact, the vast majority of devices were Tom-Tom devices, therefore explaining this lack of interest from the forensic community (Dickson, 2014). However, he also acknowledged such devices should be documented, as well as the procedure needed to investigate them.

The review of GPS limitations highlighted a concern within the forensic community, about locational data being inaccurate and prone to manipulation. Although this concern is generally mentioned as something to be aware of, little research have actually been carried on GPS anti-forensics. The closest similar study was an experiment conducted by Lallie & Benford, (2011), in which pictures were extracted from an IPhone, their locational data were modified and the picture were putted back in the device. During their experiment they did not modified any timestamps that could assess the modification. This study then inspired part of this study, dedicated to locational anti-forensics on Garmin devices.

6.2.2 Objective n°2

The second objective was met by the creation of a set of experiment, aiming to investigate the different forensic methods, and the artefacts recovered. This objective is reported in Chapter 3. Those experiments have been divided into three categories. In total, seven experiments were designed, based on Research questions issued from the literature and personal reflections.

The three firsts are related to forensic acquisition and intends to evaluate tools and methods that can be used to acquire the memory inside Garmin devices. The literature reviewed also showed that interaction between the user and the device were likely to be log by the OS of the device. As such, characteristic might influence the logical integrity of the system. An experiment has been designed accordingly in order to document which interaction was likely to be logged, and what impact it would have on the memory.

Two experiments are then related to forensic analysis, focused on where data of interest might be hold, and for how long it is likely to remain on the memory. In order to evaluate the reminiscence of the data on the memory, the structure of the files must be known, in order to carve them out of the unallocated clusters, based on their header and trailer. The successfulness of the first experiment has therefore a direct impact on the success of the second.

The last two experiments are related to anti-forensics and investigate whether Garmin devices are prone to anti-forensic techniques or not. In order to evaluate this. The targeted data needs to be accessed at a byte level, hence preventing the OS to update any timestamps.

6.2.3 Objective n°3

The third objective, reported in Chapter 4, was to conduct the set designed as second objective. All experiments were conducted successfully and provided some very interesting results. These latter were collected and permitted to highlight several outcomes.

On the question of forensic acquisition, the tools were evaluated based on their execution time. The results collected show that every tools considered in the experiment were equivalent by the minute. The performance of the acquisition therefore does not rely upon the tool used.

The experimentation also enumerated cases where the device logged events inside its memory. On this matter, it has been shown that turning on/off a Garmin device, or connecting it to a computer results in the memory of the device being altered. The experiment permitted to pinpoint the files containing the log entries. Moreover, is has been shown that a connection to a windows machine without the use of a write-blocker, lead to all the files "accessed timestamp" being updated. To prevent this, this thesis proposes a manipulation of the Microsoft Registry, aiming to set up a write-protect policy.

For the purpose of artefact location, three Garmin devices were carried when traveling with a car around Edinburgh. The procedure tried to consider as mush case study as possible, beginning with those described in Nutter, (2008). This experiment permitted to recover most of location where the user has been, apart from when the device was in sleep mode. Concerning the literature formerly reviewed, this experiment had never been carried out on Garmin devices before. Results can nevertheless be compared to those obtained on similar devices such as Tom-Tom, which has been done in the Chapter 5.

Before this project, no study seemed to have documented the reminiscence of locational data within a GPS device, nor the best methods to recover deleted information. The experiment conducted discovered it was possible to recover more information than with the standard forensic tools by carving the information, based on fixed headers and footers. It has also be demonstrated that for the carving process to be more efficient, the smallest entity of information should be considered. In the case of this study, the information about where the user has been is contained in a ".gpx" file,

which contains a set of "tracks" – each track being a set of timed-coordinates composing the journey of a user – and waypoints – being the user's favourite locations. By carving tracks and waypoints rather than ".gpx" files, the information is less likely to be corrupted. However, the experiment should be conducted on a larger sample to draw conclusions.

The last experiment being conducted aimed to assess the possibility of anti-forensics techniques on Garmin devices. As this type of experiment had not been conducted on GPS devices, the procedure was inspired by a study on IPhone pictures' geo-tag reliability. All the procedure were carried out successfully, meaning Garmin devices were prone to anti-forensic techniques.

6.2.4 Objective n°4

The fourth objective has been met by the discussion of the results occurring in Chapter 5, which was drawing the outcomes of this project, by correlating the results obtained and the literature formerly reviewed. The discussion also permitted to regroup the different outcomes and address the leading goal of this project, which was exploring forensic methods applicable to Garmin devices, and document locational artefacts located on them.

Comparing the results obtained through experimentation to those obtained in similar studies permitted to highlights the main contributions of this study, which is of use to many practitioners.

Regarding acquisition practices, the current work listed the interactions investigators are likely to have with the device, which results in timestamps being modified. This information makes investigators aware of their repercussions when acquiring Garmin devices, and can help them to decide whether to conduct the acquisition or not.

On the question of locational artefacts, the study recovered timed locational data, permitted investigators to investigate up to 6 month of a suspect's whereabouts. This is of paramount value to investigators, especially as Tom-Tom devices do not hold such data and are only able to provide computed routes. Moreover, the data recovered through carving into the unallocated clusters might expand this period. However, the data recovered within unallocated clusters has not been dated.

Anti-forensics is an interesting area, where the research community and practitioners are strongly in disagree on the sociologic aspect of the question, being whether or not a criminal would use such techniques. However, about the possibility of anti-forensics, this thesis clearly demonstrated that such techniques were possible on Garmin devices, and were undeniably prone to be automated.

6.3 Future work

In order to help forensic examiners to handle Garmin forensics successfully, more research is needed.

The scope of the present study was limited to locational artefacts. However, the literature reviewed showed other information related to the user were likely to be found on such devices. As these devices are more and more considered as mass storage devices, investigators can expect the same data that can be found on a standard personal computer. Moreover, the features offered by these devices to connect user's smartphones may lead to the recovery of data belonging to the cell phone, inside the GPS.

The use of NAND-based flash memory inside GPS devices has been mentioned, however, its impact on the data reminiscence has not been evaluated. This would be a good area to research, as it has been demonstrated that wear levelling and garbage-collection mechanisms do have an impact on forensics investigations.

As it has been previously mentioned, the behaviour of the Triplog feature whist the device is in sleep mode should be subject to further experimentation. Although this thesis addressed partially this case study, the results whilst driving with the device in sleep mode where inconsistent. Sometimes the device would record the location for hours, whereas during other experiments, the logging would stop as soon as the device enters the mode.

Other memory should be investigated, such as the RAM, or the GPS chips itself. It has been proven that RAM inside Tom-Tom devices contains valuable information such as timestamps. Garmin may hold also a great deal of information within volatile memory.

Concerning acquisition methods, more experiments should be conducted. In order to assess the possibility to acquire Garmin devices through JTAG boundary scanning, it would be interesting to dismantle the device and compare the reference of the CPU to verify the presence of a JTAG port.

References

AccessData. (2014). FTK Imager. Retrieved June 27, 2014, from http://www.accessdata.com/support/product-downloads

Agarwal, A., D'Angelo, A., & Jin, K. (2008). Targeting advertisements in a social network. *US Patent App. 12/ ….* Retrieved from http://www.google.com/patents/US20090070219

Baker, S. (2003). Method and apparatus for distributing location-based messages in a wireless communication network. *US Patent 6,505,046*. Retrieved from http://www.google.com/patents/US6505046

Ball, C. (2008). Legal Technology - GPS Evidence Might Drive Your Case Home.

Barnes, S. (2006). A privacy paradox, *11*(9), 1–9. Retrieved from http://firstmonday.org/issues/issue11_9/barnes/index.html

Barrett, T., & England, G. Civil Use of the Global Positioning System (2008). Retrieved from http://www.gps.gov/policy/docs/2008-dod-dot-agreement.pdf

Beebe, N. (2009). Digital forensic research: The good, the bad and the unaddressed. *Advances in Digital Forensics V*. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-04155-6_2

Bekraoui, N., Cazorla, G., & Léger, L. (2010). Les systèmes d'enregistrement et d'analyse quantitatifs dans le football. *Science & Sports*, *25*(4), 177–187. doi:10.1016/j.scispo.2010.03.006

Breeuwsma, I. M. F. (2006). Forensic imaging of embedded systems using JTAG (boundary-scan). *Digital Investigation*, *3*(1), 32–42. doi:10.1016/j.diin.2006.01.003

Breeuwsma, M., & Jongh, M. De. (2007). Forensic data recovery from flash memory. *Small Scale Digital …*, *1*(1). Retrieved from http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf

cargpsrating.com. (2014). TomTom VS Garmin 2014 - Car GPS Ratings 2013 - 2014. Retrieved July 05, 2014, from http://www.cargpsratings.com/tomtom-vs-garmin/

Carrier, B. (2005). *File system forensic analysis*.

Casey, E. (2011). *Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet* (pp. 633–669). Academic Press; 3 edition.

China National Space Administration. (2014). BeiDou Navigation Satellite System. Retrieved June 25, 2014, from http://en.beidou.gov.cn/csnclist.html

Colombini, C. (2009). Experimental testing of a forensic analysis method on the tomtom gps navigation device. Retrieved from http://www.gpsforensics.org/downloads/tomtom_forensics_colombini_english.pdf

Colombini, C. M., Colella, A., Castiglione, A., & Scognamiglio, V. (2012). The Digital Profiling Techniques Applied to the Analysis of a GPS Navigation Device. *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 591–596. doi:10.1109/IMIS.2012.202

Cusack, B., & Simms, M. (2011). Evidential recovery from GPS devices. *Journal of Applied Computing and Information Technology*. Computing and Information Technology Research and Education, New Zealand (CITRENZ). Retrieved from http://citrenz.ac.nz/JACIT/JACIT1501/2011Cusack_EvidentialRecovery.html

Daily Mail. (2012). Higinio O. Ochoa III: FBI led to Anonymous hacker after his girlfriend posts picture of her breasts online. Retrieved June 26, 2014, from http://www.dailymail.co.uk/news/article-2129257/Higinio-O-Ochoa-III-FBI-led-Anonymous-hacker-girlfriend-posts-picture-breasts-online.html

David Lee Vs Commonwealth. D. Lee Vs Commonwealth of Virginia (2012).

Dickson, M. (2014). *Interview of the 14 July 2014*. Edinburgh.

Digital Dispatch. (2014). DDS Digital Dispatch. Retrieved July 07, 2014, from http://www.digital-dispatch.co.uk/

Doherty, E. P. (2013). *Digital Forensics for Handheld Devices* (pp. 32–36;105–126). Boca Raton: CRC Press.

Dubey, S., Wahi, R., & Gwal, A. K. (2006). Ionospheric effects on GPS positioning. *Advances in Space Research*, *38*(11), 2478–2484. doi:10.1016/j.asr.2005.07.030

European Commission. (2011). Mid-term review of the European satellite radio navigation programmes. In *REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL*.

