2017

A non-device specific framework for the development of forensic locational data analysis procedure for consumer grade small and embedded devices

Peter Hannay
Edith Cowan University

Edith Cowan University

Copyright Warning

A Non-Device Specific Framework for the Development of Forensic Locational Data Analysis Procedure for Consumer Grade Small and Embedded Devices

This thesis is presented for the degree of

Doctor of Philosophy

Peter Hannay

Edith Cowan University

School of Science

2017

Copyright and access declaration

I certify that this thesis does not, to the best of my knowledge and belief:

(i) incorporate without acknowledgment any material previously submitted for a degree or diploma in any institution of higher education;

(ii) contain any material previously published or written by another person except where due reference is made in the text; or

(iii) contain any defamatory material

Signed: 

Dated: 26th October 2017

Abstract

Portable and wearable computing devices such as smart watches, navigation units, mobile phones, and tablet computers commonly ship with Global Navigation Satellite System (GNSS) supported locational awareness. Locational functionality is no longer limited to navigation specific devices such as satellite navigation devices and location tracking systems. Instead the use of these technologies has extended to become secondary functionality on many devices, including mobile phones, cameras, portable computers, and video game consoles. The increase in use of location aware technology is of use to forensic investigators as it has the potential to provide historic locational information. The evidentiary value of these devices to forensic investigators is currently limited due to the lack of available forensic tools and published methods to properly acquire and analyse these data sources. This research addresses this issue through the synthesis of common processes for the development of forensic procedure to acquire and interpret historic locational data from embedded, locationally aware devices.

The research undertaken provides a framework for the generation of forensic procedure to enable the forensic extraction of historical locational data. The framework is device agnostic, relying instead on differential analysis and structured testing to produce a validated method for the extraction of locational history. This framework was evaluated against five devices, selected on a basis of market penetration, availability and a stage of deduplication.

The examination of the framework took place in a laboratory developed specifically for the research. This laboratory replicates all identified sources of location data for the devices selected. In this case the laboratory is able to simulate cellular (2G and 3G), GNSS (NAVSTAR and GLONASS), and Wi-Fi locationing services. The laboratory is a closed-sky facility, meaning that the laboratory is contained within a faraday cage and all signals are produced and broadcast internally.

Each selected device was run through a series of simulations. These simulations involved the broadcast of signals, replicating the travel of a specific path. Control data was established through the use of appropriate data recording systems, for each of the simulated location signals. On completion of the simulation, each device was forensically acquired and analysed in accordance with the proposed framework.

For each experiment carried out against the five devices, the control and experimental data were compared. In this examination any divergence less than those expected for GNSS were ignored. Any divergence greater than this was examined to establish cause.

Predictable divergence was accepted and non-predictable divergence would have been noted as a limitation. In all instances where data was recovered, all divergences were found to be predictable.

Post analysis, the research found that the proposed framework was successful in producing locational forensic procedure in a non-device specific manner. This success was confirmed for all the devices tested.

Acknowledgements

First of all I would like to dedicate my sincere gratitude to my wife, Gwyn, who stood by my side throughout this research journey. Her consistent encouragement and prodding was a key component in my motivation, and I am sure that this work would not have been possible without her.

I would like to acknowledge my mother and sister for their understanding and support of the time commitments which kept me from seeing them as much as we would have liked, often shortening my presence at family events and special occasions.

The support provided by my supervisors, Craig Valli and Andrew Woodward, cannot be overstated. Their seemingly eternal patience and well timed nudges concerning my research progress were essential in the completion of this work. I also owe a special thanks to Tony Watson who gave my thesis a detailed review, despite being in retirement.

For the provision of specialist facilities that were purpose built to accommodate the needs of this research, I would like to thank the Security Research Institute. Many hours were spent in this work space and I am grateful for having this modern environment in which to spend my days.

The WA Police Major Crime Squad also deserve a special mention for seeking my support on investigative matters, allowing me the opportunity to demonstrate this work in both the field and the courtroom.

I would like to provide thanks to Alexandra Elbakyan and all those who stand in solidarity with her for their work in preserving academic freedom.

Finally, thank you to everyone out there on the tubes who has supported me over the years and all the others I am unable to mention. You guys rule.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Background to the study

Small and embedded device forensics is a field of research focused on the acquisition, analysis, and interpretation of data from such devices. A small or embedded device is one, which is based around a microcontroller and is intended to fulfil a specific function within a large device (Heath, 2003). These devices are by definition purpose specific and are often not intended for general computing tasks such as those addressed by general-purpose computers (such as desktop PCs). An example of such a device would be a Satellite Navigation unit, where the embedded system involved serves the purpose of receiving locational data and principally performing navigational functions.

A significant portion of consumer grade small and embedded devices are portable in nature, and as such the typical use case involves these devices being used in a number of locations. These portable devices have the potential to contain historical data, which can, in turn, provide historical locational information of forensic interest. This historical locational information can be of significant interest to forensic investigators attempting to discern the previous location or locations of these devices. Such information may be of use in determining the movement of persons, vehicles or other objects of interest.

During the course of a forensic investigation there are many pieces of information that are of value. The most important of these relate to establishing a timeline of events as they lead up to and take place after the commission of a crime. In creating such a timeline, the use of positioning and timing data allows for a forensic investigator to piece together the movements of the associated physical items. Such a timeline can prove beneficial in both in terms of investigatory and evidentiary support.

Small and Embedded devices pose a particular challenge to digital forensics. The wide variation in embedded hardware and supporting software systems have historically not lent themselves well to standard forensic software or standardised methods. In the absence of a standard architecture for these devices, a different forensic method needs to be developed to analyse each individual device. The absence of standards creates significant workload, costs and other impediments for enforcement and other digital forensic investigators.

This research identifies the similarities between locationally aware small and embedded Global Navigation Satellite System (GNSS) capable devices and provides a framework for the development of forensic methods for these devices. The creation of the framework

is based on analysis of the core functionality and characteristics that locationally aware devices commonly share. Due to these similarities, the framework is applicable to a wide variety of devices and is not specific to one make, model or type of device.

1.1.1 Global Navigation Satellite Systems

These networks have become a part of everyday life, through the pervasiveness of embedded devices such as navigation units, phones, in-car systems, and other smart location-based devices. There are of course the positioning elements of GNSS, which beyond assisting drivers in getting to their destination help with a large number of tasks:

- Allows Unmanned Aerial Vehicles (UAV) to operate autonomously
- Assists in air and sea navigation
- Provides a way for cargo to be tracked in transit
- Tracking of vehicle fleets
- Tracking of rental vehicles to ensure compliance with the rental contract
- Modern cameras automatically tag photos with location information
- Mobile devices provide location information to end users based on GNSS
- Computer time synchronisation relies on data sent from GNSS satellites

With the importance and ubiquity of tasks relying on GNSS infrastructure, it is worth considering the possible forensic implications of this technology. Devices receiving GNSS information have access to accurate location information as well as time data precise at a nanosecond scale. It has already been established that it is possible to retrieve historical location data in the case of automotive satellite navigation systems, based on the information received from GNSS networks (Hannay, 2008).

In many cases, these GNSS devices have no inbuilt functionality that would allow their historic locational data to be readily displayed or extracted. Even if it were a feature of a specific device, however, the forensic implications of using such a feature would need to be questioned. Forensic concepts prefer that the original evidence being acquired from original sources not be altered. However, as ACPO (2003) states in the situation that the data must be altered that any of these alterations are documented, and the impact on potential evidence is understood.

The research focussed on the acquisition and subsequent analysis of historical locational data from a range of location-aware devices. Many of these units make use of storage in the form of internal flash memory, external flash media, and hard disks in order to store

operational data, logs, and other potentially significant data. The large number of GNSS capable devices on the market, however, has led to a situation where acquisition techniques must be developed for each individual device (Jansen, Delaitre, & Moenner, 2008). The research identified the similarities between location aware devices and developed a series of forensic procedures that cater for number of devices based on these similarities.

1.2 Significance

The research presented in this document addresses this issue through the definition of a framework to be used in the development of forensic data acquisition and analysis procedures for locationally aware devices. This framework provides the means to create new methods enabling the determination of locational history for GNSS capable devices. This framework provides structure, minimising the often-lengthy periods of research and development required for the interrogation of a new device. Previous works in this area focussed on the development and testing of acquisition and analysis methods for specific devices. This research differs significantly as it provides non-device specific guidance for the development of specific forensic analysis procedures.

The framework resulting from the research undertaken provides significant value to society. Significance is demonstrated through enabling investigation of devices in a timely, transparent, and cost effective manner. Such application of the developed framework has applications in the investigation of any crime where a locationally aware device is present and available to investigators.

Methods defined through the framework have been used in the preparation of evidence for criminal cases. In each of these cases, capital offences were being investigated, and the method yielded data of significance to the investigation. The admission of this data into evidence provides validation of the forensic method and framework defined by this research. In a number of instances, the resulting analysis provided law enforcement with the location of bodies related to the appropriate investigations. The details of a sample of these cases are outlined below. The names of the victims and accused are not included due to the sensitive nature of these matters.

Case 1 involved the disappearance of two persons. A satellite navigation unit recovered from a vehicle belonging to the accused was provided for analysis. Using the method resulting from this research the device was analysed. It was determined that a number of locations had been entered into the device, however, these were not useful to the investigation. Secondary data was recovered from a series of log files which were

encrypted using keys known only to the vendor. These files and associated information were passed to the investigating officers who communicated with the vendor via Interpol to organise the decryption of the files. The resultant data was provided to the researcher for interpretation. The resultant analysis allowed law enforcement to locate the bodies of the two persons. Subsequently, the accused were sentenced to over 30 years in prison.

Case 2 involved two suspects who were investigated and sentenced to approximately 20 years in prison for the murder of one victim. In this instance, a satellite navigation device was provided to the researcher for analysis. The device was examined in accordance with the framework defined in this thesis. As a result, a series of addresses and route information were produced. This data was produced as evidence in the trial which resulted in a guilty verdict for the accused, as it linked the device to key locations involved in the transportation of the body of the victim.

Case 3 resulted in the conviction of one person for the manslaughter of his former partner and sentenced to ten years in prison. In this instance, the body was recovered through the use of historical location data gathered from a provided satellite navigation unit. The device was analysed in accordance with the framework presented in this document.

There are numerous other cases which have been supported by evidence derived from the framework defined in this thesis. The cases presented above represent less than half of the total case volume supported by the framework and the research. In each instance, the data provided has assisted the investigation and subsequent court hearings having produced pivotal, non-polemic evidence leading to conviction(s). The evidence not only placed the perpetrators in corroborated timelines around the criminal act but it also allowed law enforcement to recover the bodies of the deceased in a timely and precise manner. This precision on location saved significant costs associated with discovery and recovery. The rapid recovery also assisted in the preservation of critical evidence. In addition, the work also provides significant social benefit in rendering justice against these perpetrators and gives closure and respite to the grieving parties.

2 Literature Review

2.1 Modes of Location Awareness

2.1.1 Global Satellite Navigation Systems

2.1.1.1 History of Global Positioning Systems

TRANSIT was the first satellite navigation network. TRANSIT was developed to provide location data to the United States Navy's Polaris submarine forces (Parkinson & Gilbert, 1983, p. 1117). The TRANSIT network became operational in 1963 and the use of this network lead to the US Navy, and US Airforce to consider further use of this technology. At that stage, the US government was unable to implement two separate networks due to budget issues. These factors led to the inception of the NAVSTAR network. NAVSTAR was to be a resource that would be shared among US military agencies; the first NAVSTAR satellites were launched in the 1970s (Braunschvig, Garwin, & Marwell, 2003).

NAVSTAR was designed as a dual-use system, in that it would be shared with military and civilian users. The civilian signal was degraded for the purpose of denying precise location data to enemies of the United States. The degradation was to be known as 'selective availability' and would lead to the insertion of inaccuracies up to 500 metres. In 1983 US President Ronald Reagan approved NAVSTAR for use in commercial aircraft and subsequently selective availability was altered so that the signal would be accurate within 100m (Parkinson & Spilker, 1996, p. 601).

In May 1st, 2000 Bill Clinton announced that selective availability would be set to zero (Braunschvig et al., 2003). The result of this was that the civilian NAVSTAR signal would no longer be artificially degraded and as such a wide range of commercial uses for the technology became feasible.

Tensions between the US and the USSR during the cold war lead to the creation of a Soviet-owned satellite navigation network known as *ГЛОбальная НАвигационная Спутниковая Система* or GLONASS (Parkinson, 1997, p. 22). The system became operational and available for civilian use in 1995 (Polischuk & Kozlov, 2002, p. 154).

As a result of concerns that the US controlled the NAVSTAR network and had the ability to degrade or tamper with the signal the European Union (EU) proposed a satellite navigation network named Galileo. The Galileo network provides interoperability with

the existing NAVSTAR network and to provide increased levels of accuracy and reliability to both civilian and military users (Braunschvig et al., 2003; Hossam-E-Haider, Tabassum, Shihab, & Hasan, 2014).

2.1.1.2 Operation of Global Positioning Systems

The NAVSTAR global positioning system is comprised of a network of satellites in medium earth orbit, at an altitude of 20,200 kilometres (Revnivykh, 2012). Each of these satellites is equipped with an atomic clock, which measures time based on the electronic transitions of Cesium-133 or Rubidium isotopes, the yearly drift of these sources, alongside other reference sources are shown in Table 2-1 (Parkinson & Spilker, 1996, p. 21; U.S. Coast Guard Navigation Center, 2014). This precise and accurate measurement of time is critical to the accurate operation of the network as a whole.

The signals from the GNSS satellites (GNSSS) contain various encoded data, including the location of the satellite in three-dimensional space relative to the earth and the time as reported by the satellites internal atomic clock. The GNSS receiver receives the signal and the time information is used to calculate the receiver's location from the GNSSS. The signals from multiple satellites are used in order to calculate the position of the GNSS receiver. It is estimated that a variance of one millisecond would lead to a 300 metre error in the calculated position, as such the system is reliant on the accuracy of time information available from each satellite (Walter, 1996).

Table 2-1 The stability of Quartz, Oven Controlled Crystal Oscillator (OCXO), Rubidium, Caesium, Hydrogen, and Strontium frequency sources in Allen Deviation. The corresponding yearly drifts are provided in picoseconds (Lewis, 1991).

	Stability $\sigma_y(\tau)$ – Daily	Drift – 1 Year
Quartz	1e-10	36,525,000 ps
OXCO	5e-10	182,625 ps
Rubidium	1e-13	36.52500 ps
Caesium	2e-14	7.30500 ps
Hydrogen	1e-14	3.6525 ps
Strontium	3e-17	0.0109575 ps

A number of processes are used in combination to allow GNSS receivers to determine their location. The key processes from a high-level perspective are Time of Arrival (TOA) and trilateration. These processes are discussed below.

Time of arrival (TOA) is used to determine the distance from a receiver and transmitter. TOA requires the transmitter to send the time as part of its transmission. The receiver compares the time transmitted with the current time at the location of the transmitter and

makes a determination of the distance between the two based on the speed of the signal. As the speed of the signal varies depending on the media through which it is traversing, some knowledge of this media is required in order to make an accurate determination of distance.

Trilateration makes use of the concepts of TOA with multiple transmitters of known location and a single receiver for which the location is unknown. The receiver determines its distance (*d*) from the receiver through the use of TOA. If signals are received from three or more transmitters, it is possible to determine the location of the receiver. Spheres of radius *d*, centred on the transmitter(s) are plotted and the point(s) where the surfaces of these spheres intersect are possible locations of the receiver. The equation to calculate the position of the receiver is shown below in Equation 2-1.

Equation 2-1 Formula for trilateration, top allows for y and x positions to be solved, bottom allows for z position to be solved subsequently

$$y = \frac{r_1^2 - r_3^2 - x^2 + (x-i)^2 + j^2}{2j} = \frac{r_1^2 - r_3^2 + i^2 + j^2}{2j} - \frac{i}{j}x$$

$$z = \pm\sqrt{r_1^2 - x^2 - y^2}$$

In Figure 2-1 presented below, we can see a single point within the overlap area of two spheres provided. The satellites exist at the centre of each sphere with a radius being the calculated distance from each satellite. The area of overlap represents space in which the receiver could potentially exist. It is due to various atmospheric effects they can introduce error that results in the overlapping area not being a single point. There exist other sources of potential error such as multipath effects, Doppler, and relativistic effects, a summary of these sources of error is shown in Table 3-2.

The accuracy of the calculated distance from a satellite is also dependant on a number of factors aside from the accuracy of time data. Such factors include the path taken by the signal and the media that the signal travels through on the way to the receiver. These variables can both impact the length of time taken for the signal to reach the receiver. For example, if the signal bounces off a body of water several kilometres away from the receiver thus taking a non-direct route this will result in an incorrect distance being calculated for the satellite in question as the signal will take longer to reach the receiver. In order to reduce this effect, a number of error analysis and correction methodologies can be employed, however, the discussion of these is beyond the scope of this thesis (Parkinson & Spilker, 1996, pp. 469-483).

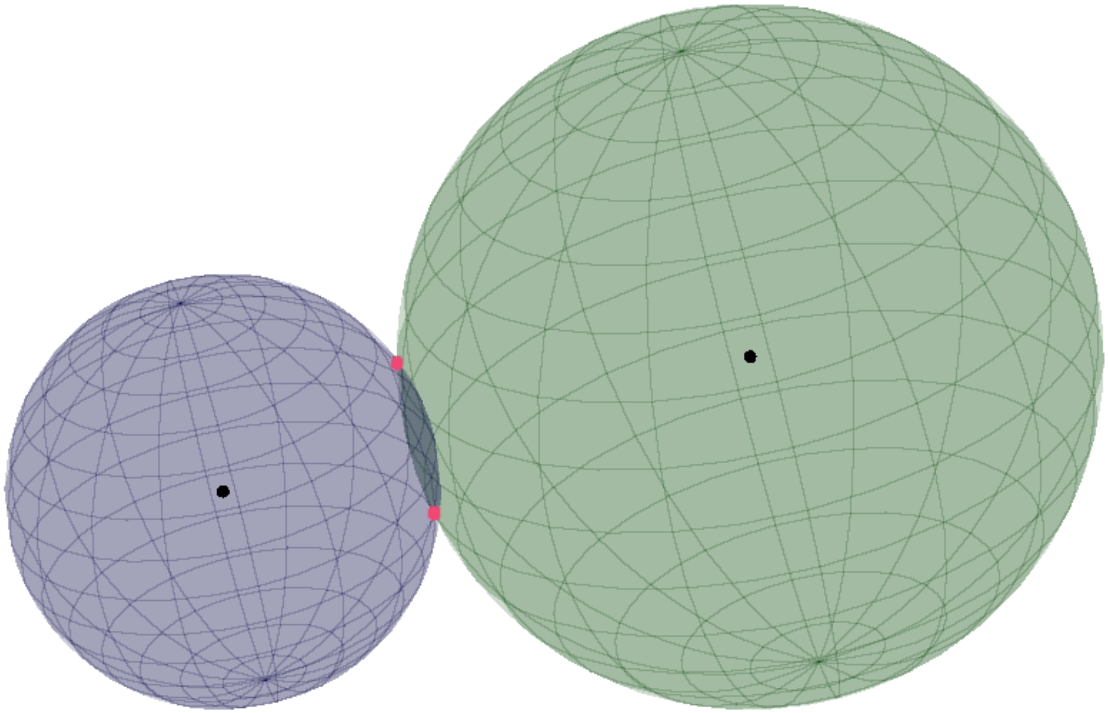

Figure 2-1 Two intersecting spheres demonstrating the mechanism for trilateration. The black dots represent GNSS satellites while the pink dots represent intersection points for the surface of each sphere. The radius of each sphere is determined based on the time taken for a signal to reach the receiver. The points of intersection are potential locations of the receiver.

The operation of GNSS requires that signals pass uninterrupted from the transmitter to the receiver. Unfortunately, perfect line of sight is rarely the case, as the signal will often be reflected or diffracted as it interacts with various materials (Kos, Markezic, & Pokrajcic, 2010). As the signal is broadcast over a wide area, this results in multiple duplicates of the signal being received. The most direct signal is received first, followed by the reflected signals, which have travelled a longer distance. The receiver discards signals arriving a significant period after the primary signal i.e., long delay reflections. Short delay reflections pose increased difficulty when conducting error analysis, as they interfere with the original signal itself. Figure 2-2 shows the three scenarios discussed here, short delay reflection, long delay reflection, and direct signal paths (Kos et al., 2010).

There are two primary modes for processing multipath effects; these are spatial processing and time domain processing. Spatial processing relies on modifications to antenna design, relying on previous knowledge of the source of multipath effects. Multipath reduction is often utilised with fixed location GNSS receivers or for maritime GNSS receivers, in the case of which an antenna can be designed not to receive signals from below the horizon (Rost, 2012). Such designs often make use of a “choke ring” design, in which multiple concentric conductive rings are arranged in such a way that they absorb signals from undesirable origins (Braasch & van Dierendonck, 1999). In many cases, it is not possible to predict the origins of multipath signals or alternately the orientation of the antenna itself. In these instances the purely signals analysis based approach of time-domain processing is preferable (Yujie & Bartone, 2004). The time domain processing methods consist of a number of approaches, incorporating reference waveforms, heuristics, signal compression, and probabilistic functions (Grewal, Andrews, & Bartone, 2013, pp. 269-283). While the specific implementations of time domain processing methods are out of scope here, it is worth nothing that a key differentiator between older and more modern receiver designs is the available bandwidth for time domain analysis. Higher bandwidth designs allow for a longer period to be analysed, thus allowing more complete waveforms to be examined (Grewal et al., 2013, pp. 269-283).

