Investigation Into The Current Use Of Computer Forensic Tools

In The Area Police Force And Their Effects On Finding Police Evidence.

Written By Lucy Taylor

St20036591

Supervised By Dr Hilary Berger

BSc (Hons) Business Information Systems

Cardiff School of Management

April 2016
Declaration

This work has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree.

Signed .................................................. (Candidate)

Date.....................................................

Statement

This Dissertation is the result of my own investigations, except where otherwise stated.

Other sources are acknowledged by explicit references.

Signed .................................................. (Candidate)

Date.....................................................

Statement

I hereby give consent for my dissertation, if accepted to be available for photocopying and for inter-library loan, and for the title and abstract to be made available to outside organizations.

Signed .................................................. (Candidate)

Date.....................................................
Abstract

This dissertation investigates the current computer forensic tools used in the area police force (South Wales Police) and the effect that these tools have when finding police evidence. It focuses on the types of tools used currently within forensic departments, the laws and legislations used when collecting police evidence, and the types of evidence each investigator extracts from the suspects devices. As there has been little academic research into the particular tools that are used within the forensic departments of the South Wales Police this study has focused on the knowledge and research specific to this topic area. Thus a critical review of extant literature included published articles, journals, books and webpages aimed as providing an insight into which tools are currently adopted and their utility. The empirical data collected from five semi-structured interviews conducted with members of the police forensic departments identifies the forensic tools used and evidences how they were used and their efficacy. Findings illustrate some interesting results. Although the participants reported good performance of the forensic tools in question, they further highlighted other forensic tools that they use but which are not significantly acknowledged in the available secondary research. This suggests that the South Wales Police use a number of different tools to those reportedly used within forensic departments in other areas.
Acknowledgements

I would like to express my gratitude to the following people, for without the completion of this dissertation would not have been possible:

Dr Lynne Norris-Jones whom supervised the dissertation during term one and Dr Hilary Berger who supervised the dissertation from term 2 onwards. I thank these two lovely ladies for putting their dedicated time and effort into guiding me through all chapters of the dissertation.

All research participants who participated in the semi-structured interviews and my neighbors (who are in the law enforcements) for giving me their time to verify that the research questions were suitable for the interviews.

My Immediate family (Elizabeth, Alistair and James) for providing continuous love and support. Especially to Elizabeth Taylor who provided me with contacts to find my research participants.
## Contents

<table>
<thead>
<tr>
<th>Chapter 1: Introduction</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Title</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.3 Background</td>
<td>2</td>
</tr>
<tr>
<td>1.4 Aim</td>
<td>4</td>
</tr>
<tr>
<td>1.5 Research Questions</td>
<td>4</td>
</tr>
<tr>
<td>1.6 Objectives</td>
<td>4</td>
</tr>
<tr>
<td>1.7 Research Methods</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 2: Literature Review</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Laws to obtaining Police evidence</td>
<td>6</td>
</tr>
<tr>
<td>2.2 The three C’s</td>
<td>7</td>
</tr>
<tr>
<td>2.3 Legislations</td>
<td>8</td>
</tr>
<tr>
<td>2.4 Types of Police evidence obtained by forensic tools</td>
<td>11</td>
</tr>
<tr>
<td>2.5 Digital Forensic tools used to obtain data</td>
<td>15</td>
</tr>
<tr>
<td>2.5.1 Types of Software Tools</td>
<td>15</td>
</tr>
<tr>
<td>2.5.1.1 Encase</td>
<td>16</td>
</tr>
<tr>
<td>2.5.1.2 Vogon Forensic Software</td>
<td>17</td>
</tr>
<tr>
<td>2.5.1.3 Visual Time Analyzer</td>
<td>18</td>
</tr>
<tr>
<td>2.5.1.4 X-Ways</td>
<td>18</td>
</tr>
<tr>
<td>2.5.1.5 Toolkits</td>
<td>19</td>
</tr>
<tr>
<td>2.5.2 Types of Hardware Tools</td>
<td>20</td>
</tr>
<tr>
<td>2.5.2.1 No Write</td>
<td>21</td>
</tr>
<tr>
<td>2.5.2.2 Write Protect Card Reader</td>
<td>21</td>
</tr>
<tr>
<td>2.5.2.3 ImageMASSter Solo 3</td>
<td>22</td>
</tr>
<tr>
<td>2.5.2.4 FireFly IDE and FireFly SATA</td>
<td>23</td>
</tr>
</tbody>
</table>

| Chapter 3: Research Methodology | 24 |
# List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>EnCase Diagram</td>
<td>17</td>
</tr>
<tr>
<td>Figure 2</td>
<td>ImageMASSter Solo 3</td>
<td>23</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Research Onion</td>
<td>24</td>
</tr>
</tbody>
</table>
1.0 **Introduction**

1.1 **Title**


1.2 **Introduction**

This Dissertation will be discussing the implementation of digital forensic tools used by the South Wales area police force and the impact these tools have had in the finding of police evidence. The dissertation will also be looking deeper into the data types collected by the tools mentioned. Primary and secondary views have been gathered from forensic tool users and those with deep knowledge in this area to represent the local area police force.

It is likely in the year of 2016 that households hold up to 4 devices (i.e Desktop, Laptop, IPad, Mobile phone, IPod) or more per household. The 2015 statistics show that 40% of the whole world population has Internet connection when only 10 years ago, only 1% of the population used the Internet. Internet live stats (2016). From the statistics shown, it does not come as a surprise that the use of computer evidence in the forensic field has increased dramatically over the years.
Digital devices and computers are evolving on a day to day basis, there is a bigger demand for computers to perform functions that would only be dreamt of 10 years ago. Therefore the forensic tools used to access information on these computers have to evolve in conjunction with the computers in order to access these new functions. For example a fairly new technological advancement is the use of Cloud Computing. Gregg and Oriyano (2013) explain that the cloud made an appearance in 2007 but already holds some security issues and is easily accessible via forensic tools.

1.3 Background

Computer Forensics is a very popular way of collecting and analyzing digital data, it can be used in a range of different ways but mainly in the detection and prevention of crime. The data to be analyzed can be found on any digital device that is capable of storing data, not just computers. If the stored data is seen as suspicious it is often reported to the police forces to investigate. Computer forensics can be applied in many different ways but is mainly used in the police force in the detection and prevention of crime. For a lot of cases, most evidence can be found on a computer device, evidence can be found in a number of different forms such as emails, Internet history, documents, pictures, social media conversations and many more.
However, in order to detect the sorts of data that enables Investigators to prove someone innocent or guilty, the digital forensic team requires specific tools in order to extract hidden information that is not obvious to the eyes at first glance. This can be done using two different types of forensic tools, Hardware and Software.

These two tools are then used to retrieve two different types of data, Persistent data and Volatile data. Persistent data is usually found within files and databases and has to be held in secondary storage such as a disk or a tape because persistent data tends to have a high volume than primary storage can hold. Persistent data is the most important data on a computer system however it cannot be collected directly and so is usually accessed through a sub-section that exists externally to a programming language (Rosenberg and Koch, 2012).

Volatile data is also known as temporary data. Unlike persistent data, it not stored on disk and so therefore is lost immediately if the desktop shuts down. This is data stored on systems such as the random access memory, cache memory or video cards. It is because of this that it is advised that volatile data be collected first since after the computer shuts down, the information will have disappeared (Shinder, 2002).
Further detail on hardware and software tools, as well as the different data types can be seen in chapter 2.0.

1.4 **Aim**

To investigate current computer forensic tools and evaluate their use and effects on finding evidence in the area police force.

1.5 **Research question**

How useful are computer forensic tools in finding vital evidence?

1.6 **Objectives**

1. To Examine the current status of computer forensic tools used by the South Wales Police force

2. Discuss the effectiveness of tools are used to find evidence in the South Wales Police force

3. Analysis the specific benefits and obstacles that each tool brings

4. Put forward recommendations of how forensic tools could be improved

1.7 **Research Methods**

The research has taken a phenomenological qualitative approach using inductive research strategy. Semi-structured interviews were used to collect the relevant
data which provides the flexibility for both the researcher and the participant to have ability to give their views and opinions. Participants are members of the South Wales police force and so were selected using purposive sampling. Details on the rationale behind the research methods can be found in Chapter 3.
1.0 Literature Review

This chapter discusses and critically reviews the literature associated with computer forensics tools in computer technology. It considers the application of these tools within the police force and the impact they have in deriving information to use in police investigations. Various viewpoints will be collected from different sources on the effectiveness of the tools and how critical they are in the use of a case. The data types that these tools collect is also be a topic of discussion along with what precautions that have to be made while dealing with forensic evidence. The dissertation also explains some well-known examples of how these forensic tools have been used by criminals themselves to commit further crime.

