



**UNIVERSITY OF PIRAEUS**  
**DEPARTMENT OF DIGITAL SYSTEMS**  
**M.Sc IN DIGITAL SYSTEMS SECURITY**

**GPS Forensics**

**“A systemic approach for GPS evidence acquisition through  
forensics readiness “**

Vassilakopoulos Xenofon



University of Piraeus

Dept. of Digital Systems

M.Sc in Digital Systems Security

---

Master Thesis

Digital Systems Security

Final Assignment

GPS Forensics

“A systemic approach for GPS evidence acquisition through forensics readiness”

*Supervisor:* Professor Dr. Lambrinoudakis Kostas, Dept. of Digital Systems, University of Piraeus

*M.Sc Student:* Vassilakopoulos Xenofon (mte-0209)

## *Abstract*

*The use of Satellite Navigation Systems (SNS) has become increasingly common in recent years. The wide scale adoption of this technology has the potential to provide a valuable resource in forensics investigations. The potential of this resource is to provide historical location data from the device while maintaining forensics integrity. The main purpose of this thesis is to provide a systemic approach to forensics redlines. The goal of this study is to provide an automotive process that implements the collection and acquisition of forensics GPS evidence. The main purpose of the system is to provide availability of the evidence to authorized digital investigators. The system has to offer Confidentiality of the coordinates that collects from the GPS receiver and also has to provide integrity of the collected data to prove the originality and not alteration of the evidence acquired. The Data that shows individuals location called sensitive data need special treatment inside the GPS device or inside PDAs. The system developed has the ability to collect data from the GPS receiver and encrypt them using symmetric and asymmetric cryptography accompanied with hash algorithms for providing integrity of the original coordinates at the desirable encoding format (NMEA) .Another step is to save those encrypted coordinates into a file somewhere in the file system of the device together with timestamps and date provision, which should be accessible only from digital investigators. The design and implementation of this system is simulated and shows the steps that causes the desirable methodology.*

## Acknowledgements

*My appreciation goes to my supervisor, Professor **Konstantinos Lambrinoudakis**, for his relentless effort in various forms of guidance, knowledge and moral support during my entire difficult period of writing and implementing this project.*

*Thank you*

<b>1. Introduction.....</b>	<b>8</b>
1.1. Aim .....	8
1.2. Objectives.....	9
1.3. Motivation.....	9
1.4 The Legal forensics examination process of GPS satellite navigation systems .....	11
1.4.1 The benefits of forensics examination of Global position system or Satellite navigation .....	12
1.4.1.1 Law Enforcement Officers.....	12
1.4.1.2 Prosecutors.....	12
1.4.1.3 Defence Lawyers.....	13
1.5 The project plan .....	13
<b>2. GPS Satellite navigation systems, the embedded technology and storage ...</b>	<b>15</b>
2.1 The Definition of The embedded device .....	15
2.2 The Memory of Embedded system.....	15
2.3 NAND and NOR flash memory architecture .....	16
2.3.1 Characteristics of NOR and NAND memories.....	17
2.3.2 The Structure and functionality of NAND and NOR memory.....	17
2.4 Linux OS on GPS devices.....	19
2.5 The Internal architecture of a GPS device.....	20
2.6 GPS Receivers.....	22
2.7 Expansion Ports and Interfaces between GPS device and kernel in embedded systems.....	23
2.8 NMEA Data.....	24
<b>3. The Policies and procedures of carrying out forensics examination .....</b>	<b>25</b>

3.1 The methodology of Carrying out forensics examination.....	26
3.1.1 Collection.....	26
3.1.2 Preservation.....	27
3.1.3 Analysis.....	29
3.1.4 Presentation.....	30
3.2 Roles and Responsibilities.....	30
3.3 Evidential Principles.....	32
3.4 Equipment in a basic Forensics Kit.....	33
<b>4. General methodology of forensic investigation embedded GPS receiver.....</b>	<b>35</b>
4.1 GPS receiver storage media.....	36
4.2 The acquisition of an SD card.....	36
4.3 Proposed add-ons in methodology of forensic investigation embedded GPS receiver.....	39
4.4 File Slack Definition.....	40
<b>5. Literature review of the forensics examination of embedded device such as GPS.....</b>	<b>41</b>
5.1 Literature review.....	41
5.2 The Global Positioning System (GPS) receivers.....	42
5.3 Previous work done with GPS forensics analysis.....	43
5.4 Acquisition of GPS receiver storage media.....	44
5.5 Files of forensics interest.....	45
5.6 Identifying the GPS fix location.....	45
<b>6. GPS receiver forensics examination. The General Case study.....</b>	<b>46</b>
6.1 The GPS navigation system.....	47
6.2 The system imaging.....	48

6.3 The Bit stream image.....	49
6.4 Verification of Imaging and the hash value.....	50
6.5 Case study: Forensic Examination of GPS receiver such as TomTom GO 500 .....	51
6.6 The tools using for imaging GPS receivers.....	51
6.7 Imaging TomTom GPS receiver.....	52
6.8 Methodology of imaging TomTom One GPS receiver.....	53
6.9 The Adepto Forensics tool.....	56
6.10 The Tom-Tom evidence analysis .....	60
6.11 Deleted Spaces on Device .....	61
6.12 Files of Forensics interest.....	62
6.13 The CFG Data Files .....	63
6.14 The Orphan Locations .....	63
6.15 Data analysis with FTK AccessData imager.....	64
6.16. Data representation .....	68
<b>7. The Systemic approach of the encrypted coordinates .....</b>	<b>69</b>
7.1 Problems to be solved by implementing the systemic methodology for evidence acquisition.....	70
7.2 The encrypted coordinates and the interactions with installed Applications .	72
7.3 System deployment and implementation .....	74
7.4 Inside the GPS system – Applying the technology.....	75
7.5 The embedded PKI system functionality .....	78
7.6 The Certificate Authority.....	81
7.7 Case study: Applying the authentication Mechanism .....	82
7.7.1 The communication port with the TomTom and the problems being faced for achieving correct functionality.....	83

7.7.2 The deployment process.....	84
7.7.3 The Examiner’s Role.....	90
7.8 Privacy.....	90
<b>8. The legability of Forensics evidence .....</b>	<b>93</b>
8.1 Considerations of several factors of evidence Admissibility.....	93
<b>9. Conclusion .....</b>	<b>94</b>
<b>10. Future Work.....</b>	<b>95</b>
<b>APPENDIX A .....</b>	<b>96</b>
<b>References .....</b>	<b>105</b>



## Abbreviations and Acronyms

### 1. Introduction

Mobile technology and GPS technology is constantly evolving. Mobile phones and GPS devices are equipped with new features and now work like computers, with lots of different applications. Some of those applications are using GPS coordinates for their functionality (e.g. GEOTaging – for showing the location of taking photos). This chapter is defining the boundaries of the project. It basically shapes the project in giving a clearer picture of the aim and objectives of the project. It also gives us a run down of my motivations of writing the project and how significant such a project is vital in our society of today and in the future. It finally outlines the project plans from start to the end.

#### 1.1. Aim

The Aim of this project is to investigate the feasibility of a systemic methodology to prevent first of all the exposedness of the individuals' location, and second to make the forensics process of collecting evidence more secure, available and effective in a timely manner. In other words this study aims to design and implement of a system that will provide forensics readiness for collecting GPS evidence and take them directly to the hands of the investigators.

## 1.2. Objectives

The objectives of this project are:

- Investigate the state of the art regarding forensics investigation methodology of an embedded device such as GPS receiver.
- To make a research of classification of Global Position Systems (GPS).
- Design and Develop a systemic methodology to provide forensics readiness for GPS evidence acquisition.
- Explain the reasons of the usefulness of the forensics readiness policy and procedure
- Explain the potential of the forensics readiness methodology regardless of the GPS forensics methodology
- To illustrate the correlation of the law enforcement and the forensics process and how forensics readiness is accepted from court.

## 1.3. Motivation

The field of digital forensics has long been cantered on traditional media like hard drive. Being the most common digital storage device in distribution it is easy to see how they have become a primary point of evidence. However, as technology brings digital storage to be more and more of larger storage capacity, forensic examiners have needed to prepare for a change in what types of devices hold a digital fingerprint. Cell phones, GPS receiver and PDA (Personal Digital Assistant) devices are so common that they have become standard in today's digital

examinations. These small devices carry a large burden for the forensic examiner, with different handling rules from scene to lab and with the type of data being as diverse as the suspects they come from. Handheld devices are rooted in their own operating systems, file systems, file formats, and methods of communication. Dealing with this creates unique problems for examiners. Performing a forensic examination on a GPS receiver takes special software and special knowledge of the way these devices work, as well as where possible evidence could be stored. Since the GPS receivers have been ubiquitous and more prevalent in the commission of crime, it is worth while to understand how these devices work forensically. The GPS receiver has proved to be excellent in tracing

Position world wide and provide evidentiary data if the following areas are examined: Track logs, Track points, Routes store locations, Home, Office, favorite, Call Logs, (miss, Dialed, received calls) and incoming and outgoing text messages. In some GPS receivers we can also have video, photos and Audio. If all the above mention point are examine forensically, a good deal of information will be harvested which could be used as an irrefutable evidence in a court of law. It is also recognized the fact that there is a need to develop methods and systems that should make an approach to forensics readiness for these small devices as well as laptops and PCs. Readiness provides solutions and prevents the large time of process for evidence examination . Also provides less effort from the examiners and make their job easier. Although the information has to be stored in specific locations in the file system so that it will be accessible only from the authorized investigator who will be responsible for the research. Also there has to be a policy documented for any device that is produced for sale out in market. The forensics readiness policies have to specify the availability of the type of evidence, the confidentiality of the data, the eligibility of the information examined, the privacy of individuals that are involved in the examination process through evidence, and the integrity of the data examined

to prove the data are not altered during the process. The policy process has to be implemented and executed through a developed system inside the device. As we can see digital forensics getting more complicated because of the continually evolved species of digital devices that come from digital technology evolution. Different devices bring different operating systems with different file system formats. The collectivity of evidence is getting more and more difficult to proceed. GPS devices and PDAs as well as smart phones are the only devices that the suspects can have with them at all times based on their size, and they have immediate access to them because they have immediate boot cycle devices. In addition, these are the devices that typically hold all our dirty little secrets with colourful pictures and descriptive text messages. The information ranged from complete address books, work related e-mails, to pictures that were of intimate moments.

#### 1.4 The Legal forensics examination process of GPS satellite navigation systems

The examination process of any forensics evidence has to be proceeding under particular rules and circumstances in accordance with guidance of the legal authorities, because at the end of the day the last confirmation and evaluation of the process and also the usefulness of the evidence will be from the side of law and mainly from court. So the examination of such evidences is crucial and has to be analyzed with respect to law enforcement regulations. Even the forensics tools that will be used in such cases have to follow the rules and regulations to provide finally the right results to finally prosecute the incident to court.

## 1.4.1 The benefits of forensics examination of Global position system or Satellite navigation

### 1.4.1.1 Law Enforcement Officers

The police or other law enforcement agencies may be able to exactly pinpoint the position of an accused person if that person used a Satellite Navigation system. Consider the fact that a person is accused from law enforcement agent because he/she was near the crime scene at that time because there are witnesses that claim they seen him around. Also think about the fact that the person's car was 200 meters away from the scene. The Car GPS navigation system is the only way of proving that the person was there at the time that the crime scene was evolving. Or the same way around the GPS system can prove the opposite, like the person wasn't there at the time. So it gives an alibi to the accused person for his own benefit.

### 1.4.1.2 Prosecutors

The prosecutors are lawyers that are recognized from court as legal professionals and their job is to show to court the state of the crime, collect and analyse the situation and finally give the prosecution to the person accused. They usually only become involved in a criminal case once a suspect has been identified and charges need to be filed. Prosecutors have to give exact and analysed evidence to the court. The accusations have to be as accurate as possible without mistakes and misunderstandings. GPS navigation systems, if used, in case of digital evidence give accurate information to prosecutors of the time and place the accused person was being. As the above, is clearly a benefit for prosecutors to involve GPS Evidence in their analyses.

### 1.4.1.3 Defence Lawyers

Defence Lawyers are there to examine any and all evidence and try to pick flaws in it. If a law enforcement agency has not yet examined the Satellite Navigation system, the evidence produced may well be enough to have the accused proved innocent or cast doubt over his guilt. It is this reason that the more and more defence lawyers are turning to Satellite Navigation Forensics.

## 1.5 The project plan

The project that is about to be analysed in this assignment will be presented as follows. First there will be presented the current forensics policy for GPS Evidence acquisition as described from [ ] and thus will be explained the process of forensics evidence collection and examination. Then will be a brief analysis of the process with implementation example. The implementation example will show the steps of

- evidence acquisition,
- imaging of GPS hard drive,
- The file system NTFS format of the targeted device and the reason for the chosen format,
- how will prove the image integrity and Evidence integrity be proved
- And finally will present the evidence analysis using the forensics tool TomTology.

The following Chapters will show the methodology and policy of the proposed systemic approach of evidence acquisition and analysis. After the presentation of

the steps of the proposed methodology, an analytic comparison between the current acquisition process and the process proposed will be presented. There will be accurate points of interest describing why the proposed process is better for the evidence acquisition than the current methodology based on tom-tom GPS devices. What are the benefits of this proposition and what are the problems and threats that we are facing of, while using this method. There are also possible threats at the time of forensics readiness process that will be presented. The general scepticism of the methodology is that it is based on an automated way of catching the evidence data from the GPS receiver, encrypt them into a file with a unique name, and then sign the file, with the public key. The process follows as the signing of the file will be encrypted with the hash algorithm SHAv1 and it will show the integrity of the evidence been acquired. The authenticity of the investigator will be at the time of using his own private key to decrypt the file, as he/she (investigator) will be the owner of the private key. There are also applications installed inside the GPS device that need to use the coordinates being acquired. Those applications need to have a programmable interface that will find the file that holds the coordinates in a cryptographic format, which will be somewhere in the disk with a unique name for identification. When the coordinates being successfully acquired then there has to be a process taking place which will start decrypting the encrypted file and finally gain the originated coordinates in a format that the GPS mapping system would easily read. The process of acquiring the evidence from the investigations examiner is the same as the process of the coordinates to be acquired from the API of the applications being installed inside the device. The whole process will be analytically presented to the following chapters of this assignment.

## 2. GPS Satellite navigation systems, the embedded technology and storage

The embedded system has apparently a different type of forensics investigation procedure as opposed to the normal forensic examination of a hard disk. Most of the embedded devices use the Flash memory technology in data storage. The existence of global navigation system and its early method of navigation are well discussed. The history of the global positioning system and the different type of GPS receiver is well elaborated in this chapter, and narrowly stream down to the automobile Navigation GPS

### 2.1 The Definition of The embedded device

An embedded system is some combination of computer hardware and software, either fixed in its capability or programmable. It is specifically designed for a particular type of application device. The impact of this design in forensics is dramatic because the tools the examiner uses must understand not only the operating system on the device that chooses how the data is stored, but also the design of the device to the chip set level to gauge how much storage is available on the device. The forensics tool used must understand how to communicate with the device in order to gain access at a low enough level to acquire all data available on that device for evaluation. (AMBER, S. 2007)

### 2.2 The Memory of Embedded system

The embedded devices use the Flash memory technology. Flash is an extension of



the floating gate method of manufacturing non-volatile memory. There are two kinds of flash memory namely the NOR and NAND. These two terms are names of types of logic gates, the negated OR function and the negated AND function. There is a big difference between the type of architecture, the NAND has a significantly die size than does the NOR. This translates to significant cost savings. NAND does not behave as other memory while NOR, SRAM, DRAM are random access devices. The RAM means Random Access Memory. The NAND is part random and part serial. Once an address is given to the device, there is a long pause, then that address and several adjacent addresses' data come out in a burst. The life time of a flash memory is measured as being 100,000 erases per block. (THOMAS, M. 2008)

### 2.3 NAND and NOR flash memory architecture

In the neither internal circuit configuration of NOR Flash, the individual memory cells are connected in parallel, which enables the device to achieve random access. This configuration enables the short read times required for the random access of microprocessor instructions. NOR Flash is ideal for lower-density, high-speed read applications, which are mostly read only, often referred to as code-storage applications. NAND Flash was developed as an alternative optimized for high-density data storage, giving up random access capability in a trade-off to achieve a smaller cell size, which translates to a smaller chip size and lower cost-per-bit. This was achieved by creating an array of eight memory transistors connected in a series. Utilizing the NAND Flash architecture's high storage density and smaller cell size, NAND Flash systems enable faster write and erase by programming blocks of data. NAND Flash is ideal for low-cost, high-density, high-speed

program/erase applications.

### 2.3.1 Characteristics of NOR and NAND memories

The Characteristics of the NAND flash memory are

- High Density
- Medium Read Speed
- High Write Speed
- High Erase Speed
- Indirect I/O access

The Characteristics of NOR flash memory are

- Lower Density
- High read speed
- Slow write speed
- Slow erase speed
- Random access interface

### 2.3.2 The Structure and functionality of NAND and NOR memory

As we can see at Figure-1 the read speed execution is low because of the fact that when a bit is requested from Bit Line Select Transistor, all the bits that are in front

of it will be causing a latency for the requested bit to be read. The significant amount of die space is reduced due to the availability of space from the union of transistors that can communicate from single bit line. This way the data moves back and forth ascending the response time of the read functionality.

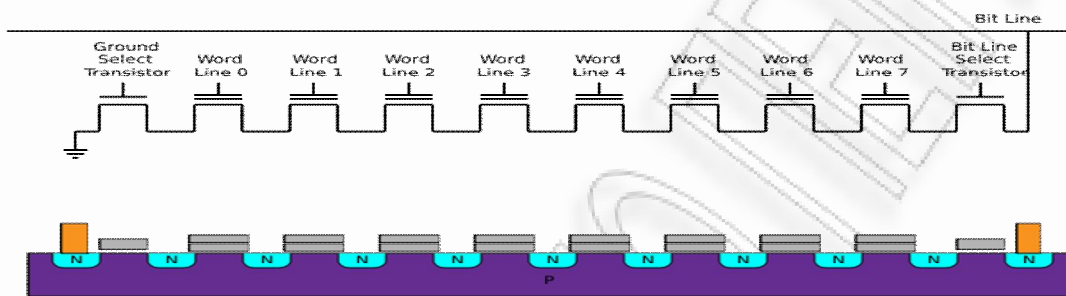


Figure-1. The NAND Structure

At the second Figure we can see the difference between the NOR flash memory and the NAND flash memory more clearly. Every word has its own bit line selector to communicate with the main bit line, so the read speed in this situation is significantly higher than the NAND memory. The selection of the requested bit is faster as the bits can reach the destination bit Line at about the same amount of time and its not far away to get there.

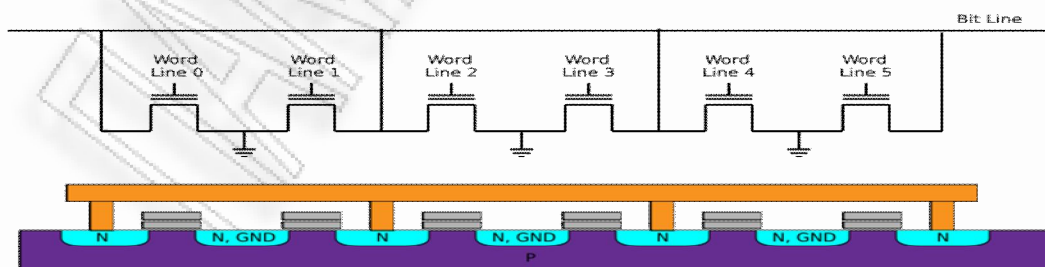


Figure-2. The NOR Structure

The NOR is mostly used for code storage and the NAND for data storage. This means that the end user will continually be erasing and rewriting the data in the NAND. The erase and write cycles in the NAND is said to be 100,000 times. Most of the embedded devices normally use the NAND technology in storing data. Some of the flash memory formats are the PCMCIA card, Compact Flash, Memory Sticks, Secure Digital (SD) cards, multi media card etc.