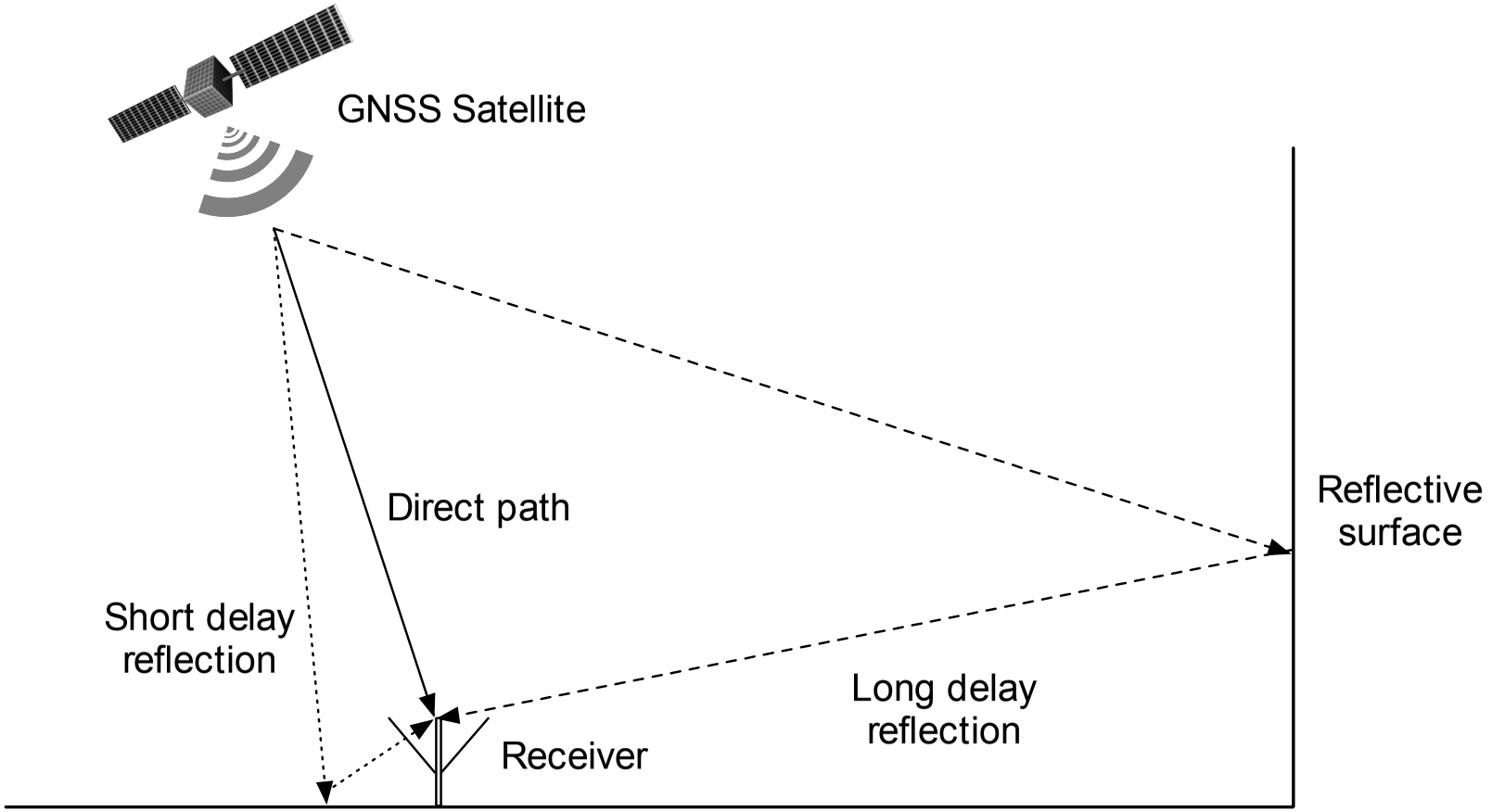

Figure 2-2 Direct path and multipath received signals due to signal reflection. Both long delay and short delay reflections are shown in this example (Kos et al., 2010).

2.1.2 Assisted GPS (AGPS)

Assisted GPS (AGPS) refers to a collection of technologies that provide GNSS-like services or enhance GNSS services through the use of support from other, typically cellular, networks (Djuknic, 2001). There are two primary modes of operation for AGPS; mobile station based (MSB) and mobile station assisted (MSA) (Van Diggelen, 2009, p. 43). MSB and MSA refer to the role of the mobile station, i.e., the device receiving GNSS signals, such as a mobile phone. The principal mechanism used to support the location determination process is known as frequency based assistance. GNSS Receivers can make use of AGPS in either satellite assisted or network only modes.

To understand the role of AGPS we first need to understand how a standard GNSS receiver determines its location from a cold start. In the situation of a cold start, the receiver has no information about the location, velocity or state of any GNSS satellites or the state of the network as a whole. (Van Diggelen, 2009, p. 44). To resolve this lack of information, the device must determine the operating frequencies, expected location of satellites, and current GNSS network time. These items of data are known as the almanac, ephemeris and clock respectively.

In a cold start situation, the receiver must establish communication with at least one satellite. At this stage, the device does not know its location, the locations, paths, or velocity of any satellites. This location, path, and velocity data is required in order to determine the Doppler frequency shift of a given satellite (El-Rabbany, 2002, pp. 8-10). Without this frequency shift data, it is not possible to know which frequency to listen on to receive signals from the satellite. As such, a brute force operation must be performed for the 50 candidate frequencies and 1,023 code delays (otherwise known as chipping). The search operation takes a minimum of 20 seconds (Van Diggelen, 2009, pp. 34-38). Once the search operation is complete, the receiver can begin receiving data from the satellite being targeted.

The concept of chipping allows for increased error tolerance in digital communications at the cost of throughput. The process of chipping applies a mask to a data sequence at a higher bitrate than the original data using an XOR operation, as shown in Figure 2-3. The receiver of the signal will perform the same process in reverse and in the event that the widened message contains complete sequences of identical bits there is increased confidence in the integrity of the data stream.

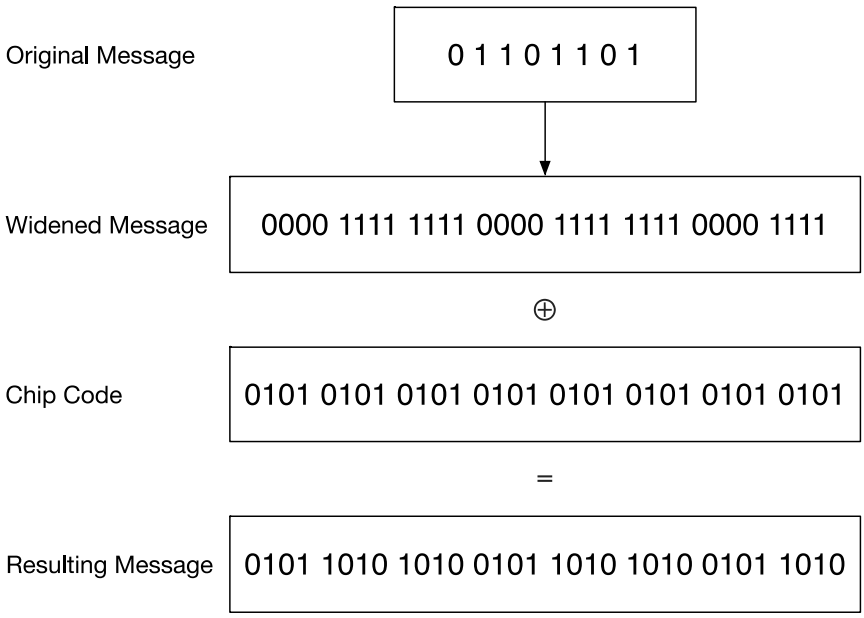

Figure 2-3 The concept of chipping is shown demonstrated here. The original message is extended by some factor via repetition of individual bits. A chip code is then XORed against the widened message to produce the resulting message for transmission.

The almanac is transmitted by each GNSS satellite at a rate of 50 bytes per second, and it takes a total of 12 minutes and 30 seconds to receive the full almanac. If the data connection is interrupted then the process must be restarted (Bertorelli, 1996). The almanac contains data describing the orbit and expected location of each GNSS satellite at any given point in time (ShareTechNote, 2013). The ability to accurately predict the location of satellites depends on the age of the almanac; Table 2-2 shows almanac accuracy versus time. With this almanac data, the position of the satellites can be derived and the Doppler shift calculated for their movement relative to the receiver. These calculations allow the receiver to determine which frequencies to monitor to receive signals from a particular satellite at a given point in time (Parkinson & Spilker, 1996, pp. 246-248).

Table 2-2 Table showing almanac accuracy degradation based on time since transmission (Parkinson & Spilker, 1996, p. 140)

Age of data - time since transmission	Almanac accuracy
1 day	900 metres
1 week	1,200 metres
2 weeks	3,600 metres

Ephemeris data provides far greater accuracy for the location of each satellite at any given point in time than the almanac. Each GNSS satellite transmits ephemeris data for itself only, and this data is transmitted every 30 seconds and is considered valid for up to four hours (ShareTechNote, 2013). The ephemeris data is used in conjunction with the time signal broadcast by a satellite to deduce the location of that satellite (Parkinson & Spilker, 1996, pp. 121-125).

Each satellite within a constellation keeps time via an internal atomic clock. Clock drift is compensated for via a synchronisation mechanism between the satellites in the cluster. The receiver performs trilateration by determining the difference in time indicated by arriving signals from each satellite (El-Rabbany, 2002, pp. 8-11). The ephemeris data in combination with the time of transmission allows the receiver to determine the location of the satellite at the broadcast time. With the location of a number of satellites known and the difference in the signals' time of arrival, it is possible to determine the receiver's location.

A capable receiver can request frequency assistance and will be provided with the current almanac and ephemeris data. Through this mechanism it is possible to speed the acquisition process, effectively bypassing the time delays associated with a cold start. In essence, frequency assistance removes the need to receive almanac or ephemeris data from the GNSS satellites themselves and instead acquire such data from a trusted third party.

From the previous explanation of the cold start process, we can determine that we would need almanac, ephemeris, time, and the approximate location of the receiver in order to determine the frequency offsets and satellite location prior to satellite communication. Frequency assistance provides mechanisms to meet these requirements. The implementations of frequency assistance differ slightly in MSB and MSA.

Mobile station based frequency assistance provides the time, almanac, ephemeris, rough position (typically computed using trilateration to determine the location of the receiver), and reference frequency data. The reference frequency data is used to calibrate the receiver's clock to allow for increased time precision (LaMance, DeSalas, & Järvinen, 2002). The mobile station assisted approach provides the time, reference frequency, and calculated Doppler offsets directly to the receiver (Van Diggelen, 2009, pp. 45-46). The primary difference between MSB and MSA is which system is responsible for performing the required Doppler calculations.

The above assistance mechanism is valid for both network only and satellite assisted modes with one essential difference. In network only mode the MSB functionality is used, and all data other than the rough position is discarded. This rough position allows for coarse positioning in the absence of any dedicated GPS hardware (LaMance et al., 2002). As an MSA provides no location data, it cannot be used in network only mode and must be used in conjunction with satellite assistance.

2.1.3 Time Difference of Arrival (TDOA)

Time Difference of Arrival (TDOA) technologies are intended to allow for the location of a device within a network. There are two primary modes of operation which differ based on the role of the transmitting and receiving parties. TDOA determines the location of a device based on the known location of a number of transmitting devices. While Uplink Time Difference of Arrival (UTDOA) provides details of a transmitter through the known location of a number of receivers, the existing implementation of the technology does not aim to address the historical location of such devices. This historical record keeping is left to the individual device, network, or implementation as deemed necessary by the implementer.

TDOA is employed by systems using trilateration or multilateration. It is important to note the difference between trilateration and triangulation in order to understand the terminology used. Triangulation specifically refers to the determination of location through the measurement of angles. In such implementations location would be determined through the measurement of relevant angles to transmitters at known locations. Through comparison of these relative angles, the position can be derived. Conversely trilateration or multilateration can measure the time of flight, signal strength, or other observable and measurable phenomena to determine location.

Trilateration is preferred as omnidirectional antennas can be used without adverse effects. In the case of triangulation, highly directional antennas must be utilised, either

moving or arranged in complex arrays. In many instances, these requirements are prohibitive for portable devices, due to the size and complexity of such arrays, and the required mechanisms to keep such arrays stable.

2.1.3.1 Operation

TDOA systems operate through the observation of time taken for a signal to reach a destination. The receiver of the signal then analyses the difference when a number of signals are received and uses trilateration to determine its own location. If these transmitters are stationary, there may be existing knowledge as to their location which the receiver can utilise. In other situations, the transmitters may be in motion during transmission and as such their location must either be derived from existing knowledge or transmitted with the locational signal.

In a UTDOA system, the location of the transmitter is unknown, as such the location of the receiver must be known to allow the system to operate. Each receiver node communicates the time the signal was received by some central node and these are trilaterated to determine the location of the transmitter.

2.1.3.2 Limitations

Time synchronisation is critical for a (U)TDOA network to achieve its function. TDOA and UTDOA have different requirements in this regard. With frequency synchronisation and time synchronisation being the critical factors in each of these technologies respectively.

Frequency synchronisation is required to ensure that each transmitter is producing waveforms in a synchronised fashion. This frequency synchronisation is of importance for two key reasons. The first reason is that signals at different frequencies will travel at a different speeds over the course of a trip over long distances through varying transmission media. The cause of this effect is attributable to optical dispersion as well as the resulting differences in path and group and phase velocity (Astrophysics, 2015). Conversely, in UTDOA systems, synchronisation is of importance as the receiving units must be able to receive and interpret the signal in a way which is consistent with the other nodes.

The dispersion of locationing nodes (either receiving or transmitting) has a measurable impact on the accuracy of locationing. In cases where the locationing nodes are clustered closely, the differences in time of flight are minimised. In such instances the precision of location is reduced, this is known as dissolution of precision (DOP). To reduce the DOP, we can either acquire more sensitive equipment or alter the distribution of locationing

nodes. In an ideal situation, the locationing nodes would be dispersed evenly around the unit being located thus maximising precision. In reality, the careful planning of the location of nodes and constant measurement of the DOP is undertaken to calculate any limitation of precision.

2.1.3.3 Implementations

Some specific implementations of TDOA are discussed in this section. The general classifications of these are GNSS, Cellular, and Wi-Fi. Other locationing mechanisms do exist, and it should be noted that the TRANSIT GNSS implementation was based on the Doppler effect rather than TDOA. Doppler relies on analysing the frequency of received signals and comparing these to the known velocity of the receiver in order to determine distance from the transmitter, rather than using an encoded time signal.

GNSS refers to space-based systems with global reach, while Cellular and Wi-Fi applications make use of ground-based locators, known as Location Measurement Units (LMUs). In the cellular implementations UTDOA is employed with cell towers acting as LMUs, this enables mobile devices to be located with no additional functionality or modification to operation. This application is especially attractive due to the fact that it could be implemented entirely on the network side. This technology was first implemented in order to support the United States' E911 legislation that required that a device calling emergency services must be locatable.

Wi-Fi locationing makes use of pre-existing infrastructure which is not modified to support locationing. Instead, the location of Wi-Fi access points is recorded and comparisons of signal strength made in order to determine the location of endpoint devices via TDOA. This method was attractive as no infrastructure needed to be specifically constructed to support the functionality. A significant advantage of this approach was that it did not require line of sight to satellites in orbit. Indoor locationing can be accomplished in an achievable manner through this method.

Finally, the majority of GNSS implementations (except TRANSIT) make use of TDOA with modifications to allow for the LMUs to have non-fixed locations.

2.1.3.4 Summary

The specific implementations of TDOA are discussed in additional depth in the subsequent sections of this document. In each of these, the focus is on the specific applications of the technology and not in the underlying theory or physical phenomena that enable the technology.

2.1.4 Phone Cell ID Positioning

Cell-ID based locationing mechanisms make use of trilateration to determine the location of the receiver handset. Each base transceiver station (BTS) broadcasts the location area identifier (LAI), and it's Cell-ID (Trevisani & Vitaletti, 2004). The mobile device can then make approximations on its location by approximating its distance from a number of BTS by comparing signal strengths and time of arrival data for each BTS in a trilateration based approach. The location of each BTS must be known for a position to be approximated (Trevisani & Vitaletti, 2004). A number of services exist to provide BTS location data to MS devices, notably Skyhook, OpenCellID, as well as Apple and Google's internal Cell ID databases.

2.1.5 Wi-Fi Positioning Systems

Wi-Fi based positioning systems are primarily used to aid GNSS signal acquisition times and improve accuracy in areas where GNSS signals are degraded (Vossiek et al., 2003). These systems operate through the use of databases, which match particular Wi-Fi networks to the locations at which these networks can be detected. The means of matching these is commonly via the BSSID to a set of latitude and longitude coordinates (Halim, 2006). In some implementations, the relative signal strengths from surrounding wireless access points are considered and used for trilateration based purposes to refine further the probable location of the client device (Sapage & Franco, 2004). A number of Wi-Fi positioning services exist, notably Skyhook, OpenCellID, Wigle.net, as well as Apple and Google's internal Wi-Fi Locationing databases.

Wi-Fi positioning mechanisms are based on received signal strength indication (RSSI) in combination with trilateration. In Wi-Fi based locationing implementations the relative signal strengths from surrounding wireless access points are considered and used for trilateration based approaches to refine the probable location of the client device (Sapage & Franco, 2004). The relative signal strength data is combined with databases of access points and approximate locations to estimate the position of the receiver device (Locher, Wattenhofer, & Zollinger, 2005). In the majority of implementations, these locations are drawn from service providers' own databases, which provide approximate locations for known BSSID.

The database providers themselves collect information through a number of channels. These channels include data gathered directly through specially equipped vehicles, data voluntarily contributed from users, data provided by mobile application authors (collected from the user base), data gathered from mobile device users, and other bulk data

acquisitions. In the vast majority of cases, the quality and reliability of this data is difficult to determine. As a result of this limitation, there is a requirement that a consensus is reached from a statistically significant sample prior to the adoption of the data as known good (Feng & Gong, 2014).

Techniques have been developed for use by hobbyists and researchers aiming to gather locational data. One such example is Snoopy-NG, which provides means for establishing distributed sensor networks to collect Wi-Fi beacons and analyse the data to extract locational data. Further work in this area has shown means to determine historic locations and infer the home location of a device from the preferred network list (PNL) broadcast by the device (Chernyshev, Valli, & Hannay, 2016).

2.2 Locationally Aware Devices and Forensics

Location tracking devices have been used by law enforcement agencies to track offenders who are confined to specific premises during specific hours (Nellis, 2005). There are various implementations of these tracking devices. However, one common theme is the combination of GNSS and cellular telephone technologies. In these implementations, GNSS is used in conjunction with the mobile telephone network's assisted global positioning system (AGPS) to provide increased accuracy. This method is particularly useful when indoors, underground, or in areas where the GNSS signals are weak (Djuknic, 2001). AGPS operates on the principle of trilateration in a similar way to the standard GNSS system. However, in this case, mobile towers are used instead of satellites when determining location. These tracking devices will typically use a data logger component to record location information or make use of a transmitter and antenna to broadcast real-time tracking information (Keith, 2007, p. 25).

Thus far there have been a limited number of published works documenting the use of GNSS evidence in legal proceedings (Berman, Glisson, & Glisson, 2015). There are some incidents that have been reported by various news agencies. Significant incidents include those involving Brett Pownceby and Michael Simotas, both of which involve the use of GNSS evidence to challenge speeding fines.

An article published by the Australian Broadcasting Authority (ABA) recounts the incidents of Brett Pownceby, a Victorian farmer who was issued with a speeding fine for exceeding the speed limit by 21km/h (Watt & Crase, 2007). Supposedly a GNSS receiver was turned on and active at the time the alleged infringement occurred. It is stated that Mr. Pownceby retrieved records from the GNSS device, which showed his speed as

being within an acceptable range at the specified time. Purportedly the charges against him were dropped when he presented this evidence to an unknown member of law enforcement. However, it is stated by the ABA that the case never reached court (Watt & Crase, 2007). It should be noted that an article published by the Herald Sun newspaper reports that a representative of the Traffic Camera Office has stated that "The production of a GNSS report alone to avoid any speeding infringement is insufficient" (Whinnett, 2007).