2.1 Laws to obtaining Police evidence

Before the police can implement their tools, there are certain rules and regulations that the police have to be aware of. Information that is not collected or handled in an appropriate manor will be deemed as unfit for use, risking the outcome of the case in hand. It is also deemed important that investigators get put on cases that suit their level of knowledge, this is because data collected must be intact and handled professionally before being passed over to the court. If the police do not comply with the legislation and regulations set in 2.2 below, it could result in a punishable offence to the officers and the investigators.
2.2 The Three C’s

When handling police evidence it is suggested that police officers and investigators follow the three simple C’s of evidence:

- Care
- Control
- Chain of custody

Following these guidelines will enable evidence to be presented just as it was seized previously. In order to do this ‘the three C’s’ process requires the data handler to document evidence in its every step during its preparation for trial.

Evidence cannot be modified or altered in anyway as this may make it inadmissible to court. Therefore, the care of the evidence must be taken seriously. The evidence must also be contained in a controlled environment. If the computers are put by a magnetic source, the computers can be affected. Each piece of evidence obtained should have a custody log to show where all evidence is located, on what type of media and if it is a copy or an original to insure that if any data is altered it is done on a copy (Volonino, Anzaldua and Godwin, 2007).

Chain of custody refers to the process of which digital evidence is preserved and documented. It will be able to explain if the e-evidence presented in court has been compromised with or is in the exact state of which it was collected. The
type of documentation that is required during the chain of custody process includes where the evidence was stored, who has access to the evidence and what was done to the evidence. Without the chain of custody document it is almost impossible to prove that the information has not be altered in any way (Volonino and Anzaldua, 2008).

2.3 Legislations

Just like civilians, it is important that the police abide by the law when handing and collecting information. Not doing so is punishable by law and can effectively send the individual dealing with the evidence to confinement. Laws are also drawn up so that police have certain rights when collecting evidence. For example the Police and Criminal Evidence Act (1984) protects the law enforcement when obtaining computerized information. This section of the dissertation will be explaining the different legislations acts involved when collected forensic e-evidence.

The Police and Criminal Evidence Act (1984) give the law enforcers the power to stop and search an establishment that is under suspicion. With this act the law enforcements have to right to search and seize any items within the establishment that may be used as evidence in court. The police are also protected when documenting the evidence in criminal proceedings, which will allow a full investigation to go ahead. A search of a property and belongings is
lawful without a warrant if the police have a reason to do so, however if an individual has done nothing punishable by court it is possible that he or she could sue the police for their actions.

Federal Rules of Evidence (1975) explains what types of evidence can be held up in trial. It explains that information gathered from an electronic device will have to be analyzed with the rules of evidence first. When extracting information the rules of evidence states that only relevant information should be extracted and all information that is collected should be presented to the prosecutor before the trail.

Computer Misuse Act (1990) is not only used for civilians but also is applied when the law enforcers are dealing with computer forensic evidence. A couple of the legislations within this act that the police have to be mindful about are listed below:

- (S1) Unauthorized Access to Computer Material, Gaining unauthorized access is referred to as hacking and the minimum sentence for this kind of offence is 6 months. Only a circuit judge can grant a warrant for police to seize items that could be evidence of the offence. This legislation refers to the idea that it an offense to gain access to data that is not been authorized. Individuals will need to provide proof that authorization has
occurred and will need to be aware of the consequences if he/she decides to commit such an offense.

- (S2) Unauthorised Access With Intent to Commit Other Offence. This offence is punishable for up to 5 years. In order to commit this offense an individual has to firstly commit S1 of the computer misuse act. After access has been granted a further offence will occur if the offender decides to perform any malicious acts with the data. Malicious acts include blackmail, sharing personal data or modification of the data.

- (S3) Unauthorised Acts With Intent To Impair Operation. This is intending to change any of the evidence or computer in any way. The maximum penalty is 10 years. This act in enforced when a person modifies the content of a computer knowing that he/she is unauthorised to do so. Impairing content refers to damaging or changing the operation of a computer, hindering access to programs or changing important information stored on a computers database. Association of Chief Police Officers Police (2015)

Electronic Communication Privacy Act (1986) states that if the police have no reason to inspect a computer then they will not be allowed to gain access. This act explains that it is a federal crime to wiretap or use a machine that had not been approved by the court and violations of this crime can result in imprisonment for up to five years and/or fines up to $250,000 (Doyle, 2012).
Federal Wiretap Statute (1968) ‘This provision of the statue requires that all recordings captured during the time of the wiretap be given to the judge within a reasonable amount of time or the contents of those recordings are inadmissible’ (Volonino, Anzaldua and Godwin, 2007. P.419).

2.4 Types of Police evidence obtained by forensic tools

Digital evidence exists in different formats and locations throughout a digital device. Forensics officers must be thoroughly trained in order to locate the evidence and extract it in one piece from the digital device. To do this forensic officers use special software and hardware tools that allow them to reach all different types of data stored on each digital device. Volonino, Anzaldua and Godwin (2007) list 6 different types of data that can be collected during the extraction stage. Police must search for each type before concluding their search, the types of data are explained below.

- Active Data. This is data used by the operating system that does not need any forensic tools to access, this data is free for anybody and everybody to gain access too. Types of active data can be seen in files and documents such as images, video files, emails, instant messages and even the computers browser history. A famous murder case in 2000 found Michelle Theer guilty after investigators found 88,000 emails and instant messages on her computer, messages documenting the conspiracy to
murder Theer’s husband were found along with evidence to suggest that Theer and the victim John Diamond were having an affair (Cantrell, 2012).

- Deleted Data. A common misconception is that data moved into your trash or deleted, is removed permanently. However this is not the case, deleted data is not destroyed data. Within an operating system if you delete a file, the system doesn’t get rid of the file but opens space for additional or new data to be stored. The file that is deleted will remain on the hard drive until it is overwritten or is wiped using specific software tools. If data is overwritten the whole file will not be easy to recover, it is very likely that only a snapshot of the file can be recovered, however this data should not be ignored as it could contain clues to find other data i.e passwords, addresses etc. Usually deleted data will remain in binary format ‘due to “data remanence (Data that remains after it has been deleted)” or the residual representation of data’ (Chen, 2013).

- Hidden, Encrypted or Password Protected Files. Some data can be password protected, hidden or encrypted to stop users from accessing data. Information that is hidden can include files that have been renamed to look like they belong to the operating system. For example, adding an extension similar to .com or .sys. Simply looking at the file header of
these files will reveal the real identity. To gain access to password protected files or encrypted files certain tools can be used. However according to Spruill (cited in Chen, 2013) most criminals do not have the skills or the patience to fully download and implement encryption software in order to protect their files. It is more common to find files that are only partially encrypted. Some use forces to access a file while others dissect the encryption key. Those that use force are the quicker methods however both types cannot guarantee access. Two examples of this can be seen in the Talk Talk hack of 2015 and the FBI Case of 2016, where 157,000 customers were affected during the Talk Talk Hack. Personal information secured by Talk Talk via encryption was stolen (BBC, 2015).

The FBI are currently finding trouble hacking into potential terrorists IPhones, Schiller (2016) explains that the security on an apple phone is so high that the FBI had to request that Apple write software to unlock the operating system of the phone. Apple have refused and so the FBI are currently finding other means of accessing the phone, there has been no success so far.

- Automatically Stored Data. This refers to persistent data that is automatically stored on a backup hard drive when a user is working on
something. Most of the time the user will not know that these files have been saved. Automatically stored data also includes the users Internet history and cache files. This type of data is usually pretty easy to access without forensic tools as it will be available to view as soon as the laptop is open. However there are tools that can be used to access the backup hard drive if needed.

- Email and Instant Messages. Forensic investigators will look through the users email messages and social media messages. Most users believe that their emails will remain confidential and if deleted are gone forever. However, investigators will be able to track exactly where the email was sent to, whom it was sent to and even read them off another users server. These apply to all types of electronic communication. A lot of evidence can be found on peoples online conversations, in 2012 83% of law enforcement personnel used social media to conduct investigations (Patzakis and Murphy, 2012). ‘The Met reported 138 crimes in which Twitter was involved in 2014, up from 105 in 2013 and the Greater Manchester Police reported 371 harassment allegations and 38 death threats on social media last year’ (RT, 2015).

- Background information. This is information that is being recorded in the background such as network usage, how many times the user has logged
onto or off the computer and how long the user was on the computer for. It will also record what user copied, made or deleted files. Most companies now have software that is designed to trace every move that their employers do on their computers. The background information will remain on the computer operating system until it is over written, it is important that all background information be collected as soon as the computer is obtained.

2.5 Digital Forensic tools used to obtain data

In a digital forensic environment a variety of forensic tools are used to extract critical information. Tools created to deal with computer forensics are designed either for one purpose only or offer a full range of functions, it is because of this that investigators must assess the investigation thoroughly to decide which tool from their tool kit will be appropriate for the job. There are two types of tools used to gain access to information, these are hardware tools and software tools. There are also specific tools to deal with specific data types, the data types that will be collected can be seen in section 2.2.