## 2.4 Linux OS on GPS devices

Linux, a popular open source operating system for servers and desktop computers, has also appeared on several PDA devices. Linux is a true multitasking, 32-bit operating system that supports multithreading. Besides commercial distributions that come preinstalled by PDA manufacturers, Linux distributions are also available for a range of Pocket PC and Palm OS devices. The success of Linux-based PDAs rests on the open source model and its ability to engage the software development community to produce useful applications. Figure 3 gives a conceptual architecture for the Linux operating system. The Linux operating system is responsible for memory management, process and threads creation, and interprocess communication mechanisms, interrupt handling, execute-in-place (XIP) ROM file systems, RAM file systems, flash management, and TCP/IP networking.

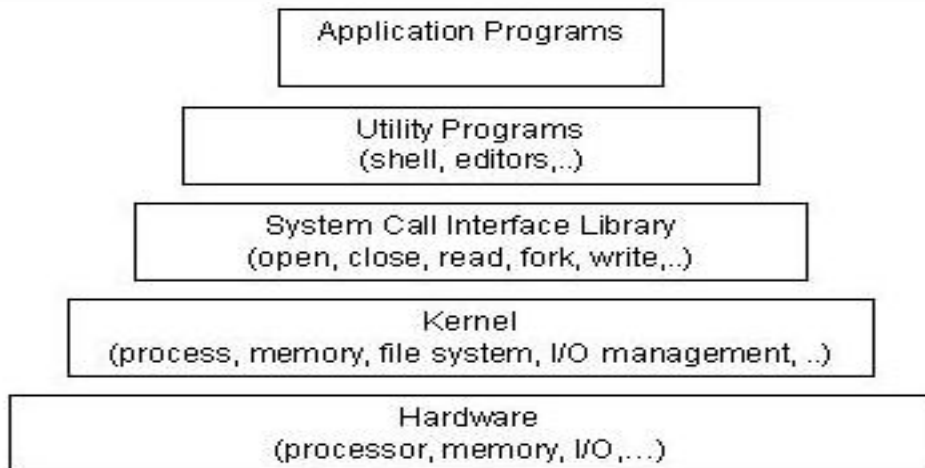


Figure-3 Linux OS Architecture

The Linux kernel is composed of modular components and subsystems that include device drivers, protocols, and other component types. The kernel also includes the scheduler, the memory manager, the virtual file system, and the resource allocator. Programming interfaces provide a standard method by which the Linux kernel can be expanded. Processing proceeds from the system call interface to request service, for example, from the file or process control subsystem, which in turn requests service(s) from the hardware. The hardware then provides the service to the kernel, returning results through the kernel to the system call interface.

## 2.5 The Internal architecture of a GPS device

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

In this project we will use the TomTom GPS device as our experimental device. TomTom the in-car satellite navigation device is connected with the U.S. NAVSTAR Global Positioning System (GPS), which utilises 32 satellites in Mid-Earth Orbit (MEO) positioned in six different orbital planes. The TomTom device itself contains an ARM processor made by Samsung, using Linux to manage the software which can read either an SD card or the internal memory. A boot loader in the computer searches the hard disk or SD card for the software and map data. It then transfers the software to the 64MB internal RAM memory and starts the software.

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

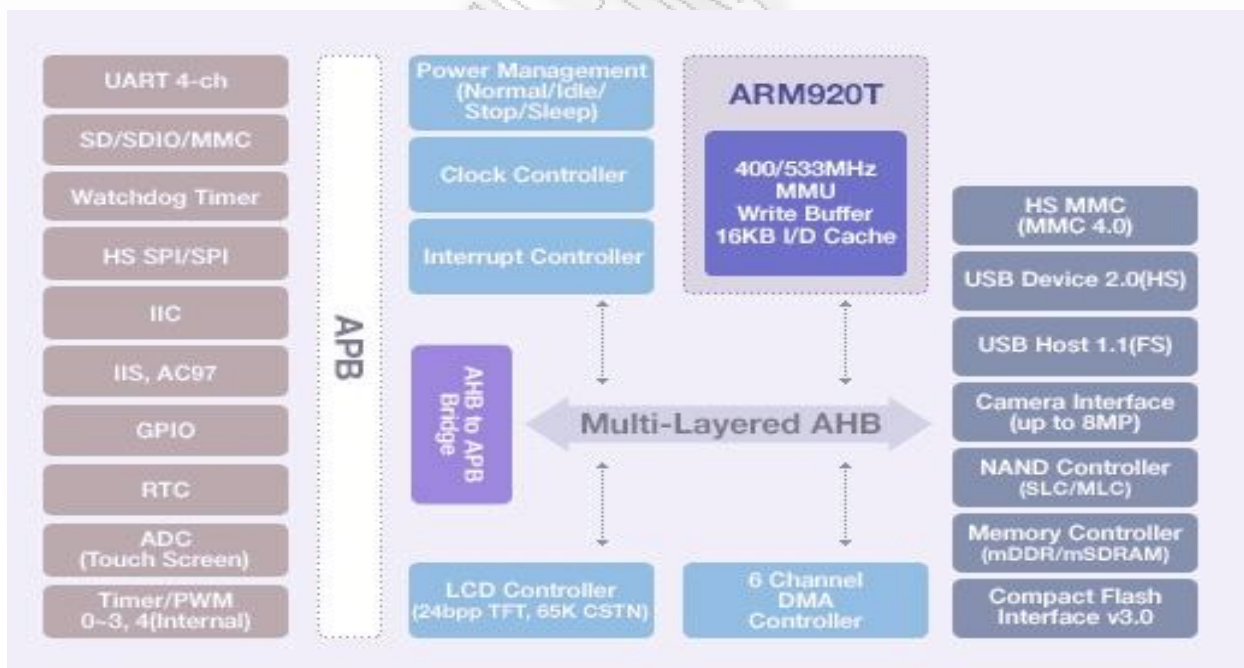


Figure-4. TomTom internal Architecture

## 2.6 GPS Receivers

The Global Positioning System (GPS) receiver uses satellites to pinpoint locations on the earth crust. The GPS is actually a constellation of twenty seven earth orbiting satellites. Twenty four of these satellites are in operation and three extras in case of any failure. The US military developed and implement this satellite network as a military navigation system but soon opened it up to everybody. Each of these 3000 to 4000 pound solar powered satellites circle the globe at about 12000 miles (19,300 km), making two complete rotations every day. The orbits are arranged in such a way that at any time, anywhere on Earth, there are at least four satellites visible in the sky. A GPS receiver's job is to locate four or more of these satellites, figure out the distance to each and use this information to deduce it own locations. (MARCHALL, B. 2008)

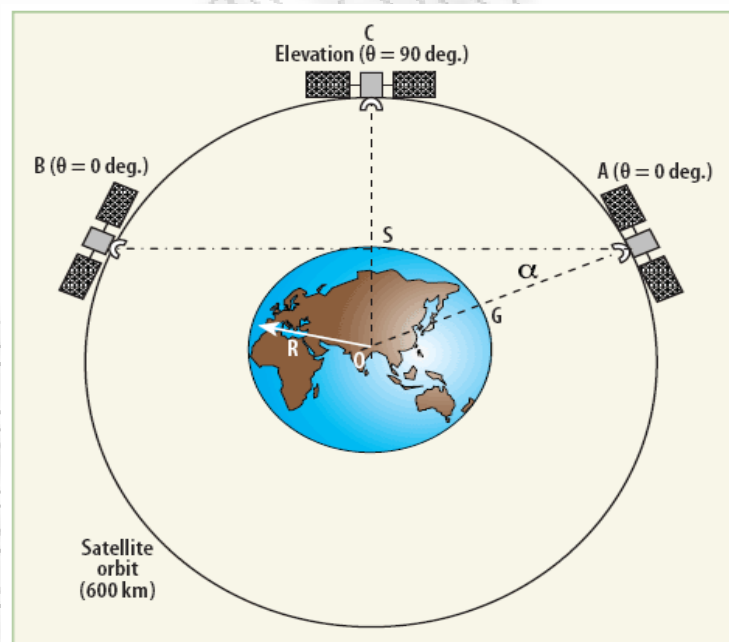


Figure-5. Satellite 'look' angles are depicted in this schematic diagram

## 2.7 Expansion Ports and Interfaces between GPS device and kernel in embedded systems

Linux kernel has specific way for interprocess communication between the software and the hardware. Especially on GPS devices the kernel communicates with the GPS chipset that is responsible for gathering satellite signals. The way that this is happening is under the specification of GPIO (General Purpose Input/Output). GPIO is a generic pin on a chip whose behaviour (including whether it is an input or output pin) can be controlled (programmed) through software. GPIO pins have no special purposes on themselves, and go unused by default. The idea is that sometimes the system integrator building a full system that uses the chip might find useful to have a handful of additional digital control lines, and having these available from the chip can save the hassle of having to arrange additional circuitry to provide them. GPIO usually communicates through the Universal Asynchronous Receiver/Transmitter (UART) that takes bytes of data and transmits the individual bits in a sequential fashion. With this situation we can retrieve GPS receiver data directly from the GPS chipset that can be readable/writable programmatically through system calls from kernel. The GPS unit is attached to the second UART of the S3C2410 (RxD1 and TxD1 pins on chip or ttyS1 in Linux) that is implemented on TomTom device. By doing this on GPS receiver can take data transition further into the embedded software and use those data straight from there before they align into the system memory RAM.



## 2.8 NMEA Data

The National Marine Electronics Association NMEA has developed a specification that defines the interface between various pieces of marine electronic equipment. The standard permits marine electronics to send information to computers and to other marine equipment. A full copy of this standard is available for purchase at their web site. None of the information on this site comes from this standard and I do not have a copy. Anyone attempting to design anything to this standard should obtain an official copy.

GPS receiver communication is defined within this specification. Most computer programs that provide real time position information understand and expect data to be in NMEA format. This data includes the complete PVT (position, velocity, time) solution computed by the GPS receiver. The idea of NMEA is to send a line of data called a sentence that is totally self contained and independent from other sentences. There are standard sentences for each device category and there is also the ability to define proprietary sentences for use by the individual company. All of the standard sentences have a two letter prefix that defines the device that uses that sentence type. (For gps receivers the prefix is GP.) This is followed by a three letter sequence that defines the sentence contents. In addition NMEA permits hardware manufactures to define their own proprietary sentences for whatever purpose they see fit. All proprietary sentences begin with the letter P and are followed with 3 letters that identifies the manufacturer controlling that sentence. As we can see below there is a figure that shows the NMEA sentences.

```
$GPRMC,054152.000,V,5202.693,N,00421.530,E,0.00,0.00,160908,*30
```

```
$GPGSV,3,1,09,26,88,171,34,15,71,285,29,28,58,091,30,08,27,069,26
```

```
$GPGSV,3,2,09,18,22,314,24,10,21,187,09,16,256,26,21,06,288,16
```

\$GPRMC,054152.000,V,5202.693,N,00421.530,E,0.00,0.00,160908,\*30

\$GPGGA,054211.000,5202.693,N,00421.522,E,0,00,0.0,-5.150,M,0.0,M,\*49

\$GPGSA,A,3,28,26,08,15,18,,,,,,,,, 43.8,32.4,29.5\*0D

### 3. The Policies and procedures of carrying out forensics examination

Forensics can be defined as the use of science and technology to investigate and establish facts in criminal or civil courts of law. The investigator must be unbiased, qualified and understand the legal issues. The first thing to consider when presented with a case is Whether or not to accept it. Many factors influence and ultimately determine whether to accept or take in a case. Some of the common criteria for taking a case include:

- Whether it is a criminal or civil case.
- The impact on the investigating organization
- Whether the evidence is volatile or non-volatile
- Legal considerations, such as the types of data that might be exposed
- The nature of the crime
- Potential victims, such as children in child pornography cases or murder cases
- Liability issues for the organization
- The age of the case
- Amount of time before the court date

A general case intake form needs to be completed when reviewing a potential case and determining whether to accept it. Among other issues, the form requests information to check for any conflict of interest between the forensics company, investigators and other concerned parties. The completion of this form is often overlooked when developing standard operating procedures. This form confirms the understanding and agreement among the parties involved and sets the stage for everything else about the case, such as chain of custody and basic evidence documentation. This intake forms differ depending on whether the case is being accepted by a law enforcement agency or a private company. (LINDA, V. et al. 2006. P. 124.)

### 3.1 The methodology of Carrying out forensics examination

The primary goal in computer forensics is collecting, preserving, filtering and presenting digital artefacts. It can also be used as guidelines to describe the computer forensics processes. The different phases can be summarised as follows;

#### 3.1.1 Collection

The collection phase of computer forensics is when artefacts considered to be of evidentiary value are identified and collected. Normally these artefacts are digital data in the form of disk drives flash memory drives or other forms of digital media and data. In this case the storage media of the suspect's computer or GPS receiver was identified as artefacts of potential evidentiary value.

### 3.1.2 Preservation

Evidence preservation is the process of seizing suspect property without altering or changing the contents of data that reside on devices and removable media. It is the first step in digital evidence recovery. In the preservation phase of computer forensics focuses on preserving original artefacts in a way that is reliable, complete, accurate and verifiable. The Cryptographic hashing, checksums and documentation are all key component of the preservation phase. Preservation involves the search, recognition, documentation, and collection of electronic-based evidence. In order to use evidence successfully, whether in a court of law or a less formal proceeding, it must be preserved. Failure to preserve evidence in its original state could jeopardize an entire investigation, potentially losing valuable information about an incident permanently. Below there is a description of how preservation can be achieved

#### Securing and Evaluating the Scene

- Ensure the safety of all individuals at the scene.
- Protect the integrity of traditional and electronic evidence.
- Evaluate the scene and formulate a search plan.
- Identify potential evidence.
- All potential evidence should be secured, documented, and/or photographed.
- Conduct interviews.
- Documenting the Scene
  - Create a permanent historical record of the scene.

- Accurately record the location and condition of computers, storage media, other digital devices, and conventional evidence.
- Document the condition and location of the computer system, including power status of the computer (on, off, or in sleep mode).
- Identify and document related electronic components that will not be collected. Photograph the entire scene to create a visual record as noted by the first responder.
- Collecting Evidence
  - Handle Computer evidence whether physical or digital in a manner that preserves its evidentiary value.
  - Recover non electronic evidence (e.g. written passwords, handwritten notes, hardware and software manuals, calendars, literature, photographs etc.)
- Packaging Transporting and Storing Evidence
  - Take no actions to add, modify, or destroy data stored on a computer or other media.
  - Avoid high temperatures and humidity, physical shock, static electricity and magnetic sources.
  - Maintain chain of custody of electronic evidence ,documenting its packaging , transportation and storage
- Packaging Procedure
  - Properly document , label and inventory evidence before packaging

- Pack magnetic media in antistatic packaging
- Avoid scratching ,bending or folding computer storage media such as CD-ROMs
- Properly label evidence containers
  - Transportation Procedures
  - Avoid magnetic sources
  - Avoid conditions of excessive heat , cold or humidity while in transit
  - Avoid excessive vibrations
- Storage Procedures
  - Ensure evidence is inventoried in accordance with authoritative policies
  - Store evidence material in a secure area away from temperatures and humidity.
  - Protect evidence material from dust and other harmful contaminants

### 3.1.3 Analysis

In this phase the investigators will attempt to filter out data which is determined not to contain any artefacts of evidentiary value and filter in artefacts of potential evidentiary value. A wide array of tools and techniques are utilized in the filtering phase. Some of which include comparing cryptographic hash values of known good and known suspect files against a known dataset.

### 3.1.4 Presentation

This is of course the final phase of computer forensics investigation. It is in this phase that the potential artefacts of evidentiary value are presented in a variety of forms. Presentation normally starts with the investigator extracting the artefacts from the original media, and then staging and organizing them on CDROM or DVD-ROM. The investigator's reports, supporting documentation, declarations, depositions and testimony in court can all be considered the presentation phase of computer forensics.(CHRISTOPHER, L. 2006 PP 6 - 8). Electronic evidence is valuable evidence and it should be treated in the same manner as traditional forensic evidence with respect and care. The methods of recovering electronic evidence whilst maintaining evidential continuity and integrity may seem complex and costly, but experience has shown that, if dealt with correctly, it will produce evidence that is both compelling and cost effective.

### 3.2 Roles and Responsibilities

Whatever the type of incident, the various types of roles involved are similar. Planning for incidents should address how existing personnel fulfill these roles when responding and conducting an investigation. A generic set of roles and associated responsibilities can be identified. They include First Responders, Investigators, Technicians, Forensic Examiners, and Forensic Analysts. In a given situation, a single individual may perform more than one role.

First Responders are trained personnel who arrive first on the scene of an incident, provide an initial assessment, and begin the appropriate level of response. The responsibilities of First Responders are to secure the incident scene, call for the

appropriate support needed, and assist with evidence collection.

Investigators plan and manage preservation, acquisition, examination, analysis, and reporting of electronic evidence. The Lead Investigator is in charge of making sure that activities at the scene of an incident are executed in the right order and at the right time. The Lead Investigator may be responsible for developing the evidence, preparing a case report, and briefing any findings and determinations to senior officials.

Technicians carry out actions at the direction of the Lead Investigator. Technicians are responsible for identifying and collecting evidence and documenting the incident scene. They are specially trained personnel who seize electronic equipment and acquire digital images resident within memory. More than one technician is typically involved in an incident, because different skills and knowledge are needed.

Evidence Custodians protect all evidence gathered that is stored in a central location. They accept evidence collected by Technicians, ensure it is properly tagged, check it into and out of protective custody, and maintain a strict chain of custody.

Forensic Examiners are specially trained personnel who reproduce images acquired from seized equipment and recover digital data. Examiners make the information on the device visible. Examiners may also acquire more elusive data using highly specialized equipment, intensive reverse engineering, or other appropriate means unavailable to Forensic Technicians.

Forensic Analysts evaluate the product of the Forensic Examiner for its significance and probative value to the case.



### 3.3 Evidential Principles

Digital evidence has both physical and logical aspects. The physical side of it involves hardware components, peripherals, and media, which may contain data or the means to access it, while the logical side deals with the raw data extracted from a relevant information source. The Good Practice Guide for Computer based Electronic Evidence [ACPO2] suggests four principles when dealing with digital evidence.

- No actions performed by investigators should change data contained on digital devices or storage media.
- Individuals accessing original data must be competent to do so and have the ability to explain their actions.
- An audit trail or other record of applied processes, suitable for independent third-party review, must be created and preserved, accurately documenting each investigative step.
- The person in charge of the investigation has overall responsibility for ensuring the above-mentioned procedures are followed and in compliance with governing laws.

The Proposed Standards for the Exchange of Digital Evidence [IOCE] suggest a similar set of principals for the standardized recovery of computer-based evidence:

- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage, or transfer of digital

evidence must be fully documented, preserved, and available for review.

- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

The above sets of principles aim to ensure the integrity and accountability of digital evidence through its entire life cycle. Proper handling of evidence is always vital for it to be admissible in judicial proceedings. However, different standards may apply to different types of investigations. The degree of training and expertise required to execute a forensic task largely depends on the level of evidence required in the case.

### 3.4 Equipment in a basic Forensics Kit

As a matter of policy and procedure, a basic computer forensics kit should always be used. Every investigation will have some unique characteristics, but the basic equipment required by a forensic expert remains the same. The following list is a guideline for what should be included in a forensics kit:

- Cellular phone: There will always come a time when you need to find additional information or call for help of some kind
- Basic hardware toolkit: Items such as standard screwdrivers, pliers, scissors, duct tape, and so on should always be part of your forensics kit.

- Watertight or static resistant plastic bags: We make sure we have Ziploc type bags of various sizes to store collected evidence
- Labels: Included in our tool kit various types of labels to tag items such as cables, connections and evidence bags.
- Bootable media: We always need to have handy a variety of bootable media such as DOS start up disks, bootable CDs, and even bootable USB drives. Our choice of bootable media will varies depending on the type of forensics software we are going to use
- Cables (USB, printer, FireWire): Depending on what type of forensic software we plan to use, our choice of cables will vary. Always carry at least a CAT 5 crossover cable, straight through cable and rollover cable. A spare power cable always comes in handy.
- Writing implements: We should have a soft permanent marker to write on labels, floppies, or CDs. A sharpie type marker is always preferable because these markers are felt tipped and will not damage CD labels.
- Laptop: A laptop is always a good tool to have even if it is not your forensics examination platform. A laptop allow us to carry a veritable library of forensics tools, give us access to the Internet, lets us keep updated manuals or schematics on hand, allow us to store information immediately if need be (volatile information such as that stored in embedded devices such as GPS receivers and PDAs) and give us flexibility to adjust to different investigative situations.
- High resolution camera: In order to document everything properly, we should take a series of photographs before you start working. Photograph taken during and after are always recommended, but you must photograph

the initial scene. A camera that labels the date and time on the photo is always a good idea.