European GNSS Agency. (2014). Galileo is the European global satellite-based navigation system. Retrieved June 24, 2014, from http://www.gsa.europa.eu/galileo-0

European Union. (2010). *European GNSS (Galileo) open service. Signal in space. Interface control document. Issue 1.1*. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:European+GNSS+(Galileo)+Open+Service+-+Signal+In+Space+Interface+Control+Document#1

Federal space agency. (2014). Information analytical centre of GLONASS and GPS controlling. Retrieved June 25, 2014, from http://www.glonass-center.ru/en/index.php

Fiorillo, S. (2009). Theory and practice of flash memory mobile forensics. *Australian Digital Forensics Conference*. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1066&context=adf

Forensics from the sausage factory. (2009). Garmin nüvi 200 Sat Nav device. Retrieved June 22, 2014, from http://forensicsfromthesausagefactory.blogspot.co.uk/2009/04/garmin-nuvi-200-sat-nav-device.html

fork(). (2013). Examination of Garmin Nüvi 1490. Retrieved June 22, 2014, from http://forensicsblog.org/research-gps-device-analysis/

Garfinkel, S. (2007). Anti-forensics: Techniques, detection and countermeasures. *2nd International Conference on I-Warfare and* .... Retrieved from http://books.google.co.uk/books?hl=en&lr=&id=qH7hAXN0b4sC&oi=fnd&pg=PA77&dq=anti-forensics&ots=Blx_eq_ice&sig=QJPbDMk8zZP5SbJLG3WjEB9PBeg

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, *7*, S64–S73. doi:10.1016/j.diin.2010.05.009

Garmin. (2014a). Garmin | United Kingdom | Forerunner 10. Retrieved July 07, 2014, from http://www.garmin.com/uk/forerunner10

Garmin. (2014b). What is a trip log and how does it work on a nuvi, dezl, LIVE, Camper/RV, or zumo device? Retrieved August 07, 2014, from https://support.garmin.com/support/searchSupport/case.faces?caseId={c1126680-af61-11dd-f60b-000000000000}

Garmin. (2014c). Why doesn't my computer detect my device when it's in USB Mass Storage Mode? Retrieved August 03, 2014, from http://support.garmin.com/support/searchSupport/case.faces?supportPage=nuvi 2595&caseId={7c0d7580-0494-11dc-e004-000000000000}&locale=en_US

Garmin Connect. (n.d.). Garmin Connect. Retrieved July 07, 2014, from http://connect.garmin.com/en-GB/

Gershman, B. L. (2009). Privacy Revisited: GPS Tracking as Search and Seizure. *Pace Law Review*, *30*. Retrieved from

http://heinonline.org/HOL/Page?handle=hein.journals/pace30&id=935&div=&collection=

Gibbons, G. (2014). China Plans to Complete BeiDou Ahead of Schedule. *Inside GNSS*. Retrieved from http://www.insidegnss.com/node/4040

Google Inc. (2014a). Chrome Browser. Retrieved August 13, 2014, from http://www.google.com/intl/en_uk/chrome/browser/

Google Inc. (2014b). Google Earth. Retrieved August 13, 2014, from http://www.google.co.uk/intl/en_uk/earth/

Greenberger, A. J., & Homayoon, S. (1994, October 11). High-speed integrated circuit testing with JTAG. Retrieved from http://www.google.com/patents/US5355369

Guizzo, E. (2011). How Google's Self-Driving Car Works? *IEEE Spectrum*. Retrieved from http://spectrum.ieee.org/automaton/robotics/artificial-intelligence/how-google-self-driving-car-works

Hand, L. (1958). The Bill of Rights. Retrieved from http://scholar.google.fr/scholar?hl=en&q=bill+of+rights&btnG=&as_sdt=1,5&as_sdtp=#1

Hannay, P. (2008). Forensic acquisition and analysis of the tomtom one satellite navigation unit. Retrieved from http://ro.ecu.edu.au/adf/45/

Harrill, D., & Mislan, R. (2007). A small scale digital device forensics ontology. *Small Scale Digital Device Forensics Journal*, *1*(1), 1–7. Retrieved from http://ssddfj.org/papers/SSDDFJ_V1_1_Harrill_Mislan.pdf

Hofmann-Wellenhof, B., Lichtenegger, H., & Wasle, E. (2007). *GNSS – Global Navigation Satellite Systems: GPS, GLONASS, Galileo, and more (Google eBook)* (Vol. 2007, p. 548). Springer.

Huang, P.-C., Chang, Y.-H., Kuo, T.-W., Hsieh, J.-W., & Lin, M. (2008). The Behavior Analysis of Flash-Memory Storage Systems. *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, 529–534. doi:10.1109/ISORC.2008.33

Hubbard, B. (2008). Police turn to secret weapon: GPS device. *Washington Post. Retrieved January*, 11–13. Retrieved from http://chrisleibiglaw.com/documents/secretgps.pdf

Humphreys, T. (2012). How to fool a GPS. *TED.com*. Retrieved June 24, 2014, from http://www.ted.com/talks/todd_humphreys_how_to_fool_a_gps#t-25631

Iqbal, M., & Lim, S. (2008). Legal and ethical implications of GPS vulnerabilities. *J. Int'l Com. L. & Tech.* Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jcolate3&section=21

Jones, D., Sutherland, I., & Tryfonas, T. (2008). Global Positioning Systems: Analysis Principles and Sources of Evidence in User Devices. In *2008 Third International Annual Workshop on Digital Forensics and Incident Analysis* (pp. 30–39). IEEE. doi:10.1109/WDFIA.2008.12

Kahveci, M., & Can, N. (2013). Legal issues in GNSS applications: Past, today and tomorrow. *... in Space Technologies (RAST), 2013 6th ...*, 395–399. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6581239

Karim, W. (2004). Privacy Implications of Personal Locators: Why You Should Think Twice before Voluntarily Availing Yourself to GPS Monitoring, The. *Wash. UJL & Pol'y*. Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/wajlp14&section=19

Key, E. (1995). Techniques to counter GPS spoofing. *Internal Memorandum, MITRE Corporation*.

King, C., & Vidas, T. (2011a). Empirical analysis of solid state disk data retention when used with contemporary operating systems. *Digital Investigation*, *8*, S111–S117. doi:10.1016/j.diin.2011.05.013

King, C., & Vidas, T. (2011b). Empirical analysis of solid state disk data retention when used with contemporary operating systems. *Digital Investigation*, *8*, S111–S117. doi:10.1016/j.diin.2011.05.013

Klobuchar, J. (1996). Ionospheric effects on GPS. *Global Positioning System: Theory and Applications*. Retrieved from http://scholar.google.fr/scholar?hl=en&q=ionosheric+effects+on+gps+klobuchar&btnG=&as_sdt=1,5&as_sdtp=#0

Koppel, A. (2009). Warranting a warrant: fourth amendment concerns raised by law enforcement's warrantless use of GPS and cellular phone tracking. *U. Miami L. Rev.* Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/umialr64&section=40

Krumm, J. (2009). A survey of computational location privacy. *Personal and Ubiquitous Computing*. Retrieved from http://link.springer.com/article/10.1007/s00779-008-0212-5

Lallie, H., & Benford, D. (2011). Challenging the Reliability of iPhone - Geo-tags. *The International Journal of Forensic Computer Science*, *6*(1), 59–67. doi:10.5769/J201101004

Larsen, P. B. (2001). Issues relating to civilian and military dual uses of GNSS. *Space Policy*, *17*(2), 111–119. doi:10.1016/S0265-9646(01)00007-8

Last, D. (2009). GPS Forensics, Crime, and Jamming. *GPS World*, 1–3. Retrieved from http://www.professordavidlast.co.uk/cms_items/f20100528133346.pdf

Lehr, J. (2010). Linux Sleuthing: Garmin GPS: What you don't know can track you! Retrieved June 27, 2014, from http://linuxsleuthing.blogspot.co.uk/2010/11/garmin-gps-what-you-dont-know-can-track.html

LeMere, B., & Sayers, A. (2009). TomTom GPS Device Forensics | ForensicFocus.com. Retrieved June 22, 2014, from http://www.forensicfocus.com/tomtom-gps-device-forensics

Lemere, B., & Sayers, A. (2009). TomTom GPS Device Forensics Mobile Phone Forensics, 4–7.

Lim, K.-S., Lee, C., Park, J. H., & Lee, S.-J. (2012). Test-driven forensic analysis of satellite automotive navigation systems. *Journal of Intelligent Manufacturing*, *25*(2), 329–338. doi:10.1007/s10845-012-0653-6

McGrath, P. (2011). Tracking Knotts: How GPS Technology Is Influencing Traditional Fourth Amendment Jurisprudence. *J. High Tech. L.*, *231*, 231–272. Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jhtl12&section=8

McWilliam, N., Teeuw, R., Whiteside, M., & Zukowskyj, P. (2005). GIS, GPS, and remote sensing - Field Techniques Manual. In *Royal Geographical Society* (pp. 79–109).

Mozilla. (2014). Download Firefox. Retrieved August 13, 2014, from https://www.mozilla.org/en-GB/firefox/new/

National Coordination Office for Space-Based Positioning Navigation and Timing. (2014). GPS. Retrieved June 25, 2014, from http://www.gps.gov/

National Geospacial-Intelligence Agency. (1984). World Geodetic System 1984 (WGS84). Retrieved June 26, 2014, from http://web.archive.org/web/20120401083859/http://earth-info.nga.mil/GandG/wgs84/index.html

Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005). First Responders Guide to Computer Forensics. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA443483

Nutter, B. (2008). Pinpointing TomTom location records: A forensic analysis. *Digital Investigation*, *5*(1-2), 10–18. doi:10.1016/j.diin.2008.06.003

Otero, A., Otero, J., & Sánchez, L. (2009). Using Fuzzy Techniques for Bounding the Tolerance of GPS-Based Speed and Distance Measurements in Taximeter Verification. *2009 Ninth International Conference on Intelligent Systems Design and Applications*, 743–748. doi:10.1109/ISDA.2009.158

Palmer, G. (2001). A Road Map for Digital Forensic Research. In *Proceedings of the 2001 Digital Forensics Research Workshop (DFRWS 2004)* (pp. 1–42). doi:10.1111/j.1365-2656.2005.01025.x

Paraben. (2014). Device Seizure. Retrieved June 27, 2014, from https://www.paraben.com/device-seizure.html

Parkinson, B. (1997). Origins, evolution, and future of satellite navigation. *Journal of Guidance, Control, and Dynamics*. Retrieved from http://arc.aiaa.org/doi/pdf/10.2514/2.4027

Piacentini, M., & Morgan, P. (2012). SQLite Database Browser. Retrieved August 13, 2014, from http://sqlitebrowser.org/

Postema, G. J. (1983). Moral Responsability in Professional Ethics. In W. L. Robison, M. S. Pritchard, & J. Ellin (Eds.), *Profits and Professions*. Totowa, NJ: Humana Press. doi:10.1007/978-1-4612-5625-0

Pozzobon, O., Wullems, C., & Kubik, K. (2004). Secure tracking using trusted GNSS receivers and Galileo authentication services. *Positioning*, *3*(1), 200–207. Retrieved from http://file.scirp.org/Html/273.html

Rabaiotti, J. R., & Hargreaves, C. J. (2010). Using a software exploit to image RAM on an embedded system. *Digital Investigation*, *6*(3-4), 95–103. doi:10.1016/j.diin.2010.01.005

Sandisk. (2013). MTP or MSC. Retrieved August 02, 2014, from http://kb.sandisk.com/app/answers/detail/a_id/162/~/mtp-or-msc

Sansurooah, K. (2009). A forensics overview and analysis of USB flash memory devices. *Australian Digital Forensics Conference*. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1069&context=adf

Sartin, B. (2006). ANTI-Forensics–distorting the evidence. *Computer Fraud & Security*. Retrieved from http://www.sciencedirect.com/science/article/pii/S1361372306703542

Spencer, E., & Weber, L. (2013, October 22). The Boss Is Watching: Tracking Technology Shakes Up Workplace - WSJ. *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424052702303672404579151440488919138

Starcom Systems. (2014). Container tracking system | Starcom Systems. Retrieved July 07, 2014, from http://www.starcomsystems.com/products/triton

Strawn, C. (2009). Expanding the potential for GPS evidence acquisition. *Small Scale Digital Device Forensics Journal*, *3*(1), 1–12. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.187.1135&rep=rep1&type=pdf

Taylor, S. K. (2011). Forensic Acquisition on MP3 Players, (May 2010), 143–147.

Theiss, A., 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. doi:10.1016/j.csi.2004.06.003

TheSleuthKit. (2014). The Sleuth Kit (TSK) & Autopsy: Open Source Digital Forensics Tools. Retrieved from http://www.sleuthkit.org/

Topografix. (2004). GPX: the GPS Exchange Format. Retrieved August 03, 2014, from http://www.topografix.com/gpx.asp

TrackYour. (2014). Track Your Child, Elderly, Pets or Possessions. GPS Trackers & More. Retrieved July 07, 2014, from http://www.trackyour.co.uk/

Trimble.com. (2014). Trimble – Agriculture. Retrieved July 08, 2014, from http://www.trimble.com/Agriculture/index.aspx

U.S. Department of Commerce. (2000). Civilian Benefits of Discontinuing Selective Availability. Retrieved June 24, 2014, from http://www.gps.gov/systems/gps/modernization/sa/benefits/

U.S. Department of Defense. (2007). DoD Permanently Discontinues Procurement Of Global Positioning System Selective Availability. Retrieved June 24, 2014, from http://www.defense.gov/releases/release.aspx?releaseid=11335

US Department for Homeland Security. (2014). GPS CONSTELLATION STATUS FOR 06/25/2014. Retrieved June 25, 2014, from http://www.navcen.uscg.gov/?Do=constellationStatus

Van Eijk, O., & Roeloffs, M. (2010). Forensic acquisition and analysis of the Random Access Memory of TomTom GPS navigation systems. *Digital Investigation*, *6*(3-4), 179–188. doi:10.1016/j.diin.2010.02.005

Volpe, J. (2001). Vulnerability assessment of the transportation infrastructure relying on the global positioning system.