2.5.1 Types of Software Tools

Software tools are tools or applications that work from within the computer to collect evidence. It is important to notice that with forensic tools, it is likely that more than one tool will be required to pick out every piece of data stored within
a computer. Before choosing what software tool should be used, the areas of focus must be investigated first to determine what tool is suitable. These areas include the operating system, File systems, email and many more. This chapter will be discussing the main software tools used in digital forensics and what they are used for.

2.5.1.1 EnCase

EnCase is a software package tool that is used by a variety of law enforcements over the world, it is primarily used to examine data from hard disks, removable media and Palm PDA’s. Effectively EnCase works in three crucial steps:

- Firstly an exact binary duplicate is drawn up of the original hard drive, floppy disk or PDA in question.

- An Image or ‘Evidence file’ will then be created and scanned to ensure that all the evidence available has not be tampered with or altered in any way.

- Once the image files have been created, the investigator can then search and analyze multiple drives at once. A case indexer within EnCase allows investigators to conduct fast and easy querying, it can also be a quick way to find common keywords. Data that can be found using EnCase include personal documents, deleted files, emails web pages and many more important evidence.
EnCase will show you a preview of the evidence first before copying it down, this enables you to decide whether it is important or not and allows you to swap around files and free space without the risk of you accidentally altering any data.

Once the investigators have bookmarked all the relevant data they can find, they will create a report suitable to present in court or present the data on a number of exported file formats (Guidance software, 2008). A simple diagram of EnCase can be seen in Figure 1.

![EnCase Diagram](Source: Guidance Software, 2016)

**Figure 1: EnCase Diagram (Source: Guidance Software, 2016)**

### 2.5.1.2 Vogon Forensic Software

Vogon offers similar productivity to EnCase as it also uses imaging software to create an exact replica of the data stored on the computers hard drive. Vogon has specifically been created to ‘*meet the needs of the government and law enforcement agencies, it offers a powerful range of imaging, processing and investigation software tools*’ (Computer Crime Research Center, 2004). Vogon
'images' a range of data storage media including CDs, memory disks, DVD’s and more. An advantage to this software tool over EnCase is that Vogon also offers a back up copy along with the first replica for safekeeping. It also offers an option to carry out searches in a wide range of languages i.e Arabic, Russian, this can be helpful when dealing with criminals who live in the UK from outside the European union.

2.5.1.3 Visual TimeAnalyzer

The program allows an investigator to see exactly when a user has logged into a computer, what programs they were using and exactly how long they were active on these programs for. The information that is gathered will be presented in graph type diagrams so that it is readable and understandable. ‘The software has some privacy safeguards and does not monitor all user data such as passwords and personal documents. Unlike spyware, it does not record specific keystrokes or run screen captures as a background process’ (Wiles and Reyes, 2007).

2.5.1.4 X-Ways

X-Ways was created by a German company to accommodate the need for forensics tools within the law enforcements. It is primarily based on the older model WinHex and holds many powerful features such as forensic cloning and imaging of sound disks. X-Ways supports a number of systems including FAT,
NTFS, Ext3 & 4 as well as featuring a built-in interpretation of RAID 0 and RAID 5. An advantage of this software tool is that it features several data recovery techniques allowing the tool to really dig into all aspects of the operating system, it works by ‘gathering slack space, free space, interpretation space and generic text from drives and images’ (Wiles and Reyes, 2007). As well as images and video files X-Ways is effective when retrieving images from inside documents i.e. PowerPoint, Microsoft word and PDF’s. It also has skin colour detection which is useful when finding child pornography images. This type of tool is well known for its ability to ‘write-protect data to ensure authenticity and integrity. It has a case management function integrated with automated activity logging and automated reporting’ (Wiles and Reyes, 2007).

2.5.1.5 ToolKits

As well as individual tools, in forensics it is also possible to purchase a complete forensic toolkit, for example NTI tools are often a popular compilation of software forensic tools. Wiles and Reyes (2007) explain that the NTI tool kit features a total of six forensic tools, each holding their own unique features to help hack into criminal evidence. These tools include:

- **Stealth Suite.** This tool is usable for all forensic investigators no matter what their ability, it works by allowing access onto a computer’s hard disk. This tool also helps identify what systems within the computer were used to access inappropriate information.
• Computer Incident Response Suite. This use uses MS-DOS and other programming elements to access into a windows platform.

• Data Elimination Suite: Used to perform computer data elimination and validation so that the possibility of data leaking is low.

• TextSearch Suite. Used to identify compressed graphic files using a file header signature. This allows the investigator to have a list of the files that could contain compressed information or graphics.

• NTI Secure ToolKit. This tool provides security to files that are stored on a computer desktop. This type of tool is NIST tested and includes approved AES 256-bit encryption, because of this NTI Secure toolkit exceeds the security requirements when working with digital forensic evidence.

• SafeBack. This tool is ‘primarily used for imaging hard disks of intel-based computer systems and restoring these images to other hard disks. It is a DOS-based program, which can be run from a floppy disk’ (Morris, 2003). Safeback is a very similar tool to EnCase and Vogon, however does not include the same precise analysis capabilities as these other software tools hold.

2.5.2 Types of Hardware tools

Hardware tools refer to the physical equipment used to collect digital evidence. These tools are often powered from a power point or from a suspect’s computer and will sometimes come in parts. It is the investigators primary job to make
sure all tools contain all possible parts. Hardware tools do not need to be downloaded onto a device so space can be saved and are also a lot quicker at retrieving data compared software tools. This chapter will be discussing the main hardware tools used in digital forensics and what they are used for.

2.5.2.1 No Write

This type of hardware forensic tool (also known as write blockers) enables the investigators to stop data from being written to the hard disk. This tool is compatible with multiple devices including USB adapters and IDE interface cables. This type of tool works by allowing read commands to pass but blocks all write commands, this will enable a user to read the evidence on the computer screen but will make it almost impossible for a user to interfere or tamper with the evidence. There are two types of NoWrite tools, Native and Tailgate. ‘A Native device uses the same interface for both in and out, for example a IDE to IDE write block. A Tailgate device uses one interface for one side and a different one for the other, for example a Firewire to SATA write block.’ (Ace Computers, 2015).

2.5.2.2 Write Protect Card reader

This tool is primarily used to transfer data from digital cameras, camcorders, PDA’s MP3 players etc. to a laptop computer. It is capable of reading several types of flash memory while blocking any writes to it. Wiles and Reyes (2007)
explain that this hardware tool appears as a palm sized package that features a USB connection to enable it to connect to a desktop. An advantages to a Write protect Card reader is that it can read up to four different media types at a time saving a lot of precious investigation time, it is also very portable and can fit within a bag or even a jacket pocket. A total of 12 digital media types can be read and recognized by this tool, this enables the device to be very diverse and will not require an investigator to carry around multiple card readers.

2.5.2.3 ImageMASSter Solo 3

This tool is primarily used for retrieving graphical images from a computer or desktop. It appears to be a lightweight portable handheld device that can be transported easily if needed to, this specific type of tool is able to acquire data from two hard drives at a top speed of 3GB per minute. Its capabilities include retrieving data from IDE, flash cards and SCSI drives. Keeping up with the recent technological advancements, the ImageMASSter solo 3 features a full touchscreen user interface and a biometric finger scanner so that only authorized users may use the device. It also automatically logs information and protects the data on the desktop from being tampered with.
2.5.2.4 FireFly IDE and FireFly SATA

Similar to the Write blockers the FireFly provides a ‘**hardware-based write-protected environment for the forensics imaging and processing of the attached IDE or SATA hard drive**’ (Marcella and Menendez, 2007). Both versions of the FireFly support FireWire 1394a and 1394b and can be set so that the user can either can read or write on the evidence. Of course the user should only write on data copies. FireFly is fully compatible with all operating systems as long as they hold FireWire support.
3.0 **Research Methodology**

3.1 **Introduction**

This chapter describes the research philosophy, strategy, design, methods and techniques adopted for this research study guided by Saunders Research Onion Model in Figure 3 below (Saunders *et al.*, 2012, p.160).

![Figure 3, Research Onion (Saunders *et al.* 2012)](image-url)
3.2 Research Methods

This section will be discussing the types of methods and philosophies that will be used within the dissertation. The research onion will be used, as a step-by-step guide on choosing which methods will be implemented.

3.2.1 Research Philosophy

The first layer of the onion that the researcher will be analyzing is the research philosophy layer. Of the three main Research Philosophies (Positivism, Realism and Interpretivism) put forward by Saunders et al. (2012), Interpretivism will be adopted as the most appropriate this is the research conducted, will include interviews. Qualitative methods will be used to gather the data and then the researcher will attempt to interpret the reasoning behind the data.