- Hardware write blocker: We never know when we will need to take a storage media out and do drive transfer, so a hardware write blocker such as Fast Bloc or Drive Lock is a small device that we should carry just in case
- Log book: It is a good practice to have a habit of carrying a log book to record investigator actions
- Gloves: As a forensic examiner, we always need to keep in mind that there are other forms of evidence such as fingerprints to keep intact. Additionally, a good set of gloves used when handling evidence shows our attention to even smallest details of evidence preservation.
- Forensic examiner Platform: Platforms vary from laptops to fully equipped desktop units. The next generation of mobile forensic platforms should make the acquisition of data in the field or in entrusted environments more convenient with faster connection speeds via wired transfers, wireless acquisitions and smaller forensic platform units

#### 4. General methodology of forensic investigation embedded GPS receiver

The use of satellite navigation systems has become increasingly common in recent years. The wide scale adoption of this technology has the potential to provide a valuable resource in forensic investigations. The potential of this resource is based on the ability of retrieve historical location data from the device in question. This methodology aims to be comprehensive and straightforward, while maintaining

forensic integrity of the original evidence. Automotive satellite navigation systems such as TomTom and Garmin, aim to provide navigational assistance to its users. Often the user will provide a destination point then based on this the device will provide a map and verbal turn by turn directions to the specified destination. Such devices are becoming more common and are decreasing in price. It should also be noted that many new cars now come with Satellite Navigation System as standard.

#### 4.1 GPS receiver storage media

The GPS receiver devices can be divided into three main types: those with SD Cards, Those with internal hard drives, and those with internal flash memory with or with out SD card slots. Devices which have both internal memory and an external SD slot typically store the user data on the internal memory, using the SD card slot only for additional storage, unless the device is set to use maps which are stored on the SD card, in which case the .cfg file will be found in that map directory. As there is usually significant amount of data found on an unallocated clusters and file slack the best approach is always to take a complete forensics image rather than simply extracting the live .cfg file. Devices which store data on a removable SD card are the simplest to deal with, as the memory card can be removed from the device and imaged as normal using forensic software. (NUTER, B. 2008)

#### 4.2 The acquisition of a SD card

The SD card must be inserted into the device at all times in order for the device to function as its core operating system resides on the card. Initial research suggests

the data on the SD card is comprised of at least the following:

- X86 Boot Sector
- Mapping data
- Operating system files
- Configuration files
- Swap space

The SD card is easily accessible in a non invasive manner and it is possible to acquire the SD card with a minimum of equipment and experience. In addition to this it is possible to acquire an image of the SD card in a covert fashion, in many cases it is not possible to determine that the device has been tampered with. The procedure for acquiring a forensic image of this media involves attaching the device to a system in read only mode and acquiring a bit stream copy of the SD card. As with any forensic procedure the media should be hashed before and after acquisition, the resulting copy of the data should also be hashed in order to verify its integrity. It should be noted that powering the satellite navigation unit on whilst the SD card is inserted will result in data being written to the SD card and the hash changing. In this case the position of the write protect tab on the SD card reader is irrelevant as most of the Automobile GPS receivers do not discriminate if writing should be permitted based on the tab's position. Instead the SD card is treated as writable regardless of the tab's position. In order to perform the acquisition of the SD card it is necessary to have a write blocking SD card reader. (PETER, H. 2007) Initial examination of commercially available SD card readers has shown that it is possible to modify the devices so that they will not perform write operations. Generally the acquisition of the SD card can be done using the HELIX 3 ISO. This

is a Linux distribution that has installed many forensics tools for implementing forensics investigation. There are tools with many features implementing the dd software that also can be called individually from the terminal from any Linux distribution. The dd software is capable to perform low data operations such as performing a bit stream copy of the data to be acquired. The processes are:

- Attach write blocked USB SD card reader
- Insert a non critical SD card for testing purposes
- Perform a hash of the SD card
- Ensure the file system if any present on the SD card has not been mounted
- Attempt to write to the SD card
- Ensure that the hash matches the original
- Remove the SD card
- Insert the SD card to be acquired
- Perform a hash of the SD card
- Ensure the file system if any present on the card has not been mounted
- Acquire a copy of the SD card using dd command
- Perform a hash of the SD card
- Perform a hash of the acquired file
- Ensure that the hashes match the original
- Remove the SD card form the reader

After the acquisition has been done, the analysis of the bit stream image can be carry out with the used of Encase or Forensics Tool Kit.

#### 4.3 Proposed add-ons in methodology of forensic investigation embedded GPS receiver

As we can see from the previous paragraph the general methodology shows that the steps of the forensics evidence acquisition comes in at a logic order where the investigator performs a series of steps but unfortunately less is done for security aspects of the method being approached. Meaning that there is not a specific interest of the investigator authenticity as well as of the GPS coordinates authenticity. Another aspect of the previous methodology that isn't being covered is that the coords are readable from anyone and is not encrypted .The non cryptographic parameter takes a lot of consideration as it gives ease to criminals for altering or even delete the coordinates form inside the device. Certainly cryptography isn't a hundred percent solution such that any criminal may destroy all the file system formatting the hard drive, but sure it is an obstacle as it is certainly prevent criminals from easily find the coordinates because of the non understandable format or because is too hard to find the desirable format .the main reason for encryption is that it prevents criminals from capturing historical data that live in slack spaces and to use them for their own benefit. But otherwise criminals can also hide their fingerprints by using wiping tools for cleaning slacks and destroying evidence. Destroying the device is not a good practice because it gives more incriminating evidence to the person being accused and so, he/she will definitely search to find other ways of hiding evidence. The main action that has to be added and has an important value, at my opinion, is the authenticity of the investigator.



## 4.4 File Slack Definition

Every computer system at these days has a significant behaviour when dealing with static or dynamic memories. The fact is that the file system architecture is dealing with different lengths while the memory is allocated in different clusters and fixed blocks depending on the operating system. So in our case GPS devices are small computers which have the classic file system architecture that main computers have. Forensically that's a serious work for the forensics examiner to be occupied because it's very important to capture all the data that are hiding inside the system. The most serious situation is when criminal activities use anti forensics tools to hide evidences such as wiping tools.

Generally files are created in varying lengths depending on their contents. Operating Systems such as DOS and Windows NT-based store files in fixed length blocks of data called clusters. Rarely do file sizes exactly match the size of one or multiple clusters perfectly. The data storage space that exists from the end of the file to the end of the last cluster assigned to the file is called "file slack". Cluster sizes vary in length depending on the operating system involved. Larger Cluster sizes mean more file slack and also the waste of storage space. However this computer security weakness creates benefits for the computer forensics investigator because file slack is a significant source of evidence and leads.

File Slack is created at the time a file is saved to disk. When a file is deleted under DOS, Windows, Windows 95, Windows 98 and Windows NT/2000/XP, the data associated with RAM slack and drive slack remains in the cluster that was previously assigned to the end of the 'deleted' file. The clusters which made up the 'deleted' file are released by the operating system and they remain on the disk in the

form of unallocated storage space which is then overwritten with data from a new file.

Linux based OS that our GPS Device TomTom has installed performs installation to files and creates them in blocks of data in addition with windows that use clusters. Generally is the same thing. Blocks are specific sized containers used by file system to store data. Blocks can also be defined as the smallest pieces of data that a file system can use to store information. Files can consist of a single or multiple blocks/clusters in order to fulfil the size requirements of the file. When data is stored in these blocks two mutually exclusive conditions can occur; the block is completely full, or the block is partially full. If the block is completely full then the most optimal situation for the file system has occurred. If the block is only partially full then the area between the ends of the file the end of the container is referred to as slack space. Linux write nulls on slack space. This means to find data in slack space on Linux systems are rare. However, it is not impossible.

## 5. Literature review of the forensics examination of embedded device such as GPS

### 5.1 Literature review

The satellite navigation uses Global positioning System (GPS) for pinpointing location on the earth crust. GPS was developed by the department of defence in the United States of America. It was designed to be a high quality system for navigation accuracy. The GPS system works by using a network of 24 NAVSTAR satellite orbiting the earth. NAVSTAR stands for Navigation System using Timing and Ranging. It function round the clock that 24/7 at a height of 10,900 – 12,625

miles above the earth surface. The satellites with an impressive two tons are 18.5 feet long; transmit on two frequencies 1575.42 MHz for civilians and 1227.60 MHz for military service. The NAVSTAR orbits the earth in just 12 hours. These satellites are designed to be resistant to interference and jamming thus they make incredibly good positioning beacons when used in conjunction with one another to give accurate position. The GPS receiver then communicates with the GPS in order to have an accurate position world wide.

## 5.2 The Global Positioning System (GPS) receivers

The GPS receiver can play an integral part of an investigation. Since GPS receiver has become widely used in cars these days, there is a high chance of finding useful information about the route and time of an event. Satellite navigation is used commonly as a route finder on all forms of transport. These incredibly useful devices are now used by the public, and have a high availability. Most modern vehicles use satellite navigation systems, and it is the information in this system that can give assistance in providing information to others, be they law enforcement officers, defence lawyers, employers or members of the public. These satellite navigation systems have logs and configuration files that need to be examined and broken down into readable and understandable information. The satellite navigation or GPS receiver has both hardware coding written to itself and software. Examination and interpretation of this software enables us to find waypoints, predominantly on marine satellite navigation systems and directions requested on vehicle satellite systems along with directions given and time that the journey was taken. The GPS receiver like TomTom or Garmin can be broken down into three main types, those with SD cards, those with internal flash memory and those with

internal hard drive. The goal of forensically examine a GPS receiver is to find out whether information of importance can be harvested in the storage media. Forensically we need to first of all acquire a bit stream image of the memory card or acquire it directly from the receiver itself (those with internal hard drive). The GPS receiver allows the user to plan routes, save favourite destination and look up point of interest (POI). Some devices can also pair with phones and if so can yield call history and contact data and connected to a computer act as a USB mass storage device. New version have inbuilt MP3 players and picture viewers. The GPS receiver is operated via touch screen menu driven interface, which allows the user to enter locations, plan routes or itineraries, save favourites or look up POI. The user can also operate a paired mobile phone via the TomTom to make calls, read or write text messages. If a wireless connection has been set up, the user can access addition service via a TomTom Plus account, Such as weather information real time traffic information or additional downloads like extra voices or updated maps. (NUTTER, B.2008)

### 5.3 Previous work done with GPS forensics analysis

The GPS receivers store information on the in a file called dot cfg file (.cfg file). The analysis has been focus on the boot loader, since rewriting this allows alternative software to be run. In a presentation, at the first forensics forum, Weall, 2006 noted that each record contain two set of coordinates, (the longitude and the latitude in the WGS 84 datum), a Text label for the address and further two sets of coordinates. His hypothesis was that since the first set of coordination seemed to relate to the actual location, the other three related to nearby feature that is nearest road and junctions. The analysis of the 'dot cfg file' point out that the first

destination in 'dot cfg file' is the home location if entered, and that the last two entries relate to the start of the last calculated route and the last entered destination .(NUTTER, B.2008). With this information gathered in a file it is really useful for the examiner to see and analyse the coordinates, but what about unallocated space. It might be possible to say that a location was the start of a route, but it is likely that a location may be found in the slack space with no information about the original location in the file. In that case, it will be difficult to say how significant it might be. To understand more than that, decoding the individual record is required.

#### 5.4 Acquisition of GPS receiver storage media

Since there is always a significant amount of data found in unallocated clusters and file slack the best approach is to carry out a bit stream image of the storage media . Bit stream copying of the storage device means that all the (.cfg files) will definitely be imaged. When an image is acquired form the hard drive of TomTom via USB the Timestamp of the following files are changed: TTPnPD.log, clmdata, settings.dat, ITN\temporary.itl. And when imaging a flash memory of a TomTom via USB, the time stamp of the same files are changed including the map directory\MapSettings.cfg. The device which store data on a removable SD card reader are easy to deal with, as the memory card can be removed from the device and imaged as normal using forensic software and write protected card reader.

## 5.5 Files of forensics interest

Once a forensic image has been obtained, that image can then be analyzed. There are a number of files of possible interest to the examiner, including:

- \contacts\called.txt – which contains numbers called by the phone paired to the TomTom
- \contacts\callers.txt – which contains numbers of phones which have called the phone paired to the TomTom
- \contacts\contacts.txt – which contains details of numbers in the address book of the phone paired to the TomTom
- \contacts\inbox.txt – contains incoming text messages
- \contacts\outbox.txt – contains outgoing text messages
- TTGO.bif – contains device information (e.g. serial number) and current home location (in later application versions);
- settings.dat – contains the name and MAC address of a paired phone, if one has been connected, wireless data settings and data provider if this has been set up, and home phone number information and owner information, if set10;
- \itn\ – directory containing itineraries, if any have been entered (temporary.itn is the currently active itinerary).

## 5.6 Identifying the GPS fix location

Possibly the most significant benefit is that it is possible from this to identify

locations where the TomTom has actually been. Siezenga (2008) has noted that the second to last location in the cfg file is the start of the last calculated route. In the majority of journeys, this will be the location where the TomTom was when the route was calculated, as it only begins calculating a route when a GPS fix is obtained. If deviating from the route the Tom-Tom has planned, a new route is calculated, and the point of deviation becomes the new starting point for that route. Upon driving past an entered destination, the TomTom will then begin calculating a route back. Or when turning a TomTom on without clearing a route, a new route will be calculated to the last entered destination. Any of these four events will result in a start location being recorded which is a location where the TomTom has obtained a GPS fix. (NUTTER, B.2008)

## 6. GPS receiver forensics examination. The General Case study

There is a lot of work done in the field of GPS forensics with tools already installed in several distributions of tool packages for using them to carry out important information and evidence, valuable for examination and criminal investigation. This chapter will provide a standard methodology of carrying out GPS evidence from a GPS device such as tom-tom one. After this chapter done and all the steps explained well enough, there will be another case study which will show the steps for evidence acquisition accompanying with a plugged in methodology which is under development in this assignment. The two methodologies will be compared and analysed and finally there will be a conclusion.

## 6.1 The GPS navigation system

There are many types of GPS navigation in the world today but the most popular ones being TomTom, Garmin, Mio Technology, Navman, and Magellan. Research from the Canalsys Q2 2007 on global mobile navigation has proven that TomTom and Garmin both increased their share year on year and sequentially. After two years at the top by several percentage points, TomTom was narrowly overtaken by Garmin as the leader in the global mobile navigation device market in Q2 2007, according to the latest estimates from analyst firm Canalsys. The Canalsys figures include all mobile devices used for turn by turn road navigation with built in GPS and on board software including not only Portable navigation Device (PND) such as the TomTom GO range and Garmin Nuvi but also smart phones, handhelds and other similar classes of device. The total device shipments for the quarter stood at 7.4 million, up 116% on the same quarter one year ago and almost 2 million above last quarter's figure. The statistics below proves that the TomTom and Garmin is actually the most popular device used world wide.

<b>Worldwide integrated on-board mobile GPS navigation device market</b>					
<b>Hardware vendor market shares Q2 2007, Q2 2006</b>					
<b>Vendor</b>	<b>Q2 2007 shipments</b>	<b>% share</b>	<b>Q2 2006 shipments</b>	<b>% share</b>	<b>Growth Q2'07/Q2'06</b>
<b>Total</b>	<b>7,448,050</b>	<b>100.0%</b>	<b>3,445,540</b>	<b>100.0%</b>	<b>116.2%</b>
<b>Garmin</b>	1,852,150	24.9%	699,370	20.3%	164.8%
<b>TomTom</b>	1,806,970	24.3%	829,790	24.1%	117.8%
<b>Mio Technology</b>	683,500	9.2%	290,590	8.4%	135.2%
<b>Magellan</b>	421,080	5.7%	64,950	1.9%	548.3%
<b>Navman</b>	232,780	3.1%	171,410	5.0%	35.8%
<b>Others</b>	2,451,570	32.9%	1,389,430	40.3%	76.4%

**Source: Canalsys estimates, © canalsys.com Ltd. 2007**  
Includes PNDs, PMPs and smart mobile devices with integrated GPS used for turn-by-turn road navigation



Due to the above statistics it was worth while to carry out a forensics examination of the most popular devices since many people are using it today and thus can give a good leads in crime investigation if GPS navigation was used during or after the commission of the crime.

## 6.2 The system imaging

It is unarguable that disk evidence is easily the cornerstone of computer forensics, if for no other reason than digital evidence on disk is as easy to relate to a judge and jury as files in a file cabinet. However, the completeness and accuracy of digital evidence collection is often questioned in the legal arena. In an effort to fend off evidentiary challenges relating to the evidence dynamics of disk collection and analysis, computer forensics investigators have for some time placed a major emphasis on careful disk collection and handling. Due to the volatility of disk data and potential destructive nature of handling and analysis, computer forensics investigator agree that creating a bit stream copy of a disk is a necessary component of disk evidence collection and analysis. This bit stream copy with obviously include both the allocated and unallocated clusters. In order to keep with the court acceptable standards of completeness and accuracy, computer forensics investigators should created a bit-stream image of the original evidence when copying form source media to destination media whenever reasonable. According to the National Institute of Standard and Technology (NIST) guideline, imaging tool must have the following features:

- The tool shall be able to acquire a digital source using each access interface visible to the tool

- The tool shall be able to acquire either a clone of a digital source or an image of a digital source, or provide the capability for the user to select and then create either a clone or an image of a digital source
- The tool shall operate in at least one execution environment and shall be able to acquire digital sources in each execution environment.
- The tool shall completely acquire all visible data sectors from the digital source
- The tool shall completely acquire all hidden data sectors from the digital source
- All digital sectors acquired by the tool from the digital source shall be acquired accurately
- If there are unresolved errors reading from the digital source then the tool shall notify the user of the error type and location.

(CHRISTOPHER, B. 2006. PP 236 – 237)

### 6.3 The Bit stream image

A forensic investigator will always collect a bit stream image of the original media. This image collection allows for subsequent analysis and reporting, leaving the original media safely locked away. The bit stream image collection takes place when the investigator will essentially access the data through a software tool and stream the data sector by sector from the evidence media into a file or group of files residing elsewhere. The bit stream image data will always contain the head and the

trailer information. It is also very important to note that the file size of the destination drive of FAT32 file system when imaging could not store more than four Gigabytes of data at one time but the NTFS file system does not have this limitation.

## 6.4 Verification of Imaging and the hash value

A cryptography hash is an algorithm used to produce fixed-length character sequence based on input of arbitrary length. Any given input will always produce the same output called the hash. If an input bit changes, the output hash will change significantly and in a random manner. In addition, there is no way the original input can be derived from the hash. The two of the most common used hashing algorithms are MD5 and SHA1. These cryptography hashes are normally used in the forensics field as a tool to ensure data integrity. A cryptography hashing function or algorithm has the following technical characteristics:

- A hash algorithm transforms an arbitrarily block of data into a large number called a hash value
- The value has no correlation to the original data, and nothing about the original data can be inferred from it
- Small changes in the original data produce large, essentially random changes in the hash value
- Generated hash values are evenly dispersed throughout the space of possible values (that is all possible values are equally likely to occur)

(CHRISTOPHER, B. 2006. P. 247)

When a bit stream image of a digital device is completed the hash value will always be generated and it is used to prove the integrity of the imaging process.

## 6.5 Case study: Forensic Examination of GPS receiver such as TomTom GO 500

TomTom GPS navigation devices are one of the most popular kinds of Satellite navigation devices in the UK, and are increasingly being examined in criminal cases to identify data of evidential value. The navigation functionality of TomTom device allows the user to plan routes, save favourites destinations, and look up points of interest (POIs). The device has the potential to yield call history and contact data if paired with phones connected to the computer, it acts as a USB mass storage device. Newer versions have inbuilt MP3 players and picture viewers. The TomTom receiver under the forensic investigation must follow the rules and principle of carrying out the forensics investigation of digital devices as stipulated in the ACPO guide lines. When the device has been collection for investigation the next point will be the imaging of the memory found inside the device. This imaging supposed to be done by the used of an imaging tool world wide known in digital forensic communities.