A similar incident involving Michael Simotas, who as it was reported in the Sydney Morning Herald newspaper, was charged with exceeding the speed limit by 25km/h. The article states that Mr. Simotas made use of an expert witness and GNSS evidence acquired from the satellite navigation unit in his car in an attempt to prove his speed at the time of the incident. Initially, the court ruled against Mr. Simotas, however, the charges were dismissed by the District Court of New South Wales on appeal (Wainwright, 2007). It should be noted that the article does not state that the GNSS evidence used was taken into consideration as part of the ruling. The article also reports that the police operating the radar unit at the time of the incident admitted to not using it correctly and instead were making a visual estimation of Mr. Simotas' speed (Wainwright, 2007). The EziTrack website states that the GNSS device used was an "EziTrak® GPS Security and Tracking System" which can record time, date, and vehicle speed (EziTrak, 2007a). However, it is worth noting that Michael Simotas is listed as a distributor of the EziTrack product, and as such this information may not be impartial (EziTrak, 2007b; Pye, 2007).

In 2012, Twitter user @anonw0rmer posted an image of his then girlfriend with a sign claiming credit for an illegal server compromise. The image with a sign reading: "PwNd by w0rmer & CabinCr3w <3 u BiTch's !" also contained EXIF formatted metadata (Mezzofiore, 2012). The metadata was found to contain geolocation data showing a residence in Melbourne, Australia. Investigators linked w0rmer's persona to other forums' accounts and a facebook account belonging to Higinio O. Ochoa III. Higinio's facebook account contained several other photos of the woman shown in the original image. Higinio was later arrested at the Melbourne residence identified from the coordinates embedded within the EXIF metadata (Diaz, 2012).

Research undertaken by Rose and Lisker (2016) examined the contents of images posted to the dark net market sites present within the Dark Net Market Archives. The Dark Net Market Archives is a dataset containing the listings on 89 dark net markets from 2013 to 2015 (Branwen et al., 2015). The images included in these listings were analysed to identify and extract any locational EXIF metadata. The researchers found that 229 of

the 126,773 analysed contained locational data. Rose and Lisker (2016) identified that each location identified would often have a cluster of images associated within a radius of a few metres. This finding would suggest that a seller of illicit goods was habitually including this data with the images they provided with their listings.

2.3 Digital Forensics Aims

Forensic science is the application of scientific principles to the preparation and presentation of evidence in a court of law (Agarwal, Gupta, Gupta, & Gupta, 2011). In extending this to digital forensics Weiser, Biros, and Mosier (2006, p. 17) define digital forensics as "Scientific knowledge and methods applied to the identification, collection, preservation, examination, and analysis of information stored or transmitted in binary form in a manner acceptable for application in legal matters." In a similar fashion, the Scientific Working Groups on Digital Evidence and Imaging Technology (2015, p. 6) in their glossary of terms describe Computer Forensics as "A sub-discipline of Digital & Multimedia Evidence, which involves the scientific examination, analysis, and/or evaluation of digital evidence in legal matters". Extending this definition Carrier (2005, p. 13) defines digital forensic investigation as "a process that uses science and technology to analyse digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred". Carrier (2005, p. 13) extends this to explain that a forensic investigation is a restricted form of an investigation which must meet the criteria in a court of law. Jones and Valli (2008, p. 7) examine these definitions to define further digital forensics as the collection, analysis, and presentation of evidence "obtained from digital devices and associated peripheral devices through the application of digital investigation and analysis techniques, the data from which is preserved in a scientifically sound manner in an electronic form".

For the purposes of this research the following amalgam of definitions is used: Digital forensics is focused on the acquisition and analysis of digital evidence in such a way that it is admissible in a courtroom setting.

To understand the aims of digital forensics we revisit the standards for the field for forensics itself. Ryan (2009) proposes that the Daubert standard is the primary unifying standard for theories and techniques to be admissible in court. The Daubert standard suggests that five criteria are to be evaluated to determine if evidence is to be admissible. First "whether the theory or technique in question can be and has been tested; [Second] whether it has been subjected to peer review and publication; [Thirdly it is] known or potential error rate; [Fourth] the existence and maintenance of standards controlling its operation; and [finally] whether it has attracted widespread acceptance within a relevant

scientific community" (Ryan, 2009). The Daubert standard is US centric, and other jurisdictions may impose individual other evidentiary requirements.

From the above we can determine that the aim of digital forensics is to acquire and analyse digital data in such a way as to determine previous actions that have been undertaken. Regardless of the nature of the case, the key goal must always be to show the truth of a previous situation in a way that is legitimate and honest as to what the evidence suggests (Valjarevic & Venter, 2015, p. 3).

2.4 Digital Forensics Guidelines

As previously defined, digital forensics is focused on the acquisition and analysis of digital evidence in such a way that it is admissible in a courtroom setting. To achieve this outcome, we focus on procedure and documentation regarding the handling of any potential evidence.

HB171 is a handbook published by Standards Australia and aims to serve as a reference to best practice for the management of electronic evidence (HB171, 2003). The Good Practice Guide for Computer based Electronic Evidence published by the Association of Chief Police Officer (ACPO) is a resource which focuses on the acquisition and handling of digital evidence (ACPO, 2003). This resource and a number of other guidelines are in current use and are discussed below.

The 2013 Australian and New Zealand Guidelines for Digital Imaging Processes (ANZGDIP) provides recommendations for the handling and production of digital images. In this case, digital images refer to optically captured images. The focus is on crime scene photography and CCTV imagery. ANZGDIP proposes the same key points proposed by other guidelines. Primarly preservation of original evidence, maintaining an audit trail, and ensuring complete and accurate evidence capture (ANZPAA NIFS, 2013).

The Australian Federal Police make use of standards devised by the National Association of Testing Authorities, Australia (NATA) in an attempt to standardise procedure across forensic facilities in Australia and New Zealand (AFP, 2011; NATA, 2014). These standards were ratified and published by Standards Australia and given the designation AS 53881-4. These standards serve as the basis for laboratory accreditation, covering the full chain of evidence, end to end. Each standard addresses a specific phase of the forensic process. The phases referred to are recognition, recording, recovery, transport and storage, analysis and examination of material, interpretation, and reporting (Standards Australia, 2012a, 2012b, 2013a, 2013b).

HB171 is an Australian guideline which defines six separate stages for the management of IT evidence. The first two stages are focused on the design of computer systems to produce electronic records that can be used as part of a forensic investigation if needed. As the proposed research is focusing on the acquisition and analysis of evidence from devices that we have no control over, these stages are not relevant to the research. However the remainder of the document is useful in that it provides guidelines for the storage, labelling, and related documentation activities associated with an investigation (HB171, 2003).

NIST SP800-101 provides guidelines and information concerning mobile forensics (Ayers, Brothers, & Jansen, 2014). The report provides a classification system for mobile forensics utilities, based on the method of data acquisition, ranging from manual (inspection of data through the screen on a mobile device) to microcode analysis (examination of NAND memory with an electron microscope). The guidelines for forensic procedure provide general end to end advice for the preservation, acquisition, examination and analysis, and reporting (Ayers et al., 2014). NIST SP800-101 is targeted for consumption by US law enforcement agencies and exists primarily within this context. Each section provides background information on the topic and then provides suggested workflows to perform the procedure being discussed. While the guidelines are fairly useful as a source of background information, they do not provide technical information or guidance, instead assuming an audience dependent on commercial tools.

The NIST Computer Forensics Tool Testing Handbook differs from the other resources examined in this section, as it provides results of evaluation of specific pieces of forensic software. These evaluations were carried out against the specifications outlined in NIST Mobile Device Tool Specifications (NIST, 2016a). These specifications were adapted into a series of test assertions and test plans, these are presented in NIST Mobile Device Tool Test Assertions and Test Plan (NIST, 2016b). These three documents are designed to accompany one another, with consumption based on requirement.

Digital forensics is faced with unique issues associated with the intangibility and volatile nature of the evidence being handled. The nature of digital evidence is that it is a separate entity from the physical media which stores or carries the digital evidence itself. It is critical that the integrity of the data can be demonstrated and fully understood. A number of techniques are commonly employed to achieve this goal. These include hashing algorithms and the use of interfaces which allow media to be read but not written to (HB171, 2003, pp. 17-18).

A forensic investigation can often be divided into several distinct phases. The first of which is the collection of evidence from the scene. There are a number of views on how potential evidence is best collected with minimal impact on the integrity of the evidence. An example of this is based on the state of the equipment found at the scene. If a computer is turned on the recommended actions may differ from those if the computer was turned off (ACPO, p. 10). However in the case of PDAs, smart phones, or other volatile devices, the ACPO guidelines suggest that the device not have its power state changed and should be connected to a power source as soon as possible to prevent the loss of potential evidence (ACPO, p. 13). This limitation occurs because unlike PCs, these devices often make use of volatile memory for data storage, with this type of memory losing its contents shortly after power is removed.

The later phases of forensic investigations generally consist of the creation of an evidentiary copy that is a bitstream or exact copy of the original evidence. A bitstream copy is a complete bitwise representation of the digital stream being copied. In essence from the beginning to the end of the storage device, every single bit of data is copied, in order, without regard to the contents (Altheide & Carvey, 2011). This mode of acquisition is in contrast to a logical acquisition or file level acquisition in which context with respect to the host operating system, is used to acquire specific pieces of data. An example of a logical acquisition would be copying just the files present on a device (Kizza, 2015). The use of bitstream copies is important as it ensures that all data is acquired, even that which may exist in unallocated or slack space on the storage medium.

The analysis of this evidence, associated documentation and frequent re-verification of the integrity of the evidentiary copy ensure that the integrity of any findings is maintained (HB171, 2003, pp. 18-22). A record of all actions performed during the investigation and details of methodologies followed should be documented so that the analysis can be repeated if verification of results is needed (HB171, 2003, p. 21). This verification is consistent with a hallmark of forensic investigation, which is scientific repeatability.

2.5 Digital Forensics Procedure

Digital forensics investigations can be broken down into four distinct phases. These are collection, acquisition, analysis, and presentation (HB171, 2003). Each of these phases must be conducted in agreement with forensic principals and guidelines. Failure to do so has the potential to impact the integrity of collected data adversely. Loss of data integrity can reduce the potential for information to be extracted, and may result in evidence being deemed inadmissible in court (Kent, Chevalier, Grance, & Dang, 2006).

In any forensic investigation it is critical that a chain of evidence be maintained to support the credibility of evidence (Agarwal et al., 2011). The chain of evidence is established as soon as the intent to collect is realised. In RFC3227 Brezinski and Killalea (2002) state that it is required that a chain of custody record the following:

- Where when and whom the evidence is handled, collected, or examined
- Who had custody of the evidence, when they had custody, and how it was stored
- When and how transfer of custody occurs

Brezinski and Killalea (2002) note the importance of maintaining a log of actions undertaken at all phases as well as strong documentation in the form of chain of custody. This requirement is justified by the authors as it is commonplace that court testimony be required years after the investigation took place.

2.5.1 Collection Phase

The collection phase involves the physical gathering of devices from the scene, discovery of any remote or network devices of relevance. In this phase, it is important to ensure that devices are handled in such a way that the data contained within is impacted in a minimal manner (Kyung-Soo & Sangjin, 2008). For instance, there are specific instructions regarding the power state of the device being collected. Certain devices should be powered off using their built-in shutdown functions while others should have power removed from them and others still should remain powered throughout the collection and subsequent processes (ACPO, 2003). Different procedures for handling the power state of devices also exist for specific operating systems that may be running on a particular piece of hardware (Kent et al., 2006).

The network state of devices also plays a pivotal role during the collection and evidence handling processes. In the situation of mobile phones and other network aware devices, it is often required that the network connection is severed to prevent the device from potentially being tampered with over a present network connection (ACPO, 2003). In the case of desktop computers and servers this can be as simple as removing a network cable or significantly complicated due to cloud provisioning arrangements (Delport, Köhn, & Olivier, 2011). Matters are complicated in the case of mobile phones and other devices with wireless network connections. In these cases, it is often recommended that the device is placed in an electromagnetically shielded container (Bennett, 2012). These containers, often referred to as Faraday cages are specifically made in such a way that radio signals cannot penetrate them in such a way to allow communications to occur (Bennett, 2012).

In addition to shutdown procedures, there are a number of other issues to be considered during the collection process. Proper documentation at the scene is a necessity as it may be necessary to be able to show how the devices were connected, where devices were located, as well as establishing the legal right to collect specific items (ACPO, 2003). This documentation can be crucial when establishing who likely had access to the devices in question and who the intended user was. In these cases it is good practice to label each piece of evidence and take clear photographs of the scene, showing these devices with the attached label (ACPO, 2003).

2.5.2 Acquisition Phase

The purpose of the acquisition phase is to obtain a copy of the original evidence so that it can be examined without unnecessary risk of contamination (Baber, Smith, Panesar, Yang, & Cross, 2006). Typically, a copy will be created from the original evidence, and this copy will be used to create further copies, which will be analysed (Noblett, Pollitt, & Presley, 2000). The purpose of this second copy is to reduce the likelihood that the original evidence will have to be acquired again, thus reducing the probability that the original will be contaminated.

The acquisition phase usually concerns the creation of a bitstream or one to one copy of the data contained within the device. Bitstream copies vary from a topical or file system level copy in a critical way. In the instance of a file level or topical copy, the files and folders located on a storage medium are simply transferred over to another storage medium. However, none of the associated data that may be present in free or slack space will be copied (Noblett et al., 2000). The result of this is that the copy is incomplete as there may be significant information in unallocated space, such as remnants of deleted or temporary files (HB171, 2003). In the case of a bitstream copy, each bit of data from the device is copied sequentially starting from the first.

Cryptographic hashing provides means for forensic investigators to prove the integrity of data acquired in the course of an investigation. The principals of cryptographic hashing require that they provide a pseudo-unique consistent, fixed length output for a given input (Kizza, 2015). The characteristics of these algorithms dictate that they be one way in nature, e.g. that no mechanism exists to convert a hash (the output of a hashing algorithm) back to its original source through a reversal of the hashing algorithm itself (Casey, 2009).

In implementation it is not true that cryptographic hashes are unique, given an infinite number of inputs and a fixed length output it is a mathematical certainty that multiple

distinct inputs will exist for which the same output will be produced. These inputs with the same hashes are produced, this occurrence is known as a collision (Rogaway & Shrimpton, 2004). In some cases, means to intentionally produce these collisions have been discovered. In these situations, the hash algorithm is considered to be insecure for ongoing use. To minimise the impact of hashing algorithms being compromised it is considered best practice to use two distinct hashing algorithms whenever hashing data (Thompson, 2005).

To ensure that the acquisition was successful, and the acquired copy is a complete and accurate representation of the original, the technique of cryptographic hashing is often employed (Caloyannides, Memon, & Venema, 2009). Cryptographic hashing is a mathematical process in which an input of any length is inserted into an algorithm, and a fixed length output related to that input is produced (Kessler, 2003). Typically, the original evidence will be processed via the hashing algorithm then an evidence copy taken and both the original hashed and the copy hashed. The hashes would then be compared. By ensuring that the hashes in each case are identical, it can be demonstrated that the original evidence has not been altered in any way and that the copy is a true representation of the original (ACPO, 2003).

2.5.3 Analysis Phase

The analysis phase is based on the examination of the collected data to determine what actions involving the device have taken place. Typically this analysis is performed in conjunction with a collection of tools and techniques used to uncover the actions of a user of a particular system or to discover accurate data to support an investigation (ACPO, 2003).

2.5.4 Presentation Phase

The presentation phase involves the formal presentation of information uncovered during the proceeding phases. The focus is on presenting the evidence in a manner that can be understood by a jury, judge or other legal entities (Köhn, Olivier, & Eloff, 2006). In some cases, the presentation may also include the investigators involved with the investigation (Penrod & Cutler, 1995).

Each of these phases contributes to the overall procedure, and if each has adhered to a conclusive and forensically, sound investigation can be conducted. In each phase, there is a specific requirement for repeatability. Repeatability is important as it allows another investigator to follow the steps taken to verify that the results achieved were accurate and consistent, allowing for a reproducible, scientifically valid result.

2.6 Locational Forensics

Hannay (2007) proposed a method for the forensic acquisition of the TomTom One satellite navigation unit. In this research the researcher determined that the operating system, data files and settings for the TomTom navigation device are stored on an SD card if present; otherwise, these are stored on internal non-volatile flash media. The media can be acquired through traditional methods, such as using a write blocking SD card reader or USB write blocking device and performing the bitstream acquisition using 'dd' or a similar utility.

In a follow up paper Hannay (2008) discusses the analysis of data acquired from the TomTom One. The majority of historical locational data is stored within the *MapSettings.cfg* file for each map used by the device (as such if there are multiple maps installed, there will be multiple *MapSettings.cfg* files present). The *MapSettings.cfg* file contains the home location, recent destinations, and custom locations that have been accessed or saved by the user. A summary of the data stored in *MapSettings.cfg* is shown in Table 2-3. In his work Hannay (2008) makes use of a process taking multiple bitstream copies of the data on the TomTom One device and comparing the differences between these copies with the baseline data set. A verification process then follows to ensure repeatability. Nutter (2008) continues work on the TomTom devices, using a TomTom Go 720 and a TomTom Go and a TomTom Go 910. The results found concur with those provided by Hannay (2008). The research presented by Nutter (2008) does not provide details of the research method used to gather the presented findings.

Cusack and Simms (2011) provide a method for the acquisition and analysis of four Navman satellite navigation units. In their paper Cusack and Simms provide guidance on the usage of propriety software to obtain a bitstream copy of the data on the devices. The acquisition is performed via a USB mass storage mechanism. Analysis is performed through the examination of several XML and log files. Cusack and Simms (2011) identify that the XML files contain details about system state and user interaction, while the log files are NMEA-0183 formatted records containing locational history. The paper does not discuss how the method for analysis was produced or validated, nor does it examine the accuracy of the locational history obtained.

In his master's thesis Arbelet (2014) has produced work for Garmin branded satellite navigation units. In his work Arbelet (2014) adapts the research method outlined by Hannay (2008) to his analysis of the Garmin Nuvi 1340, 2515, and 2595 satellite navigation units. The research found that the Garmin devices record both user interaction and locational history. A high level examination is provided demonstrating that the data

recovered during examination appears to be accurate when compared to the control dataset.

Lim, Lee, Park, and Lee (2014) examine Mappy, a South Korean satellite navigation solution. The research presents a test driven method for the identification of potential forensic artefacts on an embedded system. The method used consists of the repetitive testing, acquisition, comparison, and restoration of the data on the device under examination. Through this process a collection of files altered during use of the device are identified. Subsequent to this identification a semantic analysis is conducted based on the intuition and experience of the researcher to identify and interpret any artefacts of forensic interest. Lim et al. (2014) identify records of both locational history and user interaction stored on the device.

The common theme among these publications is the documentation of forensic acquisition and analysis of a particular satellite navigation unit or line of units. Aside from the work of Arbelet (2014) and Lim et al. (2014), it is noted that none of the literature examined provides background on the development, verification or validation of the forensic techniques outlined. In the case of Arbelet (2014) and Lim et al. (2014), procedure for forensic development were presented, making use of procedures based on those presented by Hannay (2008). In these two cases details of verification and validation of the results are absent, nor is there analysis of the accuracy of the data extracted from the devices.

Table 2-3 Operational Modes of TomTom device and recoverable information (Hannay, 2008, p. 4)

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

3 Research Methodology

In developing the approach to this research, the three components as identified by Creswell are considered. These approaches are philosophical worldviews, research designs, and research methods (Creswell, 2013, p. 5). In this section each of these is discussed in relation to the research undertaken and decision-making process involved in the planning thereof.

Each of the philosophical worldviews (shown in Table 3-1) as defined by Creswell (2013) will be discussed in the section below as to their research methodologies. A summary of each of these worldviews is provided in this section.

Table 3-1 The four philosophical worldviews as defined by Creswell (2013, p. 6)

Post-positivism	**Constructivism**
Determination	Understanding
Reductionism	Multiple Participant Meetings
Empirical Observation & Measurement	Social and Historical Construction
Theory Verification	Theory Generation
Transformative	**Pragmatism**
Political	Consequences of Actions
Power and Justice Oriented	Problem-centred
Collaborative	Pluralistic
Change Oriented	Real World Practice Oriented

Ontology is concerned with that things are, in terms of what actually exists. This concept can be extended to the processes or interactions between entities. In essence, ontology is concerned with the study of reality. Ontological discussions often focus on the debate about the nature of reality, perception, and observation (Cater-steel & Al-Hakim, 2009, p. 37).

Epistemology is the study of the development of knowledge. Specifically, epistemology deals with the concept of processed knowledge. Simple observation is not enough to acquire knowledge, further processing and augmentation are required. With access to a reality, knowledge can be gathered and processed (Cater-steel & Al-Hakim, 2009, p. 38) as long as one has the faculties to comprehend and contextualise their experiences (Kant & Meiklejohn, 1934).

Post-positivism is referred to by a number of terms, including the scientific method, scientific research, and empirical science. The core principle of positivism is that the absolute truth of knowledge cannot be proven (Creswell, 2013). Thus, the greatest

certainty that can be obtained is through the rejection of alternate theories, rather than demonstrating the correctness of a hypothesis (Phillips & Burbules, 2000). Post-positivism holds true that reality is deterministic, with absolute control over cause providing a repeatable effect. As such post-positivist research tends to be quantitative and reductionist in nature (Creswell, 2013).