Saunders et al. (2012, p.673) defined interpretivism as ‘The epistemological position that advocates the necessity to understand differences between humans in their role as social factors’. When collecting research, the interpretivism approach try and understand others point of view. Interpretivism is a theory used from the middle of the 19th century and has been used to differentiate nature and social sciences, it follows that of a nurture approach insinuating that people change how they are based on the cultures that they live in. (The Open University, 2014).
Positivism is ‘an epistemological position that advocates the application of the methods of the natural science to the study of social reality’ (Bryman and Bell, 2015, p.8). It is because of this that positivism more commonly associated with quantitative research studies and thus considered to be an unsuitable approach for this qualitative study. Similarly Realism, which takes a view of science and disregards social opinions and imagination is also not a suitable approach. Participants are asked to express their opinions and use their imagination towards their idea to what the future of computer forensics will be.

3.2.2 Research Approach

Next it is important to consider the research strategies of induction and deduction.

According the Saunders et al. (2012, p.672) the inductive approach is a ‘research approach involving the development of a theory as a result of the observation of empirical data’. Its purpose is to gain a better understanding of the problem and make sense of the data that is collected. Effectively induction takes a “Bottom up” approach, it suggests that a person will conduct their analysis first before drawing up a theory. The Deduction approach however, takes a “Top down” approach, suggesting propositions will be made and tested due to a theory that is already drawn up. Deduction is better suited to a positivist paradigm whereas an inductive approach is normally better suited with an interpretive paradigm.
In line with the interpretive philosophy the inductive approach is used because interviews will be conducted using qualitative data effectively using the bottom up approach.

3.2.3 Research Strategies

The researcher has decided to use the Grounded theory strategy. The grounded theory is used primarily during a research process and ties with the interpretive and inductive research approach. It aims to look at patterns in the data collected in order to then sort this data into categories according to the respondent’s answers. ‘The procedure enables researchers to examine topics and related behaviors from many different angles- thus developing different comprehensive explanations’ (Glaser and Strauss, 1967; Corbin and Strauss, 2014, P11). Grounded theory is constructed from data collected during the research process and not prior to beginning the research and is very much based on the social aspect of social collection such as interviews and observations that are to be adopted for this research study.

3.2.4 Time Horizons

Cross sectional and longitudinal studies are the two main Time Horizons to be considered. A cross sectional study looks at the facts and observes without manipulation. With cross sectional studies, different population groups are compared allowing researchers to be able to compare different variables. A cross
sectional study is drawn up based on the criteria that quantitative and qualitative data research strategies will be used. Researchers choosing to work with cross sectional studies should be aware that the cause and effect cannot be determined based solely on figured obtained at the time of the study. If a researcher is interested in that outcome, it is advised that they pursue a Longitudinal study instead. ‘A fairly typical form of such research is when the researcher employs ..semi-structured interviewing with a number of people’ (Bryman and Bell, 2015).

Like Cross-sectional, Longitudinal studies also do not interfere with the participants, however they are conducted over a sustained period of time with the same subjects. A benefit of a longitudinal study is that researchers are able to monitor changes that happen in the target audience over a long period of time and are more likely to establish a cause and effect. This research study involves a number of interviews over a short period of time and will just feature data collected at the time of the interview, it will not determine the cause and effect and so a Cross sectional study will be conducted.

3.3 Methodology

The researcher has decided that the appropriate method of analysis will include conducting a number of semi-structured interviews. Semi-structured interviews will help gather reliable and valid data ready for analysis by conversing through
conversation with the participants involved. This type of interview involves the researcher using pre-formulated questions during the interview, however he/she has no rule that these questions have to be adhered to. The researcher may add or remove questions as they conduct the interview (Myers, 2013). This type of analysis will involve using both close and open-ended questions in order to gather quantitative and qualitative data that explores all areas of the chosen topic, according to the respondents’ answers, further questions can be asked to help the unit of analysis expand on their responses.

The purpose of using this method of analysis is so empirical data can be collected to provide an understanding of how each forensic tool works, and also distinguish the difference between the effectiveness of the software tools compared with the hardware tools. Thus the semi-structured design of the interviews will allow the participants to full elaborate on their answers as appropriate.

Before carrying out the interviews it is important that all possible data quality issues are thoroughly evaluated and all scenarios planned for in order to eliminate the risk of bias. Saunders et al. (2012) explains that there are four main data quality issues that need to be studied, these include reliability, forms of bias, generalization and validity.
• Reliability. Statistically the information provided in each interview should be very similar and have a positive correlation. If this is untrue the reliability of the information will become bias. Theoretically the reliability of the information is then determined on the forms of bias explained below.

• Interviewer Bias. This type of bias occurs when the interviewers tone of voice, presence and body language can affect the respondent’s answers and responses. Throughout the interview the answers obtained need to be honest and as close to the truth as possible. It is also important to build a level of trust between the interviewer and the respondents so they feel comfortable in what information they share.

• Response bias. Within these dissertation the researcher must make sure that the questions asked are not so sensitive that the respondent cannot answer. Another risk is the respondent may misinterpret the question and give an answer that is not relevant to the question. To prevent response bias it is important that the location of the interview be a place where the respondent feels comfortable in, the interviewer must also be very aware of their behaviour and that approach to which they ask the questions.
• Participant bias. May occur when collecting the unit of analysis. The biggest issue that may arise with this form of bias will be the risk that the participants chosen may drop out of the study or researcher will not be able to get any respondents to participate in the interviews.

• Generalization. The problem with conducting interviews is that they do not often include a huge amount of participants. It is unlikely that two people can represent the thoughts and preferences of 5 billion people. This problem will be apparent in any study of any size as it is near impossible to represent the entire population. However, as the sample size in this dissertation is reduced to only the south wales police digital forensics department it will be a lot easier for the results to generalize.

• Validity. Saunders et al. (2012) explains this as “the extent to which the researcher has gained access to the participants knowledge and experience”. This issue can easily be avoided simply be conducting a series of pilot studies.

The respondents that will be taking part in the interviews will be those who work with the digital forensic teams within the South Wales police force. The researcher will obtain a total of five participants through personal connections and through contacting the police force directly. Once the participants are
contacted and have verbally agreed to take part in the interviews they will be sent a participant consent form. Please refer to section 3.4 for more on the research sample.

The types of questions that will be used during the semi structured interviews will be open questions. Hair (2015) explains that open-ended questions allow insight to the participant’s answers and allow the interviewer to reach rich information. This provides the participants with the flexibility to provide a detailed and in depth answer to the questions asked. Depending on the answers given by the respondent, probing questions may then be asked to make the respondent elaborate on their answers and for the interviewer to seek a deeper explanation.

The participants themselves will decide the location of interviews that will ensure that they participants feel relaxed at all times. This should prevent the likelihood that they should ever bias the results due to feeling insecure or stressed. Allowing the participants to choose the location is also due to the fact that the police forensics department may not be accessible by non-authorized personnel. Interviews will take place at normal working hours and will last approximately one hour. If the participant gives consent to, all interviews will be voice recorded otherwise all information provided by the participants will be recorded on paper. To ensure the security of the information and the
participants all information that is collected from the participants will strictly confidential and will only be used for research purposes and not for any other reason. No names will be mentioned when documenting the research and no personal information will be given out.

Analysis of the empirical data collected from the interviews will involve Category coding techniques using an open coding technique. This technique involves breaking down the pool of interview data collected into sub headings and master headings to identify instances of where participants mention/refer to a certain word or topic. Each interview will then be analyzed to see if any of the answers that the participants gave have any correlation. Gorden (1992) specifies six basic steps that should be considered when coding interview data. These were:

1. “Define the coding categories.
2. Assign code labels to the categories.
3. Classify relevant information into the categories.
4. Test the reliability of the coding.
5. Measure the reliability of the coding.
6. Locate the sources of unreliability in the coding.”
3.4 Sample Population

It is important that the sample chosen is considered according to the dissertation’ aims and objectives. When conducting an interview, it is important that the participants have the appropriate knowledge on the topic before the interview takes place. For example, if you are interviewing to gain an understanding on the running of a business, you are more likely to choose participants that have experience with running a business. Becker (1998 p.260) explains that ‘selecting a sample to study should represent the full set of cases in a way that is meaningful and justifiable.’ This will be fulfilled using semi-structures interviews. These interviews will be electronically recorded before being put together ready for analysis.

Therefore a Purposive Sampling Technique will be used when to identifying the sample population. Saunders et al. (2012) explains that purposive sampling is a technique used on very small samples when the purpose is to collect information that is very informative. Those who adopted the grounded theory strategy are those who are more likely to use this sampling technique.

An issue with purposive sampling however is that it cannot be representative of the general population which can cause issues when analyzing into the reliability of the information given. However, it is important to note that the research question being analyzed will not be representative of the whole population as
not all members of the population will know what forensic tools are used in the police force. As the participants will most likely be from the police force in the surrounding area it will be hard for the researcher to represent tools used in the police force outside of Wales. For example, tools used in Scotland may be a lot different to tools used in Wales. To help this, the researcher will use a specific type of purposive sampling names Homogeneous Sampling, Saunders et al. (2012) explains that homogeneous sampling works by focusing on a particular group of people based on their characteristics or hierarchy in work. As the characteristics are likely to be very similar in those in the same job role it will allow the results collected to be explored in greater depth.