## 6.6 The tools using for imaging GPS receivers

The tool used for imaging TomTom receivers are many out there such as Forensic Tool Kit imager V2.5.4, Blackthorn, Encase version Six with the used of Write Blocker and Helix 3 ISO with the used of DD command. The tool that was used to image the TomTom device used for this project was Helix 3 ISO with the used of

DD command lines. The Helix 3 ISO is a customized distribution of Ubuntu Linux and it is more than just a bootable live CD. It can still boot into a customized Linux environment that includes customized Linux kernels, excellent hardware detection and many applications dedicated to incident Response and Forensics. Helix works properly and do not touch the host computer and it is forensically sound. This Helix product do not auto mount space or any attached devices. A copy of the helix software was downloaded on their website and backup on a CD.

Bootable disks containing a clean operating system and specialized utilities are not new to the security arena. For some time now, information security professionals have used the Trinux boot floppy disk, which contained a stripped down version of the Linux Kernel. Bootable CD-ROMs allow the investigator to reboot a suspect system to the “clean” operating system and utilities, allowing for on site static bit stream disk image collection and analysis. The bootable CD-ROM can be used to host the base operating system and tools used by an investigator during live investigation in suspect net environments. By using write protected media, the investigator can keep the base operating system and utilities safe from compromise, or at least permanent compromise. The Helix 3 CD ROM provides users with a full desktop platform and is configured to leave little or no disk artefacts. The platform is of great interest to users conducting criminal activities and misuse. (CHRISTOPHER, B. 2006. PP. 230 - 231)

## 6.7 Imaging TomTom GPS receiver

Before starting the imaging process we must make sure that there is enough free space to put the image. A 500 GB external hard drive which has an NTFS file system was use as the destination device and the TomTom receiver was about 254

MB. The external hard drive was connected via a USB. And the computer was been boot from a bootable CD of Helix 3 ISO and follow the on screen instruction. When the Helix CD opens in to the GUI, we select application and choose Forensic IR and from there we select Adepto. Adepto is one of the programs found in Helix 3 ISO which is used for imaging. The advantages of creating a disk-to-disk bit stream image are that the resulting evidence disk can be mounted with write protection in a forensic workstation and many different tools can be used for evidence analysis. The second point is that it maintains the integrity of the suspect's drive by automatically calculating of the hash algorithm, which will use to later verify the disk or image integrity. (See the screen dump below) (CHRISTOPHER, L. 2006. PP 242 – 243)

## 6.8 Methodology of imaging TomTom One GPS receiver

Before starting the imaging process we must make sure that there is enough free space to put the image. A 500 GB external hard drive which has an NTFS file system was use as the destination device and the TomTom receiver was about 254 MB. The external hard drive was connected via a USB. And the computer was been boot from a bootable CD of Helix 3 ISO and follow the on screen instruction. When the Helix CD opens in to the GUI, we select application and choose Forensic IR and from there we select Adepto. Adepto is one of the programs found in Helix 3 ISO which is used for imaging. The advantages of creating a disk-to-disk bit stream image are that the resulting evidence disk can be mounted with write protection in a forensic workstation and many different tools can be used for evidence analysis. The second point is that it maintains the integrity of the suspect's drive by automatically calculating of the hash algorithm, which will use

to later verify the disk or image integrity. (CHRISTOPHER, L. 2006. PP 242 – 243)

Identification of the source and destination drive: The source and destination drive need to be mounted and check before an effective imaging process can begin. The destination drive was mounted by clicking on the drive after been connected via USB and choose mounted. This will enable us to know the name and the partition of the drive because it is useful during the entering of the dd command. The Source drive was identify as “sdc” and the destination drive as “sdb1” Thereafter the both drives are unmounted and will then be mounted with the use of dd command line. Since the destination drive has the New Technology File System (NTFS), the force command was used to mount the NTFS file system. The command been used is “sudo mount -t ntfs-3g -o force /dev/sdb1 /media/sdb1. (See screen dump below)

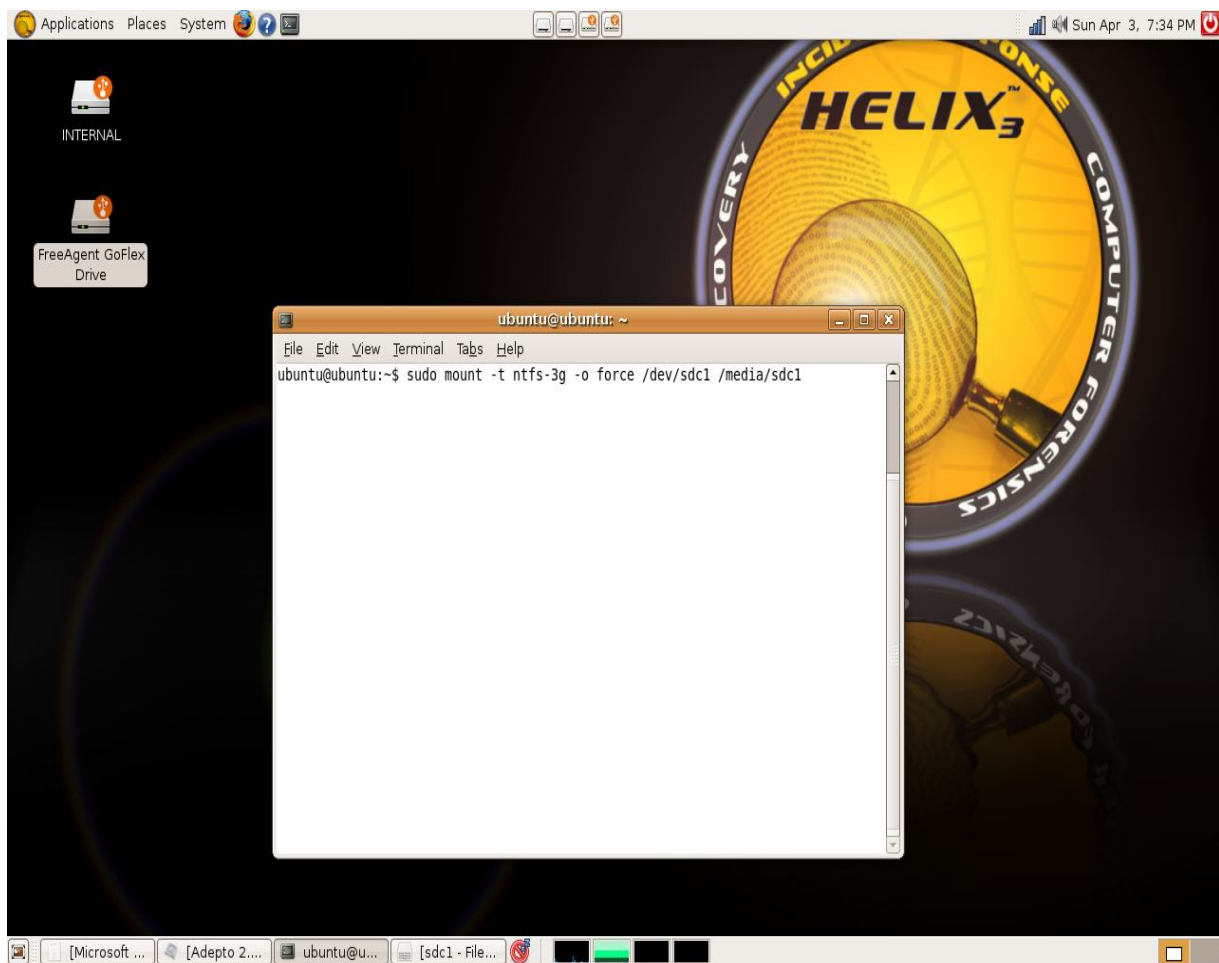


Figure 6 - mounting the device

The Adepto is a Graphical User Interface (GUI) front end to dd commands and was designed to simplify the creation of forensic bit images, and automatically create a chain of custody. The Adepto has several features and abilities, they include the following:

- Auto detection of IDE and SCSI drives, CD-ROM, and tape drives
- Choice of using either dd, dcfldd, or dd command line
- Image verification between source and destination that is the MD5 or SHA1



- Wiping or Zeroing drives or partitions
- Splitting images into multiple segments
- Detailed logging with date time and complete command line used

## 6.9 The Adepto Forensics tool

When Adepto is started, it will prompt you for a username and a case number. This is a perfect way for keeping track of multiple cases, as well as maintaining a chain of custody. The case number is based on the current date but can be modified to fit the format of any case numbering system. When those two pieces of information is entered then click on “GO”, the program allows access to another window with tabs like Device info, Acquire, Restore/Clone, Log, and chain of custody. This window is where all the other information is entered before acquisition can begin. (See screen dump below)

(Screenshot of the windows of Helix 3 used for imaging TomTom one)

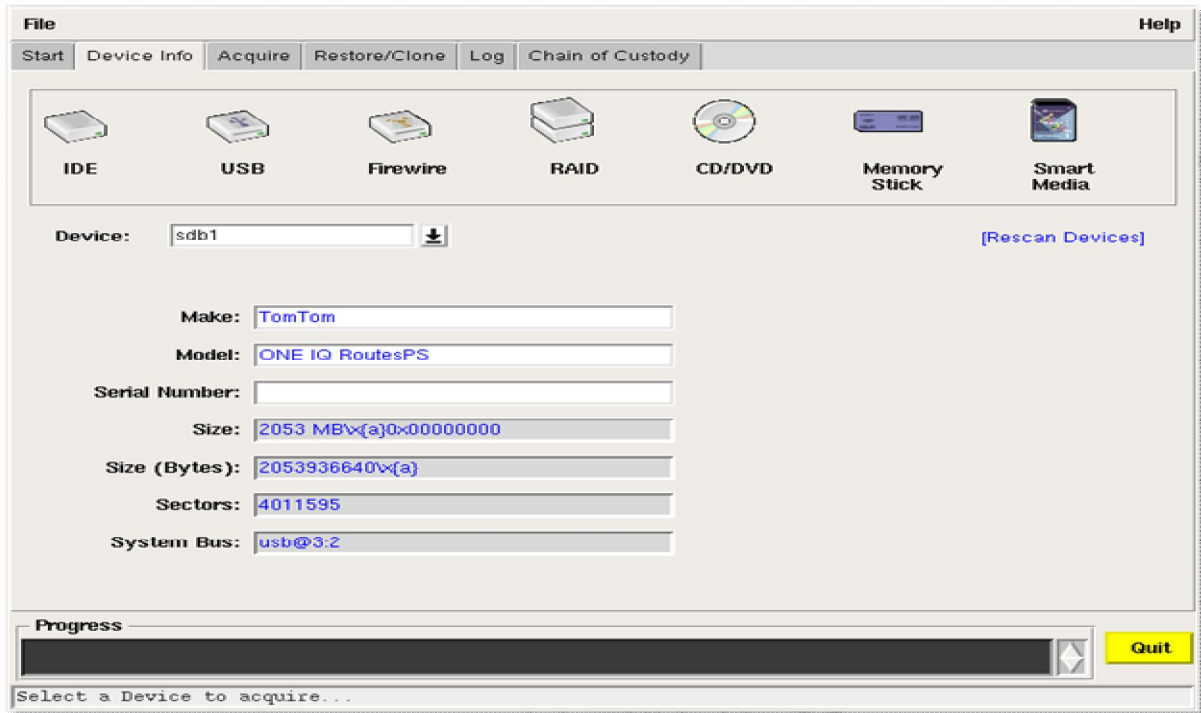


Figure 7 – Device Info

Device Info: The device info tab is used to display information about the various devices that have been mounted on the system. The name of the device that we want is selected from a pull down window. In this case the drive known as “sdc” was selected and it is our source drive which is the TomTom one to be imaged. Immediately the drive was selected, the information about it will be seen, such as the size, model and the name of the drive. If should in case the drive does not appear, the “Rescan Devices” button should be used. (See screen dump below)

The Log Tab: The log tab will display the log of all the action that has been used in order to image the drive. And it is here that the hash value (MD5) will be seen, which is of course to prove the integrity of the drive been copied. Forensically it is proven that every thing is done as it should be, if the Message digest 5 (MD5) of

the original drive is equal to that of the copied image. (See screen dump below)

(Screenshot of the window where information about the drive to be imaged is entered)

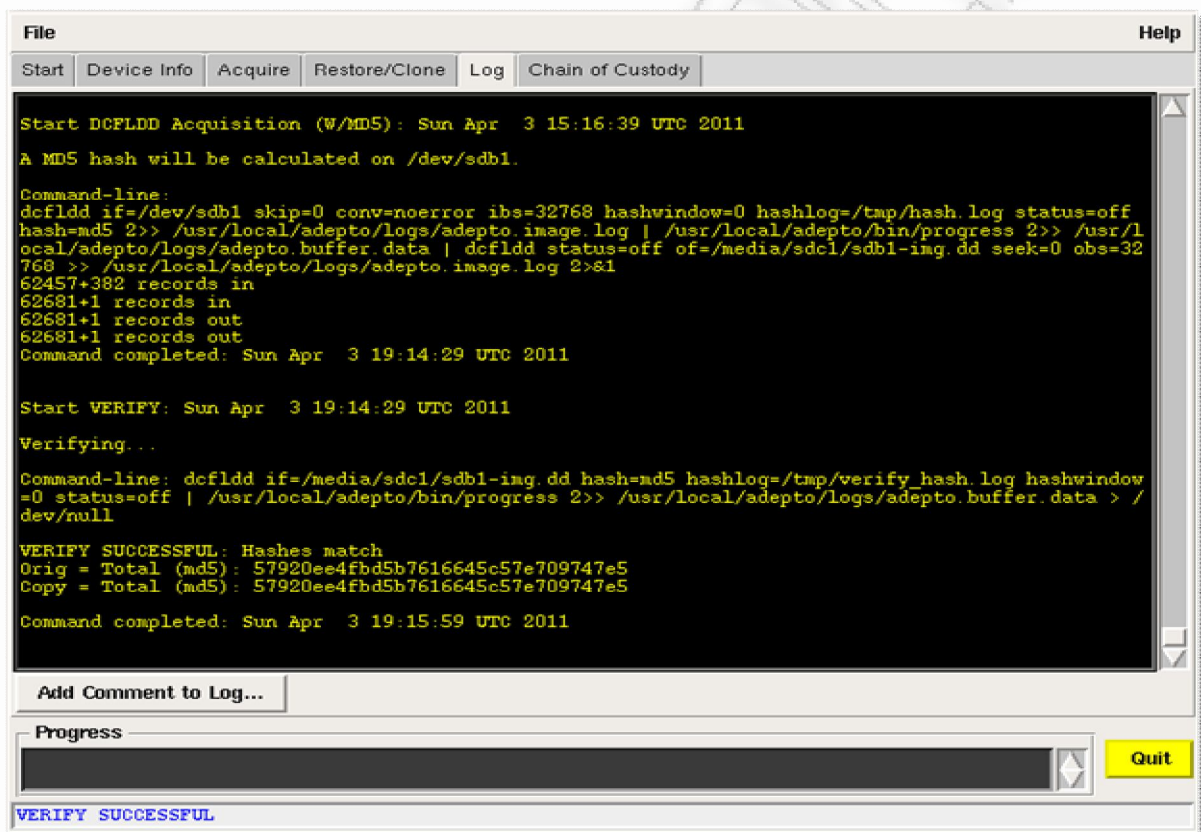


Figure 8 - Logging

The Acquire Tab: Once a device has been selected, the Acquire tab will become available, it is here that the destination drive was been entered or selected. In this case the destination drive was “sdb1”. This is where our bit stream image will be

place after the imaging process is completed. When the destination drive has been entered in the mount point, then the bit stream image process is about to begin. This process should not be disturbed until the whole imaging process is completed. (See screen dump below)

The chain of custody: The chain of custody was created automatically based on the device that was imaged. In forensic investigation the chain of custody is also very vital because it tells the examiner all what he has been doing in the past. And during the imaging of the TomTom one drive the Adepto program created a chain of custody base on the information entered, such as the username and the case number. The Chain of custody must remain unbroken to prevent evidence from being disqualified. In legal proceedings, a common method of disqualifying evidence is to argue that the custodian has failed the chain of custody requirements. A related acquisition is that evidence has been tampered with, which is often a plausible argument unless it can be proven that mishandling never occurred. (See screen dump below)

(Screenshot of the chain of custody of an imaged TomTom one device)

**File** **Help**

Start | Device Info | Acquire | Restore/Clone | Log | Chain of Custody

**Chain of Custody Items**

**EVIDENCE CHAIN OF CUSTODY FORM - FOR FORENSIC IMAGES**

**Case Number: 20119301** **Page: of:**

**HARD DRIVE/COMPUTER DETAILS**

Item #:	Description:		
Manufacturer: <b>TomTom</b>	Model: <b>ONE IQ RoutesPS</b>	Serial:	

**IMAGE DETAILS**

Date/Time: <b>04/03/11</b>	Created By: <b>xenovass</b>	Method: <b>dcfldd</b>	Image: <b>sdb1-img.dd</b>
Storage Drive:	Hash: <b>Total (md5): 57920ee4fbd5b7616645c57e709747e5</b>	Segments: <b>1</b>	

**Progress**

These items will be printed on the Custody Form

Figure 9 – The Chain of Custody

The imaging process of TomTom one was completed and the hash value was also generated which is a proof that the integrity of the bit stream image of a GPS device is guaranteed. The next step of the process will be the analysis of the imaged TomTom One device.

## 6.10 The Tom-Tom evidence analysis

There are a number of tools in market doing the data analysis of the evidence being

acquired. Such tools are TomTology, FTK AccessData Imager and lots of others. TomTology will automatically decode all of the information found on the device and will give detailed information about the following

- Home location
- Favourites
- Recent Destinations
- List of addresses that have been entered manually
- The last journey
- The location of the device (if it has last fix )

There is much information that is useful inside tom-tom that can easily be decoded for use in forensics analysis

## 6.11 Deleted Spaces on Device

A lot of useful information can be found in the deleted space on a TomTom.

Unfortunately, if the user has reset their device then no live information will be available. If not, in the deleted space, records of previous journeys plotted as well as potentially the actual GPS position of the device when the journey was plotted and it's last GPS fix for that journey can be extracted. When a journey is plotted using a TomTom device, it takes the current GPS position of the device as the start point of the journey. Until the destination is reached the TomTom stores both the Origin and the Destination. If a wrong turn is taken in the journey the TomTom will initially attempt to make the user turn around or will try to steer the user back on the route. If this fails then the TomTom will be forced to re plan the journey. In case

of this type of situation, the TomTom will again take the current GPS position as the origin, leaving the destination the same. When examined, the last journey origin will definitely be a place where the TomTom has been but it may not be the place the entire journey started from. The TomTom always records where it is when it has a GPS fix, this is the last GPS Fix. It may be in mid journey if the TomTom was turned off mid journey or it may be a place where the TomTom has been turned on since. Like the last journey origin, this is a place where the TomTom has been.

(ANDY, S. 2008)

## 6.12 Files of Forensics interest

Files of forensic examination interest are files that contain information about the movement of the suspect and places where the GPS devices have been. Such files are:

- Live CFG file data
- Live phone numbers( if the TomTom has been paired with a phone)
- Device information
- All deleted CFG files
- All locations found that are no longer in a CFG files(orphaned locations)
- All recovered phone numbers

In any location been discovered, can actually be viewed in a Google maps if there is an internet connection.

## 6.13 The CFG Data Files

The CFG files contain all the location that has been entered in the device even the ones found in unallocated cluster which has been deleted or overwritten. It means that in an investigation of TomTom devices, the CFG files are one of our main priorities. In this case study, the TomTom One bit stream image has about nine hundred and forty six entries in the CFG files. Clicking on the arrows or by typing the number directly into the box and pressing enter, we will be presented with the address that has been entering into the device. It is also possible to see the previous journey and previous GPS positions of the TomTom In this first entry, we will see the addresses entered into the device including the postcode, house number (if entered) and the latitude and Longitude.

## 6.14 The Orphan Locations

The Orphaned locations are locations stored on the TomTom that were originally in a CFG file but due to the constant writing to storage, they are no longer found in a CFG file. These have been termed “Orphan Locations.” According to Andy Sayers, these address may be those that the header of the CFG file that were originally residing within has been overwritten and so they would not be present in the “Found CFGs section. These Orphan locations can also be of potential evidentiary value and can be viewed by clicking on the Orphans tab. Functionality has been provided to view each location once if it is identical to another found location. This is enabled by default but can be disabled by clicking on the “Show Unique Hits Only” tick as seen on the screen dump below. It is also possible to show only



organs of a certain type e.g. Home or GPS Pos this can be implemented by using the filter drop down menu. These Orphans location will gives us the addresses, the users has entered which can not be found in the CFG files.