Warner, J., & Johnston, R. (2003). GPS spoofing countermeasures. *Homeland Security Journal*. Retrieved from http://72.52.208.92/~gbpprorg/mil/gps4/GPS-Vulnerability-LosAlamos.pdf

Willassen, S. (2005). Forensic analysis of mobile phone internal memory. *Advances in Digital Forensics*. Retrieved from http://link.springer.com/chapter/10.1007/0-387-31163-7_16

Williams, C. J. (2008). Watch out for the snitch sitting on your dashboard. *Los Angeles Times*, pp. 1–2.

Work, D., & Bayen, A. (2008). Impacts of the mobile internet on transportation cyberphysical systems: traffic monitoring using smartphones. *National Workshop for Research on* …. Retrieved from http://bayen.eecs.berkeley.edu/sites/default/files/conferences/cps2.pdf

Appendix A Initial Project Proposal

EDINBURGH NAPIER UNIVERSITY SCHOOL OF COMPUTING

MSc RESEARCH PROPOSAL

1. Student details

Last (family) name	Arbelet
First name	Alexandre
Napier matriculation number	40112000

2. Details of your programme of study

MSc Programme title	Advanced Security and Digital Forensics
Year that you started your diploma modules	2013
Month that you started your diploma modules	September
Mode of study of diploma modules	Full-time
Date that you completed/will complete your diploma modules at Napier	August 2014

3. Project outline details

Please suggest a title for your proposed project. If you have worked with a supervisor on this proposal, please provide the name. NB you are strongly advised to work with a member of staff when putting your proposal together.

Title of the proposed project	Forensic acquisition and analysis of Garmin GPS navigation systems.
Name of supervisor	Rich MacFarlane
I do not have a member of staff lined up to supervise my work	

4. Brief description of the research area - background

Please provide background information on the *broad research area* of your project in the box below. You should write in narrative (not bullet points). The academic/theoretical basis of your description of the research area should be evident through the use of references. Your description should be between half and one page in length.

In the early morning of May 2nd, 2000, a silent but huge step has been taken concerning the Global Positioning System (GPS). "Every civilian GPS receiver around the globe went from errors the size of a football field to errors the size of small room" (Humphreys, 2012). This change led the explosion of GPS devices in popularity. As GPS chips become smaller and cheaper, the range of application using them becomes wider (watches, navigation systems, smartphones, digital camera ...) (Strawn, 2009), hence making their presence ubiquitous.

This ubiquity, and the way GPS devices are commonly used, transform those devices into "real digital diaries" (C. M. Colombini, Colella, Castiglione, & Scognamiglio, 2012), hence being really valuable to investigator for creating digital profile of a suspect or providing one's vehicle movement history (Last, 2009). So far, the research community have published papers on how to forensically investigate GPS devices, but it either addresses GPS broadly (Cusack & Simms, 2011; Last, 2009; Strawn, 2009) or TomTom devices (C. Colombini, 2009; Hannay, 2008; Nutter, 2008; van Eijk & Roeloffs, 2010), yet challenger in the area.

The current global leader of this market is the USA-based firm "Garmin". With regards to forensic

analysis, there has been very few research that addressed Garmin devices so far, every one of each recommending further research on these devices (C. M. Colombini et al., 2012; Jones, Sutherland, & Tryfonas, 2008). Unlike other brands like TomTom or Navtech, Garmin devices seem to hide a part of their memory, making them harder to investigate (Jones et al., 2008). This characteristics led the online community "forensicfocus.com" to state the need for a deeper investigation of Garmin devices (ForensicFocus.com, n.d.).

5. **Project outline for the work that you propose to complete**

Please complete the project outline in the box below. You should use the emboldened text as a framework. Your project outline should be between half and one page in length.

The idea for this research arose from:

First, I have always been interested by positioning systems. One of my BSc coursework was dedicated Ultra Wideband indoor positioning systems and my BSc project was using this GPS and Cell-id positioning to survey individuals' locations, and trigger alerts if they were to cross predefined borders. As these devices have not been yet widely investigated, and owning a Garmin device myself, it seemed to me an interesting challenge to take up.

The aims of the project are as follows:

This project aims to provide a better understanding of GPS forensics related to Garmin devices. It aims as well to provide a road map to help forensic investigators to undertake investigation on these devices, and, if there is some time left, provide them with a tool able to retrieve these information automatically.

The main research questions that this work will address include:

- Where, physically and logically, does Garmin devices store the data related to the user's trips, searches and so on?
- What data can be retrieved from such devices?
- What does that imply for the forensic community as well as for the police?
- How can a forensic investigation be conducted in a non-invasive way, without impacting on the physical and logical integrity of the device?
- Would it be possible to create a process to help such investigation?
- Can this process be automated?

The software development/design work/other deliverable of the project will be:

- A road map to conduct forensic investigation on Garmin GPS devices.
- (If time left) - A tool automating the data gathering and the analysing process.

The project will involve the following research/field work/experimentation/evaluation:

- A research into current GPS/embedded systems forensic methodology.
- Establish a state of the art of Garmin devices forensics.
- Define a methodology and conduct a case study on a couple of Garmin Satnavs.

6. References

Please supply details of all the material that you have referenced in sections 6 and 7 above. You should include at least three references, and these should be to high quality sources such as refereed journal and conference papers, standards or white papers. Please ensure that you use a standardised referencing style for the presentation of your references, e.g. APA, as outlined in the yellow booklet available from the School of Computing office and http://www.soc.napier.ac.uk/~cs104/mscdiss/moodlemirror/d2/2005_hall_referencing.pdf

Colombini, C. (2009). Experimental testing of a forensic analysis method on the tomtom gps navigation device. Retrieved from http://www.gpsforensics.org/downloads/tomtom_forensics_colombini_english.pdf

Colombini, C. M., Colella, A., Castiglione, A., & Scognamiglio, V. (2012). The Digital Profiling Techniques Applied to the Analysis of a GPS Navigation Device. *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 591–596. doi:10.1109/IMIS.2012.202

Cusack, B., & Simms, M. (2011). Evidential recovery from GPS devices. *Journal of Applied Computing and Information Technology*. Computing and Information Technology Research and Education, New Zealand (CITRENZ). Retrieved from http://citrenz.ac.nz/JACIT/JACIT1501/2011Cusack_EvidentialRecovery.html

ForensicFocus.com. (n.d.). Project Ideas for Digital Forensics Students. Retrieved April 23, 2014, from http://www.forensicfocus.com/project-ideas

Hannay, P. (2008). Forensic acquisition and analysis of the tomtom one satellite navigation unit. Retrieved from http://ro.ecu.edu.au/adf/45/

Humphreys, T. (2012). How to fool a GPS. TED.com. Retrieved from http://www.ted.com/talks/todd_humphreys_how_to_fool_a_gps#t-25631

Jones, D., Sutherland, I., & Tryfonas, T. (2008). Global Positioning Systems: Analysis Principles and Sources of Evidence in User Devices. In *2008 Third International Annual Workshop on Digital Forensics and Incident Analysis* (pp. 30–39). IEEE. doi:10.1109/WDFIA.2008.12

Last, D. (2009). GPS Forensics, Crime, and Jamming. *GPS World*, 1–3. Retrieved from http://www.professordavidlast.co.uk/cms_items/f20100528133346.pdf

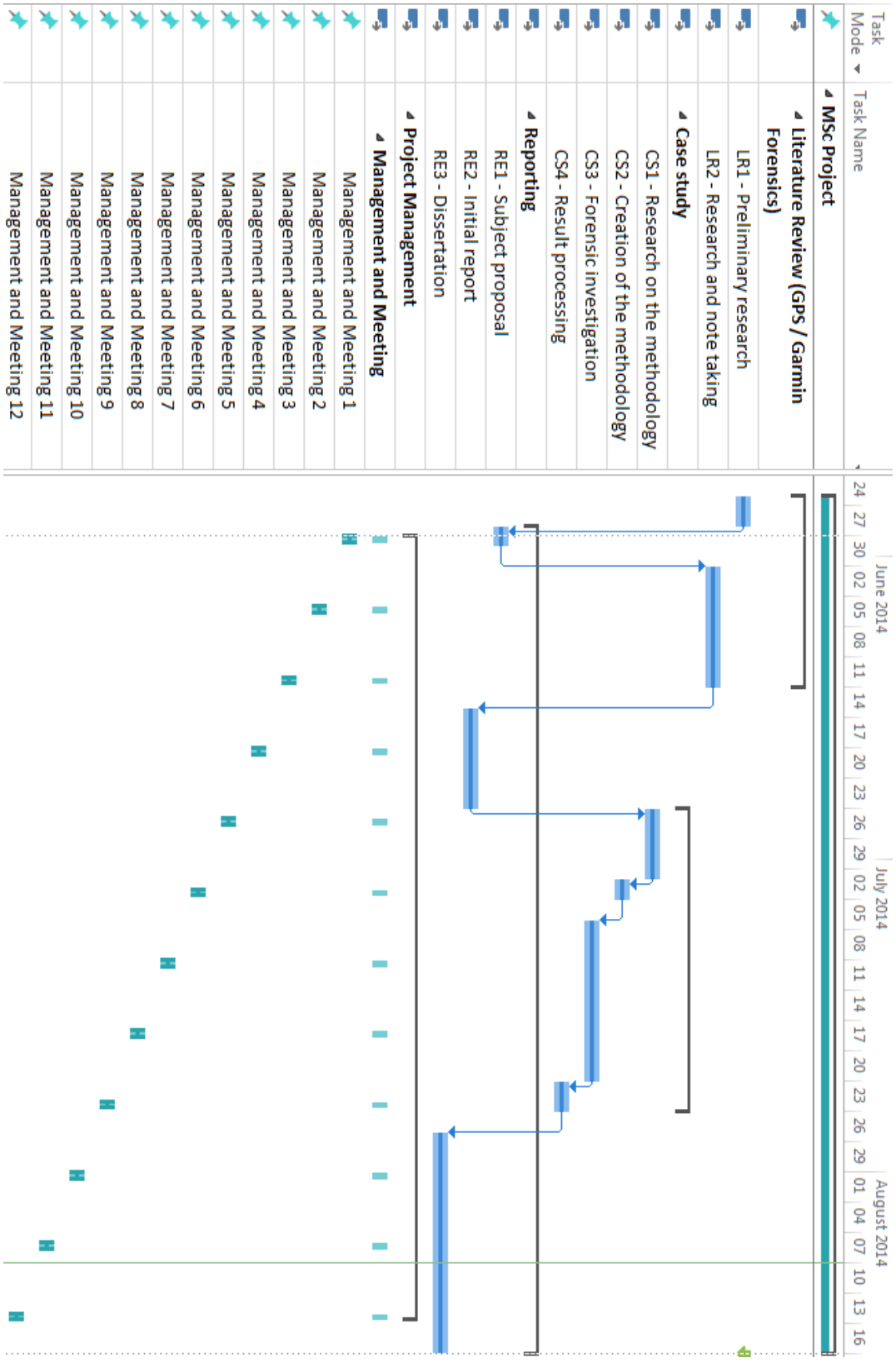
Nutter, B. (2008). Pinpointing TomTom location records: A forensic analysis. *Digital Investigation*, *5*(1-2), 10–18. doi:10.1016/j.diin.2008.06.003

Strawn, C. (2009). Expanding the potential for GPS evidence acquisition. *Small Scale Digital Device Forensics Journal*, *3*(1), 1–12. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.187.1135&rep=rep1&type=pdf

Van Eijk, O., & Roeloffs, M. (2010). Forensic acquisition and analysis of the Random Access Memory of TomTom GPS navigation systems. *Digital Investigation*, *6*(3-4), 179–188. doi:10.1016/j.diin.2010.02.005

Appendix B Project management

Gant chart:



Project diaries:

EDINBURGH NAPIER UNIVERSITY

SCHOOL OF COMPUTING

PROJECT DIARY

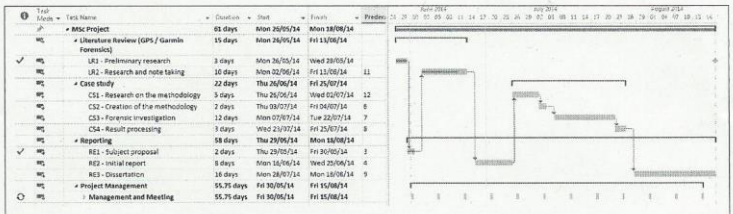
Student: Alexandre Arbelet **Supervisor: Rich MacFarlane**

Date: 14/06/2014 **Last diary date: 07/06/2014**

Objectives:

- **LR2**: Finish the literature review.
- **Project management**: Write the week diary, update project plan.