The sample population will be members of the South Wales police force that specialist in the digital forensic evidence department, the participants will be those that have a good knowledge on the forensic tools used in this department. The gender of the participant is not an affecting factor therefore participants will not be chosen based on their gender. The age of the participant is also not an affecting factor therefore participants will not be chosen based on their age. The unit of analysis will include five participants all of which will be from different digital forensic departments so that the researcher can investigate whether the opinions of each participant changes based on the police force they belong to.
Five participants have been chosen due to the factor that the forensic tools used in each forensic police department are likely to be very similar. This therefore should produce similar results. However, the sample is big enough so that if the data does differentiate from participant to participant, the researcher has enough data to analyze. The Researcher has connections with officers of the Police Force, this will enable her to get in touch with the necessary participants needed for the interviews.

3.5 Ethical Considerations

Prior to data collection formal Ethics Approval must be granted for the research study. Consequently an Ethics Approval form was completed and submitted to the Cardiff School of Management Ethics Committee and approval was granted ethics Number 2015D0570. A copy of this ethics form can be found in appendix 1.

When dealing with ethics the researcher has decided to follow the Bera Guidelines for Educational research (2011). The most Important guidelines that were followed during the research are outlined below.

Informed Consent

The precautionary steps will have to be made to ensure that all the participants know what the study is for, why their participation is necessary and how the
information recorded will be used. Ways of recording data (video/voice) will also be explained to the participants and all participants can choose whether they want to comply with these methods.

**Right To Withdraw**

Researchers must express to the participants that they have the right to withdraw from the research at any time for any or no reason. If a participant does withdraw, the researcher must accept this decision and evaluate why they may have done so.

**Privacy**

Participant’s data must be kept confidential at all times. Researchers must recognize that the participants are entitled to privacy and their rights to confidentiality must be explained to them before research starts. Researchers must also comply with the legal requirements on storing data written by the Data Protection Act (1998).

### 3.6 Analysis of Data

When analyzing the collected data, the researcher has decided to use category-coding techniques. This involves comparing all units of meaning that arise in the respondent’s answers and categorizing these units with similar units of meaning. New categories will be created if the unit of meaning has no similar units. With
thorough analysis the categories created can then be changed merged or reduced to create new relationships (Goertz and LeCompte, 1981; Maykut and Morehouse, 2002).
4.0 Results and Analysis

This chapter will be looking into the results obtained from the semi-structured interviews that were conducted. Each participant was contacted either by phone or by email and were situated in the South Wales Police at some point in their working career. The data was collected and then processed in response to the information gathered in Chapter 2. The main goal from conducting the interviews was to develop a base of first hand knowledge from police officers and staff on the developments and effectiveness of digital forensic tools. From the information gathered, it can be confirmed that this goal was accomplished. The Information gathered from the interviews will be split into categories so that the information gathered from the interviews can be analyzed thoroughly.

4.1 Response Rate

When trying to contact police officers that were based solely in the digital forensic field, the researcher was faced with problems from all angles. From the primary research it was clear that to gain contact with participants in such a field, you have to first go through a lot of first hand contacts before hand. The researcher felt that to gain her five digital forensic officers, she had to go through as many as 10 contacts prior to getting the correct people, giving a response rate of 50%.
However, once the researcher had made ground on finding the correct participants, she then found that five chosen participants were very complying and were open to being interviewed and audio recorded. 4/5 Participants were Male, this was expected as the ratio for females participating in a computer related workplace is seemed to be significantly lower than males. In fact the statistics for Females even taking a Computer Science degree is 1 in every 10,000 (Drinkwater, 2015)

4.2 Current Hardware and Software Tools being used to collect Digital Forensic Evidence

A popular hardware tool that was particularly mentioned across Participants 1, 2, 3 and 4 was the use of Tableau Write Blockers. This tool was not mentioned in this dissertation, however a very similar tool has been mentioned in chapter 2.5.2.1. Participant 4 explained “The main purpose of this tool is to enable the South Wales police force to work with data without manipulating the data in anyway” This outcome was not a surprise as when researching different types of hardware tools, the Write Blockers were a tool that appeared to arise quite frequently across books and websites.

Tableau Password-protected tools were also mentioned quite frequently throughout the interviews. For example, participants 2, 4 and 5 explained that the Tableau Device software was used to access password protected and
encrypted files. Participant 3 explained, “the use of encryption as a way to keep data hidden or safe is very, very common and shows up frequently when we come across data that is protected or hidden”.

Another Software tool that was frequently mentioned across Participants 1, 4 and 5 was the FTK Imager and other very similar disk imaging extractor tools. Participant 1 explained that they use the FTK Imager to create an “exact image of the device. This would include gaining access to emails, Images, documents and replicating these data sources onto a CD or external hard drive. The tool will not delete or remove any data in the process of doing so” Participant 5 also explained that the types of data that the FTK Imager takes is logical or live data and data from the terabit drive which is deleted data.

EnCase was a software forensic tool that appeared frequently in the interviews. It was interesting to see that every participant mentioned EnCase as a forensic software tool first and each described the tool as “very effective” and “practical”. Participant 3 got into more detail and explained that EnCase is used mainly in retrieving information from a computers Hard drives within the police department and works on making a replica image of these hard drive.

Internet Evidence Finder was a forensic tool that was touched upon by participant 1. He explained that this tool was useful for analyzing data that the
suspect has handled on the Internet. This can include Facebook data, cloud based services, E-mail application and other web browser activity. Participant 1 explained that this tool was successful and pulling up information that would otherwise take months to find.

The Sleuth Kit was another forensic tool identified through the interviewing process. Participant 5 seemed to think quite highly of the tool, saying it was “one of the most successful imaging tools used within the department”. This was interesting as it did not come up very often while conducting secondary research.

The researcher found that even though Mobile Phone forensics was not the focus of this study it was interesting to see that the majority of the participants were more interested in talking freely about mobile phone forensic tools over computer forensic tools. To capture and expand upon this further questions concerning mobile phone forensics were asked. It was found that most of the answers correlated with each other on the types of tools used. The most popular seemed to be IT Bot and JTAG for mobile phones. Participant 1 and 2 were particularly interested in talking about these types of Mobile Forensics tools, both tools were used to unlock phones and accessing data but JTAG in particular worked by using data acquisition methods by connecting to the chips within a mobile phone and asking it to extract data kept on other memory chips.
From the above analyses it was interesting to ascertain which types of tools were most used within the departments of the South Wales Police force. It was expected that a lot of the tools mentioned in Chapter 2 would be mentioned throughout the interviews, however this was not the case. Thus reflects the fast pace of IT development in this field that continually evolves to keep up with criminal activity. The most popular tools that the participants seemed to talk about were the Tableau Write-Blockers, Tableau Password Protector tools and EnCase. This came as a surprise, as when conducting the secondary research, the Tableau tools in particular were not mentioned in any of the resources looked at.

4.3 Effectiveness of Computer Forensic Tools

When discussing this topic, it was expected that the participants would mention in detail some major issues thereby influencing the effectiveness of the tools, however form all the participants answers this was not the case. In fact none of the five participants involved had a negative aspect on any of the tools, nor thought that one tool was more effective than another. Participant 1 started this off by explaining that “not one tool is more superior than another, not one tool works every job and covers every aspect of a computer. All tools are effective in their own ways”.
Participant 2 also supports this view saying “all of the tools used in our forensic department do their job, it is not often that we ever have any issues with their performance” and “I do not think that one tool is more effective than another, they all perform different functions and are used for different purposes”.

There was an instance however where Participant 3 explained that although all the tools used in his forensic department are effective at gaining forensic evidence, new types of computer hardware and software are emerging and so new forensic tools are having to be introduced all the time in order to keep up.

4.4 Frequency of New Tools being Introduced

When asked “How often are new forensic tools being built and introduced into the police force?” it was clear from the results that the South Wales Police department are on top of this all the time. From the respondents answers you could conclude that there was a strong correlation between the time that a system was updated to the time a new tool was introduced. Participant 1 explained that they are “playing catch up all the time, especially with software. Mobile phone applications in particular are updating constantly and so new software tools and codes are having to be brought via every update”.

Participant 2 and 3 explained that they often just get updates to tools that they already hold, for example write blocker tools that were introduced 10 years ago
are not going to be compatible with recent technology and so they will be sent the most recent tools as soon as they are discovered.

Participant 4 and 5 did not have much to say on the topic however were both happy to say that there tools are continually updated. Participant 4 explained that he finds that their software tools are persistently updated a lot more than their hardware tools and that their hardware tools are a few years old now but still as effective as they were when they arrived.