(ANDY, S. 2008)

### 6.15 Data analysis with FTK AccessData imager

FTK imager is a tool like TomTology which is gathering information and make it accessible from the examiner when he acquires computer evidence, so he can use FTK Imager to create an image of the source drives or files. He can also create a hash of the original image that he can later use as a benchmark to prove the validity of your case evidence. FTK Imager verifies that the image hash and the drive hash match when the image is created. After you create the image and hash the data, you can then use FTK to perform a complete and thorough computer forensic examination and create a report of his findings. In the figure below we will see how the image is mounted into the forensics tool for analyzing data.

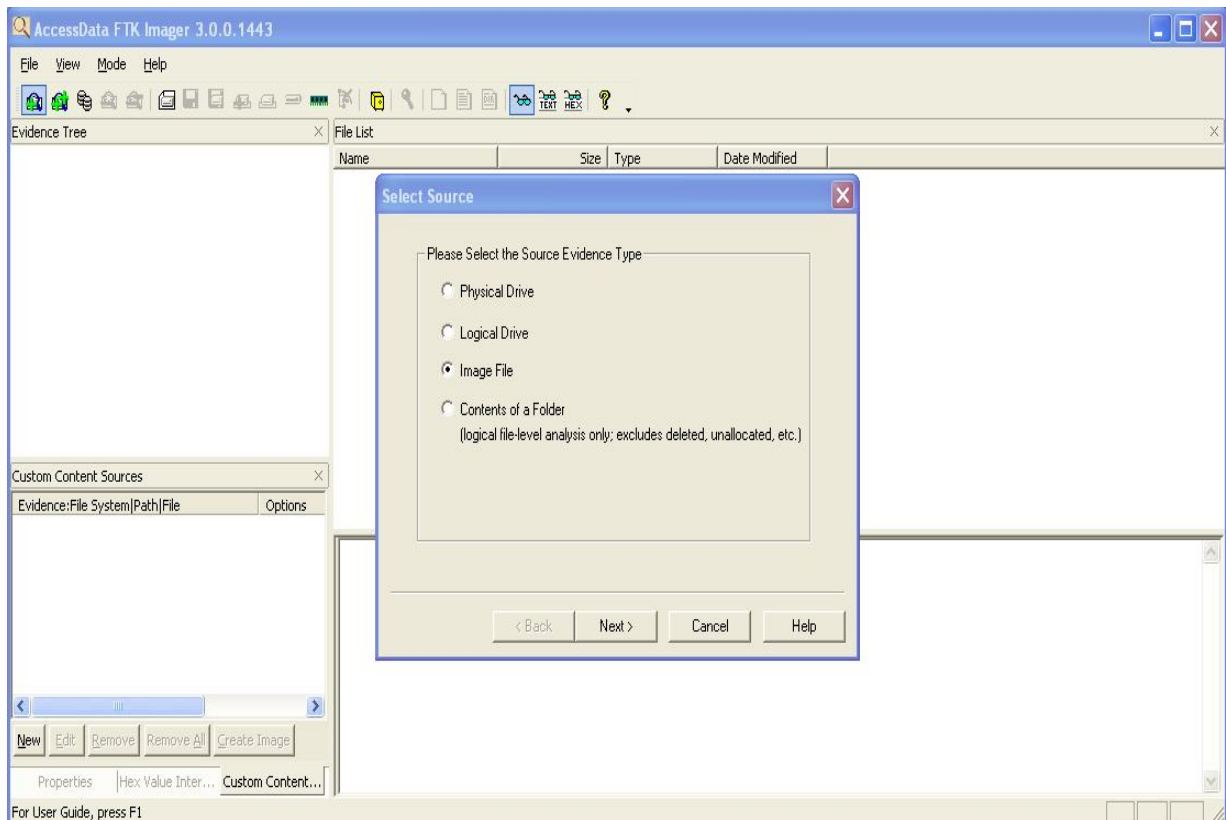
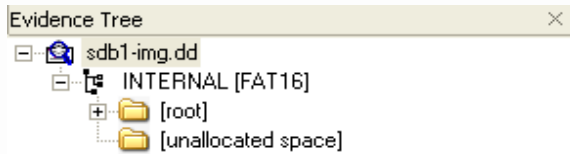


Figure 10- Image as Source Evidence

After the image is mounted in the tool we will have the tree internal file system ready to be analyzed , the internal FAT32 file system will be divided on two different tree catalogues , the root catalogue where the whole system is saved and the unallocated space where an examiner can search for slack evidences.



As you can see in the image below there is a specific place in memory where an examiner can find evidence. There is a different representation where at the left side we can see data to be represented as where they located in memory in hexadecimal format and at the right side we can see data to be represented in clear plain text. At the picture below we can see some coordinates that we found using the tool .there is a specific reason of the different representations .There are non-resident data and resident data or the actual data that are important to examiners.

00	2D 0D 0A 30 2E 30 30 30-30 30 0D 0A 35 30 2E 34	--0.00000--50.4
10	36 36 36 37 0D 0A 36 2E-38 36 36 36 37 0D 0A 34	6667--6.86667--4
20	35 2E 31 36 36 36 37 0D-0A 31 30 30 30 0D 0A 35	5.16667--1000--5
30	30 30 30 0D 0A 31 36 34-38 0D 0A 31 32 37 32 0D	000--1648--1272-
40	0A	.

As we can see below we have an image captured that shows the whole picture of FTK imager forensics tool

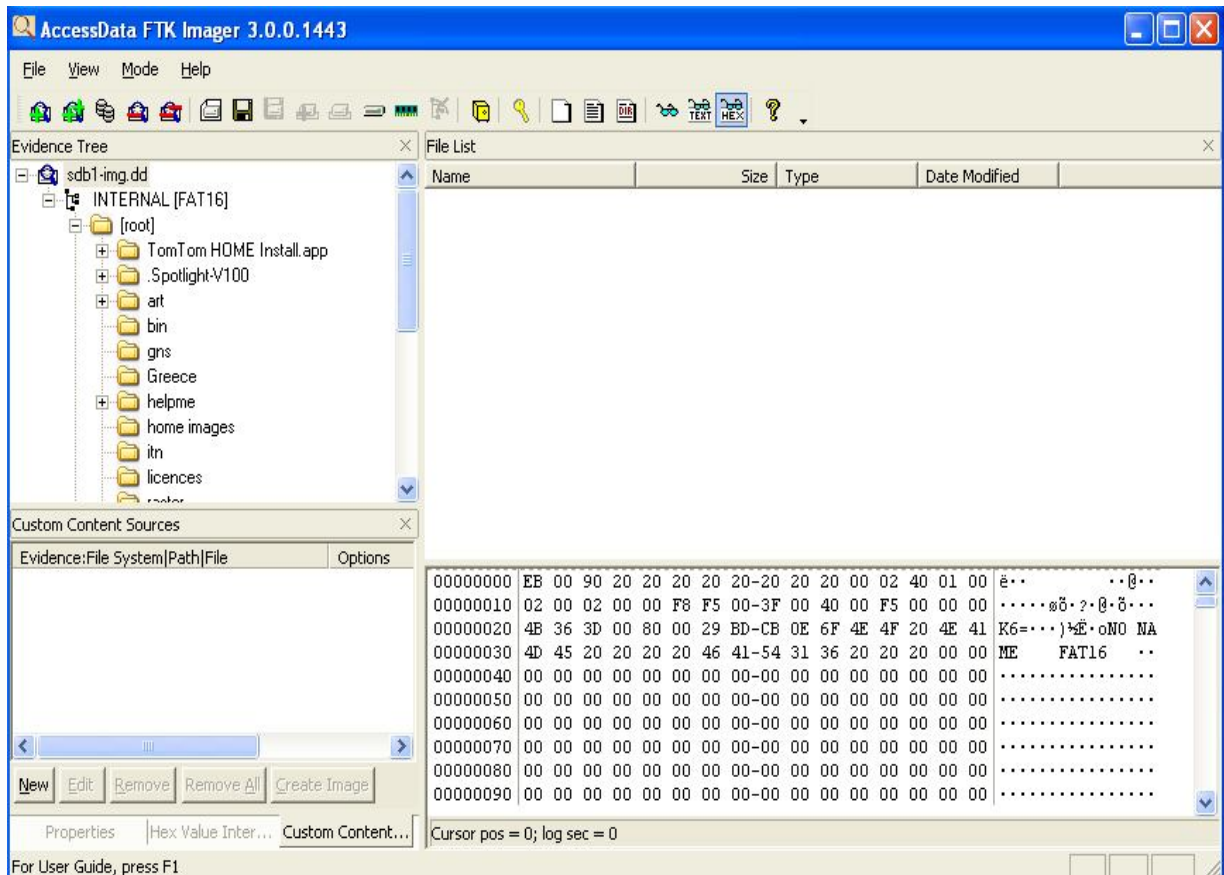


Figure 11 – AccessData tool

As you can see in the above image we have mounted the TomTom OS image taken with the adepto tool which we saw at a previous chapter. The AccessData FTK Imager screen is divided in several windows and inside of them we can have a lot of useful information.

## 6.16. Data representation

After finding the data inside the file system and after exhausting search we can now represent the data at the map using poi Edit, attaching latitude north and east coordinates to represent the location

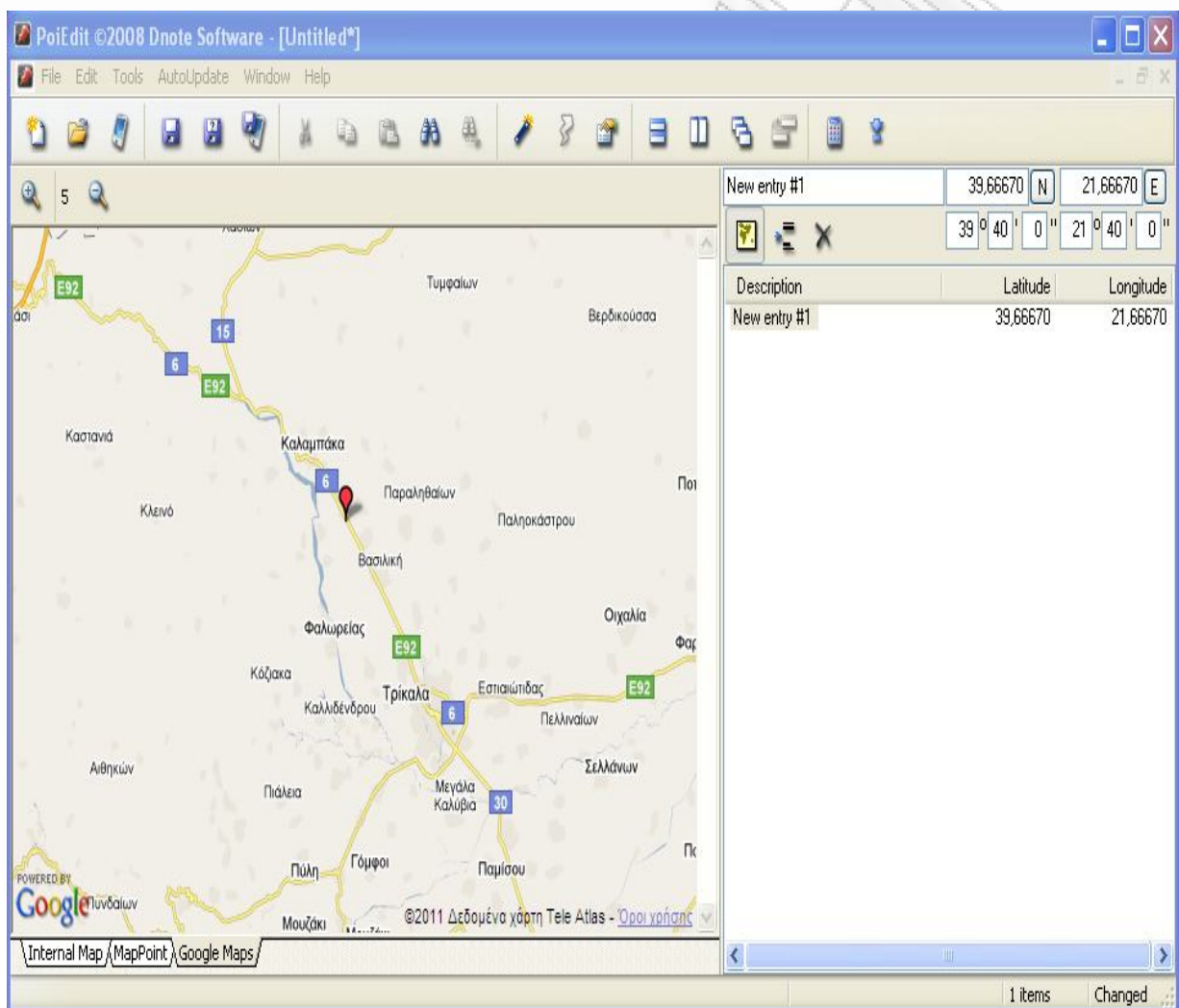


Figure 12 - POI edit showing position

So at this chapter we saw how the investigating process talking place using tools

and methodologies for catching searching and representing data on the map showing useful information about the location of the person that is being accused. The question here is “can we implement the PKI methodology for achieving authorization and be authenticated before we start processing and analysing data? and the answer is “yes” , so the importance of being authorized and be identifiable has its own value and must be implemented.

## 7. The Systemic approach of the encrypted coordinates

As we saw at some chapters previously, there was being implemented a standard methodology for the acquisition of the forensics evidence. In this chapter we will see how we can move further a step and to build a system inside the embedded device to automatically encrypt the GPS coordinates for confidentiality and removing the vulnerability of plain texts and public expose of the evidences. Encrypted evidence can only be acquired from authorized persons such as investigators providing their secret key for authorization, sign them for verification and implement hash values for integrity. It is generally accepted that the digital evidence should be hashed before and after the acquisition for the importance of the evidence integrity, as the investigators need to show the correct evidence to court. The integrity with the accompany of encryption make things more secure end at least more confidential preventing flaws and possible threats altering the data before they will be acquired. There are many things to be considered in this research as it has many problems to be solved, and for that we will discuss it later in this assignment.

## 7.1 Problems to be solved by implementing the systemic methodology for evidence acquisition

There is a consideration generally in the forensics community about and how digital investigators can be absolutely certain for the realness of the collected evidence. In every day life there have been many cases that have found a haven of terrorists with electronic devices that hide important information that should be investigated. There is a time frame between the crime incident and the authority response which can give the opportunity to the criminal to take serious actions for altering the data or wiping out any electronic information. That information can be found from the authorities and finally lead them to sufficient conclusions for the crime scene and also show them the way to the criminals. This time frame should be narrowed and if it is possible it should be eliminated. The information must be located inside the electronic devices in a secure manner to make criminals life difficult and to prevent them from reading the information trying to learn about the places that the original holder of the device was visited. In such cases this assignment gives suggestions about how to secure the digital information. The systemic approach shows that there is a way of securing the data. Specifically the GPS receivers provide valuable information and thus it's forensically accepted that the investigation can make huge steps and find the leads easily if such a device exists at the crime scene. The public key cryptography can give authorization to investigators and also can provide encryption to those valuable data such as GPS coordinates. Information security gives the fundamental implementation of public key cryptography and its benefits.

Like I said before digital evidence provide lots of information especially if it comes from GPS devices. Most of those devices are holding evidence for a sort period of time until the GPS receiver start function again and begin collecting new

coordinates from a new location. In fact this situation can show to us that there is not an actual reason to encrypt GPS coordinates that holding the current location. The main reason for implementing this methodology is to keep historical GPS coords and other files contain valuable data with forensics interest in a secure manner in some hidden place in memory. Of course there is a way of holding current location GPS coordinates secure inside the memory, but in some other place less suspicious and more secure inside the file system, something like a back up file which will be overwritten in a specific timeframe after it receives the new data. The diagram below shows how that should be implemented

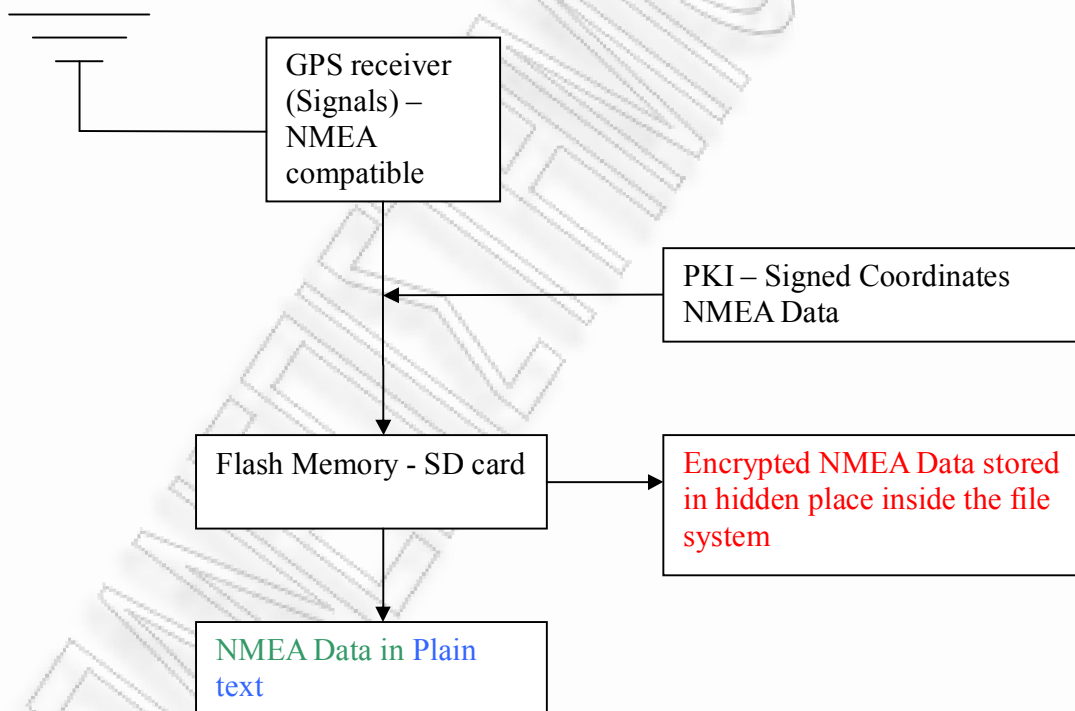


Figure 13 – Diagram showing the encryption store procedure

The above diagram shows that there is a need of two files to be saved, one file in an



encrypted format and another file in plain format for the reason explained before. The timeframe which will overwrite the coordinates would be calculated and after some minutes the other file which holds the encrypted coordinates will get overwritten with the new encrypted coordinates. This technique will prevent from losing current data.

## 7.2 The encrypted coordinates and the interactions with installed Applications

Generally most devices these days are “smart “ Devices implying that many applications are installed performing different actions and tasks from holding files saved , capturing videos , even watching movies and hear music. The most of those smart devices have preinstalled the GPS receiver which gives the significant meaning that GPS is a really valuable tool that every person needs these days. But also other applications need GPS receiver’s coordinates, such as applications which store photos in an organized manner performing tasks like GEO-tagging pointing the spot that the specific photo was captured. So it is very common truth that GPS receivers enable other functionalities inside the device and so they have to implement a function to achieve those coordinates. In our case GPS coordinates are encrypted with a private key awaiting the public key to decrypt them. So applications must obtain the public key from the file system and use it for decryption and to be authenticated. My proposition to this is that it has to implement an interface between the main functionality of the app and the input reception of the coordinates just to decrypt and receive the coordinates in a readable format such as NMEA format and that has to be applied in every application which deals with the GPS coordinates.



Figure 14 –Smart Phone Applications

So as you can see above there are hundreds or thousands applications that are available to be installed to our smart phone or even other devices. The diagram below shows the thinking of the implementation of the API.