Progress:



Task Mode	Task Name	Duration	Start	Finish	Predec
	MSc Project	61 days	Mon 28/05/14	Mon 18/08/14	
	Literature Review (GPS / Garmin Forensics)	15 days	Mon 26/05/14	Fri 13/08/14	
✓	LR1 - Preliminary research	3 days	Mon 26/05/14	Wed 28/05/14	
	LR2 - Research and note taking	10 days	Mon 02/06/14	Fri 13/08/14	11
	Case study	22 days	Thu 26/06/14	Fri 25/07/14	
	CS1 - Research on the methodology	5 days	Thu 26/06/14	Wed 02/07/14	12
	CS2 - Creation of the methodology	2 days	Thu 03/07/14	Fri 04/07/14	8
	CS3 - Forensic investigation	12 days	Mon 07/07/14	Tue 22/07/14	7
	CS4 - Result processing	3 days	Wed 23/07/14	Fri 25/07/14	8
	Reporting	58 days	Thu 29/05/14	Mon 18/08/14	
✓	RE1 - Subject proposal	2 days	Thu 29/05/14	Fri 30/05/14	3
	RE2 - Initial report	8 days	Mon 16/06/14	Wed 25/06/14	4
	RE3 - Dissertation	16 days	Mon 28/07/14	Mon 18/08/14	9
	Project Management	55.75 days	Fri 30/05/14	Fri 15/08/14	
	Management and Meeting	55.75 days	Fri 30/05/14	Fri 15/08/14	

LR2: I came across some new literature, mainly about solid state disks forensics and GPS forensics liability. It would be interesting to explore the implication of liability on forensics, and antiforensics. I have still some papers to read, which could be done within a day. The task could be considered finish at 90%.

General progress: The project I currently one day left. The remaining literature can be read pretty quickly and this delay will be fix soon.

Supervisor's Comments:

Some good work on Lit. review.
Excellent level of understanding of area. Draft Lit review for end of next week. Try to organise interview with forensics investigator. Revisit workshop materials and the handbook! + Add Aim & Obj's to Intro Chapter.

EDINBURGH NAPIER UNIVERSITY

SCHOOL OF COMPUTING

PROJECT DIARY

Student: Alexandre Arbelet **Supervisor: Rich MacFarlane**

Date: 04/07/14 **Last diary date: 14/06/2014**

Objectives:

- **LR2**: Finish the literature review.
- **RE2:** Draft of literature review for the end of week 6 (23-27 june)
- **Project management**: Write the week diary, update project plan. Catch up with the plan.
- **Misc.:**
  - Try to organize an interview with forensics investigators and DIs.
  - Revisit workshops materials and handbook.
  - Add aim and objectives to intro chapter.

Progress:

LR2: The literature has been reviewed and notes have been taken. Other paper are likely to appear, but the vast majority has already been done.

RE2: The draft is ok, some correction remaining + some work to do on "Garbage collection".

Project management: Is up to date

Misc: I have had a look over the workshops and the handbook (the notation). Aim and objectives have been added to the dissertation.

Supervisor's Comments:

Great 1st draft of Lit. review. Some improvements suggested regarding critical writing / ref's, and some improvements regarding content. Start design/methodology section based on ideas discussed and organise meeting with forensic investigator Mike Dipton.

EDINBURGH NAPIER UNIVERSITY

SCHOOL OF COMPUTING

PROJECT DIARY

Student: Alexandre Arbelet **Supervisor: Rich MacFarlane**

Date: 23/07/2014 **Last diary date: 14/07/2014**

Objectives:

RE2: Finish writing the literature review. Improvements to do regarding the critical writing. Need to go further into some forensics concepts (solid state drives) and more critical on the GNSS part.

CS1: Research on different methodology, re-read the literature that contains experiments. Get inspiration from it.

CS2: Create a methodology aiming to answer the question posed in the aims & objectives part.

Misc.: Prepare an interview on Garmin/other GPS devices investigation.

Project Management: Update Project plan and project diary.

Progress:

RE2: The literature review has been corrected and updated with regards to the previous meeting decisions (04/07/2014).

CS1-2: Is the methodology concern the design of the experiments, or the forensic acquisition of the data? Should the methodology part be renamed experiment design or something? A draft has been designed, although it remains to be written in the dissertation.

Misc: Done

Project management: Part of the lost time has been made up. The project is currently a day late regarding its initial planning. I believe this lateness won't impact the overall project nor its deadline.

Supervisor's Comments:

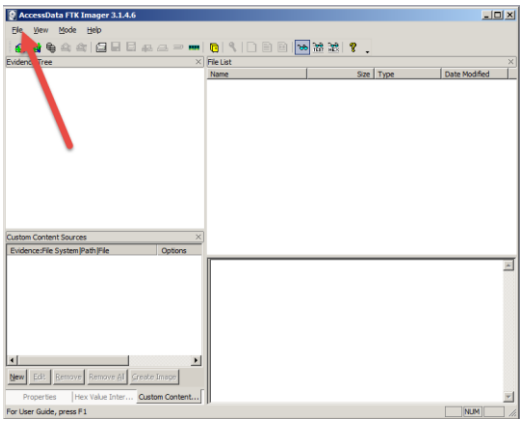
Good work on design and meeting was very well thought out and executed very well. Design and implementation aspects need to progress rapidly from now, with changes to overall aim/obj's changed as discussed.

Appendix C FTK Acquisition

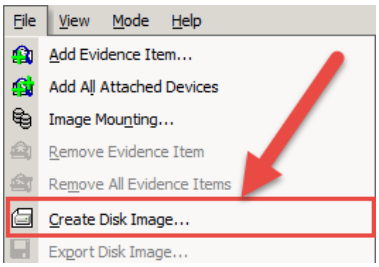
This annexe details the procedure to image a Garmin device[1] with FTK Imager. FTK Imager is a freeware distributed by *Access Data*. The tool can be downloaded here.

1. Connect the device to the computer. The device will then entered a "mass storage mode", the progression is reported by a green loading bar.

2. Wait for the device to have the opposite display. It means the device is in "mass storage mode". Open FTK Imager.

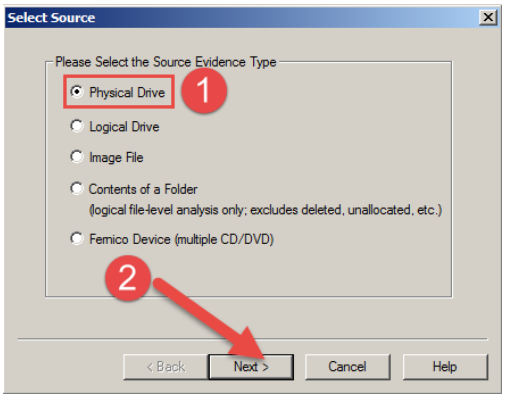


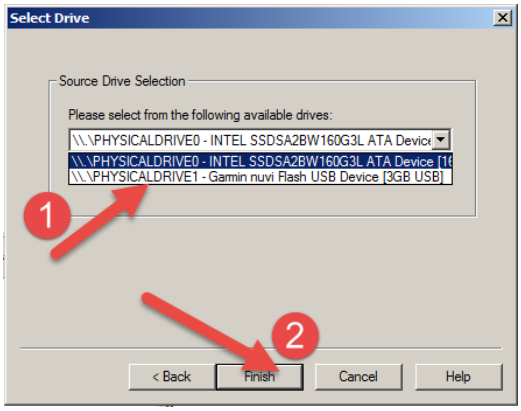
3. Click "*File*". In the menu, click on "*Create Disk Image…*", as shown below.



[1] The device considered for this procedure is a Garmin Nüvi 1340.

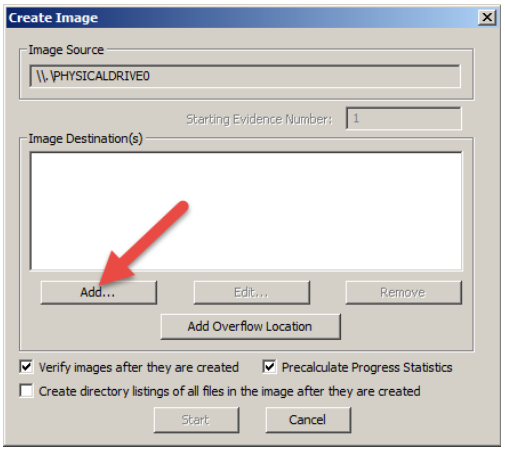
4. When the window opens, select "*Physical Drive*", and then click on "*Next >*".

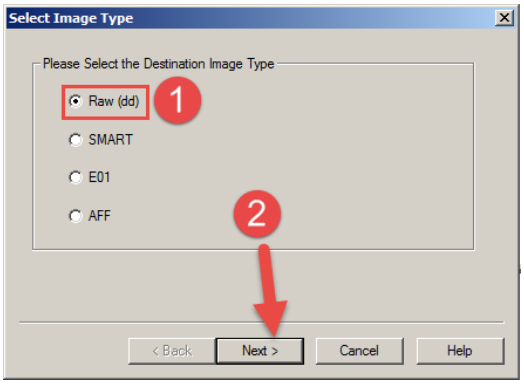




5. You are then invited to select the drive you want to image. Select the one containing "*Garmin nüvi Flash USB*" [2], and then click "*Finish*".

6. When the window opens, click on "*Add…*".

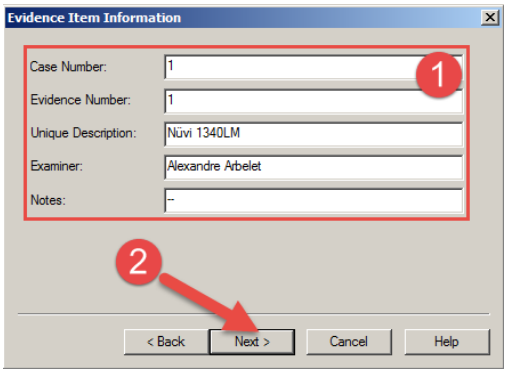


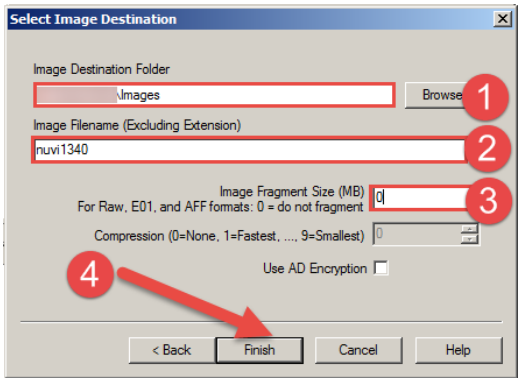


7. Select "*Raw (dd)*" to get a raw image or the device, or another format. Then click on "*Next >*".

[2] If the Garmin device does not appear in the list, please refer to the Appendix G, on how to mount recent Garmin devices as mass storage devices.