Constructivism is focused on understanding the views of participants in the research. This worldview is concerned less with the observation of reality and more on analysing the reality perceived by participants in the research (Crotty, 1998). As such constructivist research generally uses multiple participants and relies on analysis of social constructions for theory generation. When examining results, the social and historical context of the participants is taken into consideration in order to aid interpretation (Creswell, 2013).

The transformative worldview found its origins with individuals who felt that the post-positivist or scientific worldview marginalised the oppressed. In order to address this, various communities developed a worldview based on the concept that politics and political change must be embedded within the research paradigm (Mertens, 2010). In contrast to other worldviews transformative research aims to change the lives of the participants, rather than observe for the pursuit of knowledge. The transformative philosophy often calls on participants to be active in all stages of the research, from design through to analysis (Creswell, 2013).

Pragmatism makes use of a plurality of research methods and mechanisms which are selected based on the choice of the researchers (Creswell, 2009). The pragmatic approach allows the researchers to examine the problem at hand and build research methods around research in an iterative manner (Morgan, 2007). Under critical evaluation pragmatism has the weakness of allowing too wide a berth for researchers during research design, which may lead to an overall weakening of the work being undertaken.

In selecting a worldview for the undertaken research, each of the four were considered. As constructivist and transformative worldviews are focused on social research and human participants these are not suitable for this research. Subsequently post-positivist and pragmatic research paradigms may have been appropriate for this research. Post-positivism was selected due to the more consistent framework for inquiry that is provided over the flexibility of pragmatism. As a result of this the ontology of the research is focused on rejecting the hypothesis through a quasi-experimental mode of inquiry. Post-

positivism espouses an observationally focused epistemology, where knowledge is synthesised through the direct observation of reality.

The research was conducted using a quasi-experimental methodology with empirical components. This mixed approach using combined methodology has been selected, as the nature of embedded devices is such that they require data from external sources to determine location. The external data sources were for the most part out of the researcher's strict control. While steps were taken to mitigate the impact of these variables, it was not possible to control all of them due to a number of factors. Firstly, the constant movement of NAVSTAR satellites and environmental changes impact the paths of GNSS signals, causing minor variations in a devices determined location. Other potential sources of locational data such as cellular towers, Wi-Fi access points and the databases that correlate these to geographical locations are maintained and operated by external individuals and organisations. Due to a lack of influence over these external agents, it is not possible reliably to control these variables.

The use of empirical methods is appropriate due to the experimental nature associated with the forensic examination of existing physical objects. The devices being analysed to address the research questions make use of opaque internal processes as part of their core operation. Due to these factors observation of the outcomes and behaviour of these devices is an essential part of addressing the requirements of this research.

There were two sets of data generated as a result of testing. These are a control set and an experimental set. The control set is comprised of recorded locational data. This control set represents the actual location of the device being populated with data at the time.

The chosen research method is the "Nonequivalent Control Group Posttest-Only Design" (Jackson, 2008, p. 348). This method has been selected as of the quasi-experimental designs it is the most appropriate design for this research. This research design is used in research where the assignment of a sample to a group is not random. If we were to consider a clinical trial we could have two groups, one that undergoes treatment and a control group which receives a placebo. In the case of this study being conducted that type of assignment is not possible as the control set of data is generated at the time of experimentation alongside the data to be evaluated. The posttest only design is required as no data at all exists until the test is conducted, both the control set and the experimental set are created at the same time, albeit through different processes.

Equivalent designs are not possible, due to the fact that sources for the data set are not assigned to any particular group at random, nor could they be. The control group is chosen as it is a set of environmental data and is a baseline value not useful for comparison other than evaluating the accuracy of data extracted from the second group. The test group (second group) is comprised of data extracted from tested devices. These devices have undergone the same data population (testing) procedure as the control group. The difference between the groups is that one is the “real location” and environmental data while the other is the “perceived location” based on post-test analysis.

When considering Pretest Only & Combined Pretest/Posttest, it can be concluded that these are not appropriate designs due to the lack of any data prior to testing. Quite simply, before testing has taken place there is no data to collect. Additionally, Single Group designs are not feasible due to the presence of multiple concurrent data sets to be compared. Finally time series designs are not appropriate as there is not a consistently changing data set over a large population of data sources. This method was not deemed appropriate for the research undertaken.

3.1 Variables Impacting on Research Questions

A number of variables exist with the potential to impact on the research questions.

- Make, model and version of selected embedded devices unit(s)
- Identified sources of data for acquisition
- Software and hardware used for acquisition
- Route taken when conducting tests
- Sources of error inherent to the GNSS network(s)
- Significant changes in surrounding infrastructure during the research period
- Free space available on media of selected embedded devices
- Power state of the selected embedded devices during operation and subsequent acquisition
- Functional state of the selected embedded devices during testing

The above are variables that may have impacted on the proposed research. A change in the above variables could have potentially impacted the quality and quantity of recoverable data. These impacts had the potential to delay the progress of the undertaken research. Each of these points have been outlined below and where possible a strategy utilised for mitigation has been outlined.

The make and model of the selected embedded devices has potentially impacted the outcome of the research. This impact is due to the slight variations in the design of both software and hardware that can result in differing sources of data. These variations act as a key validation mechanism in determining the generic use case for the methodology resulting from the research undertaken.

The software and hardware used for the acquisition of devices could cause inconsistencies in the data retrieved. These inconsistencies could potentially arise as different software/hardware could retrieve and/or store the data in a different manner. An example of such an effect is memory-dumping tools that store ECC (Error Correction Code) data compared to those that store only the data itself. To mitigate this issue, a single consistent set of hardware/software tools has been selected for each embedded device.

The route simulated when testing could have a potential impact on the operation of devices due to different route calculation routines. This impact was mitigated by ensuring any data collection took place with each of the devices travelling the same simulated path during testing.

Errors will be present in the perceived location of embedded devices due to identified sources of error in the GNSS network(s) themselves. The error sources encompass both technological issues and atmospheric issues, the average impact in terms of metres variance in perceived location is shown in Table 3-2. To reduce the impact of these errors, a number of known locations will be established based on mapping and geographic markers. Error correction will then be applied based on the average error between these known locations.

Table 3-2 Sources of error in GNSS (Kyung-Soo & Sangjin, 2008)

Error Source	Approx. Impact of error
Ionospheric effects	± 5 metres
Shifts in satellite orbits	± 2.5 metres
Time error in satellite clocks	± 2 metres
Multipath effect	± 1 metre
Tropospheric effects	± 0.5 metres
Calculation and rounding errors	± 1 metre

The impact of changing infrastructure (roads, buildings, and other infrastructure) during the research period is primarily due to multipath effect. The multipath effect is caused by signals bouncing off various objects resulting in multiple copies of the same signal being received or inconsistencies in trilateration due to signals travelling different distances than expected based on a satellite's location. However due to the localised nature of these objects the variance is quite minimal (Kowoma, 2009). In addition to this, the error correction methods outlined in the previous paragraph will serve to mitigate the impact of this issue to the point that any error introduced will be negligible.

The state of the embedded device hardware being tested could potentially have an impact on the data recorded by such devices. This impact would potentially be caused by software or hardware on these systems reacting to differing system states. In order to reduce the impact of this variable, all tests will be conducted with the devices in the power state determined to be the most common for that particular device. For example, an automotive Satellite Navigation unit would be tested in the powered state.

The active function of each device could also cause differing data to be recorded. This impact has already been demonstrated in the TomTom satellite navigation unit, where no historical locational data is recorded if the device is simply displaying current location (Hannay, 2007). In order to address this, issue a number of device functions will be identified and tested for each device where that function exists.

4 Research Questions

The research undertaken was centred around the creation of a framework for the development of procedures that allow for the forensic acquisition and analysis of a selected set of locationally aware embedded devices. The following research questions were developed:

RQ1. Can a standard framework be implemented to develop specific forensic analysis procedures for the selected locationally aware embedded devices?

RQ2. Can the accuracy of historical locational data be determined through a standardised framework for the development of a forensic method?

RQ3. Can the scope of historical locational data available from a device be determined through a standardised framework for the development of a forensic method?

4.1 Hypotheses

For each research question a hypothesis was formed to guide and evaluate the findings of the research:

H1. A standard framework can be implemented that allows the development of specific forensic analysis procedures for the selected locationally aware embedded devices.

H2. The accuracy of historical locational data can be determined through a standardised framework during the development phase of a forensic process.

H3. The scope of historical locational data available from a device can be determined through a standardised framework for the development of a forensic method.

5 Research Design

The research design is split into six main phases:

1. Identification & Selection of Devices
2. Identification & Analysis of Components
3. Develop Testing Procedure
4. Data Population & Collection
5. Developing of Analysis Procedure
6. Testing & Verification

The flow of these phases is illustrated in Figure 5-1. Each subsection of this section is accompanied by a figure illustrating the process undertaken. These are numbered as Figure 5-2 to Figure 5-7.

Phases 2, 3, 4, 5, and 6 form the framework under evaluation. This framework was developed as a potential means through which specific analysis procedures for any given device could be developed. Phases 1 and provides means for sample selection

.

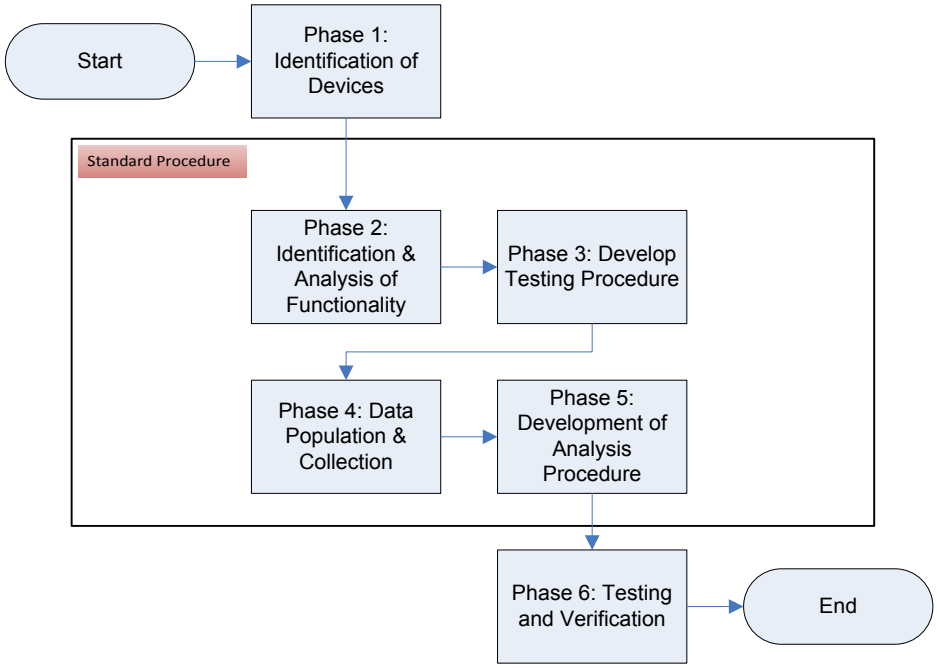

Figure 5-1 Flow chart showing the phases of research undertaken as part of the defined research

5.1.1 Phase 1 – Identification and Selection of Devices

The selection of devices for research was made based on two criteria. The first being market penetration, by selecting devices that are widely used, this research will be of increased relevance for forensic applications. The second criterion is that there are minimal duplicate devices. Devices which have identical hardware and software, were avoided to ensure that the research meets its goals of being applicable over a range of different devices. Finally, time and budget constraints for the acquisition of each device were considered and exclusions made where needed.

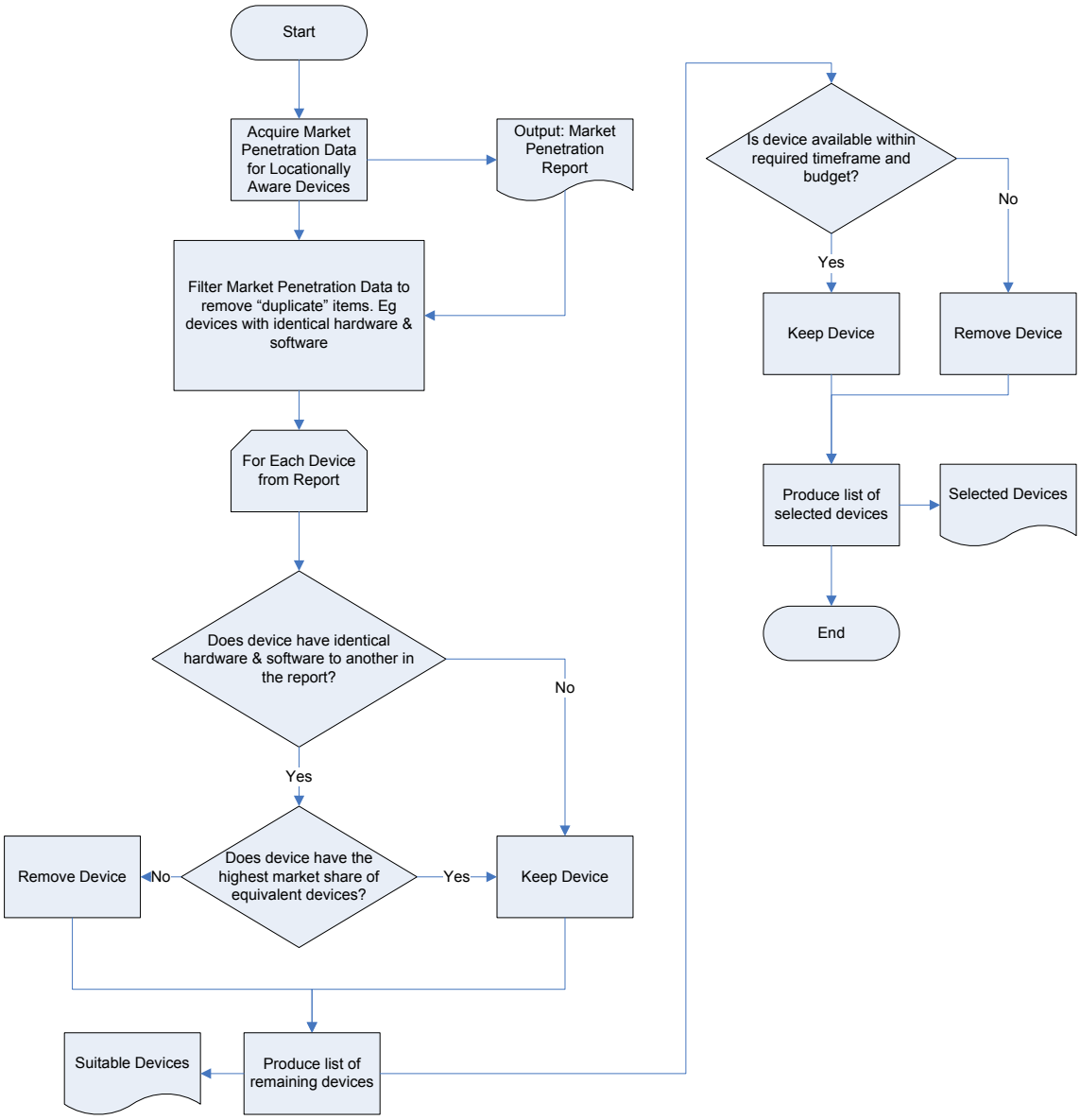

Figure 5-2 Flow chart showing the process for identification and selection of devices to be used in experimentation.

5.1.2 Phase 2 – Identification and Analysis of Functionality

The identification and analysis of components involved a functional analysis of the selected devices. Once the locational functions of the device were determined, these items of functionality were documented. The aim of this phase was to identify potential sources of locational information for each device.

The process began with the identification of each function of the device being examined. This identification was performed through examination of the documentation for the device and practical examination. The practical examination component is critical as device specifications and documentation may not be accurate. It is worth noting that something as simple as powering the unit on was considered an item of functionality for the purposes of this methodology.

Each identified function was examined in order to determine the sources of information utilised by the function. If we consider the functional item of looking up an address, for instance, we can identify a number of information sources. These information sources could be an internal address database, the global positioning system information (used to prioritise close addresses), and a database of previously visited locations. Once the information sources were identified, these sources were examined for the presence of anything that could be used to derive the location of the device. In the outlined example, the current location of the device is such a source of information and as such the item of functionality would have been identified for use in a subsequent phase of the methodology.

The phase concludes once all devices have had their functions analysed and recorded through this process.

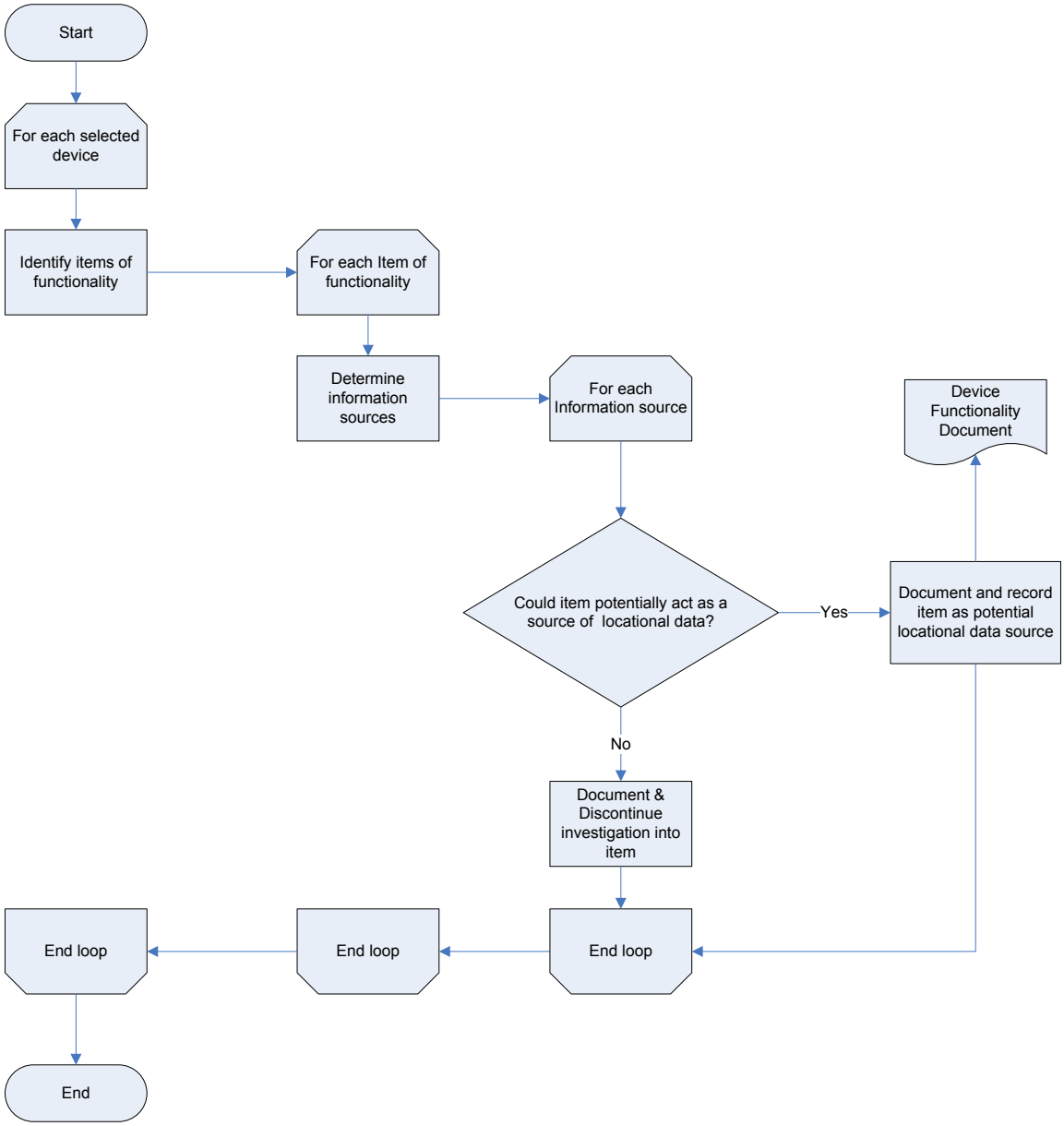

Figure 5-3 Flow chart showing the process for identification and analysis of locational functionality of the selected devices.

5.1.3 Phase 3 - Develop Testing Procedure

The testing procedure was developed which provides inputs for all information sources as identified in Phase 2. In addition, all user interactions required to trigger functionality associated with an information source must be documented. The resultant test plan provides means to ensure accurate and complete testing of the device, which was critical to the development of forensic procedures.

For each of the information sources identified in the previous phase the means to provide external data to the devices in order to support its function and the means to record this data to establish a non-equivalent control were determined. If one were to examine GNSS as an information source, an identified means of feeding input into this system could be the use of a GNSS simulator to provide NAVSTAR signals to the device. The means of providing data forms part of the testing control plan.

In establishing non-equivalent control data collection methods, it was determined how to capture the data provided by a specified input. In the case of a simulator providing NAVSTAR signals, capture, was accomplished via the use of a USB GNSS receiver and appropriate software to record the broadcasted information. This approach was utilised instead of collecting logs from the simulator as it allowed for the determination of the information as it would be received, not as it was intended to be transmitted. These collection methods form the testing control plan.