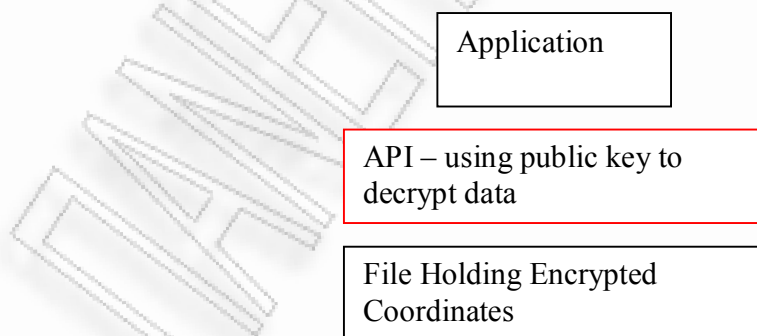


Figure 14 – Application Verification and decryption Layer

### 7.3 System deployment and implementation

In this research the main consideration for deploying the system is to make the evidence acquisition happen straight from the GPS receiver to encrypt the data and finally store them to the SD card. The importance of the system to entrance between the GPS receiver and the RAM is crucial because as we know from the familiar problem of file slack, drive and memory slack , the evidence will spread into the file system , for example without being wiped out after deletion. Below figure 5 shows the implementation diagram.

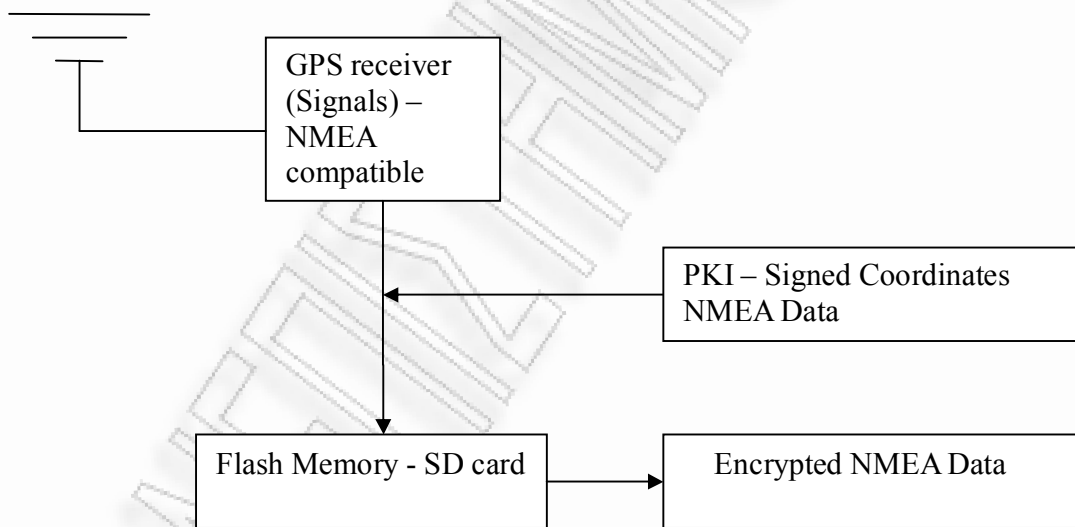


Figure 15 – implementation diagram

As we can see from the diagram our system is a PKI based with a man-in-the-middle approach between the receiver and the SD card with means of implementing digital signatures and public key cryptography. We will discuss later

on about how this PKI system will finally be implemented and also how the keys will be generated and stored inside the file system. The reason that we use the Flash memory in our diagram is because of the use of the TomTom GO 500 device which is based on SD cards.

#### 7.4 Inside the GPS system – Applying the technology

As we mentioned before the systemic approach of encrypting and signing the evidence within the GPS device, in my opinion is a very important step because it releases the investigator from the feeling that the evidence have been compromised and altered in some way before the acquisition is made. As we agree with this I will explain how this system will function and how evidence will be kept securely.

First of all the main job is to provide an accurate acquisition on the evidence capturing them from the receiver as we said in a previous paragraph. This will happen with some low level programming techniques that will help us making the right actions on the chipset that communicates with the device driver at a specific port. Specifically there is a need to provide force connectivity to the pins that control the I/O functionality. As I have studied the ARM9T microcontroller I found specifications and libraries that helped me to understand the PI of the hardware. Finally the conclusion comes from the use of GPIO chipset functionality that is connected to the GPS receiver through 16 or 32 pins. As in the case i have the control of GPIO there is a need to synchronize the bit rate with baud rate configured at 11200 bits/sec clock through the chipset UART that is being responsible of transferring the data streaming from the hardware device GPS receiver to the application through specific kernel system calls. The GPS device is NMEA compatible and the data will be shown in NMEA format on the screen.

After the data will be acquired the UART will transmit them in a sequential fashion and the GPS coordinates will be shown on the screen or will be saved into a .cfg file. Ideally the main purpose of capturing the data has been reached. The GPIO driver source can be found on /drivers/Barcelona/GPS/. The program is been written in C++ and is been mounted at the APPENDIX of this assignment. The next step of course is to analyse the programming functionality as through the PKI model after the coordinates has been reached. The GPS device is attached to the second UART of the S3C2410 .There is a header file defined on lib Barc\_gps.h that uses GPIO registers and configures them for specific memory locations. In order for the TomTom GPS device to function there have to be some modifications of the registers such as shifting left or right some bits for example as we can see from the class reference above SET\_GPS\_GPH has to be shifted like  $3 \ll 20$  or  $3 \ll 18$  depending on the GPS model (TomTom GO 500,700 ...).those modifications will function to the Barc\_gps.h lib. After build from source we need to compile and make the new S3C2410.o.

```
24  #define SET_GPS_OFF      (~ (0x0400))
25  #define SET_GPS_ON      (0x0400)
26  #define SET_GPS_SET     (0x0200)
27  #define SET_GPS_RESET   ~ (0x0200)
28  #define SET_GPS_UPDATE_ON  (0x0002)
29  #define SET_GPS_UPDATE_OFF (~ (0x0002))
30  //#define SET_GPS      (~ ((0xf<<16) | 0xf))
31  //#define CONFIGURE_GPS  ((5<<16) | 6)
32
```

```

33  /* Configure GPG REPROG for GPS */
34
35  #define SET_GPS_GPG      (~(3 << 2) | (3 << 0))
36  #define CONFIGURE_GPS_GPG ( (1 << 2) | (2 << 0))
37
38  /* Configure GPH RUN/RESET for GPS */
39
40  #define SET_GPS_GPH      (~(3 << 20) | (3 << 18))
41  #define CONFIGURE_GPS_GPH ( (1 << 20) | (1 << 18))
42
43
44  /* delay */
45
46  #define DELAY_SMALL      1
47  #define DELAY_HIGH      2
48
49  LOCAL INT32 gs32GpsMajor = BARCELONA_GPS_MAJOR_NUMBER;
50
51  /* forward declaration */
52
53  LOCAL INT32 gpsOpen (struct inode *, struct file *);
54  LOCAL INT32 gpsIoctl (struct inode *, struct file *, UINT32, ULONG);
55  LOCAL INT32 gpsRelease (struct inode *, struct file *);
56  #endif
57
58  #ifdef __cplusplus
59  }
60  #endif /* __cplusplus */
61  #endif /* __INCGpsh */
62

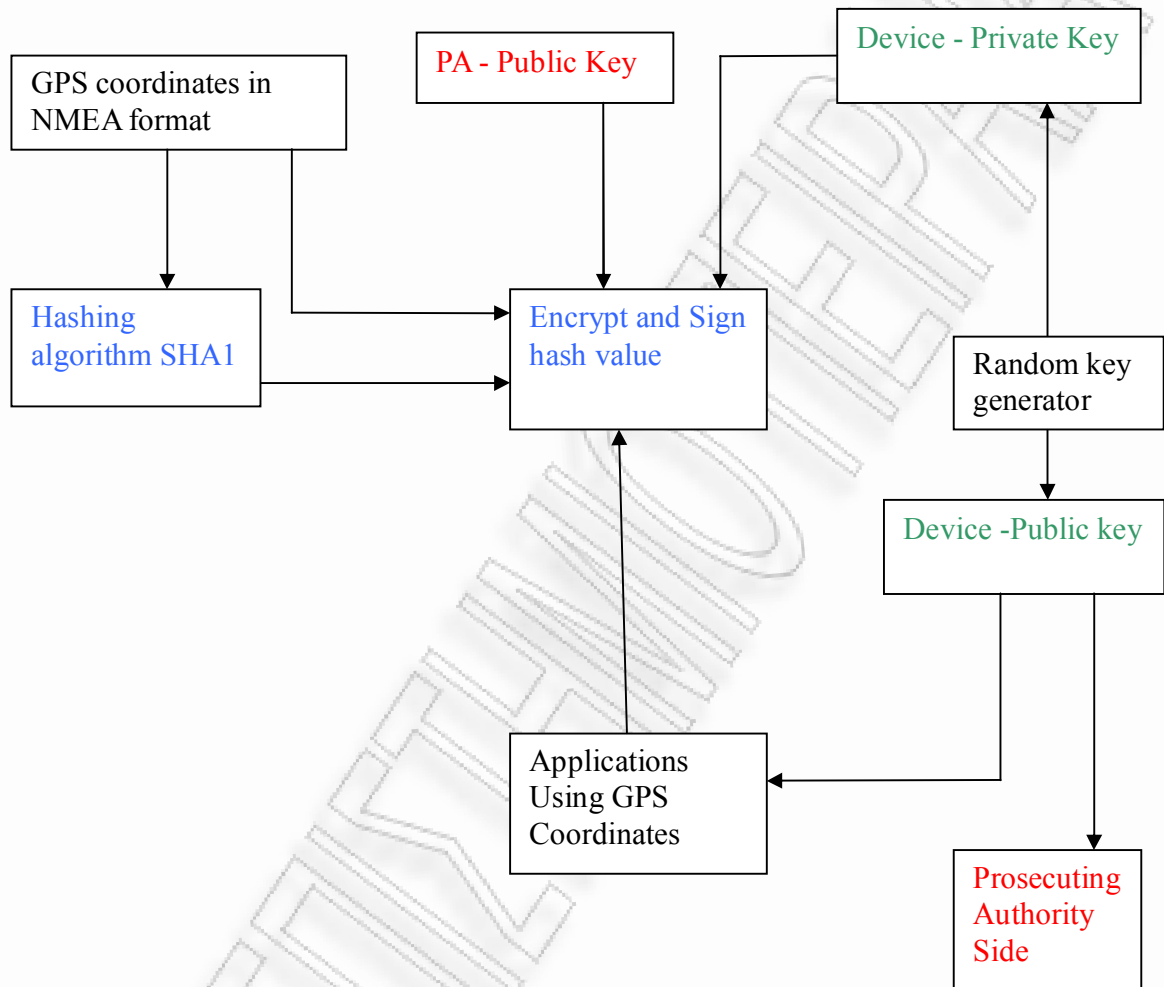
```

As we can see at the source code above this is a part of the TomTom GPS driver that shows that Macros are placed in memory in standard places and also define run reset or reconfigure GPS functionality representing the shifting bits that have to occur for making GPS work. The code above is a part of another code that implies a communication port to GPIO pins. The main activity that has to be done under technological aspects is to find the way to plug into the driver the code that can apply cryptographic methods to encrypt and sign data after they will be received

## 7.5 The embedded PKI system functionality

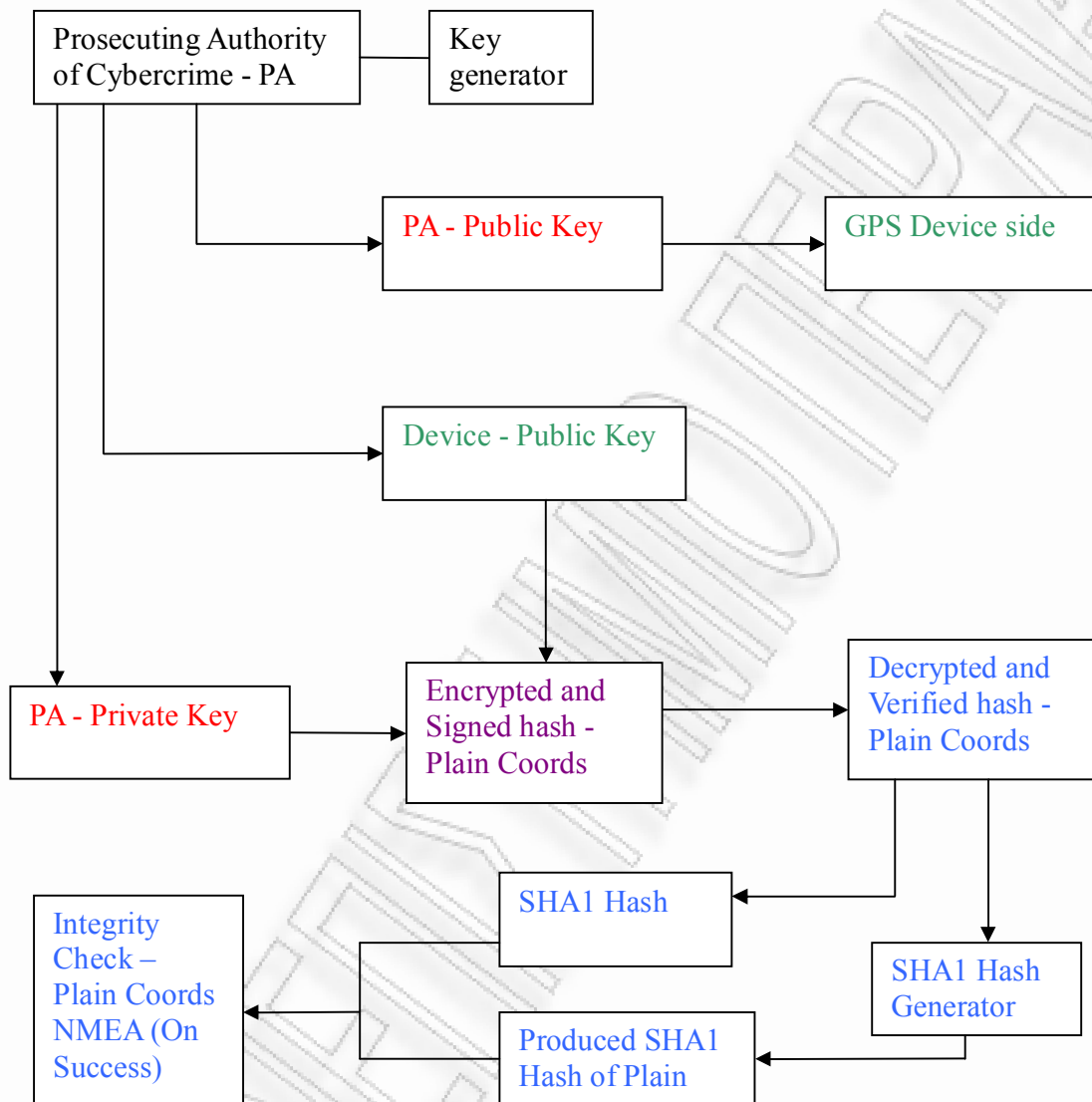
Ensuring of the data has being reached we can now manipulate the coordinates. The use of the first approach which is the private public key generation functionality, and after that the keys will be stored somewhere in file system. Secondly the SHA algorithm version one will be used to make a hash value of the Data. After the hashed value is done, the private key will be used to sign the data in a way ensuring the validity hosted coordinates inside the device .the investigators public key will be used for the encryption of the data ensuring confidentiality of the encrypted data. At this point there's a lot of consideration about the creation of the investigators keys and of course the whole creation of the infrastructure behind this, such as how it suppose to be implemented, the general acceptance of this infrastructure and finally the cost of implementation. Afterwards of the systemic procedure the encrypted file with the extend .cfg that holds the GPS coordinates will be kept inside the SD card of the GPS receiver holding the coordinates in a secure manner. As we can understand from this system, it's all about the interaction that is provided between the public keys from either sides, the investigators side and the device's side, performing a mutual authentication between them. At Figure-6 below we can see the diagram that shows the methodology of public key encryption and verification accordingly to each side.

From the side of the GPS Device





From the side of the investigators Authority



At the above example there is a fact that we have to consider. The key production is becoming very important because we need a trusted Certificate authority to take advantage and implement the mechanism that produces the private and public keys

that endlessly will be used for authentication and authorization of the investigator. In this assignment I recommend that the CA has to be the Prosecuting Authority for Digital crimes. Specifically for the GPS devices its common truth that today more and more people use the devices location to move to different geographical places. Most cars today have in the stationary location devices as a standard equipment witch shows that the comfort of having a GPS device is becoming more and more popular these days. In this study it is important to say that the processing time for computation of the signature, encryption and verification of the Data it is not such a costly process from a time perspective, because the investigation itself is a slow and time consuming process that takes day's even weeks and months to be completed.

## 7.6 The Certificate Authority

As I mentioned before there has to be a Certificate authority for managing the key generation and distribution to the devices across the country or even a continent. Also there is a need for creation of the digital investigators team that should be evaluated to be authorized to conduct digital investigations in such devices like GPS receivers. There also has to be a built in policy for the creation and evaluation of rules that will perform a full set of principles to be followed from the investigators to finally do their job. All the GPS devices must be loaded instantly with the cryptographic keys before they go out to market. The process is likened to the introduction of a new drug to market by a company which must first pass an inspection by the national drug agency to evaluate and standardized for the sake of public health. Of course the keys must be stored inside the devices in a digital envelope named with an encoded format without prompts for suspicious behavior.

Generally in the situation of the GPS receivers we need to accept that , those devices can be found inside to almost every PDA device that is about to be produced today in the markets.

### 7.7 Case study: Applying the authentication Mechanism

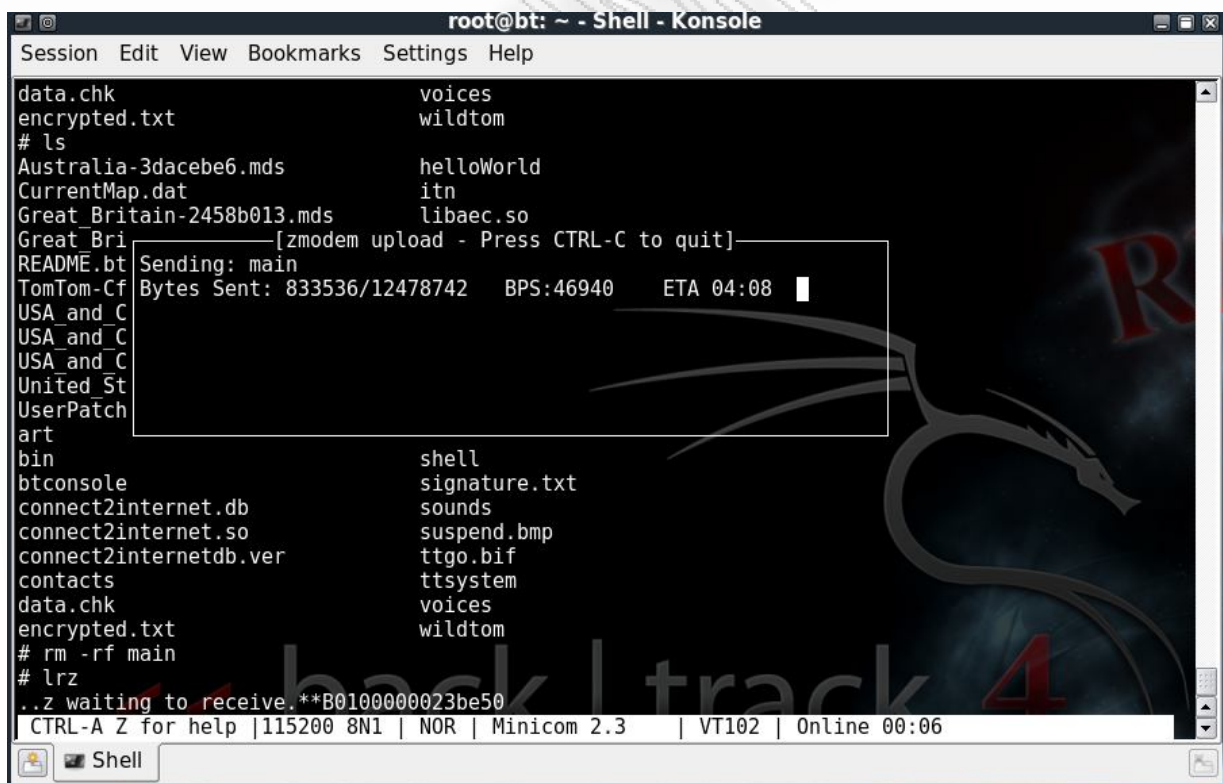
At this point of this assignment I will show and explain the steps that needed for implementation and deployment of the systemic approach of the public key encryption methodology for providing authentication trust and integrity of the valuable data inside the GPS Device. As I mentioned before the system's intention is to get into the middle of the GPS receiver and the system memory to achieve the coordinates to encrypt them using RSA encryption algorithm and finally to save the file. So I have build and compiled encryptData.cpp for encryption and signing with following signature procedures using the private key and verifyData.cpp which is making the verification of the signature and decryption of data. Also there is another in C++ that is using libcryptopp.cpp and libcryptopp.h. The first program activates the GPS receiver and the second gets the output from the first program creating the private and public key and the file containing the signed GPS coordinates. The two programs are installed into the GPS device as well as statically linked with the appropriate libraries as libcryptopp++.a witch implements some of the functions used for the RSA encryption. The encryptData.cpp program also uses the investigators public key to encrypt the coordinates. This chapter will show these deployment steps of those programs and how technologically can do our work. At this point I want to mention that this implementation is just a demonstration of what the thoughts are and what the special meaning for this effort is.

