Anti-Forensics: A Practitioner Perspective

Richard de Beer, Adrie Stander and Jean-Paul Van Belle
Department of Information Systems, University of Cape Town
Private Bag, Rondebosch, 7701, South Africa
Adrie.Stander@uct.ac.za
Jean-Paul.VanBelle@uct.ac.za

ABSTRACT

With the increase in cybercrime, digital evidence is becoming an integral part of the judicial system. Digital evidence is to be found everywhere from computers, to mobile phones, ATMs and surveillance cameras, and it is hard to imagine a crime that does not contain any element of digital evidence. It is however not simple to extract such evidence and present it to court in such a way that there is no uncertainty that it was not changed in any way. Thus the responsibility placed on a Digital Forensics (DF) practitioner to present usable evidence to a court is increasing fast. In some respects, however, it is relatively easy to get rid of digital evidence or to hide it. Many tools exist for cybercrime criminals to prevent DF practitioners from getting their hands on information of probative value. Such tools and methods known as Anti-Forensics (AF).

The purpose of this study is to identify the abilities of DF practitioners to identify the use of AF in their active investigations. The research model used, attempts to identify all the factors and constructs of AF that impacts on investigations. This model was then used to develop a survey instrument to gather empirical data from South African DFs.

The research has shown that whilst South African DF practitioners perceive DF as having an impact on their investigations, they also perceive electronic evidence as forming only part of the evidence presented to court, and that even if most of the usable evidence of lost, some will generally remain.

It was also found that while most DF practitioners in South Africa are well versed only in the more commonly known AF techniques. They do not rate their abilities on more complex techniques well. Finally, most DF practitioners appear not to actively attempt to identify AF techniques as part of their investigations. This combined with a lack of understanding of more complex AF techniques could leave South African DF practitioners exposed by missing important evidence due to lack of technical proficiency.

KEYWORDS

Digital forensics; anti-forensic tools; anti-forensic methods; digital forensic evidence; South Africa.

1 INTRODUCTION

Forensics as a scientific discipline is the process whereby science is used to investigate artefacts or transfer of evidence and interpret its relevance to an investigation [1]. The goal of the DF practitioner is the collection and analysis of digital evidence with a view towards presenting such evidence in a court of law or other legal proceeding. Key to the success of this process is the probative value of the collected evidence [2].

Anti-forensics (AF) involves the use of methods specifically designed prevent the use of scientific methods and tools to collect and analyse forensic artefacts for use in court proceedings. This is mainly aimed at the destruction or hiding of evidence. (Harris, 2006).

Due to the ever-increasing frequency of AF tool use, greater vigilance by DF investigators will be required to ensure the integrity of investigative results [3]. The use of anti-forensics is a difficult issue to overcome and digital forensics investigators can expect these techniques and tools to become much more sophisticated and also more widespread as suspects become more aware of the techniques and tools used by digital forensic investigators. It appears that this is a growing problem and that investigators will have to ascertain that they stay informed about the latest anti-forensic techniques and countermeasures.

All research into this phenomenon up to this point has come out of the developed world, with the USA, Europe and Australia leading the way. The 2012 Verizon data breach report states that one third of all DF investigations undertaken by Verizon are affected by AF [4]. No similar research has been conducted in South Africa, and as such the current scope of the AF problem is South Africa is not known. Due to the risks inherently posed by AF and the fact the electronic evidence in South African law is still in its infancy, a real risk exists that DF practitioners in South Africa are either not aware of the AF practices being used or are incorrectly identifying information that indicates the use of AF practices or applications, and are negatively impacting court rulings based on the acceptance of digital evidence

This research aims to establish to what extent the use of AF by the subjects of DF investigations has affected the ability of DF practitioners to complete such investigations successfully in the South African context. In this instance success is defined as the existence of digital evidence of sufficient probative value to ensure the presentation of admissible evidence in a court or other legal proceeding.

The motivation for this research is the furtherance of the knowledge of AF practices, techniques and applications for the benefit of practicing DF investigators and aims to provide a basis for further research into this phenomenon with a view to expanding the academic knowledge in this area.

2 LITERATURE REVIEW

2.1 Digital Forensics and Digital Evidence

Digital forensics as a discipline is aimed at identification, collection and analysis of digital evidence following an attack [5]. The purpose is to determine the identity of the attacker or suspect (who), their actions (what), when their actions were taken, how they perpetrated the attack or crime and their possible motivations (why).