In order to provide an actionable methodology, a testing action plan was formed. For each item of functionality, the requirements to trigger the item of functionality were defined. One such example for the functionality item “navigate to address” required the device to be powered on and subsequently have an address entered as a destination.

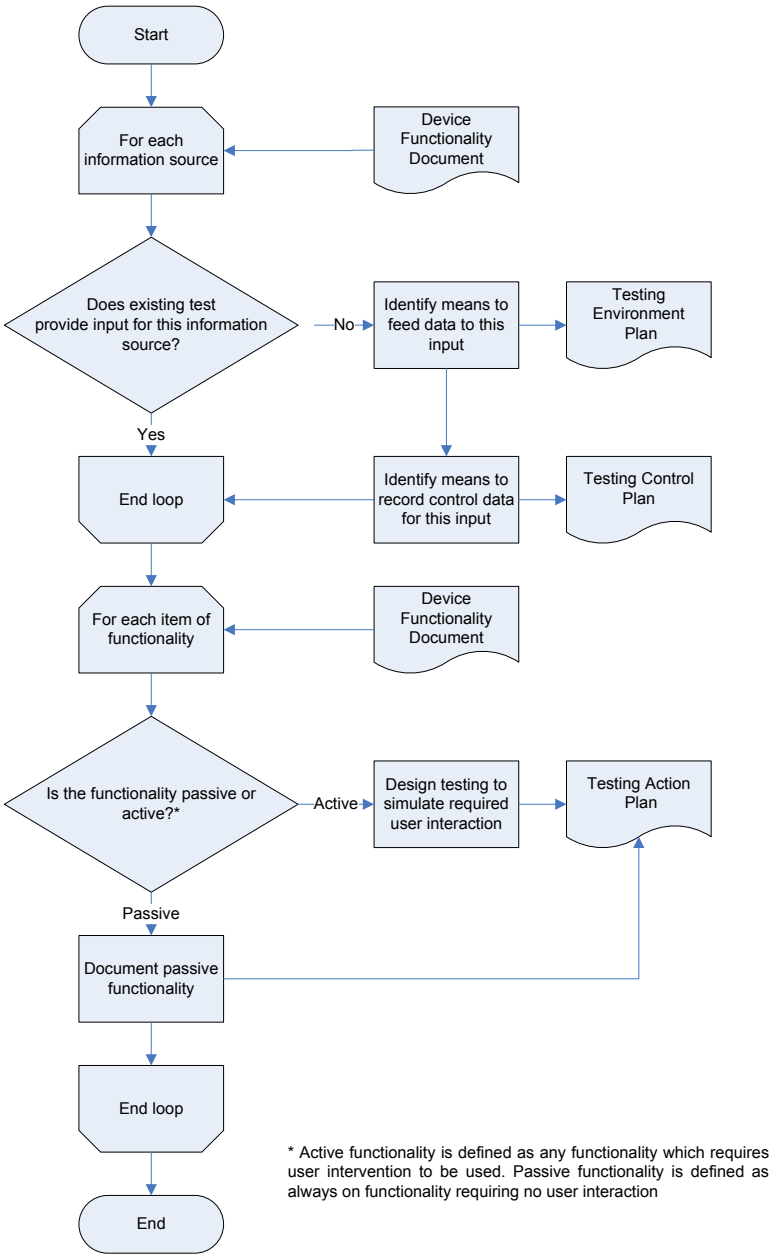

Figure 5-4 Flow chart showing the process to develop testing procedure to simulate locational data and gather control data.

5.1.4 Phase 4 – Data Population and Collection

This phase first involved the creation of a forensic image of the device. This forensic image serves two purposes. First it will act as a baseline state for comparison, and secondly, it will allow the device to be returned to a baseline state. Placing the devices into an environment, which simulated a vehicle driving a specific route, provided means to populate data. The data was then retrieved from the devices, and the devices returned to the baseline states. This phase was repeated five times in order to ensure that any results are verified and consistent.

In all instances where data is restored to, or retrieved from, the device being tested a number of mechanisms are employed to ensure that the data is a complete and representative duplicate of the original. A bitwise copy is made of the media, in this mode, each binary bit of data present on the storage medium is read from the source media and written to the destination media. This means of copying data exists in contrast to topical file system copies in which individual files are copied potentially missing information, which is not present in conventional files. It is possible to make bitwise copies of data even when no file system or an unknown file system is present.

The use of cryptographic hashing algorithms is employed in order to ensure that the data copied is bit for bit identical to the original source data. Hashing algorithms accept source data of any length and apply a one-way mathematical function to produce a pseudo-unique value known as a hash value for any given input. Hashing algorithms and hash values have been used in a courtroom setting as a matter of best practice to verify the integrity and status of images as a genuine and accurate duplicate of the original.

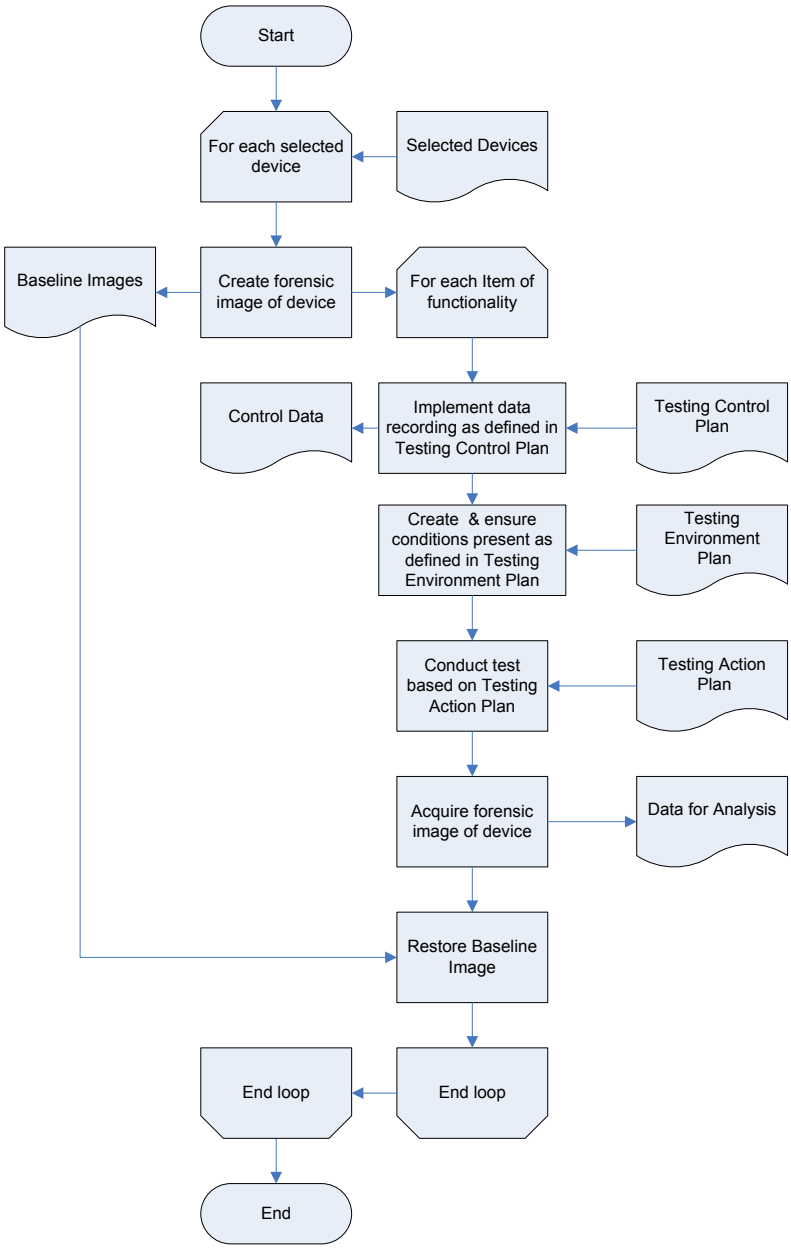

Figure 5-5 Flow chart showing the process for conducting practical testing and collecting the resultant control and experimental data sets.

5.1.5 Phase 5 – Development of Analysis Procedure

This phase involved the analysis of the forensic images collected previously. Each image was compared to the established baseline forensic images. This comparison served as the basis for analysis. These comparisons demonstrate the changes performed by the device during specific scenarios. Identified changes were examined in order to determine the presence of historical locational data. These examinations were focused on the determination of what historical locational data are present and the accuracy of this data when compared to the known historical location during data population. The output of this phase is of forensic analysis procedure for each device.

The result of this phase was the creation of analysis procedure to be used in determining the historic location of each device. In terms of the research being undertaken, the resultant procedure was evaluated to address the defined research questions.

The previously collected forensic images were compared to the baseline image to create a list of differences between the two. The comparison was performed at two levels. First, a binary difference (commonly referred to as a diff) was conducted, determining the exact differences between the images. This approach ensured a complete data set. Second, a logical comparison at the file system level between the two images was conducted to provide enhanced context for the subsequent analysis.

These differences were examined using empirical methods comprised of both literal interpretation of the data presented as well as an analytical approach. The goal of the examination was to ascertain the presence of historical locational data and the structure in which it is stored. The control data was used as part of this process in order to provide context to allow for this analytical approach to be conducted in an informed manner.

Where historical locational data was discovered the means of locating and decoding this data are used to produce an analysis procedure for the associated device. This phase was concluded once an analysis procedure had been developed for all selected devices.

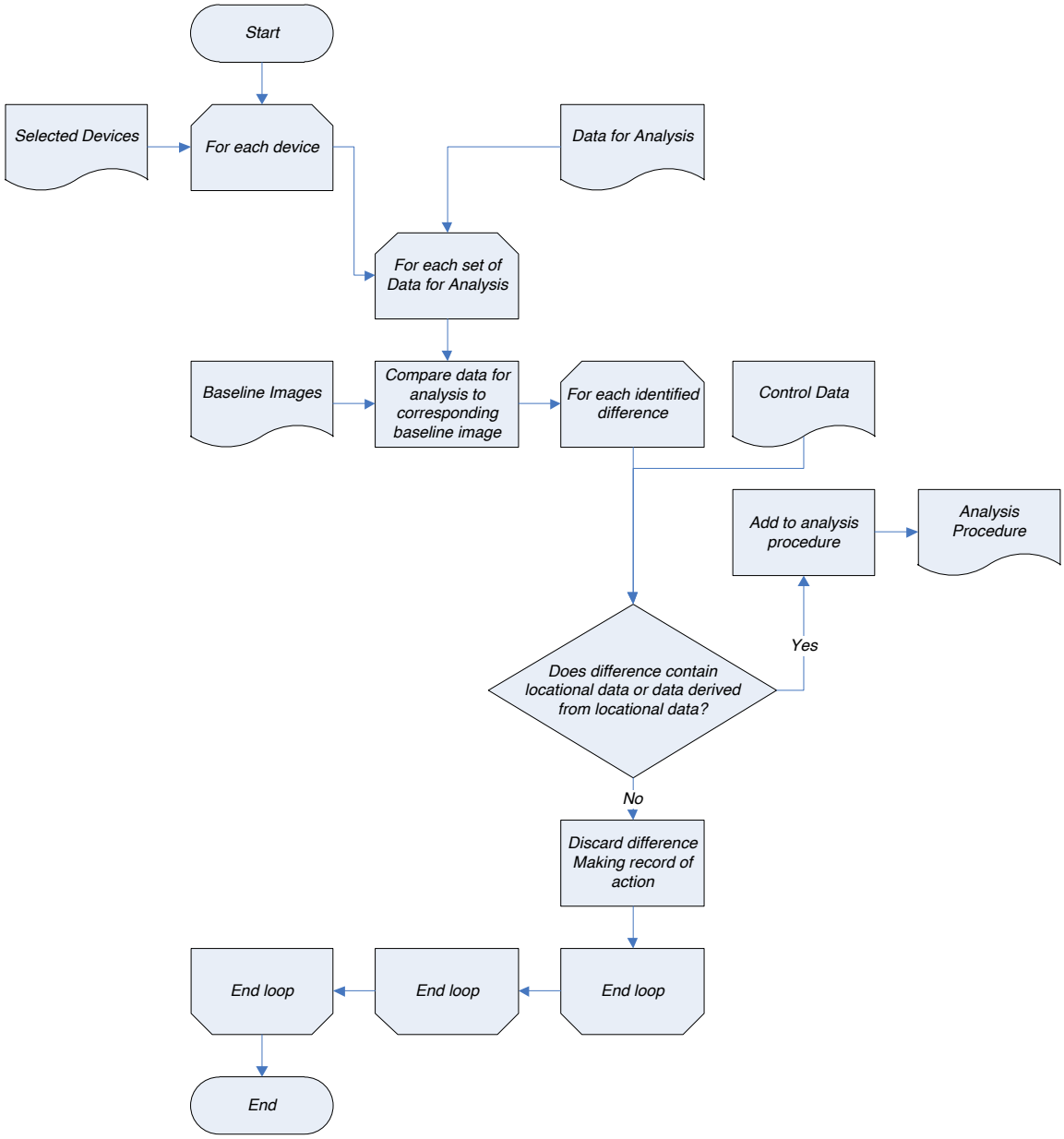

Figure 5-6 Flow chart showing the process through which analysis procedure is developed.

5.1.6 Phase 6 – Verification and Testing

The verification and testing phase are focused on the evaluation of the forensic procedure developed in Phase 5 in order to address the research questions. In this phase, new tests were conducted under the conditions utilised in Phase 4. However, the devices were not returned to a baseline state after each test. The testing, in this case, is used to verify that the procedures are valid and usable in a real world context for each selected device.

The verification and testing phase were actioned through instituting the control action plan, testing environment plan and testing action plan as defined in previous phases. The tests were undertaken in the same manner as in the data population and collection phase with the difference of baseline images not being established or restored in between data population. For the purposes of verification and testing, a number different scenarios were utilised in order to test the wider application of the procedures defined in the previous phase.

For each device the acquired data was analysed in accordance with the defined procedure and the determined historical locations were compared to the acquired control data set. The results of these comparisons were recorded in order to determine the efficacy of the defined procedure.

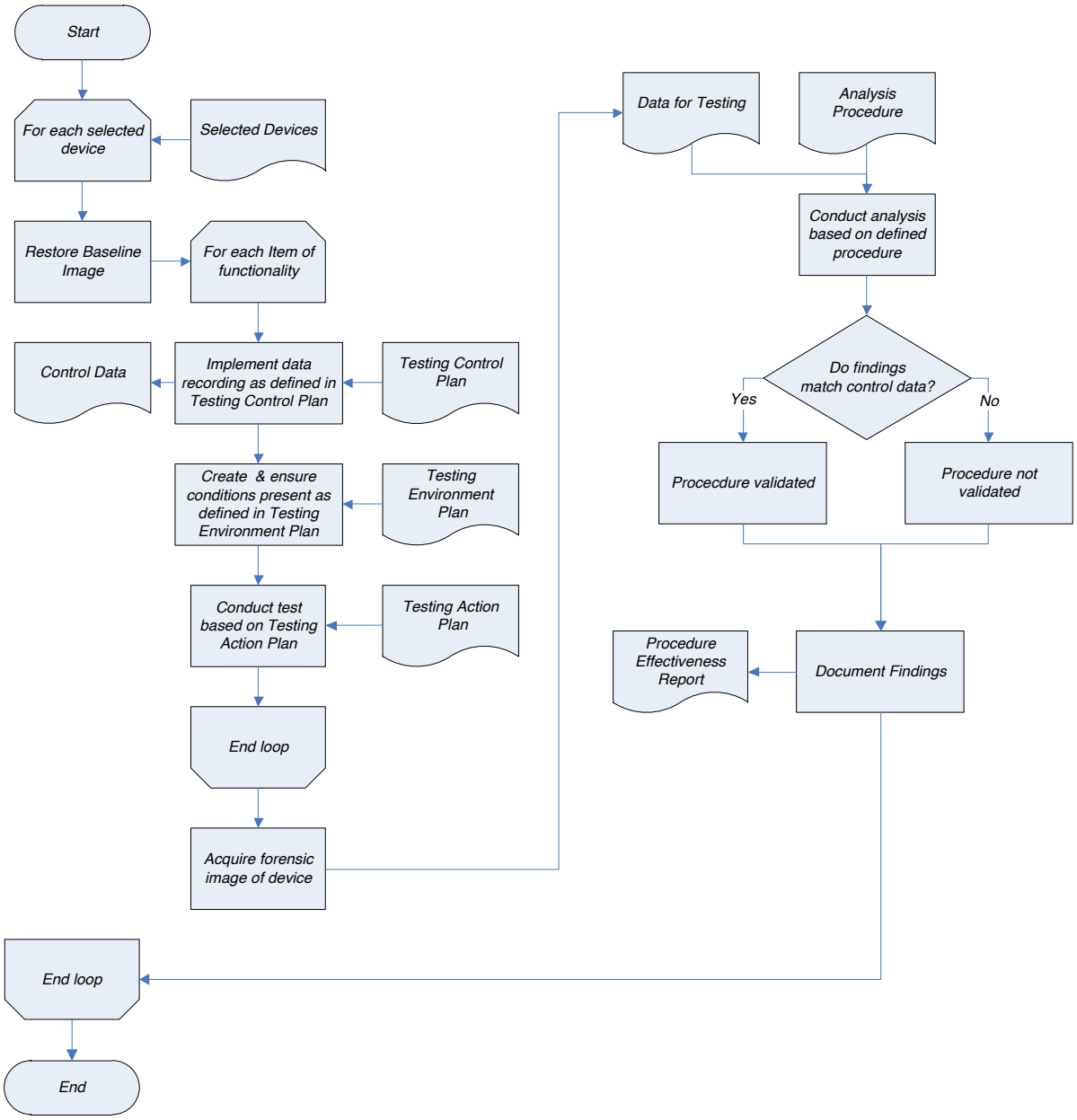

Figure 5-7 Flow chart showing the process for verification and testing of the development analysis procedure.

5.2 Data Collection & Analysis

Data collection was carried out in such a way as to minimise the impacts of the variables outlined in Section 3.1 of this proposal. While Section 3.1 refers to mitigation measures in more general terms, the specifics of implementing these mitigation strategies will be discussed below.

Prior to the data collection process, a baseline image for each of the selected components in the chosen devices will be established. This baseline image will be a factory default version of the data for that specific device. If it is not possible to obtain a factory state for the device, a baseline was established using the most recent version of the software for said device. The purpose of this baseline is to ensure that there is a known state for each of the devices for comparative purposes. The state of the device post-acquisition can then be compared to the baseline in order to determine which data is to be analysed.

Prior to undertaking the research, the means of providing the data utilised by the selected devices for locationing was determined. In the GNSS development community, there are two primary means by which devices are tested during the R&D process. These are open sky and closed sky. These approaches differ based on the use of simulated or real signals to provide the data needed for to determine the device location.

Open sky testing takes place outside the lab making use of the locationing infrastructure present and available for ongoing use. The closed sky evaluations conversely take place in the lab, with all signals simulated via the use of specialised equipment. There are a number of advantages and disadvantages to each of these approaches. We examine the relevant issues in this section.

A key aspect of computer forensics and indeed the scientific method is that procedure should be repeatable. In the case of closed sky testing, there is the possibility to repeat the exact same series of tests without environmental variance. This outcome is simply not possible with an open sky approach. As previously discussed modern GNSS systems broadcast the current time as part of their core operation, as such open sky testing does not allow for repeatability as the times would differ between tests.

Moreover, the presence of environmental factors, atmospheric conditions, unpredictable multipath effects, and infrastructure change during the research period are all factors limiting repeatability. In the closed sky environment, the same inputs can simply be replayed as required.

Closed sky testing allows for research to take place regardless of outside conditions, which may be related to weather, availability of GNSS networks, changes in configuration to these networks, or other unanticipated interference. In terms of a personal risk, perspective closed sky testing provides a significant advantage as there is no danger of traffic accidents or other risks of harm associated with repeated travel via road during the course of research.

A perceived disadvantage to the use of closed sky testing is that simulated conditions may not match those present in the real world. For instance, there may be concern that the absence of open sky phenomena such as multipath effect or adverse atmospheric conditions may limit the relevance of results obtained. This issue was mitigated through the recording and use of open sky data which was later replayed within the lab environment for the majority of testing. The only exception to this was a fixed calibration point used during one test to determine the impact of non-movement on devices. In open sky testing, it is impractical to ensure this level of consistency. This limitation is due to devices perceiving erroneous minor movement due to physical phenomena associated with the locationing technologies.

The primary factor limiting adoption of closed sky testing for GNSS development is cost. The expense related to the construction of an RF shielded environment and acquisition of the required hardware for simulation can be prohibitive. Fortunately, a lab meeting these requirements was available for use during the research period. As such the closed sky option was selected, allowing for the elimination of a significant number of variables which could have potentially impacted on the research.