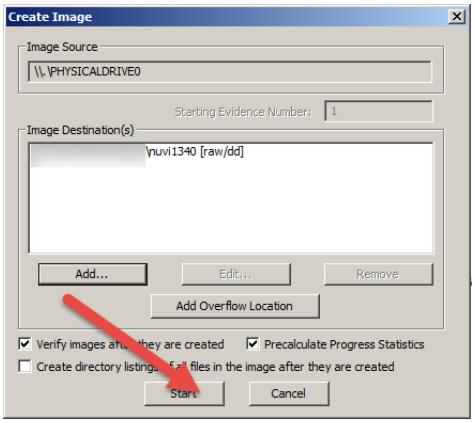
8. Fill the different fields, and click on "*Next >*".

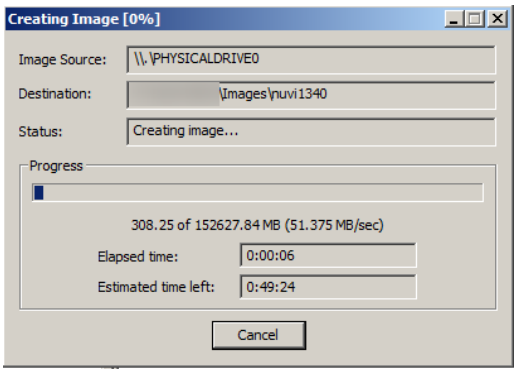




9. Select where to store the image, and give it a name. In order to have a single file, put "*0*" in the "*Image Fragment Size (MB)*" field. Click on "*Finish*".

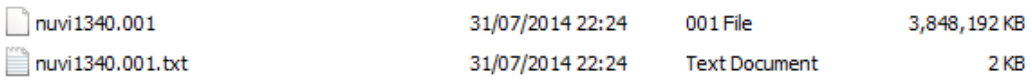
10. Click on "*Start*"





11. The device is being acquired.

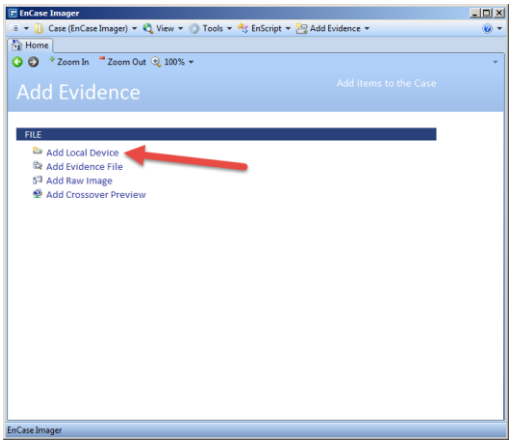
12. Once the acquisition is done, two files appears in the target folder; the image itself (extension .001), and the acquisition report (extension .001.txt).



Appendix D EnCase Acquisition

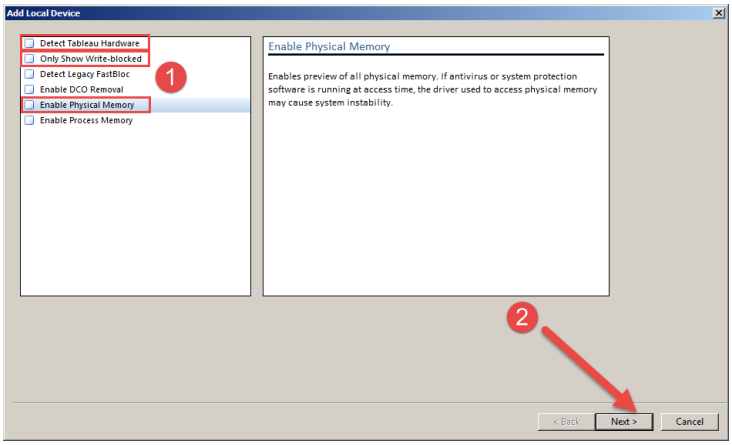
This annexe details the procedure to image a Garmin device[3] with EnCase Forensic Imager. EnCase Forensic Imager is a freeware distributed by *Guidance Software*. The tool can be downloaded here.

1. Connect the device to the computer and wait the device to be in "mass storage mode". Open EnCase Forensic Imager.

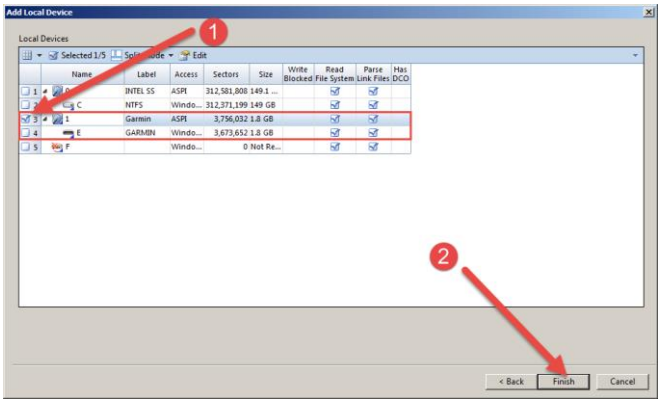


2. Click on "*Add Local Device*".

3. Deselect all the options if not using a tableau write blocker. Then click "*Next >*".

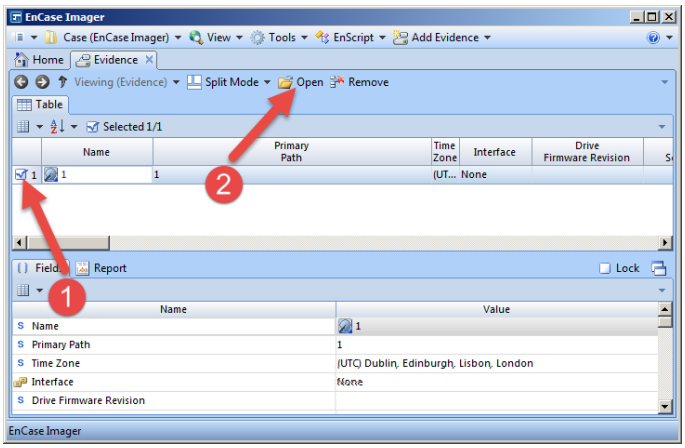


[3] The device considered for this procedure is a Garmin Nüvi 2515LM.

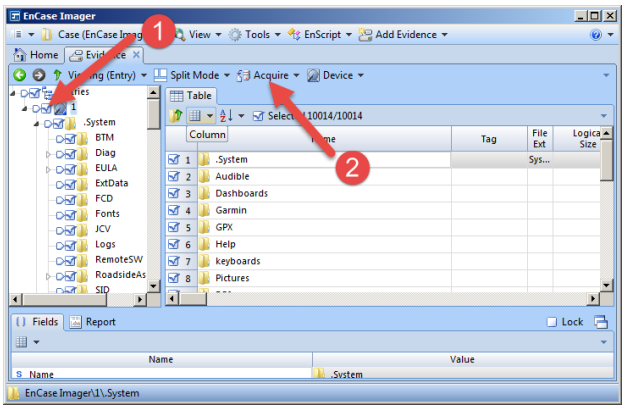


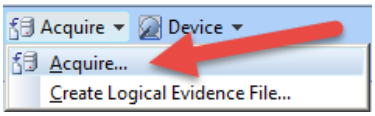
4.
Select the drive allocated to the Garmin device[4], then click "*finish*".

5.
Select the device, then click on "*Open*".

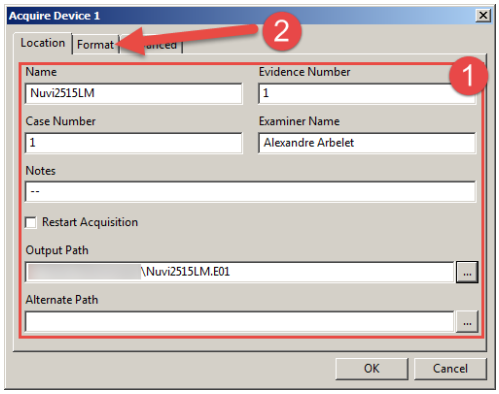


6.
Select the device, then click on "*Acquire…*".

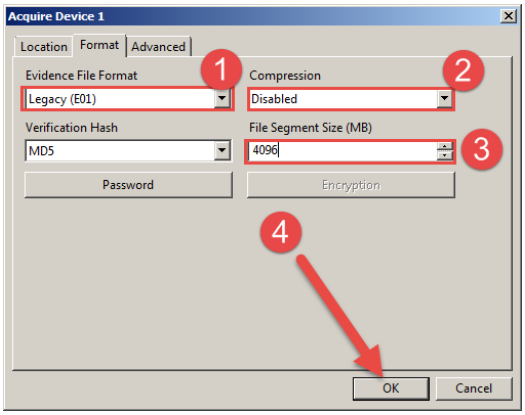




7.
Fill the information then click on the "Format" tab.



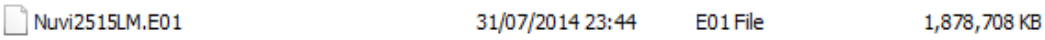
[4] If the Garmin device does not appear in the list, please refer to the Appendix G, on how to mount recent Garmin devices as mass storage devices.

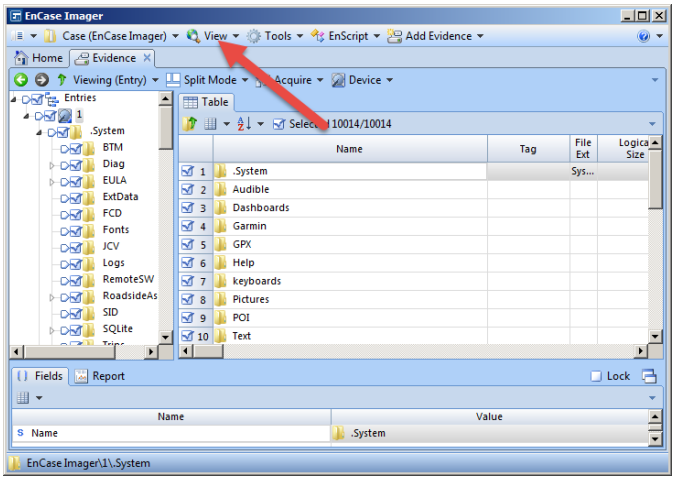


8.
Choose the "*Evidence file format*", disable the "*Compression*", and set the "*File Segment Size*" to a value superior to the device memory size in order to obtain a single file. Then click on "*OK*".

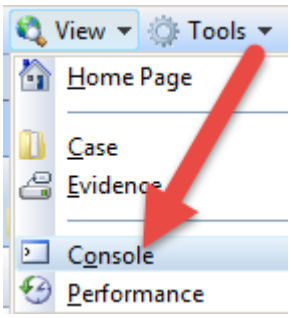
9. The device is being acquired

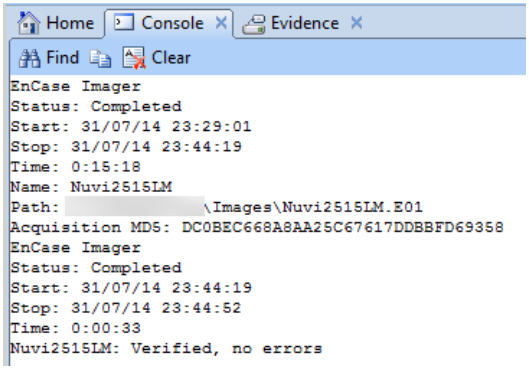
10. Once acquired, the image can be found in the target folder.