### 7.7.1 The communication port with the TomTom and the problems being faced for achieving correct functionality

The programs are being deployed using the Minicom program for establishing a communication port through rfcomm sockets via Bluetooth service connection. The programs have been transferred and loaded through zmodem file transfer protocol and the communications port speed for transfer rates settings adjusted to 115200 bauds. The executables Linked statically through ARM compiler especially for being executed by the arm processor. The GPS device TomTom GO 500 has a limited memory as many embedded system devices so they need some extra space for static memories to swap and use them for programs execution. At this part i have being used a flash memory in about 2 GB for this purpose. In order to avoid having unwanted situations such as being out of memory there is a need to increase memory by stopping the ttn application which is responsible for holding the interface which shows the map, continuously on screen absorbing lots of memory capacity. Under these circumstances it is better to kill the ttn application and after the memory is released, to start the ttn again. So it's something about to sustain the device in function mode without to be reset of the system. This situation releases lots of memory and applications which are large enough can function correctly. In our situation libcytpo++ library is quite big and if this library will be linked statically in the application makes the app quite bigger and needs lots of memory for being executed. The resulting problem in that situation if we don't take measures for memory overloading is that the application cant execute and it causes a freezing screen which don't give us the ability to do anything further just to reset the device and start over again.

## 7.7.2 The deployment process

At this point I will show the process of deploying the executable applications that produce the private and public keys as well as the signed and encrypted files. First of all we need to connect to the device to promote into the device the applications that do our job. The way we achieve this is by grabbing a Bluetooth communication port and using rfcmm to bind a socket to establish a communication port for listening via specific channel with the right bandwidth.



```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
data.chk          voices
encrypted.txt    wildtom
# ls
Australia-3dacebe6.mds  helloWorld
CurrentMap.dat         itn
Great Britain-2458b013.mds  libaec.so
Great_Bri             [zmodem upload - Press CTRL-C to quit]
README.bt             Sending: main
TomTom-Cf             Bytes Sent: 833536/12478742  BPS:46940  ETA 04:08 █
USA_and_C
USA_and_C
USA_and_C
United_St
UserPatch
art
bin                shell
btconsole          signature.txt
connect2internet.db  sounds
connect2internet.so  suspend.bmp
connect2internetdb.ver  ttgo.bif
contacts           ttsystem
data.chk           voices
encrypted.txt      wildtom
# rm -rf main
# lrz
..z waiting to receive.**B0100000023be50
CTRL-A Z for help |115200 8N1 | NOR | Minicom 2.3 | VT102 | Online 00:06
Shell
```

Figure 16 – Minicom on transfer mode via zmodem

Minicom is a text-based modem control and terminal emulation program for Unix-like operating systems, Minicom is a menu-driven communications program. It also has an auto zmodem download. zmodem is the protocol used for transferring files from, to the device. As we can see at the image above the file transfer from Linux pc to tomtom device with zmodem.

```
Welcome to minicom 2.3

OPTIONS: I18n
Compiled on Oct 24 2008, 06:37:44.
Port /dev/rfcomm2

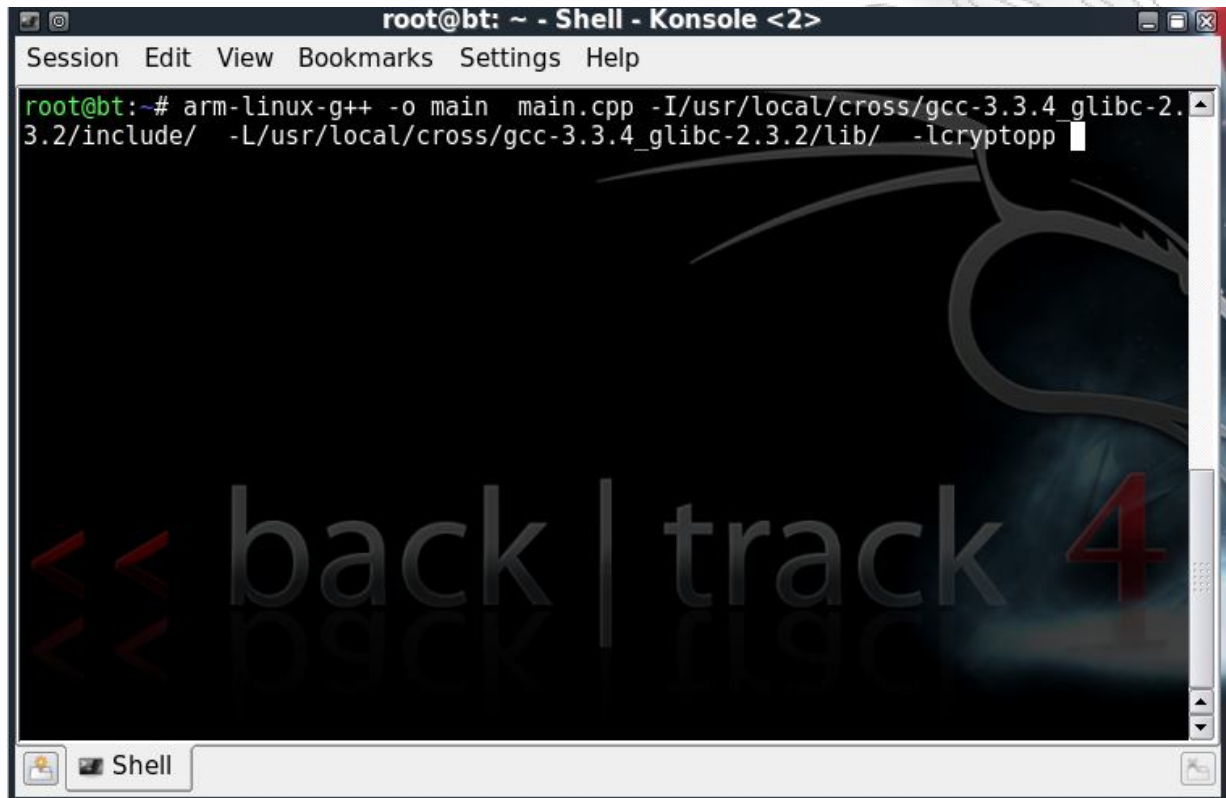
          Press CTRL-A Z for help on special keys

AT S7=45 S0=0 L1 V1 X4 &c1 E1 Q0
BT> CMD
BT> CMD AT S7=45 S0=0 L1 V1 X4 &c1 E1 Q0
/mnt/sdcard/wildtom/btshell: 14: AT: not found
BT> █
```

Figure 17 – Minicom Welcome page

Before transferring the files into the device we have to build and compile the code using specific compiler for running in the device. The compiler is called arm-Linux-g++ and used only for ARM processors just because of the different memory mapping that give different instructions for the binaries to be executed than Intel's processors. Also we need to compile and build from source our crypto library called libcrypto++ which have our needed routines that gives as the solution of RSA cryptography using hash algorithms such as SHA1 for integrity purposes . At

the picture below we will see how we can compile the source file to run under ARM processor



```
root@bt: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help
root@bt:~# arm-linux-g++ -o main main.cpp -I/usr/local/cross/gcc-3.3.4_glibc-2.
3.2/include/ -L/usr/local/cross/gcc-3.3.4_glibc-2.3.2/lib/ -lcryptopp
```

Figure 19 – using the specified compiler

At this point I have to mention that we need to compile the source file to build the binary with the libraries attached in it using static libraries. That is happening because the SD card is NTFS formatted and if we pass into the device the shared libraries we just can't create symbolic links to the library path to use them. It just doesn't work with NTFS or FAT.

There are some problems added to all this such as the familiar problems like stocks of memory. This is a huge problem because libcrypto++ is quite big library

containing many files that are connected to each other. The solution to all this is that we need to free some memory to make the programs run.

```
#!/bin/sh

killall ttn &&
while(true)
do
echo \0 > /dev/watchdog
sleep 10
done
```

As we can see at the code above we just need to kill ttn application because it uses too much space in memory and to try to sustain alive the watchdog daemon. If this will be succeeding then there will be free memory available to run the program. If the above scenario doesn't work there is another scenario being available such as like the code below

```
#!/bin/sh

# Suspend ttn
killall -q -SIGSTOP ttn

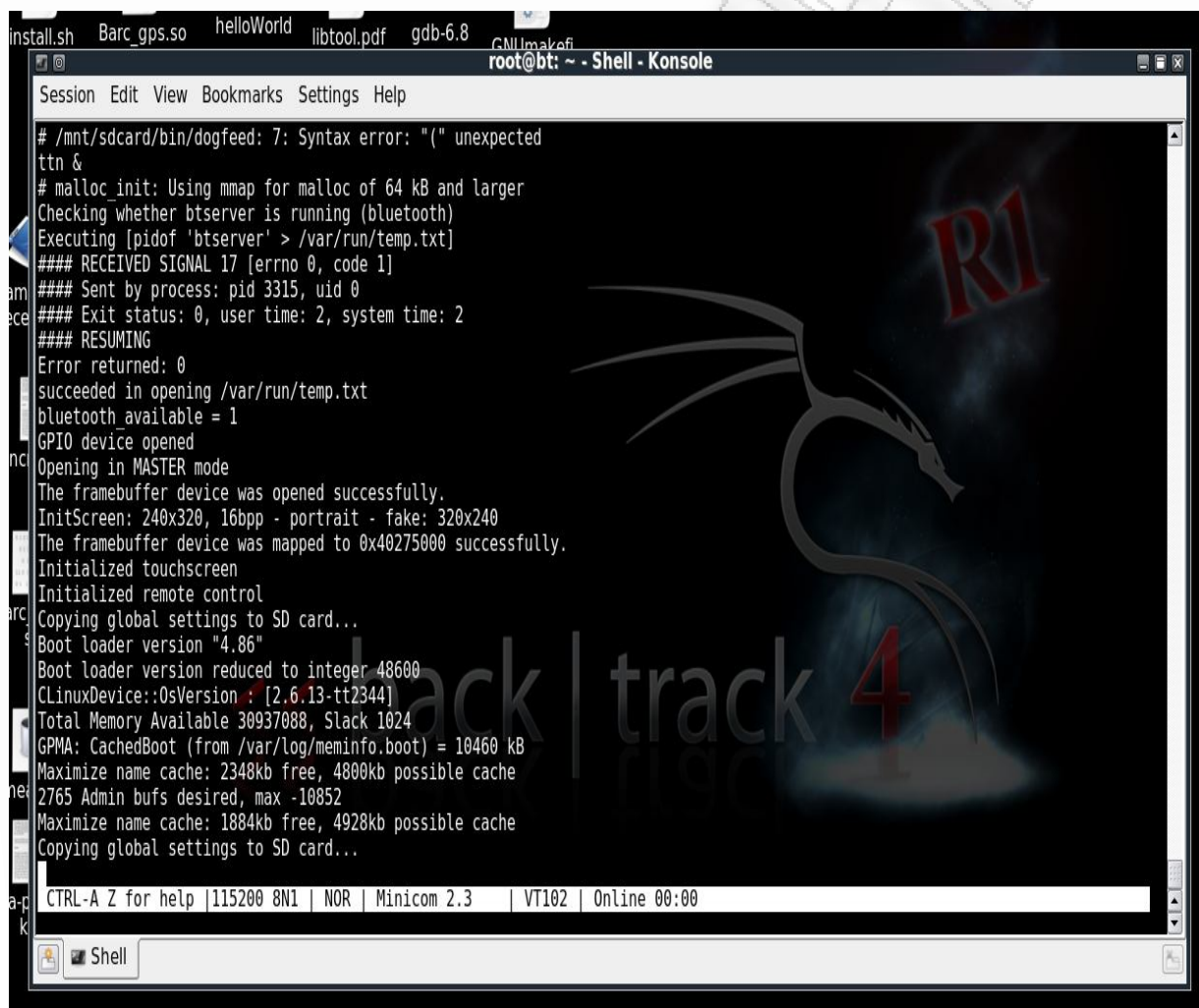
cd /mnt/sdcard/

./encrypt

# We're done, let ttn continue.
killall -q -SIGCONT ttn
```



At this solution we just stop ttn program which is responsible of showing the touch interface with the maps and the available apps offering by tomtom ,and we run our binary .After that situation , we sent a signal to the kernel to continue running the ttn application .



```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
# /mnt/sdcard/bin/dogfeed: 7: Syntax error: "(" unexpected
ttn &
# malloc_init: Using mmap for malloc of 64 kB and larger
Checking whether btserver is running (bluetooth)
Executing [pidof 'btserver' > /var/run/temp.txt]
#### RECEIVED SIGNAL 17 [errno 0, code 1]
#### Sent by process: pid 3315, uid 0
#### Exit status: 0, user time: 2, system time: 2
#### RESUMING
Error returned: 0
succeeded in opening /var/run/temp.txt
bluetooth available = 1
GPIO device opened
Opening in MASTER mode
The framebuffer device was opened successfully.
InitScreen: 240x320, 16bpp - portrait - fake: 320x240
The framebuffer device was mapped to 0x40275000 successfully.
Initialized touchscreen
Initialized remote control
Copying global settings to SD card...
Boot loader version "4.86"
Boot loader version reduced to integer 48600
CLinuxDevice::OsVersion : [2.6.13-tt2344]
Total Memory Available 30937088, Slack 1024
GPMA: CachedBoot (from /var/log/meminfo.boot) = 10460 kB
Maximize name cache: 2348kb free, 4800kb possible cache
2765 Admin bufs desired, max -10852
Maximize name cache: 1884kb free, 4928kb possible cache
Copying global settings to SD card...
CTRL-A Z for help |115200 8N1 | NOR | Minicom 2.3 | VT102 | Online 00:00
```

Figure 20 – memory release

As you can see the picture above showing how much memory is getting free and

that the free cache memory goes up to 2348kb from 4800kb. There is information about how much memory is available it says that 30937868b and RAM slack 1024b. This paragraph indicates that those small devices such as tomtom have a minimum percentage of memory.

Using the program to open GPS receiver and capture Data it's obvious that the GPS Data is under NMEA format as we can see below.

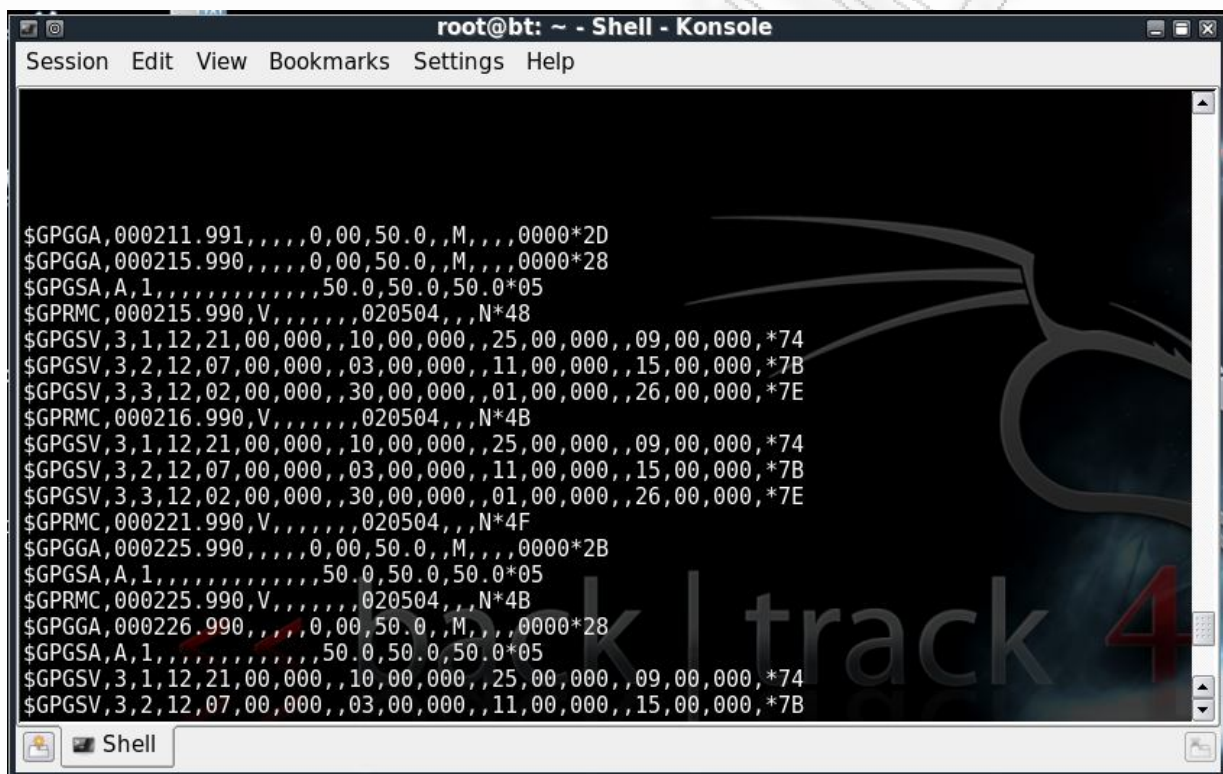
A screenshot of a terminal window titled "root@bt: ~ - Shell - Konsole". The window contains several lines of NMEA data. The data includes sentences like "\$GPGGA,000211.991,,,,,0,00,50.0,,M,,,0000\*2D", "\$GPGSA,A,1,,,,,,50.0,50.0,50.0\*05", "\$GPRMC,000215.990,V,,,,,020504,,N\*48", "\$GPGSV,3,1,12,21,00,000,,10,00,000,,25,00,000,,09,00,000,\*74", "\$GPGSV,3,2,12,07,00,000,,03,00,000,,11,00,000,,15,00,000,\*7B", "\$GPGSV,3,3,12,02,00,000,,30,00,000,,01,00,000,,26,00,000,\*7E", "\$GPRMC,000216.990,V,,,,,020504,,N\*4B", "\$GPGSV,3,1,12,21,00,000,,10,00,000,,25,00,000,,09,00,000,\*74", "\$GPGSV,3,2,12,07,00,000,,03,00,000,,11,00,000,,15,00,000,\*7B", "\$GPGSV,3,3,12,02,00,000,,30,00,000,,01,00,000,,26,00,000,\*7E", "\$GPRMC,000221.990,V,,,,,020504,,N\*4F", "\$GPGGA,000225.990,,,,,0,00,50.0,,M,,,0000\*2B", "\$GPGSA,A,1,,,,,,50.0,50.0,50.0\*05", "\$GPRMC,000225.990,V,,,,,020504,,N\*4B", "\$GPGGA,000226.990,,,,,0,00,50.0,,M,,,0000\*28", "\$GPGSA,A,1,,,,,,50.0,50.0,50.0\*05", "\$GPGSV,3,1,12,21,00,000,,10,00,000,,25,00,000,,09,00,000,\*74", "\$GPGSV,3,2,12,07,00,000,,03,00,000,,11,00,000,,15,00,000,\*7B". The terminal window has a menu bar with "Session", "Edit", "View", "Bookmarks", "Settings", and "Help". The status bar at the bottom shows "Shell".

Figure 21 – GPS coordinates capturing

So we can see how easy using a custom program we can take the coordinates from the receiver. The step now that we have to implement is to encrypt those coordinates and to sign them for authorization and authentication purposes. Before the coordinates finally be saved into the file system. Of course the whole structure

of how the data finally will be read from file system and the ttn application will be changed but however this is something that will be under construction if this system finally adopted from market.