The specific configuration of control devices and subsequent manipulation of the control data was performed to ensure that an accurate record of locations and times are known for the duration of all data population exercises. The control devices will consist of three GNSS receiver devices capable of streaming NMEA formatted location data; these devices will be connected to a laptop which will record this data in NMEA format. In addition to this one software defined radio will be set to receive raw data from the GNSS network, this device will also be connected to the laptop which will, in turn, be recording the data in the same raw format. Additional control measures will be employed in the form of points on the driven route, which have known latitude, and longitude coordinates. The time at which these points are reached will be recorded so that additional correction can be made to recorded locational data.

The data population process will involve a closed sky approach for the acquisition of GNSS signals; this involves setting up the devices to be tested alongside a number of

receivers for control purposes. Once the devices are set up and configured for acquisition, a predetermined route was simulated in order to populate data to these devices with the required data for later analysis.

The comparison of collected data to baseline data would be conducted by using a utility called “diff” which compares the contents of two files and outputs the differences including the location of these differences within the files. These differences are identified in the raw binary data. The locations of changes output by the diff utility would be used to locate the exact location within the file system (or raw data if no file system present). Once the locations of modified data are known, the analysis would proceed using an intuitive approach based on identifying encoding types, patterns in file structure, and repeated data elements. This method requires examining the data by hand in the raw machine encoded form.

The previously unknown nature of the data to be collected, limited the ability to define specific methodologies for the analysis of acquired data. If locational data is present in the acquired data, it will be compared to the control data to determine the relation of this data to the actual historical location of the device in question. This comparison provides evidence to support the effectiveness of the acquisition and analysis methodology utilised.

5.3 Limitations of the Study

The limitations posed by this project are due to constraints on resources. Primarily it is not possible to exhaustively test all Satellite Navigation devices, and instead, the focus was prioritised for those that were likely to be most relevant to Australian forensic practitioners, while providing the widest possible exposure for testing of the hypothesis.

There are also some limits on the accuracy of control data collected, as outlined in Section 3.1, there are a number of sources of error which may impact the control data set, whilst mitigating steps are taken to address this, there may be some issues in the comparison of data when using the live NavStar network as a source for locational data. In order to mitigate these issues a closed sky approach was utilised.

6 Development of Case Study Parameters

The outcomes of the first three phases are documented in this section. These results have been broken into subsections based on the phase of research in which they were produced. Due to the volume of data produced during the creation of forensic and baseline images, these have not been included. Summary data is provided in place of baseline and test images with sufficient detail to meet the requirements of the research. The execution of the proposed framework is demonstrated through a number of case studies which are included in their own sections.

6.1 Phase 1 – Identification and Selection of Devices

In phase one of the research, a number of devices were selected for analysis. The criteria used to select these were applicability to the study, availability, and a stage of de-duplication. These devices include automotive satellite navigation units aimed at the consumer market.

To be considered applicable to the study, the device needed to have the potential for locational awareness. To meet these criteria, some form of communication with locationing technologies had to be feasible. To this end, any device with inherent locationing functionality was considered relevant to the study. Some the devices do not have such as a core part of their functionality or in some cases any documented part of their functionality. The determination of these devices as potentially locationally aware was made solely through the presence of I/O mechanisms that have the potential to support the determination of location.

The devices available and considered applicable to the study were as follows in Table 6-1 below.

Table 6-1 A table showing the devices available for inclusion in the study, listed by the manufacturer, model, and serial number.

Device Classification	Manufacturer	Model	Serial	Selected
SatNav Unit	TomTom	One v2	23537M00036	Yes
SatNav Unit	Uniden	GNS8365	X11-15302	Yes
SatNav Unit	Navman	S80	B6587M04611	Yes
SatNav Unit	Navman	S50	B5Y7BM05687	No
SatNav Unit	Navman	F15	BGB8CM01149	No
SatNav Unit	Pioneer	AVIC-S2	GICZ000198AU	Yes
SatNav Unit	Laser	GPS-3.5	L608818015A	No
SatNav Unit	Laser	GPS-3.5	L608816984A	No
SatNav Unit	U-Route	Q800	Q800201512280156	Yes

A number of these devices were eliminated in the de-duplication process. In the case of two devices of the same brand where both devices were running the same software, a determination was made that these are duplicates and provided little value to the study. As such the subsequent device was eliminated from the sample set. The Navman S50 and F15 were removed from the list as they ran the same operating system as the Navman S80. Both of the aforementioned units were similar in functionality to the S80 and provided no additional functionality or unique characteristics which would have made them relevant to the research being undertaken. The two laser branded units were excluded from testing as both were non-functional and could not be repaired or replaced due to the non-availability of key components.

6.2 Phase 2 – Identification and Analysis of Functionality

The functional components of each item of each device were of critical importance to the study as they directly dictate what inputs are required to accurately simulate an open sky scenario. For each device selected in the previous phase, the functionality of the devices was examined. Where the functional items provided means for locational awareness, these were noted and provided in the device functionality report.

The functional items for the devices selected were categorised in terms of the general purpose of these items. These categories are primary locationing, networking, cellular, images and apps/features. The purpose of each of these is outlined in Table 6-2 below.

Table 6-2 Descriptions of the broad categories of functionality used to define individual functions of the selected devices.

Category	Description
Locationing	Technologies with the core purpose of enabling locational awareness.
Networking	Technologies with the core purpose of enabling network communication. These may still provide means for locational awareness through IP-based or other locationing techniques.
Cellular	Technologies to enable cellular communication. In cases where cellular technologies provide implicit locationing support, these are still categorised as cellular.
Images	Features allowing the capture or viewing of images.
Apps/Features	Specific applications or additional features implemented for the device being examined.

Each item of functionality found was classified into the appropriate category. The items of functionality and the category under which they were classified are shown in Table 6-3.

Table 6-3 A description of identified features for the selected devices, sorted by category

Category	Feature	Description
Primary Locationing	NAVSTAR	A GNSS system providing locational services
	GLONASS	A GNSS system providing locational services
	Galileo	A GNSS system providing locational services
	Beidou	A GNSS system providing locational services
Cellular	UMTS	Universal Mobile Telecommunications System, a third generation cellular protocol allowing for data, voice, and AGPS
	GSM	General System for Mobile Communications, a second generation cellular protocol allowing for data, voice, and AGPS
	HSPDA	A third-generation cellular data protocol, allowing for data transfer and AGPS
	GPRS	A second generation mobile data protocol, allowing for data transfer and AGPS
Images	Camera Front	The presence of a front facing (towards the user) camera
	Camera Back	The presence of a rear facing (away from the user) camera
	Image Viewer	The ability to view images on the device

6.2.1 Cumulative Functionality Report

Primary Locationing	**NAVSTAR**	**GLONASS**	**Galileo**	**Beidou**
	Yes	No	No	No
Networking	**Wi-Fi**	**Ethernet**	**Bluetooth**	**NFC**
	Yes	No	Yes	No
Cellular	**UTMS**	**GSM**	**HSPDA**	**GPRS**
	No	No	No	No
Images	**Camera Front**	**Camera Back**		
	Yes	No		

6.3 Phase 3 - Develop Testing Procedure

The execution of Phase 3 resulted in the creation of a testing environment, control, and action plan. Each of these is included in this section along with the specific details of the environmental configuration. The plans included here are the generic overarching plans which are consistent for each of the case studies conducted. Where a case study required specific variation, these are documented in the individual case studies. In addition in-depth explanation of the testing environment is provided in Section 6.3.1 below.

6.3.1 Testing Environment Details

6.3.1.1 GNSS Data

Of the GPS technologies the only mechanism employed by any of the chosen devices is NAVSTAR. As such a LABSAT2 and compatible amplifier, antennae pair was used to meet the broadcast requirements. The LABSAT2 is a device capable of broadcasting NAVSTAR and GLONASS signals to simulate a route being traversed. The LABSAT2 operates in two primary modes. The first is a simulated route in which map locations and speeds are selected, the device software then determines signals to broadcast to facilitate the simulation. The second mode of operation uses a recording of an actual route being travelled and replays the NAVSTAR & GLONASS signals from this journey. For the purposes of this study, the simulated route mechanism was chosen. Through this mechanism, we eliminate multipath effect and signal degradation from atmospheric conditions.

A mechanism for gathering control data is established through the use of an off the shelf NAVSTAR capable GNSS receiver. In this case, a BU-353-S4 device is used for this purpose in serial mode. In this mode, the device provides NMEA-183 formatted data via a serial interface to a computer system configured to record this data.

6.3.1.2 Networking Data

The cumulative networking functionality identified for the devices is comprised of Wi-Fi, Ethernet, and Bluetooth, each of these mechanisms is addressed in this section. For each mechanism, a means of simulating the required input is provided. Location can be determined from these via IP-based geolocation or in the case of Wi-Fi through the use of public databases of BSSIDs against geographical coordinates.

IP-based connectivity is provided by a router which simulates public IP addresses and routes traffic to the public Internet via NAT mangling. The current simulated location was looked up in the GeoLite2 open IP geolocation database, and an IP address within the range for that location is randomly selected and used until the locale changes. Traffic from the devices is routed to the public Internet via means of NAT mangling. A control data set is simple to achieve in this instance, as it is simply a matter of logging the IP addresses chosen for simulation. All data transmitted via the router is recorded in a PCAP packet dump to provide completeness of data for analysis purposes.

Wi-Fi data input exists by two mechanisms, one each to address the different types of geolocation mechanism commonly employed in the course of Wi-Fi locationing. The first mechanism examines the BSSID broadcasts received by the device and makes use of Wi-Fi locationing services to determine position. To provide BSSID positioning data, the chosen route is travelled and the BSSIDs encountered are logged. The logged BSSIDs are then broadcast when the simulation reaches the appropriate location. The broadcast itself is transmitted via a USB Wi-Fi device in conjunction with the MDK3 software. The second mechanism of locationing via Wi-Fi makes use of IP addresses assigned to the devices after successfully establishing a connection to a known Wi-Fi access point. In order to address the IP-based mechanism, the device is configured to connect to a wireless access point attached to the router outlined in the previous paragraph. The control data set for both of these positioning mechanisms is produced via the use of an additional USB Wi-Fi devices set up to log wireless data using the Wi-Fi sniffing software KISMET.

Bluetooth locationing is currently performed solely through the use of IP-based mechanisms. As such a system is configured to provide a Bluetooth networking bridge to the router addressed previously in this section. Control data for this is provided via the same logging mechanism employed by the router mentioned above.

6.3.1.3 Cellular Data

Cellular technologies identified within the devices are based on a number of differing communication standards. These are GSM, UTMS, and HSPDA. The cellular broadcast software and hardware used for this research is only capable of GSM transmission, on the surface, this presented issues as far as the research method is concerned. On further analysis of the devices selected it was determined that each of these in the absence of UTMS and HSPDA will fall back to using GSM functionality if available. As such for the experiment, the decision was made to address the GSM mechanism only and rely on this fall-back mechanism.

The broadcast of cellular network identifiers is accomplished through the use of the Universal Software Radio Peripheral 2 (USRP2) and OpenBTS software. The USRP2 acts as the hardware platform, in this case, providing a software interface to radio transmission and receiver hardware. To use the USRP2 for our purposes, we must make use of compatible software, which is capable of instructing the device to broadcast cellular network IDs at intervals appropriate for the current simulated location. We perform this task through the use of OpenCellID database, for each simulated location

determining an appropriate set of cellular tower network IDs to broadcast. The OpenBTS software is then instructed to facilitate these broadcasts via the USRP2 hardware.

A control data set is attained through the use of a mobile phone set to record cellular ID broadcasts. This data set then forms the basis for comparison against any data collected during experimentation.

6.3.2 Test Control Plan

This plan provides means for the collection of control data whilst locational simulation is undertaken. The outputs of this process are discussed in the individual case studies.

1. Confirm RF Isolation - Use a spectrum analyser to observe spectrum in the 1.8 GHz, 2.4ghz, and 850mhz ranges. If signals above background noise levels are detected immediately, halt testing.
2. Trigger GNSS cold start - Execute *cold-start.py* on Linux PC to reset the internal state of GNSS receiver.
3. Commence GNSS control data collection - Commence GNSS monitoring and data logging. Observe state of GNSS cluster to ensure that satellites are detected but no data is being transmitted.
4. Establish WiFi Control - Enable *kismet* to capture WiFi traffic.
5. Commence packet capture - Enable packet logging on the router.
6. Complete the test action plan, and resume the test control plan once complete.
7. End GNSS control data collection - End GNSS monitoring by pressing Ctrl+C. Perform MD5 and SHA256 cryptographic hash algorithms over the produced data and store appropriately.
8. End WiFi control data collection - Close *kismet* by pressing Ctrl+D. Perform MD5 and SHA256 cryptographic hash algorithms over the produced data and store appropriately.
9. End packet capture - Disable packet capture logging on the router. Download files from the router, then perform MD5 and SHA256 cryptographic hash algorithms over the produced data. Store the captured data appropriately.

6.3.3 Test Action Plan

The testing action plan was devised to trigger any needed interactive elements of the device functionality. This section outlines both the general steps taken and the steps taken for three scenarios utilised to analyse the forensic impact of various interactions.

1. Restore device to baseline state.
2. Confirm restore through the use of appropriate cryptographic hashing algorithms.
3. Power device on and ensure boot process succeeds.
4. Monitor location acquisition process during the no-motion period of simulation. Abort test if location is not aquired, restart testing after the issue is resolved.
5. Conduct testing as per specific scenario being undertaken.
6. Power device off at end of scenario.

6.3.3.1 Scenario A – Non-Interactive

1. Do not interact with the device

6.3.3.2 Scenario B – Interaction with movement

1. After simulated movement has commenced search for an address that exists within the devices database
2. Observe device to determine when simulated movement ceases
3. Cease interaction

6.3.3.3 Scenario C

1. After location fix has been acheived search for an address that exists within the devices database
2. Cease interaction

6.4 Phase 4 – Data Population & Collection

The data population and collection portion of the case study include details on the case study specific portions of the processes involved in preparing the devices for experimentation and collection of data post experiment. The processes followed here are fairly generic across the devices with some minor deviation. Any deviation from the following is outlined and explained in each case study.

Prior to the commencement of testing, it was required that for each device a means to restore them to a baseline state was established. Wherever possible within the parameters of the research this should be a bitwise copy of the internal data storage of the device being examined. In situations where this is not possible, a topical extraction of files was performed in place of the bitwise copy. The implications of this limitation as it applies to the research are understood.

The bitwise acquisitions were conducted using a utility named *dcfldd*. This utility is a fork of the *dd* program which allows for bitwise reads and writes to and from block devices and files. The differences between *dcfldd* and *dd* are in the form of added functionality, in this case, the ability to easily see the progress of the data acquisition process and to perform cryptographic hash functions simultaneously.

dcfldd was used in order to acquire these bitwise copies via the USB mass storage interface present on the device or in cases where storage was via an SD card was present the same process was used via a USB to SD adapter. In the case of acquisitions write blocking mechanisms were utilised in order to prevent unintended contamination or alteration of the data present on the storage media. Hashes were recorded whenever an acquisition or restore took place and confirmed to be as expected.

Before each iteration of experimentation, each device was returned to its baseline state through the use of the *dcfldd* utility or via a topical file restore where direct access to the device storage was not possible. During the restoration process, the integrity of the data was confirmed via the use of cryptographic hashing.

Subsequent to experimentation the devices were acquired via the use of the *dcfldd* utility and were cryptographically hashed. The aquired files and computed hashes were recorded and stored in multiple locations. The control data from the WiFi and GNSS sources was taken after each round of testing, cryptographically hashed, labelled and stored in multiple locations alongside the experimental data.

6.5 Phase 5 – Development of Analysis Procedure

The procedure outlined in phase 5 were undertaken and documented as part of each case study. In this section, we examine how the process is conducted and the tools utilised. The goal of this process is to generate forensic procedure that can be followed in order to determine the locational history of the device under examination.

Each case study follows the same process for development of analysis procedure as defined in Section 5.1.5. In practical terms, the examination of the files was performed through the use of the *dhex* utility. *dhex* is a utility that provides details of differences within binary files. Each differing section was examined using the *sleuthkit* utility to determine if the modified area was currently allocated to a file. In the affirmative case, the file is noted and is examined as a whole. In the negative case the addresses of the altered data are noted and are examined as is.

The examination of differing files was conducted using the *difffork* utility. *difffork* visually shows the difference between two files. The difference is examined to determine if it has the potential to contain historical locational data. If this is confirmed the structure of this data was defined and analysis procedure was written as required.

In some instances, the data appeared to be random or of unknown format. In such instances the entropy of the data was calculated using the *binwalk* utility. *binwalk* performs a number of functions related to the analysis and unpacking of unknown binaries. If the data showed uniformly high entropy throughout it was assumed that the data is random or encrypted and is discarded from the study. It is accepted that there may be potential for information of use to be located within. However cryptographic attacks were deemed out of scope for this study, this is noted as a limitation.

If the data being examined is not uniformly random and is not of known purpose, then experimentation would have continued in order to increase the number of variations available. It should be noted that this contingency did not arise during the research undertaken.

6.6 Phase 6 – Verification and Testing

The testing and validation phase of the case studies aim to examine the validity of the generated forensic procedure for each device. This validation was conducted through the restoration of each device to baseline and then the new simulation was executed.

The reason for this is to determine the fitness for purpose of the developed procedure outside of the simulations used in the development of the procedure.

The data from the devices is acquired through the same process as was utilised during testing, with hashes being taken and noted. Rather than engage in comparative analysis in this instance the procedure is followed and the results compared to the control data set acquired during the validation simulation.

The nature of the comparison is highly dependent on the availability of historical location as determined during the previous phases. In the case of points of location in the form of date and coordinate pairs (or any data from which this can be derived) a comparison takes place to determine the variance in metres between the control and experimental data at each given point in time. Statistical analysis is performed to determine the correlation coefficients between the time series data collected for both control and experimental data sets. Descriptive statistics are produced for the geodesic distance between the two sets. Where the difference exceeds the cumulative error shown in Table 3-2 the cause of this was investigated. These cases are examined individually in the case studies that follow and the interpretation of the results is presented in the discussion section.

At the request of the author,

Chapters 7 – 11 are not available in this version of the thesis.

12 Results

In this section we examine the output of the experimental work carried out in relation to the hypotheses and research questions provided in Section 4. The implications of the research undertaken are discussed in terms of impact on the field outside of the primary research, as well as providing a critical examination of the research process as it was undertaken.

12.1 Outcomes of Research Questions

A hypothesis was derived for each of the research questions that were defined in Section 4 of this thesis and these research question and hypothesis pairs are presented in Table 12-1. These hypotheses were evaluated through the processes defined in Section 5 and the results shown in the case studies. The goal of post-positivist research is to test the null hypothesis (a situation in which we predict that the independent variables have no effect on the dependent variable) through experimentation in order to answer the research questions. This section examines the relationships between the research questions, hypotheses and results in light of the outcomes of the experimentation.

Table 12-1 The research questions examined and the derived hypothesis evaluated throughout the course of the research. Shown are the research questions with their corresponding alternative and null hypotheses.

Research Questions	Alternative Hypotheses (H_1)	Null Hypotheses (H_0)
RQ1. Can a standard framework be implemented to develop specific forensic analysis procedures for the selected locationally aware embedded devices?	H1. A standard framework can be implemented that allows the development of specific forensic analysis procedures for the selected locationally aware embedded devices.	$H1_0$. A standard framework cannot be implemented to allow the development of specific forensic analysis procedures for the selected locationally aware embedded devices.
RQ2. Can the accuracy of historical locational data be determined through a standardised framework for the development of a forensic method?	H2. The accuracy of historical locational data can be determined through a standardised framework during the development phase of a forensic process.	$H2_0$.The accuracy of historical locational data cannot be determined through a standardised framework during the development phase of a forensic process.
RQ3. Can the scope of historical locational data available from a device be determined through a standardised framework for the development of a forensic method?	H3. The scope of historical locational data available from a device can be determined through a standardised framework for the development of a forensic method.	$H2_0$. The scope of historical locational data available from a device cannot be determined through a standardised framework for the development of a forensic method.

12.1.1 RQ1: Can a standard framework be implemented to develop specific forensic analysis procedures for the selected locationally aware embedded devices?

In order to answer this question, we must first examine the conditions that must be met in order for the null hypothesis to be rejected. H1 contains a number of statements which are broken down and required conditions presented below. The effectiveness or accuracy of the framework is not examined in this section, as these items are addressed by RQ2 and RQ3.

C1. A framework was developed;
C2. Specific forensic analysis procedures for the selected devices resulted from the framework being executed;
C3. The selected devices were locationally aware;
C4. Where available, the analysis procedures yielded an output of locational history.

C1 requires that a framework was developed. Indeed, a framework was created and explained as a component of the research design in Section 5 of this thesis. Specifically Phases 2, 3, 4 and 5 of the research design comprise the entirety of the framework. While phases 1 and 6 serve to select the devices to be evaluated and validate the framework. As the framework does indeed exist the null condition for C1 has been rejected.

Through the execution of the framework the null condition of C2 was rejected. This finding is demonstrated through the development analysis procedures which resulted from implementation of the developed framework. The resultant procedures can be found in Sections 7.5.2, 8.5.2, 9.5.2, 10.5.2, and 11.5.2.