Courts of law base the adjudication of all cases on evidence presented. In examining AF and its effect on the punctiliousness of digital evidence presented, it is first necessary to examine digital evidence closely. Evidence can be defined as anything presented to logically prove or disprove an issue at hand in a judicial case [6]. Digital evidence is information of legal probative value that is stored or transmitted in electronic form [3]. Digital evidence is similar to traditional evidence in that it contains information that is used to confirm or refute a hypothesis placed before the court or legal proceeding [7].The only difference is that such information is stored digitally. As such the quality of such evidence remains a critical factor as with any other case.

The proliferation of electronic devices has meant that digital evidence can be relevant to any case and not just for computer crimes. By its very nature digital evidence is fragile. Incorrect handling, examination or intentional destruction or modification can alter digital evidence to a point where it is no longer usable. The greatest challenge to using digital evidence in court is the fact that manipulation or alteration of the evidence can be achieved very easily without leaving any indication of such actions [5].

Whilst digital evidence is valuable as a source of evidence in any variety of investigations, it also introduces a new level of complexity that could potentially confound digital forensic investigators [3].

2.2 Anti-forensics

Anti-forensics (AF) in the digital realm is the process of removal or obfuscation of digital forensic artefacts with the aim of invalidating digital forensic investigations [8]. Typically, one or more of the following strategies are used: data hiding, data destruction, trail obfuscation, data contraception, data fabrication, file system attacks [9]. AF aim to remove all traces of a digital event, invalidate the data or increase the complexity of the investigation, remove evidence of its own use, or generally cast doubt on the investigation

[10]. The various AF methods are discussed below in more detail.

Data hiding

Data hiding refers to the practice of storing data where it is unlikely to be found, or employing the method of security through obscurity [9]. Simple methods such as extension renaming or signature editing exist, but these are generally easily identified by most current forensic software. In data communications, data hiding refers to the art of adding an obscure message signal in a host signal without any perceived distortion of the host signal. This composite signal is typically referred to as the 'stego' signal, and employs a different communication scheme than normal data communications [11].

One of the simplest and most effective methods of data hiding is Steganography. Whilst the practice of hidden writing has been around for millennia, the ability to hide any form of digital data within another carrier file poses a difficult challenge for digital forensic investigators [8]. In addition to its versatility to hide any data, Steganography is also very hard to detect. At the moment the only Open Source tool that effectively detects data hidden by modern steganography tools is StegDetect by www.outguess.org [12].

Some steganography algorithms hide the information in such a way that it is impossible to recover such information without knowing the key to the algorithm. Whilst that may sound like cryptography, it is accomplished simultaneously with the cloaking of the information in a masquerade file, and as such, is still steganography [13]. The most obvious difference between cryptography and steganography is that cryptography essentially hides data by disguising it as completely random data which is sometimes referred to as random noise. Stenographic algorithms are generally not trivial to break, even if the examiner has learned that there is hidden data to be discovered, which is often not simple to achieve in the first place.

Encryption

Encryption is simply a process of protecting data by using an algorithm to scramble the data and make it either intelligible or undetectable unless a key is used to decrypt the data [14]. Encryption has been used since ancient times in one way or another to protect against the interception of messages [15]. Encryption is used in many facets of digital data storage and transmission. When seen in the context of AF data-hiding, encryption tools provides the user, who are attempting to thwart the efforts of the DF investigator, with an extremely powerful tool.

Open-source encryption software is becoming more mainstream. Software such as TrueCrypt even offers the ability to hide one encrypted volume within another. TrueCrypt is a cross-platform encryption tool that uses 'On the fly encryption (OTFE)' to encrypt and decrypt files as they are accessed, and makes all data within the encrypted area available as soon as the decryption key is entered [16].

The most popular forms of data storage encryption include the encryption of a virtual or physical disk or partition and system encryption whereby the system (boot) files are encrypted.

Network traffic can also be quite easily encrypted using standard protocols such as SSL (secure sockets layer), SSH (Secure shell) or TLS (transport layer security). Whilst these protocols were developed as security protocols for the legitimate protection of information transmitted over either a public or private network, they can be used by criminals to transmit data securely.

Program packers

Program packers such as Armadillo and UPX are used to encrypt and/or compress an attack program and then incorporate the file in a new 'packed' file that is wrapped with a suitable extractor. When the seemingly innocuous process is run the packed attack application is then run simultaneously.

Hiding data in system areas

There are methods available to hide information in areas reserved as system space or file slack (area between the end of the logical file data and the end of the cluster). One such tool is 'Slacker', by the Metasploit Project [17]. Creators of this project claim that Slacker is the first ever tool that allows you to hide files within the slack space of the NTFS file system.