4.5 Cost of Tools

Throughout the interviews the question about cost almost always came up despite it not being a question that was included on the interview questions sheet. The researcher found that across all interviews the answer to this category varied depending on what devices or what tools they were going to be using. All Participants were unable to specifically state the costs of the tools they used so figured cannot be drawn up. However, an interesting finding came from Participant 1 who explained that often, (particularly with mobile phones), the police will take a device to be unlocked or taken apart via mobile unlock shops and will use online Chinese companies to ship over digital forensic tools due to the small cost of doing so. As it stands there were no data security issues in doing so as all tools are tried a tested before being used on particular devices.
When asked to comment on the biggest weaknesses of using computer forensic tools, 4/5 participants were quick to mention that the cost of the tools, particularly the Hardware tools were very expensive for the police to purchase.

However, it was also mentioned between most of the participants that if (on the off chance) the department does not have a specific forensic tool that they need to access a device, a request for that specific tool will be filled out and will be available in the workplace within the next day, suggesting cost would not be an issue. Participant 1 and 2 explained that this was found to be more of a case with software tools. Everyday new free software is being transferred over to the company, this is due to the apps on digital devices changing and upgrading constantly. A constant game of “catch up” is being played as long as devices are evolving.

4.6 Strengths and Weakness’s of Tools

Another question each participant was asked was what they thought the strengths and weaknesses were of the tools that they were using. Participant 1 started off by explaining that a big plus for his department was that all the tools were easy to use, you do not need to hold that much knowledge on computer science to understand how to use each tool, he also explained that the tools that come into the forensic department are easy to find access too and are required when requested. He also explained that with software, it is being updated
constantly and this allows the police to stay on top of evidence all the time. He stated “70% of a device is readable by software alone and the hardest parts of computer to access are disks that are full encrypted.”

Participant 2 mentioned that each tool has their own strengths and weakness “It would be nice to have a number of tools that is compatible with multiple platforms and can perform multiple tasks. At the moment the offices are filled with hundreds of different tools and it’s hard to keep track of each tool”.

Participant 3’s view was that each tool “Does what they say on the tin and don’t really vary. Each tool does what you ask it too, the only issue that we find with tools is that they can get very expensive” Participant 3 also went on to say that at times when new technology (such as a new mobile phone) comes into the department for analysis, none of the software tools available are adaptable to the technology, therefore the forensic department have to wait for the correct tool to be created, which can take a few weeks.

Participant 4 held a very similar view to the participant above, he also thought that each tool is as effective as it is supposed to be, they work as they should and it is not often an issue arises with the products. He did however also mention that the cost of some of the computer forensic tools are “extortionate” and “ridiculous” for the functions that they provide, especially hardware tools as
you could be spending hundreds on a tool that only helps you if you accidently slip up and tamper with evidence.

### 4.7 Future of Digital Forensic Tools

The last question that the participants were asked was what they thought the future would be looking at for Digital Forensic tools. Two out of the five participants (P4 & P5) were quite taken aback by this question and found it very difficult to answer. Participant 4 (P4) explained that the tools do not really advance unless they have a reason to, the future of digital forensics all depends on the future of technology. Although this did not directly answer the question that was posed it did however put in perspective that digital forensic tools often really do rely a lot on the advancement of technology in order for new tools to be built.

Three of the participants however did manage to answer the question and put forward a few ideas as to what they think they will see in the future of Computer Forensics. When Participant 1 was asked this question he explained that “Software is getting more complicated and analytical by the moment and just like computers have advanced so much already, new tools will need to advance with the progression of software. More functions mean new tools, the speed
Participant 2 believes that tools in the future will become a lot easier to use. So much so that the operator of a computer may not have to physically go searching for anything through these tools or will need any advanced training on how to use these tools. Researchers who have not necessarily studied computer science such as an art degree or psychology degree will be able to learn how to use these tools and help police track down vital evidence.

Participant 3 explained that he predicts, “A lot less hardware will be involved and files such as Images, PDFs, videos etc. will be stored within the cloud. There will become a time where you no longer have to search the hardware of a computer because cloud computing will be storing all the necessary information”
5.0 Conclusion

5.1 Aims and Objectives Review

This dissertation was set out to explore the impact of Computer Forensic tools and has identified the uses and the purposes the effectiveness and usefulness of a handful of tools used within the South Wales Police Force. The Dissertation has also sought to identify the types of data collected, the laws and ethics the Police have to abide by, what the future will bring for Computer Forensic tools. The general theoretical literature on this subject was inconclusive regarding the effectiveness of the tools used within specifically the South Wales Police Force. The reason for this is not clear however it is suggested that this is due to the newness of the topic area, making it harder to find current publications on the topic. South Wales is also a very small area in the UK and so would not be in high demand to research into. Therefore the study sought to answer the following Aim:

- To investigate current computer forensic tools and evaluate their use and effects on finding evidence in the area police force.

Both primary and secondary research methods were utilized to establish the current forensic tools being used and illustrate how these tools have played a vital part in gathering evidence.
The research objectives have been achieved as set out below: Research Objective 1

- To examine the current status of computer forensic tools used by the South Wales Police force

Objective 1 was established during the Primary Research stage. Members of the South Wales Forensic teams were asked to reveal the current tools used within their departments and shed light on exactly how useful they were at collecting forensic evidence. From the research it was concluded that vast majority of tools are used to collect vital evidence, not one tool performs exactly the same as another and so all tools no matter their status have their own qualities. It was surprising that the primary research answers on tools came up different to the tools collected in Chapter 2. This was especially true with the Tableau tools, when conducting all the secondary research; these tools were not mentioned or even brushed upon. We cannot ignore however, that even though these tools were important to the South Wales police forensic Departments, they may not be important to Police forces in other countries.

Although only mentioned briefly within the body of the dissertation it was interesting to see how many criminals are actually using computer forensic tools
to actually create crime. This was seen during the Talk Talk hack explained in Chapter 2.4.

Research Objective 2

- Discuss the effectiveness of tools are used to find evidence in the South Wales Police force

Objective two ties in closely with the dissertation's research question, therefore is seemed to be one of the more significant objectives. In order to meet this objective the researcher conducted both primary and secondary research to analyze how each tool is implemented and integrated into the forensic field. From the research conducted via both research types, it was understood that there were minimal problems with any tools used in police forces across the world. This could then confirm that the effectiveness of both Hardware and Software tools were appearing to be quite higher than expected. The biggest problem that seemed to have a significant effect on the majority of the participants was the cost of the tools, even though there were mixed opinions in this particular area, the cost of the tools seemed to have the biggest impact on the participant’s opinions on the tools.

However, although it seems that there has been no direct problems arisen within the South Wales Police force regarding the effectiveness of Computer
Forensic tools it was mentioned across 3 or 4 of the participants that this is not the case for all Computer Forensic Departments across the world, In fact a Forensic case in America being battled by the FBI could suggest that some forensic tools do in fact hold a weakness (Chapter 2.4).

Research Objective 3

- Analysis the specific benefits and obstacles that each tool brings

Objective three refers closely to the effectiveness of the forensic tools mentioned in Objective two. However, is looking significantly deeper into what makes the tools effective in the first place, by analyzing the strengths and weakness’ of each tool. From overviewing Chapter 4 it was clear from the results, that when referring to the weaknesses of each tool there were no significant problems or any problems that would prevent the officers from gaining access to forensic data. The only problem that seemed to make an impact with the participants (like mentioned in Objective two) was the cost.

From the research, it was concluded that the strengths of Computer Forensic tools strongly overweigh the weaknesses. Each tool used within the South Wales police force seemed to be in high working order with very little possibility of failure. This allows us to have confidence that Digital forensic tools are doing their jobs properly and efficiently.
Research Objective 4

- Put forward recommendations of how tools can be improved

The researcher decided to only carry out research on the South Wales area because it was in close range and was realistic for the amount of time the researcher was given to complete the dissertation. The researcher recommends that for future work it would be an idea to compare South Wales’ Forensic tools to those across wales, the UK, Europe or maybe even the world. It would interesting to see if tools are cheaper and more effective depending on where they are originally made.

Another recommendation would be to study Mobile Phone forensics as well as Computer Forensics. There seemed to be a lot of information held within this field and would be an interesting topic to research.

The researcher also suggests interviewing a larger number of participants. 5 Participants was not a big enough number to represent the whole of Wales. If the study included participants from all regions, this could create data that would be representative of all of Wales.
5.2 **Limitations**

Although the researcher had thoroughly prepared for all possible limitations or problems for the dissertation, throughout the course of completing the dissertation some small limitations did arise.

A couple of problems arose during the interviews. Although the researcher had a few connections to the Police force, she found it hard to directly make contact with people within the forensic departments. The response rate of getting participants that were fit for interviews was as little as 50%. That meant that the researcher had to wait twice as long as she had hoped to gain the relevant information for analysis.

Another problem that arose was that two of the participants were unable to conduct a face-to-face interview, because of this the researcher had to compromise and conduct a phone interview. This may have restricted the researcher in getting all the information possible out of the participants. It also made audio recording these participants very difficult, the recording equipment the researcher held failed to fully record both phone conversations.