11.
To get a feedback on the acquisition process, click on "*view*". Then select "Console".

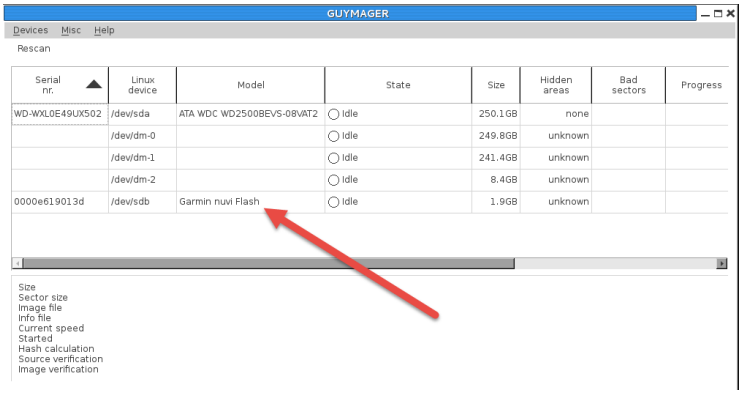




Appendix E Guymager Acquisition

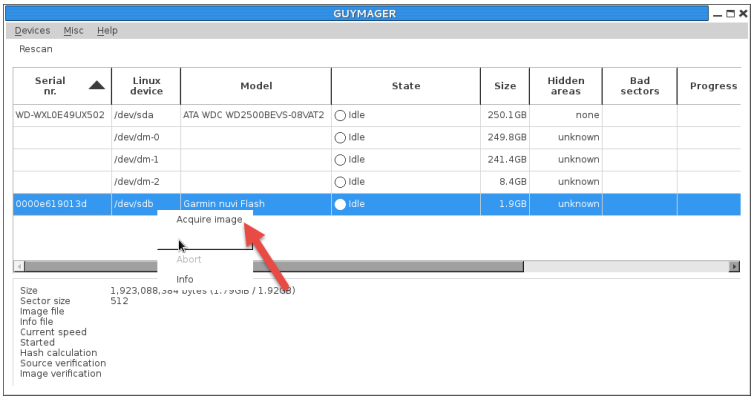
This annexe details the procedure to image a Garmin device [5] with Guymager. Guymager is an open source project embedded into Linux versions dedicated to penetration testing (e.g. Kali Linux or Backtrack) and forensics (e.g. Caine). The webpage for this tool can be found here.

1.
Connect the device to the computer and wait the device to be in "mass storage mode". Open Guymager.

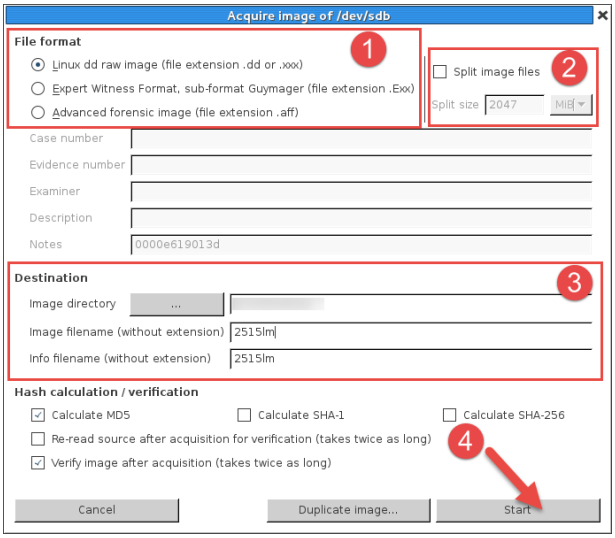


2.
Right click on the Garmin device.

3.
Click on "*Acquire image*".

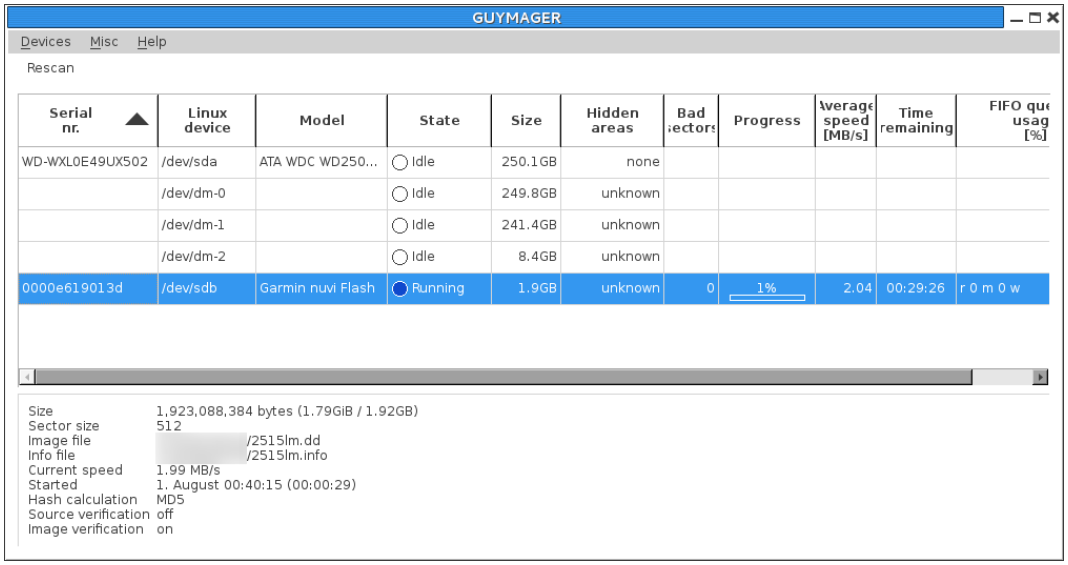


[5] The device considered for this procedure is a Garmin Nüvi 2515LM.



4.
Select the file format, disable the option "*Split image file*" to get a single file. Fill the directory, the name, and then click on "*Start*".

5. The image is being acquired.



6. Once the acquisition process is done, two files are produced, the image itself (extension *.dd*) and the acquisition report (extension *.info*).

Appendix F “dd” Acquisition

This annexe details the procedure to image a Garmin device[6] with the Linux “dd” command. “dd” is a command on Unix which is used to copy and convert files. The command is available on every Linux-based distributions. Documentation can be found here.

1. First thing is to locate the device.

```
ls -R /dev | grep -i -b2 garmin
```

```
/dev/disk/by-id:
ata-HL-DT-ST_DVDRAM_GSA-U20N_M1B973M0315
ata-WDC_WD2500BEVS-08VAT2_WD-WXL0E49UX502
ata-WDC_WD2500BEVS-08VAT2_WD-WXL0E49UX502-part1
ata-WDC_WD2500BEVS-08VAT2_WD-WXL0E49UX502-part2
ata-WDC_WD2500BEVS-08VAT2_WD-WXL0E49UX502-part5
dm-name-pentest--machine-root
dm-name-pentest--machine-swap_1
dm-name-sda5_crypt
dm-uuid-CRYPT-LUKS1-c7d564634dd44de18055d9dcc4c18761-sda5_crypt
dm-uuid-LVM-GfcpVcS2AiRmiOYWFElcSThZofAbSXUWE7tQdS6HmO7PZXakQyqKq7FH3xlmSJRc
dm-uuid-LVM-GfcpVcS2AiRmiOYWFElcSThZofAbSXUWVvh2cu3J2eeeEie8sH9fMkCZkbMnDh1N
scsi-SATA_WDC_WD2500BEVS-_WD-WXL0E49UX502
scsi-SATA_WDC_WD2500BEVS-_WD-WXL0E49UX502-part1
scsi-SATA_WDC_WD2500BEVS-_WD-WXL0E49UX502-part2
scsi-SATA_WDC_WD2500BEVS-_WD-WXL0E49UX502-part5
usb-Garmin_nuvi_Flash_0000e619013d-0:0
usb-Garmin_nuvi_SD_Card_0000e619013d-0:1
wwn-0x50014ee202ffe886
wwn-0x50014ee202ffe886-part1
wwn-0x50014ee202ffe886-part2
wwn-0x50014ee202ffe886-part5

/dev/disk/by-label:
GARMIN
```

2. Then run the dd command.

```
dd if=/dev/by-label/GARMIN of=Desktop/2515.dd
```

```
    @pentest-machine:~# dd if=/dev/disk/by-label/GARMIN of=Desktop/2515.dd
3756032+0 records in
3756032+0 records out
1923088384 bytes (1.9 GB) copied, 921.767 s, 2.1 MB/s
```

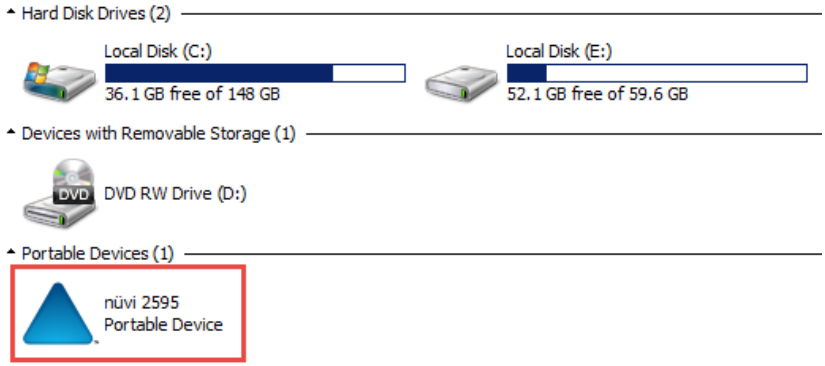
3. Once the acquisition done, a single file is created.

[6] The device considered for this procedure is a Garmin Nüvi 2515LM.

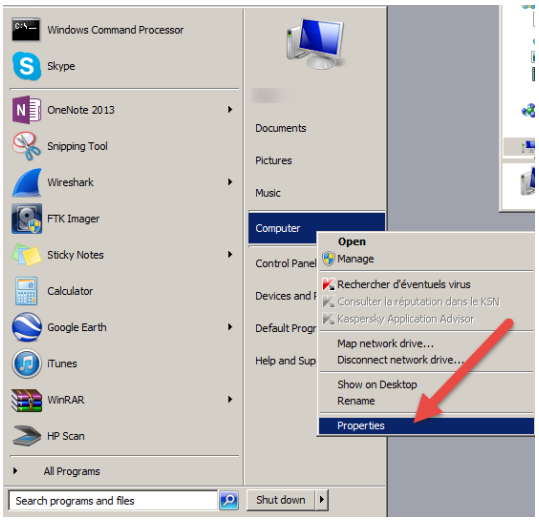
Appendix G Garmin device with MSC

This appendix describes the procedure to mount recent Garmin devices as mass storage devices instead of portable devices, thus allowing forensic imager such FTK or EnCase to access the internal memory. This procedure considers windows[7] as the underlying OS, as Linux does not use MTP to communicate with the devices.

1. Initial situation:



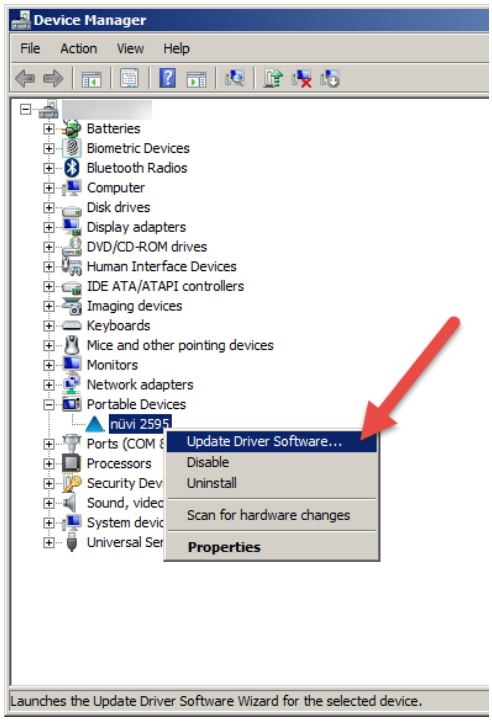
2. Open the "*Start*" menu, right-click on "*Computer*" then select "*Properties*".

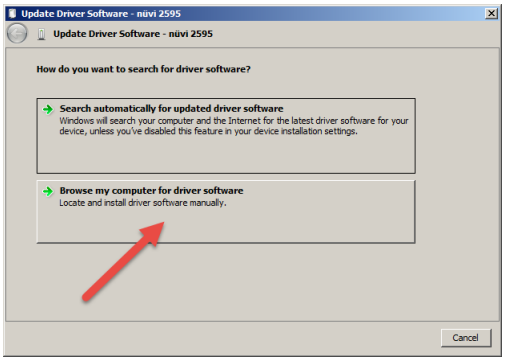


3. When the "*System*" window opens, select "*Device Manager*".

[7] The present procedure has been carried out using Windows 7.