In addition, custom attacks created using software exploit frameworks such as the Metasploit framework are generally delivered using payloads created using tools such as ‘Msfpayload”, which allow the creator to create custom file signatures that will not be detected by forensic signature analysis.

More advanced tools such as ‘FragFS’ exist that have the ability to store information in the NTFS file system’s Master file table ($MFT file) [9].

Rootkits represent a malicious method of data hiding. Such programs allow attackers undetected administrative access to a computer [18]. In this instance the attacker can affect multiple states on the infected computer, such as executing programs, logging keystrokes or even storing data.

Rootkits are mostly installed on computers through the binding of a malicious program to a seemingly harmless one. An example of this is where a user downloads an MP3 or e-book from a file sharing site, and once the user runs the file they inadvertently install the rootkit on their computer. To further confound the issue, many rootkits are self-healing, and will automatically reinstate themselves if deleted or uninstalled. An example of this is the Computrace client that consists of both an application agent and a persistence module.

Data destruction

The destruction of data by wiping of files is a commonly used AF method which has been used for a long time. For the cybercriminal the wisest course of action is to simply remove all traces that anything untoward took place [19]. A simple delete essentially leaves the data intact. Though not visible to the general computer user, such data is easily recoverable using data recovery or forensic tools.

By using any one of a number of freely available data wiping tools (Including, Eraser, PGP etc.) the user is able to securely delete files by overwriting the clusters occupied by those files with random data, any number of times, according to existing standards such as Guttmann (35 times) and DoD standard 5220.22-M (US DoD, 1995) (7 times) [10]. Recovery of such securely deleted data is normally not possible [8].

Other tools also exist that focus on securely removing artefacts that pertain to activities of the user, such as internet history, file access, file downloads, peer to peer networking and Internet Messaging. A good example of a tool such is this is CCleaner by Piriform which is available as a free download.

Tools such as these perform a secure delete of the artefacts mentioned above to ensure that such remnants are not recoverable, after deletion. Such tools can also quite easily be configured to securely wipe all hard drive free space, including slack space, either manually or automatically at scheduled intervals.

In addition to data destruction by wiping or overwriting, there are also more drastic measures that cybercriminals sometimes revert to. These are degaussing the drive – sweeping the drive with a powerful magnet, thereby rendering the data unstable – or the physical destruction of the storage media.

Trail obfuscation

Trail obfuscation follows three basic methods. The first has the aim of obscuring required information from the would-be investigator. This is achieved by either replacing relevant information with false information (such as IP address spoofing) or using third parties to act as proxies of the source data in order to remove all traces of the origin of the data from the transmission at the destination (such as mail anonymizing services).

The second form of obfuscation involves altering the data associated with forensic artefacts by altering metadata such as date and time stamps.

Finally, trail obfuscation can also take the form of log deletion or modification in order to hide log entries that would identify the identity or action of the perpetrator. Securely wiping or modifying log files can be achieved by using freely available tools such as Touch [8].

Data contraception

Data contraception, also referred to as evidence source avoidance, is the process whereby the perpetrator uses software and methods that have been designed to leave no traces on the host operating system. A number of different methods can be used [20]:

- Portable applications – these applications do not install any files on the host computer (e.g. TrueCrypt and FTK imager lite).
- Live distros – these are fully functional operating systems from bootable devices such as CD’s or Flash drives. As all functions run in memory, no traces are left on the local hard drive, as the local hard drive is in fact not even required (e.g. Windows CE or BartPE) [18].
- Syscall proxying – A local system call or function is proxied to another system to complete.
- Remote library injection – Information (typically a Dynamic Link Library) is inserted directly in RAM of the host leaving no traces on the hard drive.
- DKOM (Direct Kernel Manipulation) – The process whereby the memory space utilized by kernel objects are penetrated and used by other inserted processes.
- Utilizing ‘in-private’ browsing on web browsers such as Mozilla Firefox will keep all cache and history in memory and will not write any information to disk for later analysis.

Data fabrication

This practice, also referred to as evidence counterfeiting, is very similar to some of the practices followed for trail obfuscation as discussed elsewhere in this document. In Windows, the Modified, Accessed and Created dates are referred to as the MAC information.

Modifying the MAC information on the computer serves both the purpose of obfuscating the original data and also can be seen as fabricating data [18].

Another data fabrication practice that is employed, is the creation of excessive amounts of data of a certain type in order to side-track and investigation to the point where cost-effectiveness becomes the deciding factor in the continuance of the investigation.