The recording equipment then broke and so the researcher unsuccessfully managed to record any of the interviews in full. However, the researcher was not disheartened by this and managed to get all the information she needed
down on paper. This information was then types up straight away so that the information was fresh in the researchers mind.

Other limitations include the size of the sample and location. The Size of the sample cannot be representative of all police officers thoughts and opinions. Just because these five participants prefer to use tableaux tools, just not mean that all police officers will.

The Location chosen for this dissertation is also not representable for all police forensic departments across the world. Tools used in South Wales can be completely different compared to the ones used in America or the rest of Europe.
References


Legislations


Appendix 1: Application for Ethics Approval

When undertaking a research or enterprise project, Cardiff Met staff and students are obliged to complete this form in order that the ethics implications of that project may be considered.

If the project requires ethics approval from an external agency (e.g., NHS), you will not need to seek additional ethics approval from Cardiff Met. You should however complete Part One of this form and attach a copy of your ethics letter(s) of approval in order that your School has a record of the project.

The document Ethics application guidance notes will help you complete this form. It is available from the Cardiff Met website. The School or Unit in which you are based may also have produced some guidance documents, please consult your supervisor or School Ethics Coordinator.

Once you have completed the form, sign the declaration and forward to the appropriate person(s) in your School or Unit.

PLEASE NOTE:
Participant recruitment or data collection MUST NOT commence until ethics approval has been obtained.

PART ONE

<table>
<thead>
<tr>
<th>Name of applicant:</th>
<th>Lucy Taylor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor (if student project):</td>
<td>Dr Hilary Berger</td>
</tr>
<tr>
<td>School / Unit:</td>
<td>Cardiff Metropolitan University, CSM</td>
</tr>
<tr>
<td>Student number (if applicable):</td>
<td>St20036591</td>
</tr>
<tr>
<td>Programme enrolled on (if applicable):</td>
<td>Business Information Systems</td>
</tr>
<tr>
<td>Project Title:</td>
<td>Investigation into the current use of computer forensic tools in the area police force and their effects on</td>
</tr>
<tr>
<td>Expected start date of data collection:</td>
<td>01/02/2016</td>
</tr>
<tr>
<td>Approximate duration of data collection:</td>
<td>01/03/2016</td>
</tr>
<tr>
<td>Funding Body (if applicable):</td>
<td>N/A</td>
</tr>
<tr>
<td>Other researcher(s) working on the project:</td>
<td>No</td>
</tr>
<tr>
<td>Will the study involve NHS patients or staff?</td>
<td>No</td>
</tr>
<tr>
<td>Will the study involve taking samples of human origin from participants?</td>
<td>No</td>
</tr>
</tbody>
</table>
Does your project fall entirely within one of the following categories:

<table>
<thead>
<tr>
<th>Category</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper based, involving only documents in the public domain</td>
<td>No</td>
</tr>
<tr>
<td>Laboratory based, not involving human participants or human tissue samples</td>
<td>No</td>
</tr>
<tr>
<td>Practice based not involving human participants (eg curatorial, practice audit)</td>
<td>No</td>
</tr>
<tr>
<td>Compulsory projects in professional practice (eg Initial Teacher Education)</td>
<td>No</td>
</tr>
<tr>
<td>A project for which external approval has been obtained (e.g., NHS)</td>
<td>No</td>
</tr>
</tbody>
</table>

If you have answered YES to any of these questions, expand on your answer in the non-technical summary. No further information regarding your project is required. If you have answered NO to all of these questions, you must complete Part 2 of this form.

In no more than 150 words, give a non-technical summary of the project:

Forensic tools in the police force are very important in gaining evidence that can be used in court. They can be the key to finding evidence that decides whether or not an offender goes to jail or not. These tools are improving all the time and with technology increasing day by day it is important that the forensic teams keep up to date with it all in order to keep offenders at bay and keep the general public safe. This dissertation will be discussing the implementation of computer based forensic tools used by the police force and the impact these tools have had in the finding of police evidence. To do this the student will be using semi-structured interviews on members of the police to gain primary data on their use of forensic tools. The student will also use secondary data to provide an initial understanding of the project.

DECLARATION:
I confirm that this project conforms with the Cardiff Met Research Governance Framework

I confirm that I will abide by the Cardiff Met requirements regarding confidentiality and anonymity when conducting this project.

STUDENTS: I confirm that I will not disseminate any material produced as a result of this project without the prior approval of my supervisor.

Signature of the applicant: Date:

FOR STUDENT PROJECTS ONLY

Name of supervisor: Date:

Signature of supervisor:
PART TWO

A RESEARCH DESIGN

A1 Will you be using an approved protocol in your project?  No

A2 If yes, please state the name and code of the approved protocol to be used

N/A

A3 Describe the research design to be used in your project

For the project the Primary data will be collected using Semi-Structured interviews. The participants for these interviews will be members of the police force. Once the data has been collected, it will be analysed using a Data cloud and Category coding in order to conduct an in depth analysis. Semi-Structured interviews have been chosen so that the student can prepare for the interview beforehand but it also gives the student the ability to ask questions off book enabling the student to have the ability to gain in-depth information. It will also allow the participants to have freedom of speech to give their full views and opinions.

Semi-Structured interviews will allow both qualitative and quantitative data to be collected. The planned sample for the interviews will be approximately 5 participants. All 5 being members of the police force. Since the sample is very specific, purposive sampling will be used. Each participant will be contacted via phone and/or email in order to request an interview. Only 5 participants have been chosen due to the fact that the forensic tools used in each forensic police department are likely to be very similar.

1 An Approved Protocol is one which has been approved by Cardiff Met to be used under supervision of designated members of staff; a list of approved protocols can be found on the Cardiff Met website here
and so the results gained from each interview are predicted to be alike. However, the sample is big enough so that if the data does differentiate from participant to participant, the student has enough data to analyse. Some of the participants will be made through person connections, others will be found via snowballing sampling.

The interviews will be carried out in the location in which the participant prefers, as access into the police forensics department may not be granted. This will likely be in an office within a police building or meeting room. Interviews will take place in normal working hours and will last approximately one and a half hours. All interviews will be voice recorded if the participant gives consent to do so, otherwise all information provided by the participants will be recorded on paper. All questions have been looked over by a member of the police force and have been approved as feasible questions that can be asked during the interviews.

All information that is collected from the participants will strictly confidential and will only be used for research purposes and not for any other reason. No names will be mentioned when documenting the research and no personal information will be given out. Each participant will be told that they are going to be recorded during the interview and will have the opportunity to give consent if they do not wish to be voice recorded.

Research questions have been looked over by a police forensic officer already, therefore we know that the questions asked will not be too sensitive to the participants.

| A4 Will the project involve deceptive or covert research? | No |
| A5 If yes, give a rationale for the use of deceptive or covert research | N/A |
| A6 Will the project have security sensitive implications? | No |
| A7 If yes, please explain what they are and the measures that are proposed to address them | N/A |

**B PREVIOUS EXPERIENCE**

B1 What previous experience of research involving human participants relevant to this project do you have?

None

**B2 Student project only**

What previous experience of research involving human participants relevant to this project does your supervisor have?

The students supervisor has a 12 years of experience conducting research involving human participants.
### C POTENTIAL RISKS

#### C1 What potential risks do you foresee?

When evaluating potential risks this research will be referring to the BERA guidelines to ensure that the best is done to eliminate all potential risks. However here are some of the risks that could possibly arise.

- All interviews will be arranged in advance however; this does not exclude the risk of one of the participants pulling out last minute. This could potentially interfere with my timeline and set me back with my research.
- Another risk could be that the participants do not consent to being interviewed meaning I would have to go out and find new participants, which would also be time consuming.
- Another risk could be the possibility of interviewer bias. If the interviewer talks in a specific tone or in a certain way, this could influence the participant’s answer.
- Participant bias will also have to be monitored. The participant should be truthful and not just say what he/she thinks that the interviewer wants to hear.

#### C2 How will you deal with the potential risks?

As said above to eliminate the possibility of potential risks the researcher will be referring to the BERA guidelines. Here are some of the ways in which the researcher can try and prevent risks.