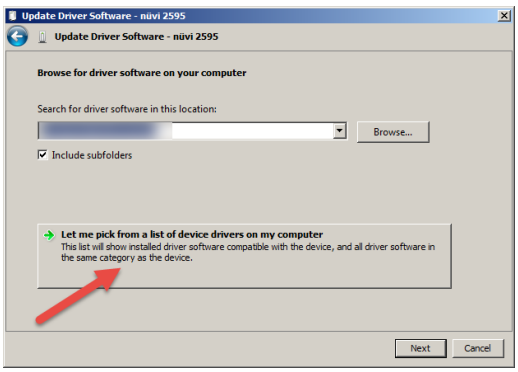
4.
Search for the Garmin device then right-click on it. Select "*Update Driver Software…*"

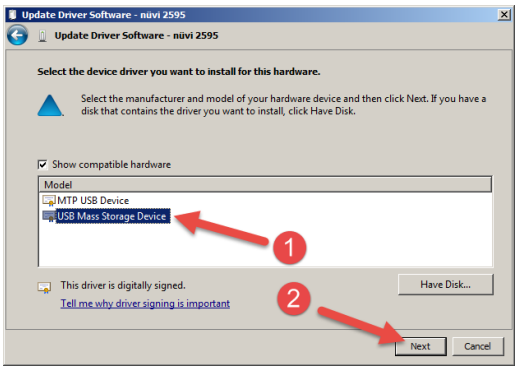




5.
When the window opens, select "*Browse my computer for driver software*".

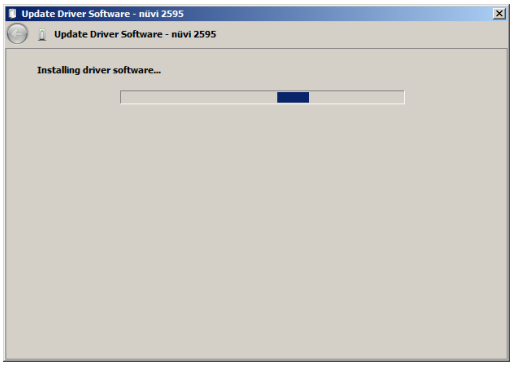
6.
Select "*Let me pick from a list of device drivers on my computer*".



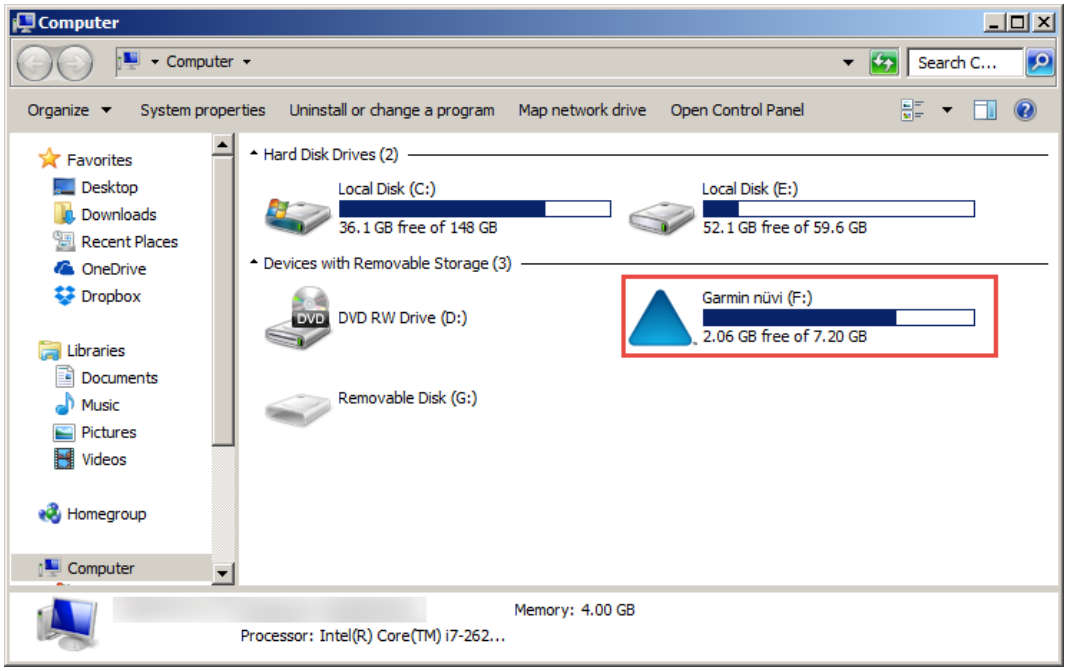


7.
Select "*USB Mass Storage Device*" then click "*Next*"

8.
The new driver is being installed.



9.
Once the procedure done, the device is accessible as a mass storage device, and therefore can be image by EnCase and FTK.



Appendix H Carving procedure

GPX file carving:

Configuration:

```
# GPX Files
     gpx   y     5000000     <gpx\x20xmlns=”  </gpx>
```

Command:

```
scalpel –b –c gpx_carving.conf –o output_folder image.dd
```

Waypoint carving:

Configuration:

```
# Waypoints
     wpt   y     500000      <wpt\x20lat="    </wpt>
```

Command:

```
scalpel –b –c wpt_carving.conf –o output_folder image.dd
```

Track carving:

Configuration:

```
# Tracks
     trk   y     500000      <trk>       </trk>
```

Command:

```
scalpel –b –c trk_carving.conf –o output_folder image.dd
```

Results:

Data	Device	Archive Files name	File browser	fls	Scalpel
.gpx files	Nüvi 1340	[44.gpx – 63.gpx]	22	23	26
	Nüvi 2515	{1.gpx} [7.gpx – 26.gpx]	21	22	26
	Nüvi 2595	[26.gpx – 45.gpx]	21	22	22
Total waypoints	Nüvi 1340	--	11	11	19
	Nüvi 2515	--	5	5	5
	Nüvi 2595	--	7	7	7
Total tracks	Nüvi 1340	--	1965	1965	1992
	Nüvi 2515	--	232	232	294
	Nüvi 2595	--	2107	2107	2192

Appendix I Anti-forensics #1

```
Monday 14 July - 16:10
Investigator: Alexandre Arbelet

Anti-forensics study on a Garmin nüvi 2515LM.
================================================
File considered: /root/2515.dd
md5 : bfb891232e5f73706c9ab331a24b8b8c
Original copy : /root/2515.orginal.dd
md5 : bfb891232e5f73706c9ab331a24b8b8c
================================================

$fls /dev/disk/by-label/GARMIN
d/d 22: GPX

$fls /dev/disk/by-label/GARMIN 22
r/r 32113798: Current.gpx
d/d 32113800: Archive
r/r * 32113802: Position.gpx

$fls /dev/disk/by-label/GARMIN 32113800
r/r 32139270: 61.gpx
r/r 32139272: 62.gpx
r/r 32139274: 63.gpx
r/r 32139276: 44.gpx
r/r 32139278: 45.gpx
r/r 32139280: 46.gpx
r/r 32139282: 47.gpx
r/r 32139284: 48.gpx
r/r 32139286: 49.gpx
r/r 32139288: 50.gpx
r/r 32139290: 51.gpx
r/r 32139292: 52.gpx
r/r 32139294: 53.gpx
r/r 32139296: 54.gpx
r/r 32139298: 55.gpx
r/r 32139300: 56.gpx
r/r 32139302: 57.gpx
r/r 32139304: 58.gpx
r/r 32139306: 59.gpx
r/r 32139308: 60.gpx

$istat /dev/disk/by-label/GARMIN 32139308
Directory Entry: 32139308
Allocated
File Attributes: File, Archive
Size: 1104840
Name: 60.GPX

Directory Entry Times:
Written: Wed Dec 4 08:07:06 2013
Accessed: Thu Jan 1 01:00:00 1970
Created: Thu Nov 28 19:38:18 2013

Sectors:
2070136 2070137 2070138 2070139 2070140 2070141 2070142 2070143...
```

```
$dd if=/dev/disk/by-label/GARMIN bs=512 skip=2070137 count=1 | xxd
1+0 records in
1+0 records out
512 bytes (512 B) copied, 4.4699e-05 s, 11.5 MB/s
0000000: 7369 6f6e 7376 332e 7873 6420 6874 7470 sionsv3.xsd http
0000010: 3a2f 2f77 7777 2e67 6172 6d69 6e2e 636f ://www.garmin.co
0000020: 6d2f 786d 6c73 6368 656d 6173 2f54 7261 m/xmlschemas/Tra
0000030: 636b 506f 696e 7445 7874 656e 7369 6f6e ckPointExtension
0000040: 2f76 3220 6874 7470 3a2f 2f77 7777 2e67 /v2 http://www.g
0000050: 6172 6d69 6e2e 636f 6d2f 786d 6c73 6368 armin.com/xmlsch
0000060: 656d 6173 2f54 7261 636b 506f 696e 7445 emas/TrackPointE
0000070: 7874 656e 7369 6f6e 7632 2e78 7364 223e xtensionv2.xsd">
0000080: 3c6d 6574 6164 6174 613e 3c6c 696e 6b20 <metadata><link
0000090: 6872 6566 3d22 6874 7470 3a2f 2f77 7777 href="http://www
00000a0: 2e67 6172 6d69 6e2e 636f 6d22 3e3c 7465 .garmin.com"><te
00000b0: 7874 3e47 6172 6d69 6e20 496e 7465 726e xt>Garmin Intern
00000c0: 6174 696f 6e61 6c3c 2f74 6578 743e 3c2f ational</text></
00000d0: 6c69 6e6b 3e3c 7469 6d65 3e32 3031 332d link><time>2013-
00000e0: 3131 2d32 3854 3139 3a33 383a 3139 5a3c 11-28T19:38:19Z<
00000f0: 2f74 696d 653e 3c2f 6d65 7461 6461 7461 /time></metadata
0000100: 3e3c 7472 6b3e 3c6e 616d 653e 4163 7469 ><trk><name>Acti
0000110: 7665 204c 6f67 3a20 3230 204e 4f56 2032 ve Log: 20 NOV 2
0000120: 3031 3320 3036 3a35 313c 2f6e 616d 653e 013 06:51</name>
0000130: 3c74 726b 7365 673e 3c74 726b 7074 206c <trkseg><trkpt l
0000140: 6174 3d22 3531 2e33 3834 3136 3422 206c at="51.384164" l
0000150: 6f6e 3d22 2d30 2e32 3133 3039 3122 3e3c on="-0.213091"><
0000160: 656c 653e 3238 2e30 323c 2f65 6c65 3e3c ele>28.02</ele><
0000170: 7469 6d65 3e32 3031 332d 3131 2d32 3054 time>2013-11-20T
0000180: 3036 3a35 313a 3538 5a3c 2f74 696d 653e 06:51:58Z</time>
0000190: 3c65 7874 656e 7369 6f6e 733e 3c67 7078 <extensions><gpx
00001a0: 7470 783a 5472 6163 6b50 6f69 6e74 4578 tpx:TrackPointEx
00001b0: 7465 6e73 696f 6e3e 3c67 7078 7470 783a tension><gpxtpx:
00001c0: 636f 7572 7365 3e33 3030 2e37 313c 2f67 course>300.71</g
00001d0: 7078 7470 783a 636f 7572 7365 3e3c 2f67 pxtpx:course></g
00001e0: 7078 7470 783a 5472 6163 6b50 6f69 6e74 pxtpx:TrackPoint
00001f0: 4578 7465 6e73 696f 6e3e 3c2f 6578 7465 Extension></exte

$dd if=/dev/disk/by-label/GARMIN bs=1 skip=1059910468 count=1| xxd
1+0 records in
1+0 records out
1 byte (1 B) copied, 4.9378e-05 s, 20.3 kB/s
0000000: 35 5

$echo -ne "\x34"| dd of=/dev/disk/by-label/GARMIN seek=1059910468
bs=1 count=1 conv=notrunc
1+0 records in
1+0 records out
1 byte (1 B) copied, 0.000260159 s, 3.8 kB/s

$dd if=/dev/disk/by-label/GARMIN bs=1 skip=1059910468 count=1 |
xxd
1+0 records in
1+0 records out
1 byte (1 B) copied, 7.1308e-05 s, 14.0 kB/s
0000000: 34 4

$dd if=/dev/disk/by-label/GARMIN bs=512 skip=2070137 count=1 | xxd
1+0 records in
1+0 records out
512 bytes (512 B) copied, 5.0775e-05 s, 10.1 MB/s
0000000: 7369 6f6e 7376 332e 7873 6420 6874 7470 sionsv3.xsd http
```

```
0000010: 3a2f 2f77 7777 2e67 6172 6d69 6e2e 636f ://www.garmin.co
0000020: 6d2f 786d 6c73 6368 656d 6173 2f54 7261 m/xmlschemas/Tra
0000030: 636b 506f 696e 7445 7874 656e 7369 6f6e ckPointExtension
0000040: 2f76 3220 6874 7470 3a2f 2f77 7777 2e67 /v2 http://www.g
0000050: 6172 6d69 6e2e 636f 6d2f 786d 6c73 6368 armin.com/xmlsch
0000060: 656d 6173 2f54 7261 636b 506f 696e 7445 emas/TrackPointE
0000070: 7874 656e 7369 6f6e 7632 2e78 7364 223e xtensionv2.xsd">
0000080: 3c6d 6574 6164 6174 613e 3c6c 696e 6b20 <metadata><link
0000090: 6872 6566 3d22 6874 7470 3a2f 2f77 7777 href="http://www
00000a0: 2e67 6172 6d69 6e2e 636f 6d22 3e3c 7465 .garmin.com"><te
00000b0: 7874 3e47 6172 6d69 6e20 496e 7465 726e xt>Garmin Intern
00000c0: 6174 696f 6e61 6c3c 2f74 6578 743e 3c2f ational</text></
00000d0: 6c69 6e6b 3e3c 7469 6d65 3e32 3031 332d link><time>2013-
00000e0: 3131 2d32 3854 3139 3a33 383a 3139 5a3c 11-28T19:38:19Z<
00000f0: 2f74 696d 653e 3c2f 6d65 7461 6461 7461 /time></metadata
0000100: 3e3c 7472 6b3e 3c6e 616d 653e 4163 7469 ><trk><name>Acti
0000110: 7665 204c 6f67 3a20 3230 204e 4f56 2032 ve Log: 20 NOV 2
0000120: 3031 3320 3036 3a35 313c 2f6e 616d 653e 013 06:51</name>
0000130: 3c74 726b 7365 673e 3c74 726b 7074 206c <trkseg><trkpt l
0000140: 6174 3d22 3431 2e33 3834 3136 3422 206c at="41.384164" l
0000150: 6f6e 3d22 2d30 2e32 3133 3039 3122 3e3c on="-0.213091"><
0000160: 656c 653e 3238 2e30 323c 2f65 6c65 3e3c ele>28.02</ele><
0000170: 7469 6d65 3e32 3031 332d 3131 2d32 3054 time>2013-11-20T
0000180: 3036 3a35 313a 3538 5a3c 2f74 696d 653e 06:51:58Z</time>
0000190: 3c65 7874 656e 7369 6f6e 733e 3c67 7078 <extensions><gpx
00001a0: 7470 783a 5472 6163 6b50 6f69 6e74 4578 tpx:TrackPointEx
00001b0: 7465 6e73 696f 6e3e 3c67 7078 7470 783a tension><gpxtpx:
00001c0: 636f 7572 7365 3e33 3030 2e37 313c 2f67 course>300.71</g
00001d0: 7078 7470 783a 636f 7572 7365 3e3c 2f67 pxtpx:course></g
00001e0: 7078 7470 783a 5472 6163 6b50 6f69 6e74 pxtpx:TrackPoint
00001f0: 4578 7465 6e73 696f 6e3e 3c2f 6578 7465 Extension></exte
```

```
$istat /dev/disk/by-label/GARMIN 32139308
Directory Entry: 32139308
Allocated
File Attributes: File, Archive
Size: 1104840
Name: 60.GPX

Directory Entry Times:
Written: Wed Dec 4 08:07:06 2013
Accessed: Thu Jan 1 01:00:00 1970
Created: Thu Nov 28 19:38:18 2013

Sectors:
2070136 2070137 2070138 2070139 2070140 2070141 2070142 2070143
```