### 7.7.3 The Examiner's Role

The digital forensics Examiner has a special role as a criminal investigator to cover a specific criminal case from the digital perspective of it. Examining Digital Evidence is a unique and difficult situation where the person that is attached to the role has to be checked and sometimes authenticate his/her self to approve that he/she is the one that claims to be. The same thing is happening with the system that keeps secure our information inside the device. The common logic says that only the person that is authorized can have access to this specific information. The scenario is like this. The Digital evidence is kept encrypted in a secure manner inside the devices file system to avoid any suspicious action to happen. Only authorized people can provide legibility to approach the critical information. Using a specific tool which can use the special private key that only the investigator has, provide the ability to decrypt the data. Same thing from the device perspective .So we are talking about mutual authentication. So the Examiner has the highest priority to approach the evidence and his role is commonly the top role as it is unique and he is the only person that can have access.

### 7.8 Privacy

In our case there is a need to provide Privacy restrictions to prevent from revealing sensitive information. It is commonly truth that GPS coordinates are represent

sensitive data that give meaningful information to unauthorized persons who intentionally want to harm the holder of the device keeping the GPS coordinates which in our case represent the sensitive information. In this situation it is obvious that encryption, authentication and authorization provide a good protection against criminal actions such as gathering and reading unauthorized Data which are personal and highly sensitive. So it's totally acceptable that mutual authentication is covering the field of protecting sensitive Data.

## 7.9 Running the code

It is worth to mention at this point that the libcrypto++ library was too big and the result was that the binary built and linked with static library was also too big. The code run successfully into the backtrack Linux without memory problems. Below we can see the public key and the private key that have being generated from the execution giving a random key .

### Public key

```
1 MIIBIDANBgkqhkiG9w0BAQEFAAOCAQOAMIIBCACCAQEAmNELbpjCeKUa9akFXkGI5X2lHjqX
2 O4UBtcOzRhRyW+ostaYLEzbBoUKnHZrPw7+VvGDuLeMxiJB16xq9xoUN/SqstOmVxwaQ7pJQ
3 fDO5vNeNjvoDUyFzPH1VjDyCwLbUg8m7dAJMXiuvpLHHR Ae6xL8U6f50B0c+xxXgjjxO1lHDl
4 3eWM1ghLJ5JiteDXDXQm5AfpDpOph9yQpmowul4bqHUcf26e5FKv+2w1Ymd1p4+P21ae1A/1
5 u005NvrOjsz84m3VDdsBRjtXZ3LvMJ1ceH3eEwsNTqgKd1E+1VO/S+oy6norwYgt6/HLf9QU
6 8K2sdsGqEMh2t4ZstHtfjBGukQIB
```

## Private Key

```
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCbKYwggSiAgEAAoIBAQCYOQtumMJ4pRr1qQVeQYj1
faUeOpc7hQG1w7NGFHJb6iy1pgsTNsGhQqcdms/Dv5W8YO4t4zGIkGXrGr3GhQ39Kqy3SZXH
BpDuk1B8M7m8142O+gNTIXM8fVWMPILAttSDybt0AkxeK6+kscesB7rEvxTp/nQHRz7HNeCP
E6WUcOXd5YzWCEsnkmK14NcNdCbkb+kOnSmH3JCmajC6XhuodRx/bp7kUq/7bDV1z3Wnj4/b
Vp6UD+W47Tk2+vSOzPzibdUN2wFGO1dncu8wnVx4fd4TCw1OqAp2UT6VU79L6jLqeivBiC3r
8ct/1BTwrax2waoQyHa3hmyOe1+MEa6RAgERAOIBADpuC+aFs8S3mV3tzVi+tFe/GXx/OGmU
vOOdpm2eZ/X3p67dmtKj/r2oizD3bY6cE5rZxHrO/Fnc26y3Zq3Jdko19r6NE57r7B77tVYq
XZsHH419tfojYMROCh8IE+BF59gJXkLxOefFaM4HvU1OP+HQ1w4s1caMLpd2e4H/+4uT/KZ3
uJsuiWJcImM/YeHfZKhXiRGXAdTZL1b5ALRjZlud4+OOdqkIwsG4JHtHS81G3t+XbthJwmwb
pqQ9Iu8vAyU4BjYeh2aLRW937eeKkyRpj4vfxBupsIvCOXWY5s03qwGc2GH3HO1ZbigEjTC8
/ZQ8SfOUWWZAubj4c+HZtLsCgYEAu1HbA968hsdIhee13s4cONcDZdu+ZRH3ueIgdku/OCD
113wrfY7DOb3oret+6RoZ74ulN4FTq9u6Rk82IuVpX9CycYUqMNOVx5wzaJIMS37MiC6FJLB
31GecEZhYctEGzHHdJEn07cJxcEPOXkmlJgTLxNUG1hoVRAiMSLygp8CgYEAONiqCJyDSV8P
hDeSoghpmK1Qw79Uee5I+ttqIzELnj1A41gwupZ24MsJH4+wPZuBfsCvrL9dX3iYdOZZSn33
dousNhzi1k+y9Nv4XPTDDW7Azg0lqMumONgXwW7jsUKMAzqDjvFeLQ2qBqpEvG242WUDL4PaN
57YnGoWAnN9b8M8CgYB5NPcgny6xj/5DPHWtT7sdZ9Im6YQK53nMd7KuX1q1Kb6PHqrK6p6t
/tx4WLVfEAdSL8PJvNZB+QuHxQ1A0so96077B7MDycO/5oU5w1vj1jkgb4d2uVBFNM/us6hs
dHdc4/mHqTfjWgJw51U1MEYj6e5LoxhN7ekn+2FrFpZrGwKBgQCHIshf7M1rtfr7MwSG9mJx
2Y6cxxiLlbbAb9tD8o8MCYRORB4u7ZVOBT2TeqCN3HomswGXbTjbcZpwjnGyfp54efmx3G6
EaecDdLNPauVrj9zEwLVpkduQBP/HU2dlqYrWPsBZdKVCK5BMMQgztffa15GRS6k/WSYsLyh
vbP2KwKBgQC1UefTpG4j2ecbNoJzpXhESseXBIuzWLii3SRQXyFRtAZpd+xV5ad4xufn5k6b
nAbZzmFLJyflH8qXu/8U1gepob3ofE3DyV4W6DqJO9R131rdsj2oUb1JXtfAtc7nW6pJfdnz
yELM6/RamyhnEnV8BaQG4g6dR6rmW840ZeNz
```

Encrypted NMEA Data with investigator public key and signed with the device's private key.

```
hTDgXNuIqxKZ7QO7oKhiGXP6HrWC3cmufCcz88czWVhSTDSdJ4oxLCzXB4H1CYvtjeBEqpl0
jJi+1NIeDk5am2UmObzVVxYGQfak3XSAv9JtwsZ422QLW4yRDiaadNMwEwK+cnb1yuDzJyFh
J3qppT/+kpQdFdsC1Ndte1dgVavneVSr3I91yOXE1uaNIpx9Q1BMZwIZvwEP3cXj91WW2CPW
RoQp+v8I7VwGMdHiujdDfjq/uCyhSQOuN6pPFnPsdfWofnaiWmuOqrs+MHTvU4JvShOIz622k
fVkzY4+kA2hE1psTPORBU2yOdS+W500IT2EhrYOmWnp+1L10cZen7SZbhSi9HOB3LziWu2G5
6So3q+93shw2gKXw/oddzpXqTZLQtphUMpSOR9mNpJmu75xap3Rau225VqrORUKpNNnGRPSm
5qmfVM5NaCGfJ8OBF841UP7yfrU1OSg57PrxpB/Z00IwNOBJNq5YaeOH6Q2h1bEUw4dVTUSN
m4VvmO84
```

```
YLSKr1m/4MTW4IaxtLOzRQn5VH9YXxul8IXKUFpWo3DM2YIMsrboxz3cRonruOYPFndh2u4P
8u0aZGc8a+2b3ZUax7LkcB2RkP46cezOcr1Eq/qqJaIRv615zHx++CjzPrsQzVyig11r6/qS
GsL1fc3ADZjwScU3wa8hEW5rC5pu8ViGPvYLnvB1DuLhAORfUy+I96fkuk1+jSWCHhdXN3aV
LourMr4TY14sEIuOfWewdSIJiHRFssXxFzPox5CwGaYi5X/1W+TyWtTPSz+e1PoSCJAgmziw
gF0bxGr4kZvR1hWddwbTGgJTnSrd48M1pDnXFq1351QCz9RDV+37Tw==
```

As you can see above we have the results from running the code. There are two generated files one for the public key and the other for private key in base64 encoding format. Also there is an encrypted file that keeps data in encrypt format and signed with the investigators public key. The result is that the only person who will have access to read the Data is the investigator because he holds the private key that it will verify and authorize him to see the encrypted Coordinates . in this assignment we don't have investigators private and public key so we use one generated pair of public and private keys .

## 8. The legability of Forensics evidence

As we all know is that the evidence has to be legally examined and the examiner carefully has to follow the law and the rules according to specific national laws for evidence acquisition. Evidence is sensitive information with high value because they can prove innocence or guiltiness of a person being accused. There are several principles developed, for giving the specifications of the rules and regulations that being organized under specific laws in different countries depending the national law system.

### 8.1 Considerations of several factors of evidence Admissibility

In general there is no specific test that can be used to determine whether digital

evidence possesses the requisite scientific validity. The court in Daubert suggested several factors to be considered:

- Whether the theories and techniques employed by the scientific expert have been tested
- Whether they have been subjected to peer review and publication.
- Whether the techniques employed by the expert have the error rate
- Whether they are subject to standards governing their application;
- Whether the theories and techniques employed by the expert enjoy widespread acceptance.

The above factors are not exclusive and do not constitute “a definite checklist or test”. So digital forensics evidence proposed for admission in court must satisfy two conditions

1. relevant ,arguably a very weak requirement
2. Must be derived by the scientific method and support by appropriate validation.

The important element of all this is that there is a need to standardize digital forensics and to follow the rules by a relative way of judgments and criteria that offer a trustful process by the courts and to increase admissibility.

## 9. Conclusion

Embedded systems are probably the fastest growing source of forensics digital investigations this is caused partly by technological developments where

everything gets smaller more portable and wisely connected the autonomous way in which embedded systems operate and leave digital traces ,together with limited ways for users to access these traces also contributes to their forensics relevance. GPS devices have no security concerns inside, so there are many possible ways for compromising information, having unauthorized access. The PDAs and smart phones are gadgets that are difficult to avoid having these days. PDAs even GPS devices called smart because they give very nice services to people using them. So the criminal investigation has to focus to that increment of those devices that people using to get help for doing many of their daily tasks. Crimes are more digital these days and of course digital investigators have to prove for their integrity as well as devices have to focus on secure data avoiding sensitive information of being revealed. Also there is a need to ensure privacy especially in GPS devices.

## 10. Future Work

There are many things that have to be done in the future if we want to have a complete work done for GPS security. First of all there the mutual authentication process has to be implemented at lower levels with intervention to the driver and then to pre-compile crypto libraries and the new driver with the kernel from source code. There are other issues such as how memory will be occupied if such a process will run, and how slower that process will be. Before doing all that, a statistical analysis has to be developed to provide the insurance that GPS devices are highly used in Greece or Europe and also to clarify that there are many crimes involving GPS devices and to ensure the fact that investigators have been using those devices as digital evidence to approve criminal actions. To this end, considerable attention should be paid to the considerations regarding the loadable encrypted coordinates



that might be overloaded and maybe after some time to corrupt the system.

---

## APPENDIX A

---

### libcryptopp.cpp

```
2  #include <libcryptopp.h>
3
4  libcryptopp::libcryptopp()
5  {
6  }
7
8  ~libcryptopp::libcryptopp()
9  {
10 }
11
12 public void libcryptopp::storekeys(length,const std::string filename1,
13 const std::string filename2 )
14 {
15     InvertibleRSAFunction params;
16     AutoSeededRandomPool rng;
17     params.GenerateRandomWithKeySize(rng, length);
18     // Create Keys
19     RSA::PrivateKey privateKey(params);
20     RSA::PublicKey publicKey(params);
21     privateKey.Save(StringSink(priv).Ref());
22     privateKey.Save(Base64Encoder(new FileSink(filename1.c_str())).Ref());
23     publicKey.Save(Base64Encoder(new FileSink(filename2.c_str())).Ref());
24 }
25
```

```

27 public string libcryptopp::KeyStored(file)
28 {
29
30     string lines;
31     ifstream myfile (file);
32     if (myfile.is_open())
33     {
34         while ( myfile.good() )
35         {
36             getline (myfile,lines);
37             lines.append(lines + "\n");
38
39         }
40         myfile.close();
41     }
42
43     else cout << "Unable to open file";
44
45     return lines;
46 }
47
48 //this function is used for encryption
49 public void libcryptopp::encryptopp(char const* zInputFile,string file)
50 {
51
52     RSAES_PKCS1v15_Encryptor e(this.KeyStored(file));
53     FileSource( zOutputFile, new StringSink( r ) );
54     FileSource(zInputFile, true,new PK_EncryptorFilter(rng, e,
55 new StringSink(r)));
56     FileSource(zInputFile, true,new PK_EncryptorFilter(rng, e,
57 new Base64Encoder(new FileSink(zOutputFile))));
58
59 }

```

```

63 public void libcryptopp::decryptopp(file)
64 {
65
66     RSAES_PKCS1v15_Decryptor dec(KeyStored(file));
67     StringSource(r, true,new PK_DecryptorFilter(rng, dec ,new FileSink(recovered)));
68
69 }
70
71
72 //this function generates a signed file
73 public void libcryptopp::signature(file)
74 {
75
76     // Sign and Encode
77     RSASSA_PKCS1v15_SHA_Signer signer(KeyStored(file));
78     FileSource(zInputFile, true,new SignerFilter(rng, signer,
79     new Base64Encoder( new FileSink(signature)))); // StringSource
80     FileSource( zInputFile, new StringSink( s ) );
81     StringSource( s, true,new SignerFilter(rng, signer, new StringSink(sign)));
82
83 }
84
85
86 //this function is used for verification
87 public void libcryptopp::verification (file)
88 {
89
90     // Verify and Recover
91     CryptoPP::RSASSA_PKCS1v15_SHA_Verifier verifier(KeyStored(file));
92     StringSource(s+sign, true, new SignatureVerificationFilter(verifier,
93     NULL,SignatureVerificationFilter::THROW_EXCEPTION)); // StringSource
94
95 }
96 }

```

## Libcryptopp.h

```
1  #include <cstdlib>
2  #include <cryptopp/sha.h>
3  #include <cryptopp/rsa.h>
4  #include <cryptopp/hex.h>
5  #include <cryptopp/osrng.h>
6  #include <cryptopp/oaep.h>
7  #include <iostream>
8  #include <cryptopp/base64.h>
9  #include <cryptopp/files.h>
10 using CryptoPP::RSA;
11 using CryptoPP::InvertibleRSAFunction;
12 using CryptoPP::AutoSeededRandomPool;
13 using CryptoPP::RSAES_PKCS1v15_Encryptor;
14 using CryptoPP::RSAES_PKCS1v15_Decryptor;
15 using CryptoPP::StringSource;
16 using CryptoPP::PK_EncryptorFilter;
17 using CryptoPP::PK_DecryptorFilter;
18 using CryptoPP::StringSink;
19 using CryptoPP::RSASSA_PKCS1v15_SHA_Signer;
20 using CryptoPP::SignatureVerificationFilter;
21 using CryptoPP::RSASSA_PKCS1v15_SHA_Verifier;
22 using CryptoPP::SignerFilter;
23 using CryptoPP::FileSource;
24 using CryptoPP::FileSink;
25 using CryptoPP::Base64Encoder;
26
```

```

27 class libcryptopp()
28 {
29     private:
30     std::string cipher,hold,priv,recover,r;
31     //char const* zInputFile = "/mnt/sdcard/nmea.txt";
32     char const* zOutputFile = "/mnt/sdcard/encrypted.txt";
33     char const* recovered = "/mnt/sdcard/recovered.txt";
34     char const* signature = "/mnt/sdcard/signature.txt";
35     char const* zFile ;
36     CryptoPP::SHA hash;
37     std::string sign;
38     std::string s;
39
40
41     public:
42     libcryptopp();
43     ~libcryptopp();
44     public void storekeys(int length,const std::string filename1 ,
45     const std::string filename2 );
46     public void libcryptopp::verification (string file);
47     public void libcryptopp::encryptopp (string file);
48     public void libcryptopp::signature(string file);
49     public void libcryptopp::decryptopp(string file);
50     public string libcryptopp::KeyStored(string file);
51
52 };

```

## encryptData.cpp

```
1
2  #include <termios.h>
3  #include <fcntl.h>
4  #include <stdio.h>
5  #include <stdlib.h>
6  #include <unistd.h>
7  #include <errno.h>
8  #include <iostream>
9  #include <fstream>
10 #include <libcryptopp.h>
11
12 int main()
13 {
14     libcryptopp lcr = new libcryptopp();
15
16     static int gpsfd = -1;
17     const string pki-publickey;
18     const string pki-privatekey;
19
20     gpsfd = open("/dev/gps", O_RDWR);
21     if (gpsfd < 0)
22     {
23         printf("GPS unit: Failed to open '/dev/gps'.\n");
24
25         gpsfd = -1;
26         exit (1);
27     }
28
29
30
31     char buffer[83];
32     struct termios options;
33     static int ttyfd = -1;
34
35     ttyfd = open("/dev/ttySAC2", O_RDWR | O_NOCTTY | O_NONBLOCK);
```

```

37     if (ttyfd < 0)
38     {
39         printf("TTY1 unit: Failed to open '/dev/ttySAC2'.\n");
40         ttyfd = -1;
41         exit (1);
42     }
43
44     tcgetattr(ttyfd, &options);
45     // Set the baud rates to 115200...
46     cfsetispeed(&options, B115200);
47     cfsetospeed(&options, B115200);
48     // Enable the receiver and set local mode...
49     options.c_cflag |= (CLOCAL | CREAD);
50     // Set the new options for the port...
51     tcsetattr(ttyfd, TCSANOW, &options);
52
53     int read_len;
54     int nl=0;
55     std::ofstream coordinates;
56     coordinates.open ("/mnt/sdcard/nmea.txt");
57
58     while (nl < 50)
59     {
60         read_len = read(ttyfd, &buffer, sizeof (buffer));
61         if (read_len > 0)
62         {
63             ...
64             buffer[read_len-1] = 0;
65             coordinates << buffer;
66
67
68

```

```
71     nl++;
72
73     }
74
75     }
76
77     lcr.storekeys(3072,pki-publickey ,pki-privatekey );
78     string libcr = lcr.keystore(coordinates);
79     lcr.encryptopp(pki-publickey, libcr);
80
81     // do the sign
82     lcr.signature(pki-privatekey);
83
84     coordinates.close();
85     close (ttyfd);
86     close (gpsfd);
87
88
89     return 0;
90 }
```



## DycryptVarify.cpp

```
3  #include <stdio.h>
4  #include <stdlib.h>
5  #include <unistd.h>
6  #include <iostream>
7  #include <fstream>
8  #include <libcryptopp.h>
9
10
11
12  int main()
13  {
14
15      libcryptopp lcr = new libcryptopp();
16      const string pki-publickey = "/mnt/sdcard/rsa-public.key";
17      const string pki-privatekey= "/mnt/sdcard/rsa-private.key";
18
19
20      lcr.dencryptopp(pki-privatekey);
21
22      lcr.verificatio(n(pki-publickey);
23
24
25      return 0;
26  }
```

---

## **References**

- [1] [www.opentom.org](http://www.opentom.org)
- [2] Computer Forensics: Bringing the Evidence to Court by: Cornell Walker
- [3] Forensic acquisition and analysis of the Random Access Memory of TomTom GPS navigation systems
- [4] Guide to Integrating Forensic Techniques into Incident Response
- [5] Forensics computer Theory and Practice: Towards developing a methodology for a standardized approach to computer misuse
- [6] Specifying digital forensics: A forensics policy approach, University of Idaho, Computer Science Department, Carol Taylor, Barbara Endicott-Popovskiy,1, Deborah A. Frinckec
- [7] Experimental Testing of a forensics analysis method on the tomtom navigation device, Clara Maria Colombini
- [8] Forensic Readiness John Tan, Inc. 196 Broadway Cambridge, 02139 USA
- [9] Computer Forensics: The Need for Standardization and Certification Matthew Meyers and Marc Rogers, Purdue University
- [10] Legal Aspects of Digital Forensics, Daniel J. Ryan the George Washington University