C3 concerns the selection criteria for the devices, in that they must be locationally aware. The first stage of the selection process is defined in Figure 5-2. The data presented in phase 2 of each case study provides the functional breakdown of each device as it applies to locational awareness. Specifically, Table 7-2, Table 8-2, Table 9-2, Table 10-2, and Table 11-2 list the identified locational functionality for each device. The null condition for C3 would require that at least one of the devices have zero items of locational functionality. For each of the devices there is at least one item of locational functionality identified. As such the null condition for C3 has been rejected.

C4 requires that execution of the analysis procedures requires an output of locational history, unless no such history is stored on the device. Table 12-2 below provides a breakdown of the number of locational history items that were extracted from execution of the analysis procedure. All case studies and scenarios resulted in locational results being provided, with the exception of Case Study 2, Scenario B. In this case there were no items of locational history retrieved, the cause for this result was identified as the device not storing locational history while not under motion. The Garmin Nuvi 2360 does not record locational history while it is not in motion. As this scenario was a simulation of the device remaining still while receiving locational signals, it did not record any locational history. In contrast to this, scenarios A and C both simulated movement, and as such resulted in locational history being recorded and subsequently recovered. The implication for C4 is that the null condition is rejected.

As the null condition has been rejected for C1, C2, C3, and C4, the alternate hypothesis for H1, “A standard framework can be implemented that allows the development of specific forensic analysis procedures for the selected locationally aware embedded devices.” is accepted.

Table 12-2 The presence of locational history for each case study and each scenario undertaken. The values presented indicate that it in all cases where locational data was stored by the device, that data was successfully retrieved.

Case Study	Test Scenario	Location Data Retrieved
1 – Navman S80	A	Yes
	B	Yes
	C	Yes
2 – Garmin Nuvi 2360	A	Yes
	B	N/A (Not Stored)
	C	Yes
3 – Pioneer AVIC-S2	A	Yes
	B	Yes
	C	Yes
4 – TomTom One	A	Yes
	B	Yes
	C	Yes
5 – U-Route Q800	A	Yes
	B	Yes
	C	Yes

12.1.2 RQ2: Can the accuracy of historical locational data be determined through a standardised framework for the development of a forensic method?

To evaluate RQ2 the corresponding hypothesis was separated into its component parts. Which are presented below, each of these will be addressed individually in this section. H2 was split into three components, one concerning the development of a framework, another focused on the production of accuracy information and the final focusing on the reliability of the information itself.

C1. A framework was developed
C2. Specific forensic analysis procedure for the selected devices resulted from the framework being executed
C3. Execution of the framework provided details concerning the accuracy of data

The outcomes for C1 and C2 were previously addressed in Section 12.1.1, where it was determined that the null condition was rejected. Given that C1 and C2 are consistent between RQ1, RQ2 and RQ3, they will not be discussed in this section.

In evaluating C3 we must examine the null condition; that execution of the framework provided did not provide details concern the accuracy of data. In execution of the framework, specifically Phase 6, the accuracy of all experimentation was examined, using the two simulations examined during development of the procedure and a third simulation which had not been used for development. The purpose of the third simulation was to ensure that any developed procedure was not limited to those scenarios and locations which had been examined for the process of development. As such the third simulation was of a route being travelled through a different geographical area, many thousands of kilometres from either of the developmental simulations. In this case the third simulation can be utilised as verification of accuracy findings of the developmental process.

In case study 1, the Navman S80 was examined, developmental findings indicated two-tailed Spearman's Rho and Kendal's Tau correlations between the control and experimental data sets, with values between 0.997 and 0.999 (see Table 7-13, Table 7-14, Table 7-16, and Table 7-17), indicating significance exceeding the 0.01 level. There were differences detected in both samples, in line with what would normally be expected for the analysis of raw NMEA feeds, which would normally be smoothed and processed by a host application. When evaluating the non-developmental scenario these values were found to be in line or better than that of the developmental samples. In this case

Spearman's and Kendal's correlations of and 0.999 and 1.000 respectively (see Table 7-19 and Table 7-20).

Continuing this investigation with case study 2, the Garmin Nuvi 2360 was investigated. In this case correlations between 0.977 and 1.000 (see Table 8-14 and Table 8-15) were found in the first developmental simulation. The second developmental simulation yielded no result in this case, as the device was found to not record locational history while not in motion. The non-developmental scenario yielded correlations between 0.997 and 1.000 (see Table 8-18 and Table 8-19), exceeding that of the developmental scenarios.

The third case study examined the Pioneer AVIC-S2. In scenario A, correlations of between 0.796 and 0.943 were observed (see Table 9-14 and Table 9-15). Whilst scenario B saw correlations of between 0.176 and 1.000 (see Table 9-17 and Table 9-18). In examination of the non-developmental scenario C, we saw correlations between 0.997 and 1.00 (see Table 9-20 and Table 9-21). As can be seen the correlation for non-developmental scenario C exceeded that of the developmental scenarios.

In the fourth case study the TomTom One was examined. This unit was unique in the selected devices in that it does not provide a locational history beyond the last known location. In this case there is not enough data to perform a meaningful statistical evaluation. As such the distances between the control and experimental data sets. Scenario A saw a distance of 11.83731 metres and scenario B saw a distance of 7.715252 metres (see Table 10-13 and Table 10-15). In the non-developmental scenario C, a distance of 7.958952 metres (see Table 10-17) was observed between the control and experimental data. In this case all of the values were below what are considered acceptable error thresholds by GNSS networks under normal conditions.

The final case study evaluated the U-Route Q800. The procedure developed for this unit yielded correlations of between 0.996 and 1.000 for Scenario A (see Table 11-11 and Table 11-12). Scenario C yielded correlations of between -0.19 and -0.316 (see Table 11-14 and Table 11-15). Given that scenario B is a still simulation and any divergence from a single point is due to GNSS or equipment errors, this negative correlation does not impact the results, as there is no valid change to correlate between the data sets. The difference from the control in scenario B never exceeded 7.131484 metres which is below the variance from errors within GNSS networks under normal circumstances. While the developmental scenario C yielded correlations between 0.996 and 1.000 (see Table 11-17 and Table 11-18).

In all cases the non-developmental scenario (scenario C) yielded more accurate results than the developmental scenarios A and B. As such the data suggests that it is possible to determine an expected maximum error. Through consideration of the correlations observed, or in the case of still simulations, the distance from the control, the null condition that “execution of the framework provided did not provide details concerning the accuracy of data” is rejected and the alternative hypothesis “H2 The accuracy of historical locational data can be determined through a standardised framework during the development phase of a forensic process.” is accepted.

12.1.3 RQ3: Can the scope of historical locational data available from a device be determined through a standardised framework for the development of a forensic method?

In order to address RQ3, we must address the null hypothesis that it is not possible to determine the scope of historical locational data available from a device via the use of a standardised framework for the development of a forensic method. In order to reject the null hypothesis, we must demonstrate that there exists a framework, that when executed results in a method which can provide the scope of locational data available. Breaking this requirement into its components we determine the following conditions to be met:

C1. A framework was developed
C2. Specific forensic analysis procedure for the selected devices resulted from the framework being executed
C3. The framework provides a determination on what historical locational data can be recovered from each specific device

The outcomes for C1 and C2 were previously addressed in Section 12.1.1 where it was determined that the null condition was rejected. Given that C1 and C2 are consistent between RQ1, RQ2 and RQ3, they will not be discussed in this section.

In order to reject the null condition of C3 we must demonstrate that cases exist where the framework is able to determine the scope of what can be recovered from a device. In phase 5 of the research each change between the device prior to and subsequent to experimentation and the potential for each change to have historical locational potential is examined. It is worth noting that not all items of locational significance are included in the developed forensic method. In a number of cases where multiple records of significance exist, the most accurate is chosen. A summary of the locational history

recovered is presented in Table 12-3. In examining this table, it can be seen that for each device it was determined what type of locational history was available for the devices examined. As the pre and post-test comparisons were exhaustive the null condition of C3 is rejected.

Table 12-3 A summary of the locational history available from each device selected.

Device	NMEA logs	Full locational history	Last known location	Historic destinations
Navman S80	Present			Present
Garmin Nuvi 2360		Present		Present
Pioneer AVIC-S2		Present		Present
TomTom One			Present	Present
U-Route Q800		Present		Present

12.2 Summary of Research Questions

In Section 12.1 each research question and its corresponding hypothesis were evaluated. In this section we summarise the results of this examination. In Table 12-4 the research questions, corresponding hypotheses and conditions. These items are presented alongside the outcome of the evaluation of the condition. All null conditions were rejected, with the exception of C4 for RQ1. In this instance the null condition and thus the null hypothesis could not be rejected as under a specific test the unit output no locational history. In this case the framework identified this limitation of the device being examined and as such the limitation was known prior to non-developmental testing. Whilst the null hypothesis was confirmed in this instance, it is not a failing of the framework or the research being undertaken, but rather a limitation of the behaviour of the device, which was revealed through execution of the framework.

Table 12-4 A summary of the evaluation of the research questions, the corresponding hypotheses, conditions and results. In all cases the null condition was rejected and the hypotheses accepted.

Research Question	Hypothesis	Condition	Result
RQ1: Can a standard framework be implemented to develop specific forensic analysis procedures for the selected locationally aware embedded devices?	H1. A standard framework can be implemented that allows the development of specific forensic analysis procedures for the selected locationally aware embedded devices.	C1 A framework was developed	Null condition rejected
		C2 Specific forensic analysis procedures for the selected devices resulted from the framework being executed	Null condition rejected
		C3 The selected devices were locationally aware	Null condition rejected
		C4 Where available, the analysis procedures yielded an output of locational history	Null condition rejected
RQ2: Can the accuracy of historical locational data be determined through a standardised framework for the development of a forensic method?	H2 The accuracy of historical locational data can be determined through a standardised framework during the development phase of a forensic process.	C1 A framework was developed	Null condition rejected
		C2 Specific forensic analysis procedure for the selected devices resulted from the framework being executed	Null condition rejected
		C3 Execution of the framework provided details concerning the accuracy of data	Null condition rejected
RQ3: Can the scope of historical locational data available from a device be determined through a standardised framework for the development of a forensic method?	H3 The scope of historical locational data available from a device can be determined through a standardised framework for the development of a forensic method.	C1 A framework was developed	Null condition rejected
		C2 Specific forensic analysis procedure for the selected devices resulted from the framework being executed	Null condition rejected
		C3 The framework provides a determination on what historical locational data can be recovered from each specific device	Null condition rejected

13 Interpretation and Conclusions

13.1 Research Overview

This research was primarily concerned with the development and evaluation of a framework for the generation of forensic process for analysis of locational history. The research was undertaken in six phases with Phases 2, 3, 4, and 5 being comprised of the framework under evaluation. The first and final phases however were concerned with the selection of devices for testing and the evaluation of the framework respectively.

The core development of the framework as used in this work was an iterative process based on an iterative process which consisted of an in depth pilot examination of a number of devices including eBook readers, video game consoles, mobile phones and satnav units. There were multiple reasons for this; the first being the creation of the locational simulation laboratory, which exceeded the scope of the research, allowing for cellular, Wi-Fi, and GNSS based locationing technologies to be implemented. The second reason for the range of devices being used was to allow for any developed framework to be used on a wider range of technologies, allowing for continued research into locational forensics and further evolution of the framework.

The intent of the research was to provide a formalised and documented process for the development of forensic methods specifically aimed at locationally aware embedded devices. While many frameworks, procedures and documented processes existed prior to the research commencing, there was nothing that fits the goals of both being applicable to multiple devices in a generic way and specifically meeting the unique requirements of locationally aware devices. The complexities associated with such research had not been addressed, with most forensic development work being conducted in a non-repeatable way, relying on individual observational skill, or significant reverse engineering processes and knowledge, which is out of reach for many forensic practitioners.

With the framework developed the next stage was to implement it. In order to accomplish this, phases 1 and 6 would be carried out before and after execution of the framework itself. Phase 1 was concerned with the selection of devices. The devices that were to be used in order to verify the claim needed to be determined. This determination was carried out based primarily on a set of three criteria, the first being that the device had the potential to be locationally aware, the second was that the device has significant market penetration, the third was that the device was not a duplicate of a device already

selected. Five satellite navigation devices were selected for study, the first four representing the most popular of the major brand names, the fifth was the most popular generic device available at the time of purchase.

After the selection of the devices, the component of the study referred to as the framework could be entered. This portion is a framework for development of specific analysis procedures for locationally aware embedded devices. This section consists of four phases numbered two through five. Phase 2 deals with the identification and analysis functionality for each selected device. In this phase, the potential sources of locational information for each selected device were identified. This process accomplished the identifying items of functionality supported by the device and these items of functionality were found to be: Wi-Fi connectivity, implicit location support such as GNSS, the presence of networking functionality, and support for cellular networks. In the event that an item of functionality, by definition, was one of these technologies or required one of these technologies to operate, these technologies were documented and recorded as locational data sources.

In Phase 3, testing procedures were developed for the population and collection of data from each selected device. In order to accomplish this, input from the previous phase was utilised. For each unique identified and function point, a means to simulate and to record the associated signals was developed.

For GNSS signals a GNSS simulator marketed as the LabSat2 was selected. This unit was capable of both recording live sky broadcasts and replaying those in a closed sky environment. In order to gather control data, a consumer grade USB GNSS receiver was selected.

To address the needs of cellular networks, it was determined that the OpenBTS software combined with the USRP2 hardware platform would be suitable. The OpenBTS software is capable of acting as a cellular base station when coupled with appropriate hardware. In this case it was configured to act as a base station with the cell tower ID of its real-world counterparts in the area in which the simulation was undertaken. Additionally, the software was configured to provide A-GPS location services for both mobile station based and mobile station assisted forms of locationing.

In the case of Wi-Fi-based location mechanisms, the MDK3 software was used to spoof the BSSID broadcasts of the Wi-Fi access points that would exist at the physical locations being simulated. As Wi-Fi positioning relies only on the BSSID broadcasts and not on being able to actually connect to the access points, this spoofing of Wi-Fi beacons

is sufficient for the simulation of location. A USB Wi-Fi dongle was used to record and confirm that these were being broadcast correctly.

The final step within this phase was to establish a test plan for each device. Whilst all devices would be subject to the same simulated inputs, there was a need to determine what interaction with the device would be required. The process of making this determination is once again iterating through each item of functionality for each device, with the goal of determining what interaction would be required with the device at each stage of testing. For each item of functionality, it was determined whether the functionality was passive or active. Passive functionality was defined as any functionality in which interaction was not required, an example of this could be a satellite navigation unit determining its location and displaying this on a map. An example of active functionality for the same device would be navigating to a specific location. The active interaction required in this case would be the selection of the navigation function followed by the input of an address. Each item of passive and active functionality was documented alongside details of the interaction required to achieve this functionality.

With the parameters for recording control data established the research was able to move on to the next phase of experimentation. In phase 4, data population and collection tasks were performed. For each device within the test set, the following procedure was conducted. The baseline image of the device was established through forensically valid means. The purpose of this baseline image was to allow restoration to a known state after each iteration of testing.

With the baseline images established the tests were conducted by first initiating the data recording processes as defined in the previous phase and then commencing simulation. This process was repeated and each passive and active item of interaction required in the established testing action plan. At the conclusion of each simulation, a posts test image of the device was captured the comparison purposes, and this was stored alongside the recorded control data sets. Subsequently, the baseline images were restored to the device, readying it for further testing. This phase concluded once this process had been completed for each device.

With the data acquired, Phase 5 commenced. This phase placed focus on the development of analysis procedure. This phase resulted in the output of analysis procedure for the selected devices. The procedure was evaluated in order to answer the question of whether specific forensic analysis procedures can be developed from the standardised process. In order to produce these procedures, the following process was carried out for each set of data acquired.

For each device, the baseline images taken were compared to the experimental images of the same device. The comparison was performed in a staged process, the first of which being a binary diff conducted against the image at the file system level. The purpose of this was to identify the files changed (if any) due to the experimental process. Subsequently, to this the entire image is compared to the baseline, this is intended to find any remnant data that isn't present within files. The differential data sets were then examined using a process of elimination to determine any data that could be of potential use in determining the device's historic location. An example of this process of elimination is the presence of log files indicating the time at which the device was powered on, while these may be of general significance, they were discarded if they do not have the potential to provide details of previous locations for the device. Any differential data that could be confirmed to contain locational data or cannot be trivially interpreted was retained for further examination.

An empirical approach was used in order to analyse the data discovered. As the experimental approach ensured that all data being input into the experiments was known, It was possible to interpret data in an informed way, looking for patterns and known means of interpreting the recovered data. In the case of files that could not be decoded or were otherwise not able to be interpreted, the entropy of these files was calculated. If the entropy of the file was significant, it was assumed to have been encrypted or otherwise obfuscated and eliminated from the study. It is intended that future research will examine these instances in greater depth.

With the historic data decoded and interpreted a document detailing an analysis procedure was created for each device. This document was fed into the subsequent phase of verification and testing which provides output to address the efficacy of the framework as a whole.

In the final phase of the research, the simulation of real world conditions was again commenced with a path that varies from that used during the previous phases. The devices after being restored to their baseline state are tested as per the testing action plan utilised in previous phases. On completion of testing the device was imaged once again and analysed as per the procedure outlined in phase 5, without the use of baseline images for comparative purposes. Any findings of locational history were examined to determine if they match the control data recorded during the run. If the control data and the experimental data indicate a match within an acceptable margin of error, then the procedure was validated. This is repeated for each of the devices and their matching procedures.

In each of the test cases, it was possible to determine historic location with various degrees of accuracy. In the case of the portable navigation devices (with the exception of the TomTom) it was possible to determine the historic location at intervals not exceeding 10 seconds for any time at which the device had acquired a GPS fix. This data was stored in a variety of formats, including XML, NMEA0183, and proprietary binary structures. In the case of the TomTom devices, the data available was limited to data, which had been created through user interaction and the last known location of the device, rather than the more comprehensive locational histories provided by the other devices.

Through the findings shown previously it was confirmed that it is indeed possible to utilize a single standard procedure to develop specific forensic analysis procedures for locationally aware devices. It has however been demonstrated that there exists a requirement for the device being examined record this history in some way if the framework is to be useful for its stated purpose.

13.2 Implications

Three research questions were proposed and evaluated in the course of the research being undertaken, these can be seen in Table 12-4. Each of these three questions is addressed below.

The first question “RQ1: Can a standard framework be implemented to develop specific forensic analysis procedures for the selected locationally aware embedded devices?” was answered in the affirmative. In all cases where devices were shown to record locational data, it was possible to retrieve and analyse this data via the use of the developed procedures.

The developed framework was shown to produce functional procedures for the extraction of locational history from all devices where data exists. The framework also enables exhaustive analysis to determine the conditions under which locational history is recorded and provides means to determine where no such history exists. This work has the potential to act as a pillar for the development of future forensic extraction procedure in a formalised, repeatable, and verifiable manner. Additionally, there exists potential use for these techniques outside the field of digital forensics, notably there is potential to assist with reverse engineering of unknown file structures. An example of this reverse engineering was the analysis of the structure of the TomTom One *MapSettings.cfg* file.

The second research question: “RQ2: Can the accuracy of historical locational data be determined through a standardised framework for the development of a forensic method?”, was answered in the affirmative. In this case it was confirmed that the framework was able to produce statistical examination of the data recovered. In all cases the accuracy information gathered through examination was more conservative than that gathered during non-developmental testing.

Previous works in locational forensics have focussed solely on means to acquire, extract and analyse locational history data. The work presented in response to RQ2 addresses the additional factor of the accuracy of the data acquired. Utilising the techniques presented in this work, an investigator would be able to simulate a route encountered during an investigation and approximate margins of error present within the extracted locational history. In the context of corpse recovery, this work has the capability to enable investigators to widen search areas in an intelligent and efficient manner, increasing the probability for recovery prior to decomposition. This hastened recovery provides increased potential for physical and biological examination of recovered bodies. Furthermore, the work will enable a prosecutor to address any queries raised by the defence regarding potential accuracy issues in acquired data, providing a realistic error potential at any point in the locational history of a device.

The third and final research question: “RQ3: Can the scope of historical locational data available from a device be determined through a standardised framework for the development of a forensic method?” was answered in the affirmative. In examination of this question it was found that the framework utilised an exhaustive approach for the development of forensic procedure. As such the scope of what was available was known, even in circumstances where the data would not be utilised in the resulting procedure. In the cases where data was not analysed, it was due to more precise data being available from another source of the device being examined.

In addressing RQ3 the work presented means to determine the scope of locational history identified. In practice this enables investigators to understand the context and provenance of data being recovered. For instance, locational history that includes full NMEA logs will allow for further knowledge of environmental conditions, such as the number of satellites in view, the dissolution of precision values, and other information as recorded by the device. In combination with examination of the scene this data has potential to provide details of the physical location of objects such as vehicles which may block or interfere with signals. Such information could prove vital to corroborating witness testimony. Alternately, in the case of historic locations from user interaction, an investigator can demonstrate that the user of the device searched for a particular

destination or entered a particular search term. However due to the nature of the data it may not be possible to determine if the location was actually visited. The framework presented in this thesis provides the mechanism for an investigator to accurately understand the advantages and limitations of the locational data acquired during analysis.