- All participants will be able to give voluntary informed consent; this will ensure that the participant is fully aware of what is asked from them and why they have been asked to participate.
- There will be Openness and Disclosure throughout. Deception will certainly be avoided and it will be explained to the participant that the information they give is strictly for the purpose of the research paper and that all personal information to them will not be mentioned within the paper.
- Participants will be made aware that they can withdraw from the research at any point.
- Researcher must maintain positive throughout, any negative thoughts may interfere with the mood of the interview and therefore on the participants mood.
- Researcher will use the same tone throughout the interview in order to prevent influencing the participants answers.
- Researcher will use the correct terminology when asking structured questions and special care will be taken when asking unstructured questions in order to not influence the participants answers.
- All information that the participant gives of themselves will be kept confidential and private and all stored/used information will abide by the Data Protection Act (1998).
When submitting your application you **MUST** attach a copy of the following:
- All information sheets
- Consent/assent form(s)

An exemplar information sheet and participant consent form are available from the Research section of the Cardiff Met website.
Appendix 2: Uncompleted Participant Consent Form

PARTICIPANT CONSENT FORM

Reference Number: 2015D0570
Participant name or Study ID Number: Participant 5
Name of Researcher: Lucy Taylor

Participant to complete this section: Please initial each box.
1. I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.
2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason.
3. I agree to take part in the above study
4. I agree to the interview being audio recorded
5. I agree to the use of anonymised quotes in publications

_______________________________________ Date:
Signature of Participant

Name of person taking consent: Lucy Taylor

___________________________ Date: 19/02/2016
Signature of person taking consent

* When completed, 1 copy for participant & 1 copy for researcher site file
Appendix 3: Participant Information Form

Information Sheet for Business Information Systems dissertation research

You will be given a copy of this information sheet.


Researcher name: Lucy Taylor
Contact details: 20036591@outlook.cardiffmet.ac.uk
Supervisor’s name: Dr Hilary Berger
Contact details: HBerger@cardiffmet.ac.uk

I would like to invite (participant) to participate in this research project

Details of Study:
The research aims is to investigate current computer forensic tools and evaluate their use and effects on finding evidence in the area police force.
For the project the Primary data will be collected using Semi-Structured interviews. The participants for these interviews will be members of the police force. Once the data has been collected, it will be analysed using a Data cloud and Category coding in order to conduct an in depth analysis. Semi-Structured interviews have been chosen so that the student can prepare for the interview beforehand but it also gives the student the ability to ask questions off book enabling the student to have the ability to gain in-depth information. It will also allow the participants to have freedom of speech to give their full views and opinions.
The Benefits of the research will be for the dissertation only. It will allow the student to gain an in depth analysis on the types of tools used within the South Wales police force. All information that is collected from the participants will strictly confidential and will only be used for research purposes and not for any other reason. No names will be mentioned when documenting the research and no personal information will be given out. Each participant will be told that they are going to be recorded during the interview and will have the opportunity to give consent if they do not wish to be voice recorded.
A total of five participants will be taking part in interviews across the South Wales Police force. Each participant can answer questions on their own terms, giving as little or as much information as they would like to. The number of questions asked will depend on the respondents answers but should only take around 30 minutes to complete.
Interviews will be documented on a work document and/or audio recorded.
You may withdraw your data from the project at any time up until it is transcribed for use in the final report (22nd April).
Recorded interviews will be transcribed (written up) and the tape will then be wiped clear.
If you decide to take part you will be given this information sheet to keep and be asked to sign a consent form.

You are welcome to request a copy of the dissertation once it has been completed, if you wish to do so.
Please discuss the information above with others if you wish or ask us if there is anything that is not clear or if you would like more information.
It is up to you to decide whether to take part or not; choosing not to take part will not disadvantage you in any way. If you do decide to take part you are still free to withdraw at any time and without giving a reason.

All data will be collected and stored in accordance with the Data Protection Act 1998
Appendix 4: Interview Questions

Interview Questions

These interview questions will be conducted in a controlled setting and will be used with the intention of collecting information to include in the dissertation only. Reasons for conducting the Semi-structured interview is for the student to gather information revolving around the use of hardware and software tools in police forensics. Any information given to the student will be kept confidential and will be disposed off once the dissertation is completed. The participants have the right to withdraw at anytime and will need to complete a participant consent form before taking part in the interview.

1. Do you deal with Software or Hardware tools?
   (If Software refer to Software Tools section, If hardware refer to Hardware tools section, if both read all questions)

Hardware Tools
1. Describe the types of hardware tools that are used as a method of subtracting vital digital forensic evidence

2. What types of hardware tools do you find most effective and why? Do you think any of these tools can be improved?

3. What do you believe the strengths and weaknesses are with obtaining digital forensic evidence?

4. What do you think the future will look like for forensic tools?

5. Are there ever cases where the security of a device is so high, all forensic tools fail to subtract information?

6. How often are new forensic tools being built and introduced into the police force?

7. Do you have any questions?

Software Tools
1. Describe the types of software tools that are used as a method of subtracting vital digital forensic evidence

2. What types of software tools do you find most effective and why? Do you think any of these tools can be improved?
3. What operating systems do you use to collect digital evidence?

4. How often are new forensic tools being built and introduced into the police force?

5. Are there ever cases where the security of a device is so high, all forensic tools fail to subtract information?

6. What do you think the future will look like for forensic tools?

7. Do you have any questions?

   **Work with both**

1. Are hardware tools more effective compared to software tools?
Appendix 5: Participant 1 Interview Notes

Participant 1 Interview - Phone interview

1. Tool is like a block to not more change to original evidence, makes a copy of evidence. IT is a tool for unlocking phones & ITag - chip off.

2. Not one tool is more superior than another, not one tool works every job and cares every aspect of a computer. All tools are effective in their own ways.

3. Some of the tools are free and easy to use, you don't need to hold a great deal of knowledge to understand how they work. Software update frequently, 70% of a device is readable by software more hardest parts to access are fully encrypted.

4. Speed and capability of each tool will increase and tools will become easier for people.

5. Full disk encryption & Bit locker are harder to break into.

6. Playing catch up all the time, especially with software. Mobile phones in particular, new codes and tools coming in on every update.

7. Software put to our bases if needed. Often for technology such as mobile phones, i.e. unlocking Chinese companies will ship over tools or go to mobile unlock shops.
1. Non-powered tablets. Software, FTK Imager creates an image of device, including email images, replicating these data sources onto a CD or external hard drive, not delete data. Encase, Internet evidence finder - analyzing Internet data in FB, cloud, email. Pulls up information quickly.

2. Answered

3. Windows - use forensics, use computer from a Linux disk

4. Software will get more complicated & analytical. Computer advancements - new tool to advance virtual software

5. Answered

6. Advances all the time. Storage advances = issue because will cost more. Encryption getting harder

7.

1. v different, different scenario
Participant 2 interview - face to face

1. Software

1. Tableau software i.e. password protected tools used for unlocking files that have been encrypted. Ensure - examining data on removable disks.

2. All tools in department do job, not often that there is issues with performance do not think one tool is more effective than another, perform differently, different purposes.

3. Own differences. Nice to have tool that is compatible with multiple platforms & perform multi tasks. Hard to keep track of tool.

4. Update old tools. Tools such as uuid; had issues 10 years ago, not compatible with recent tools, sent recent tools. New software is given to company free.

5. Not often can get into tech encrypted files the hardest.

6. Not easier to use, operator wont have to physically do anything, don’t need computer degree.
Appendix 7: Participant 3 Interview Notes

Participant 3 interview - Phone interview

1. both

2. Tableau write blocks & password protector tools used to access password protected & encrypted files. The use of encryption as a way to keep data hidden or safe is very common and shows up frequently.

3. Always looking out for new hardware. All tools in department are effective however.

4. Does what it says on the tin and doesn't vary each tool does what you ask it to however, it expensive. New technology i.e. phone will come, no tools compatible, how to update for new tools to come in.

5. A lot less hardware involved, go towards cloud computing i.e. the point that a computer will no longer need hardware

6. Not in our department - FBI case in America

7. Updates to tools we already have

1. Encase - used to retrieve info from compute hard drives & makes replica images

2. Very effective tool

3. Windows, Linux, Os

4. Answered

5. Answered

6. Answered

1. Work together, couldn't do it without hardware
Appendix 8: Participant 4 Interview Notes

Participant 4 interview - face to face

1. Both

1. Firefly & Tableau tools - used to protect data when looking at information.
2. Image tools are also used - can’t name.
3. Purpose of Tableau is to enable us to work with data without manipulating.
4. Tools are effective, no issues so far. Do what they are supposed.
5. Do what they are meant to. Cost can sometimes be extortionate and for licenses is recurring. Hardware more expensive.
6. Tools don’t advance unless they need to depend on future tech.
7. No cases

1. Encase, X-ways - recovered.
2. Answered
3. Windows, OS, Caine
4. Answered
5. Answered
6. Answered
7. Answered

1. Same effectiveness. Hardware more expensive
Appendix 9: Participant 5 Interview Notes

Participant 5 interview - face to face

1. Both

1. Tablar tools, FTK Imager - logical-die data, barebit drive data - deleted data
   Sleuth Kit - one of the most successful imaging tools with department
2. All tools as good as each other, different functions, can't say one is better than another.
3. Biggest weakness is cost, biggest strength is durability and success rate of tools in gaining evidence
4. (Couldn't think of anything)
5. None in department - look at American FBI case
6. Tools continuously updated, new tools only brought in when needed

1. See answer 1 above
2. Answered
3. Linux OS Monday
4. -
5. -
6. -
7. -

1. Both as effective as each other