Appendix J Anti-forensics #2

```
Wednesday 23 July - 11:12
Investigator: Alexandre Arbelet

Anti-forensic experiment on a Garmin nüvi 2595LM.

*****************************************************
Aim:
*****************************************************
This experiment aims to show how data retrieved on GPS devices
cannot be relied upon, due to the fact it could be easily
manipulated.


*****************************************************
Device
*****************************************************
Model                : Garmin Nüvi 2595LM
Image pre-experiment: 2014-07-23_2595LM.dd
MD5 Sum              : af383947516f031393b667350476f94b


*****************************************************
Manipulation
*****************************************************
$fls 2014-07-23_2595LM.dd
d/d 21:    GPX

$fls 2014-07-23_2595LM.dd 21
d/d 171155846:    Archive
r/r * 171155848:    Position.gpx
r/r 171155850:    Current.gpx

$istat 2014-07-23_2595LM.dd 171155850 | head
Directory Entry: 171155850
Allocated
File Attributes: File, Archive
Size: 2221068
Name: CURRENT.GPX

Directory Entry Times:
Written:    Wed Jul 23 12:03:10 2014
Accessed:    Tue May 27 00:00:00 2014
Created:    Sat Sep 28 10:36:32 2013

$istat 2014-07-23_2595LM.dd 21
Directory Entry: 21
Allocated
File Attributes: Directory
Size: 4096
Name: GPX

Directory Entry Times:
Written:    Wed Jul 23 12:03:06 2014
Accessed:    Thu Jan  1 01:00:00 1970
Created:    Fri Jun 14 22:29:42 2013
```

```
Sectors:
10711992 10711993 10711994 10711995 10711996 10711997 10711998
10711999

$dd if=2014-07-23_2595LM.dd bs=512 skip=10711992 count=1 | xxd
1+0 records in
1+0 records out
512 bytes (512 B) copied, 4.5466e-05 s, 11.3 MB/s
0000000: 2e20 2020 2020 2020 2020 2010 0000 0000  .           .....
0000010: 0000 0000 1400 0000 0000 4567 0000 0000  ..........Eg....
0000020: 2e2e 2020 2020 2020 2020 2010 0000 0000  ..          .....
0000030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000040: 4141 0072 0063 0068 0069 000f 0075 7600  AA.r.c.h.i...uv.
0000050: 6500 0000 ffff ffff ffff 0000 ffff ffff  e...............
0000060: 4152 4348 4956 4520 2020 2010 0000 b5b3  ARCHIVE     .....
0000070: ce42 0000 1400 ac45 f444 4667 0000 0000  .B.....E.DFg....
0000080: e550 006f 0073 0069 0074 000f 003c 6900  .P.o.s.i.t...<i.
0000090: 6f00 6e00 2e00 6700 7000 0000 7800 0000  o.n...g.p...x...
00000a0: e54f 5349 5449 4f4e 4750 5820 0000 6360  .OSITIONGPX ..c`
00000b0: f744 0000 1400 6360 f744 1069 0103 0000  .D....c`.D.i....
00000c0: 4143 0075 0072 0072 0065 000f 00f2 6e00  AC.u.r.r.e....n.
00000d0: 7400 2e00 6700 7000 7800 0000 0000 ffff  t...g.p.x.......
00000e0: 4355 5252 454e 5420 4750 5820 0000 9054  CURRENT GPX ...T
00000f0: 3c43 bb44 1400 6560 f744 1169 0ce4 2100  <C.D..e`.D.i..!.
0000100: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000110: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000120: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000130: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000140: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000150: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000160: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000170: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000180: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000190: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001b0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001c0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................

*****************************************************************
Date calculation
*****************************************************************
Last modified timestamp: 6560 f744
Offset                 : 0f6 0f7 0f8 0f9
Last accessed timestamp: bb44
Offset                 : 0f2 0f3

** We want to keep the same time, but change the last accessed
and
last modified date to the 16 instead of the 21 **

date (little endian): f744
date (big endian)   : 44f7
date (big endian)   : 01000100 11110111

 Year    Month  Day
=======  ====  =====
0100010  0111  10111
 2014      7     23
```

```
Day:
10111 => 10000
23    => 16

new date (big endian)    : 01000100 11110000
new date (big endian)    : 44f0
new date (little endian): f044

new last accessed tiemstamp: f044
new last modified timestamp: 6560 f044

Offsets to modify: 0f2 -- bb -> f0
           0f8 -- f7 -> f0


*****************************************************************
Modification on the device
*****************************************************************
** Connection to the computer with an usb cable.

$fls /dev/disk/by-label/GARMIN
d/d 21:    GPX

$istat /dev/disk/by-label/GARMIN 21
Directory Entry: 21
Allocated
File Attributes: Directory
Size: 4096
Name: GPX

Directory Entry Times:
Written:    Wed Jul 23 12:03:06 2014
Accessed:    Thu Jan  1 01:00:00 1970
Created:    Fri Jun 14 22:29:42 2013

Sectors:
10711992 10711993 10711994 10711995 10711996 10711997 10711998
10711999

$bc
**10711992 * 512 = 5484539904
**5484539904 + 0xf2 (242) = 5484540146
**5484539904 + 0xf8 (248) = 5484540152

$dd if=/dev/disk/by-label/GARMIN bs=1 skip=5484540146 count=2| xxd
2+0 records in
2+0 records out
2 bytes (2 B) copied, 9.219e-05 s, 21.7 kB/s
0000000: bb44                                      .D

$dd if=/dev/disk/by-label/GARMIN bs=1 skip=5484540152 count=2| xxd
2+0 records in
2+0 records out
2 bytes (2 B) copied, 0.000126482 s, 15.8 kB/s
0000000: f744                                      .D

$echo -ne "\xf0" | dd of=/dev/disk/by-label/GARMIN seek=5484540146
bs=1 count=1 conv=notrunc
1+0 records in
1+0 records out
```

```
1 byte (1 B) copied, 8.9676e-05 s, 11.2 kB/s

$echo -ne "\xf0" | dd of=/dev/disk/by-label/GARMIN seek=5484540152
bs=1 count=1 conv=notrunc
1+0 records in
1+0 records out
1 byte (1 B) copied, 8.6743e-05 s, 11.5 kB/s

$dd if=/dev/disk/by-label/GARMIN bs=1 skip=5484539904 count=512 |
xxd
0000000: 2e20 2020 2020 2020 2020 2010 0000 0000  .          .....
0000010: 0000 0000 1400 0000 0000 4567 0000 0000  ..........Eg....
0000020: 2e2e 2020 2020 2020 2020 2010 0000 0000  ..          .....
0000030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000040: 4141 0072 0063 0068 0069 000f 0075 7600  AA.r.c.h.i...uv.
0000050: 6500 0000 ffff ffff ffff 0000 ffff ffff  e...............
0000060: 4152 4348 4956 4520 2020 2010 0000 b5b3  ARCHIVE    .....
0000070: ce42 0000 1400 ac45 f444 4667 0000 0000  .B.....E.DFg....
0000080: e550 006f 0073 0069 0074 000f 003c 6900  .P.o.s.i.t...<i.
0000090: 6f00 6e00 2e00 6700 7000 0000 7800 0000  o.n...g.p...x...
00000a0: e54f 5349 5449 4f4e 4750 5820 0000 6360  .OSITIONGPX ..c`
00000b0: f744 0000 1400 6360 f744 1069 0103 0000  .D....c`.D.i....
00000c0: 4143 0075 0072 0072 0065 000f 00f2 6e00  AC.u.r.r.e....n.
00000d0: 7400 2e00 6700 7000 7800 0000 0000 ffff  t...g.p.x.......
00000e0: 4355 5252 454e 5420 4750 5820 0000 9054  CURRENT GPX ...T
00000f0: 3c43 f044 1400 6560 f044 1169 0ce4 2100  <C.D..e`.D.i..!.
0000100: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000110: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000120: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000130: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000140: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000150: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000160: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000170: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000180: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000190: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001b0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001c0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................

$istat /dev/disk/by-label/GARMIN 171155850 | head
Directory Entry: 171155850
Allocated
File Attributes: File, Archive
Size: 2221068
Name: CURRENT.GPX

Directory Entry Times:
Written:    Wed Jul 16 12:03:10 2014
Accessed:    Wed Jul 16 00:00:00 2014
Created:    Sat Sep 28 10:36:32 2013
```