From the above analysis it can see that the research had a positive result, with all null hypotheses rejected and alternative hypotheses accepted.

13.3 Ancillary Outcomes of Research

13.3.1 Means to develop and test locational forensic procedure

First and foremost, the research undertaken resulted in the development, implementation and examination of a framework which allows the development of locational forensic procedure. The developed framework is device and locationing technology agnostic, instead focusing on the fundamental data storage mechanisms utilised by embedded devices.

Through the implementation of this framework not only was forensic procedure produced, but also details on the accuracy and scope of information that can be recovered were revealed. Through this framework it will be possible for forensic investigators to better quantify the confidence that can be had in any finding of historical location, allowing for additional context within the legal process.

13.3.2 Development of locational simulation laboratory

In the course of undertaking the research a locational simulation laboratory was constructed. To the best knowledge of the researcher it is the only facility of its kind. While facilities do exist for closed sky GNSS simulation or closed sky cellular simulation, no references were found to a facility with the full scope of locational simulation capabilities, for both transmission and recording of data. The developed facility is able to transmit and receive both recorded and lab designed simulations across NAVSTAR, GLONASS, Galileo, GSM, 2G, 3G and W-Fi locationing technologies.

Interest has been expressed by a number of researchers in the forensic and security community to make use of this facility in order to improve the accuracy and reliability of their research. Plans are currently being developed to extend and simplify operation of the facility to allow research to be undertaken where appropriate.

13.3.3 Developed forensic analysis procedure for satellite navigation units

A forensic analysis procedure was developed for five satellite navigation devices and will be published at a later date. The core components of these procedures are included in Sections 7.5, 8.5, 9.5, 10.5, and 11.5. In each of the case studies, evidentiary artefacts were discovered which had not previously been publicly identified by the forensic community. It is hoped that this information will work to assist forensic investigators in their tasks and result in societal benefit.

13.3.4 Social Impact

The research undertaken has had significant social impact. Numerous requests for investigative support were received from law enforcement throughout the research period. Where appropriate, assistance was provided. Evidence was prepared through execution of the framework defined in this thesis. This evidence has supported a significant number of convictions and contributed to over 200 years of cumulative custodial sentencing.

13.4 Critical Review of the Research Process

While undertaking the research there were significant disruptions as at various points there were issues relating to the hardware required. These issues presented themselves as hardware failures, incompatibilities or excessive lead times to acquire the required items. One such example was the need for an amplifier capable of broadcasting NAVSTAR signals within the needed parameters. The required amplifier was used almost exclusively by space agencies who maintain their own stock. As such there was extremely low demand for this item resulting in a delay of close to six months before delivery. In retrospect it would have been far more efficient to consider the entire lab design prior to commencement of research, rather than approaching it in somewhat of an ad-hoc basis.

There were significant software developments made to facilitate the research process. For example, the production of tables, charts and maps was automated in such a way that the diagram requirements for each case study were created via the issuing of a single command. This resulted in conformity of these diagrams and significantly reduced the time taken to produce these sections. However, this was not true for all components of the research, the execution of tests was an entirely manual process, with multiple computer systems being used to provide each component of the simulation. These were

all started individually and manual inspection was required to confirm that each had commenced correctly. The same was true with forensic acquisition and analysis process, which could have benefited substantially from suitable automation efforts.

In contrast the development of the simulation infrastructure prior to the commencement of data collection or selection of devices resulted in over-engineering. The simulation environment was completely capable of simulating cellular connectivity including simulation of third party locationing technologies and cellular specific locationing technologies such as those defined in 3GPP TS 23.00. In the actual execution of the research these were not required, as the selected devices did not include any with cellular functionality. In retrospect scope would have been more clearly defined for all areas prior to commencing development.

Finally, it was difficult to adapt existing statistical methods to the analysis of time series spatial data. In order to address this latitude and longitude were evaluated separately or the data was pre-processed to calculate the difference between control and experimental sets prior to processing. In this way there was limited ability to correlate these differences to specific factors when isolated from each other. This isolation was inconvenient due primarily to the different mechanisms employed for horizontal and vertical positioning within GNSS receiver hardware. If this research were to be repeated it would be prudent to spend significant time developing new statistical methods more suited to the analysis of time series, pairwise, locational data sets. Ideally incorporating a bi-directional auto regression component, to identify differences in the time processing routines of different receiver hardware.

13.5 Recommendations for Future Research

There are a number of recommendations for future research arising from this study. The first would be to progress the research in the most direct way, by examining additional devices through implementation of the defined framework. Specifically, non-navigation devices and devices which do not support primary locationing technologies. It is the belief of the researcher that it will be possible to discern locational history from devices which only make use of non-primary locationing technologies, such as Wi-Fi, Bluetooth and cellular capabilities.

Extending the capabilities of the locational simulation laboratory is currently being planned. Specifically, the addition of magnetic, barometric and dead reckoning simulation capability. Whilst some of these pose significant challenge, especially when

deployed in combination, it is believed that the potential for such a facility warrants such investment.

13.6 Final Thoughts

The posed questions were answered in the affirmative and the original goals of the research have been realised. A framework that allows for the development of forensic procedure was developed and tested successfully. In conclusion, in light of the findings of this research, it is the recommendation of the researcher that a person should not carry electronic devices upon them when trying to covertly dispose of a body.

References

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

AFP. (2011, 3rd February). Media Release: AFP Computer Forensics Team record an accreditation first - Australian Federal Police. Retrieved from http://www.afp.gov.au/media-centre/news/afp/2011/february/afp-computer-forensics-team-record-an-accreditation-first

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS), 5*(1), 118-131.

Altheide, C., & Carvey, H. (2011). *Digital Forensics with Open Source Tools: Using Open Source Platform Tools for Performing Computer Forensics on TargetSystems: Windows, Mac, Linux, Unix, etc*: Elsevier.

ANZPAA NIFS. (2013). *2013 Australia and New Zealand Guidelines for Digital Imaging Processes*. Retrieved from https://www.swgit.org/pdf/2013%20Australia%20and%20New%20Zealand%20Guidelines%20for%20Digital%20Imaging%20Processes?docID=149

Arbelet, A. (2014). *Garmin satnav forensic methods and artefacts: an exploratory study.* Edinburgh Napier University.

Astrophysics, C. f. S. (2015, 2015). Pulsar Dispersion Measure | CAS CMS. Retrieved from http://astronomy.swin.edu.au/cms/astro/cosmos/p/Pulsar+Dispersion+Measure

Ayers, R., Brothers, S., & Jansen, W. (2014). *NIST Special Publication 800-101 Revision 1 - Guidelines on Mobile Device Forensics*. Retrieved from Springfield, VA: https://dx.doi.org/10.6028/NIST.SP.800-101r1 (link is external)

Baber, C., Smith, P., Panesar, S., Yang, F., & Cross, J. (2006). Supporting Crime Scene Investigation.

Bennett, D. (2012). The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations. *Information Security Journal: A Global Perspective, 21*(3), 159-168.

Berman, K. J., Glisson, W. B., & Glisson, L. M. (2015, 5-8 Jan. 2015). *Investigating the Impact of Global Positioning System Evidence.* Paper presented at the System Sciences (HICSS), 2015 48th Hawaii International Conference on.

Bertorelli, P. (1996, 22nd February 1997). GPS Explained. Retrieved from http://www.eaa1000.av.org/technicl/gps/gps.htm

Braasch, M. S., & van Dierendonck, A. J. (1999). GPS receiver architectures and measurements. *Proceedings of the IEEE, 87*(1), 48-64. doi:10.1109/5.736341

Branwen, G., Christin, N., Décary-Hétu, D., Andersen, R. M., StExo, Presidente, E., . . . Whom. (2015). Dark Net Market archives.

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

Brezinski, D., & Killalea, T. (2002). *RFC3277: Guidelines for evidence collection and archiving* (2070-1721). Retrieved from

Caloyannides, M. A., Memon, N., & Venema, W. (2009). Digital forensics. *Security & Privacy, IEEE, 7*(2), 16-17.

Carrier, B. (2005). *File System Forensic Analysis*: Addison-Wesley Professional.

Casey, E. (2009). *Handbook of Digital Forensics and Investigation*: Academic Press.

Cater-steel, A., & Al-Hakim, L. (2009). *Information Systems Research Methods, Epistemology, and Applications*: Information Science Reference.

Chernyshev, M., Valli, C., & Hannay, P. (2016). On 802.11 Access Point Locatability and Named Entity Recognition in Service Set Identifiers. *Information Forensics and Security, IEEE Transactions on, 11*(3), 584-593. doi:10.1109/TIFS.2015.2507542

Creswell, J. W. (2009). Editorial: Mapping the Field of Mixed Methods Research. *Journal of Mixed Methods Research, 3*(2), 95-108. doi:10.1177/1558689808330883

Creswell, J. W. (2013). *Research Design: Qualitative, Quantitative, and Mixed Method Approaches* (a, Trans.): SAGE Publications.

Crotty, M. (1998). *The foundations of social research: meaning and perspective in the research process*. St. Leonards, N.S.W: Allen & Unwin.

Cusack, B., & Simms, M. (2011). Evidential recovery from GPS devices. *Journal of Applied Computing and Information Technology, 15*(1), 2011.

Delport, W., Köhn, M., & Olivier, M. S. (2011). *Isolating a cloud instance for a digital forensic investigation.* Paper presented at the ISSA.

Diaz, J. (2012). These Breasts Nailed a Hacker For the FBI. *Gizmodo.* Retrieved from http://gizmodo.com/5901430/these-breasts-nailed-anonymous-hacker-in-fbi-case

Djuknic, G. M. (2001). Geolocation and Assisted GPS. *Computer, 34*(3), 123.

El-Rabbany, A. (2002). *Introduction to GPS: the global positioning system*: Artech house.

EziTrak. (2007a). EziTrak News. *EziTrak.* Retrieved from http://www.ezitrak.com.au/aa-News.htm

EziTrak. (2007b). EziTrak NSW Distributors. *EziTrak.* Retrieved from http://www.ezitrak.com.au/aa-NSWDistributors.htm

Feng, J. L. R., & Gong, G. (2014). Vulnerability Analysis and Countermeasures for WiFi-based Location Services and Applications. Retrieved from http://cacr.uwaterloo.ca/techreports/2014/cacr2014-25.pdf

Grewal, M. S., Andrews, A. P., & Bartone, C. (2013). Global navigation satellite systems, inertial navigation, and integration.

Halim, A. A. (2006). Wifi positioning system. *MARA UNIVERSITY OF TEKNOLOGY SHAH ALAM MAY*.

Hannay, P. (2007). *A Methodology for the forensic acquisition of the TomTom One satellite navigation System–A research in progress.* Paper presented at the Proceedings of The 5 th Australian Digital Forensics Conference.

Hannay, P. (2008). *Forensic acquisition and analysis of the tomtom one satellite navigation unit*. Paper presented at the Proceedings of the 6th Australian Digital Forensics Conference, Perth Western Australia.

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

Heath, S. (2003). *Embedded systems design* (2nd ed.). Oxford ; Boston: Newnes.

Hossam-E-Haider, M., Tabassum, A., Shihab, R. H., & Hasan, C. M. (2014, 13-15 Feb. 2014). *Comparative analysis of GNSS reliability: GPS, GALILEO and combined GPS-GALILEO.* Paper presented at the Electrical Information and Communication Technology (EICT), 2013 International Conference on.

Jackson, S. (2008). Research Methods and Statistics: A Critical Thinking Approach by Wadsworth Publishing.

Jansen, W., Delaitre, A., & Moenner, L. (2008). *Overcoming impediments to cell phone forensics.* Paper presented at the Proceedings of the 41st Annual Hawaii International Conference on System Sciences.

Jones, A., & Valli, C. (2008). *Building a Digital Forensic Laboratory*: Butterworth-Heinemann.

Kant, I., & Meiklejohn, J. M. D. (1934). *Critique of pure reason* (Vol. 909.). New York: J. M. Dent & sons, ltd.

Keith, H. (2007). Tracking "Bad Guys": Legal Considerations in Using GPS. *FBI Law Enforcement Bulletin, 76*(7), 25.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication*, 800-886.

Kessler, G. C. (2003). An overview of cryptography: Gary C. Kessler.

Kizza, J. (2015). Computer and Network Forensics *Guide to Computer Network Security* (pp. 299-324): Springer London.

Köhn, M., Olivier, M. S., & Eloff, J. H. (2006). *Framework for a Digital Forensic Investigation.* Paper presented at the ISSA.

Kos, T., Markezic, I., & Pokrajcic, J. (2010, 15-17 Sept. 2010). *Effects of multipath reception on GPS positioning performance.* Paper presented at the ELMAR, 2010 PROCEEDINGS.

Kowoma. (2009, May 19th). The GPS System - Transmitted GPS Signals. Retrieved from http://www.kowoma.de/en/gps/signals.htm

Kyung-Soo, L., & Sangjin, L. (2008, 13-15 Dec. 2008). *A Methodology for Forensic Analysis of Embedded Systems.* Paper presented at the Future Generation

Communication and Networking, 2008. FGCN '08. Second International Conference on.

LaMance, J., DeSalas, J., & Järvinen, J. (2002, March). Innovation: Assisted GPS: A Low-Infrastructure Approach. *GPS World.* Retrieved from http://gpsworld.com/innovation-assisted-gps-a-low-infrastructure-approach/

Lewis, L. L. (1991). An introduction to frequency standards. *Proceedings of the IEEE, 79*(7), 927-935. doi:10.1109/5.84969

Lim, K.-S., Lee, C., Park, J. H., & Lee, S.-J. (2014). Test-driven forensic analysis of satellite automotive navigation systems. *Journal of Intelligent Manufacturing, 25*(2), 329-338.

Locher, T., Wattenhofer, R., & Zollinger, A. (2005, 23-25 May 2005). *Received-signal-strength-based logical positioning resilient to signal fluctuation.* Paper presented at the Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2005 and First ACIS International Workshop on Self-Assembling Wireless Networks. SNPD/SAWN 2005. Sixth International Conference on.

Mertens, D. M. (2010). Transformative Mixed Methods Research. *Qualitative Inquiry, 16*(6), 469-474. doi:10.1177/1077800410364612

Mezzofiore, G. (2012, 2012/04/12/T16:43:17+01:00). Anonymous Hacker AnonWormer Unmasked by Girlfriend's Cleavage Picture. *International Business Times UK.* Retrieved from http://www.ibtimes.co.uk/anonymous-hackers-unmasked-girlfriend-s-semi-naked-327325

MiTAC. (2006). *Navman S Series User Manual* (pp. 133).

Morgan, D. L. (2007). Paradigms Lost and Pragmatism Regained: Methodological Implications of Combining Qualitative and Quantitative Methods. *Journal of Mixed Methods Research, 1*(1), 48-76. doi:10.1177/2345678906292462

NATA. (2014, June 2014). NATA - AFP gains first accreditation to AS 5388. Retrieved from http://www.nata.com.au/nata/54-nata-e-news/june2014/1005-afp-gains-first-accreditation-to-as-5388

Nellis, M. (2005). Out of this World: The Advent of the Satellite Tracking of Offenders in England and Wales*. *The Howard Journal of Criminal Justice, 44*(2), 125.

NIST. (2016a, 1st February). Mobile Device Tool Specification. Retrieved from http://www.cftt.nist.gov/documents/Mobile%20Device%20Tool%20Secification_v2.0.pdf

NIST. (2016b, 1st February). Mobile Device Tool Test Assertions and Test Plan. Retrieved from http://www.cftt.nist.gov/documents/Mobile_Device_Tool_Test_Assertions_and_Test_Plan_v2.0.pdf

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

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

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

Parkinson, B. W., & Gilbert, S. W. (1983). NAVSTAR: Global positioning system—Ten years later. *Proceedings of the IEEE, 71*(10), 1177-1186.

Parkinson, B. W., & Spilker, J. J. (1996). *Global Positioning System: theory and applications*: Aiaa.

Penrod, S., & Cutler, B. (1995). Witness confidence and witness accuracy: Assessing their forensic relation. *Psychology, Public Policy, and Law, 1*(4), 817.

Phillips, D. C., & Burbules, N. C. (2000). *Postpositivism and educational research*. Lanham, Md: Rowman & Littlefield Publishers.

Pioneer. (2007, March). User manual Pioneer AVIC-S2. v0.1. Retrieved from http://www.pioneerelectronics.com/pio/pe/images/portal/cit_3424/483473310AVICS2UserManual0823.pdf

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

Pye, G. (2007, March 14). A Knight With Shining GPS. *Rock Paper Dynamite.* Retrieved from http://rockpaperdynamite.wordpress.com/2007/03/14/a-knight-with-shining-gps/

Revnivykh, S. G. (2012). Development trends in global satellite navigation. *Gyroscopy and Navigation, 3*(4), 215-222. doi:10.1134/s2075108712040098

Rogaway, P., & Shrimpton, T. (2004). Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. In B. Roy & W. Meier (Eds.), *Fast Software Encryption* (Vol. 3017, pp. 371-388): Springer Berlin Heidelberg.

Rose, M., & Lisker, P. (2016, 2016/09/13/T18:35:48.901Z). Illuminating the Dark Web. *Medium.* Retrieved from https://medium.com/@roselisker/illuminating-the-dark-web-d088a9c80240

https://medium.com/@roselisker/illuminating-the-dark-web-d088a9c80240#.lwtf3nqu3

Rost, C. (2012). Modelling and Correction of Carrier Phase Multipath Effects. Retrieved from http://tu-dresden.de/die_tu_dresden/portrait/uni_mit_kind/die_tu_dresden/fakultaeten/fakultaet_forst_geo_und_hydrowissenschaften/fachrichtung_geowissenschaften/gi/gg/veroeffentlichungen/Poland%202012%20-%20P09%20Rost%20PR38.pdf

Ryan, M. (2009). Daubert Standard. *LII / Legal Information Institute*.

Sapage, A., & Franco, S. (2004). *Terminal Localisation Using Wireless LANs.* (Electrical and Computer Engineering Degree), Universidade do Porto.

Scientific Working Groups on Digital Evidence and Imaging Technology. (2015). 2015-05-27 SWGDE-SWGIT Glossary v2.8. Retrieved from https://www.swgde.org/documents/Current%20Documents/2015-05-27%20SWGDE-SWGIT%20Glossary%20v2.8

ShareTechNote. (2013, 9th April). LBS/GPS. Retrieved from http://www.sharetechnote.com/html/LBS.html

Standards Australia. (2012a). Forensic analysis - Analysis and examination of material (pp. 1-53): Standards Australia.

Standards Australia. (2012b). Forensic analysis - Recognition, recording, recovery, transport and storage of material (pp. 1-53): Standards Australia.

Standards Australia. (2013a). Forensic analysis - Interpretation (pp. 1-25): Standards Australia.

Standards Australia. (2013b). Forensic analysis - Reporting (pp. 1-21): Standards Australia.

Thompson, E. (2005). MD5 collisions and the impact on computer forensics. *digital investigation, 2*(1), 36-40. doi:http://dx.doi.org/10.1016/j.diin.2005.01.004

Trevisani, E., & Vitaletti, A. (2004, 2-3 Dec. 2004). *Cell-ID location technique, limits and benefits: an experimental study.* Paper presented at the Mobile Computing Systems and Applications, 2004. WMCSA 2004. Sixth IEEE Workshop on.

U.S. Coast Guard Navigation Center. (2014). Current Operational Advisories. Retrieved from http://www.navcen.uscg.gov/?pageName=currentAdvisory&format=txt

Valjarevic, A., & Venter, H. S. (2015). A comprehensive and harmonized digital forensic investigation process model. *Journal of forensic sciences, 60*(6), 1467-1483.

Van Diggelen, F. S. T. (2009). *A-GPS: Assisted GPS, GNSS, and SBAS*: Artech House.

Vossiek, M., Wiebking, L., Gulden, P., Wieghardt, J., Hoffmann, C., & Heide, P. (2003). Wireless local positioning. *Microwave Magazine, IEEE, 4*(4), 77-86. doi:10.1109/mmw.2003.1266069

Wainwright, R. (2007). Father and son stick to guns to prove radar wrong. *The Sydney Morning Herald.* Retrieved from http://www.smh.com.au/news/national/father-and-son-stick-to-guns-to-prove-radar-wrong/2007/03/11/1173548023012.html

Walter, B. (1996). Satellite navigation systems. *Sensor Review, 16*(1), 4.

Watt, J., & Crase, S. (2007, July 2, 2007). How I used my GPS to beat my speeding fine. Retrieved from http://www.abc.net.au/southwestvic/stories/s1967739.htm

Weiser, M., Biros, D. P., & Mosier, G. (2006). Development of a National Repository of Digital Forensic Intelligence. *Proceedings of the Conference on Digital Forensics, Security and Law*, 17-26.

Whinnett, E. (2007, 16 Oct 2007). GPS beats radar gun. Retrieved from http://www.news.com.au/heraldsun/story/0,21985,21999706-661,00.html

Yujie, Z., & Bartone, C. (2004, 26-29 April 2004). *Multipath mitigation in the frequency domain.* Paper presented at the Position Location and Navigation Symposium, 2004. PLANS 2004.