File system attacks

When an attack of sufficient severity is launched on a file system, it might inhibit the ability of a forensic application to make sense of the data contained therein.

An example of such sabotage would be to damage the master file table of an NTFS file system to such an extent that a forensic analysis of the logical drive is unable to extrude any meaningful data.

2.3 Trace Evidence of Anti-forensic Tool Use

As with many other computer applications, the actual use of an AF tool to remove forensic artefacts might in itself leave trace evidence.

Steganography is probably one of the most difficult methods of data hiding to detect and decipher and combines the art of hiding data from human perception and cryptography [9].

The DF practitioner must therefore first develop the knowledge or suspicion that steganographic data hiding is present in any given case, and then the practitioner has to establish which files out of all data that falls within the scope of the investigation could be affected. As there could potentially be hundreds of thousands of files on a suspect computer this is often difficult.

In this instance the detection of files affected by Steganography will often depend on the intuition and experience of the DF examiner. In the event that Steganography is suspected and the DF practitioner has identified files to target, the practitioner may use methods similar to the one below to confirm the presence of steganography and to attempt to decipher the contents.

Encryption is often quite obvious to detect. An example of this may be where a DF practitioner has attempted to image a suspect computer and is not able to access any of the data on the drive due to full disk encryption. In such examples the DF practitioner will not be able to access any of the data on the suspect drive unless such a password is provided, and it is often more practical to attempt to extract the password from the suspect using legal means than it would be to use technology.

Some forms of encryption may not be as easy to detect, such as a virtual encrypted disk. In this instance the DF practitioner will have to rely on other methods of detection such as identifying suspiciously large files and files with an unknown or no file signature. However, even in the event of detecting an encrypted volume, the challenge of decrypting such a volume still remains. Without the passkey required to decrypt and mount such a volume it is near on impossible to decrypt the information contained therein [15].

Attempting to break the password of the volume using any number of traditional methods such as brute force attacks, dictionary attacks or rainbow tables may take years to achieve [18]. In this instance the most viable option is often to attack the human factor. Often it is simply not possible to decrypt an encrypted volume using current technology and the only means available in such a case is the use of a password.

Most forensic software will detect signatures of commercial *file packers*. The forensic investigator should also be aware that such file packers typically have file signatures that can be searched for manually. An example of the UPX file packer a manual keyword search can be completed for the search term ‘UPX’, which will identify executable files that have been packed using this packer.

When using a tool such as slacker to *hide information in system areas*, the forensic investigator will likely have no specific indication that such an indication has occurred as the only change to the file assigned to legitimately occupy that sector, will be a change in the ‘date modified’ field. AF users who is thorough in their attempt at data hiding will then quite simply, use another tool such as ‘Timestomp’ to change that metadata attribute back to a value that would not arouse suspicion [21].

The data written to the slack area is not encrypted, but the metadata of the files written in slack space is encrypted. This is intended to complicate efforts to locate a list of files created using Slacker by doing metadata analysis. The most likely indication of the use of slacker will be the discovery of the Slacker executable on the suspect drive or in the event of volatile memory analysis or virtual memory analysis, a keyword search may indicate that the program had been loaded into memory. In the absence of such trace evidence the DF practitioner may still find information relating to the case in slack space by making use of a simple keyword search. Whilst this information may relate to the case, it will not provide any proof that a product such as Slacker was used to place it there.

Most anti-virus software claims to be able to detect *rootkits*. The reality is unfortunate that most Anti-virus software may stop a computer from being infected with new rootkits, but established rootkits will often remain undetected [9].

This does not mean that the DF practitioner need not run an antivirus scan on the acquired forensic image, as this remains a possible tool for detecting rootkits and viruses and can be useful in the event that the suspect decides to pursue a ‘Trojan- defence’.

When assessing the ability to detect rootkits from a forensic analysis perspective, it is important to look at two basic modes of forensic operation. These are live incident response i.e. volatile and non-volatile data analysis on a live computer, and dead' forensics, the analysis of static system data

Data destruction is often time consuming and very often the applications used do not destroy all data, as advertised. In addition to these factors, there will very often be indications that data destruction applications have been used on a computer [22].

Finally, commonly used *trail obfuscation tools* often leave certain artefacts behind e.g. by changing time/date stamps in only one system area but not others.

3 RESEARCH METHODOLOGY

3.1 Research Question and Hypotheses

The core research question is whether *the use of AF is affecting the ability of South African DF practitioners to complete DF investigations*?

To answer the main research question the research aimed to find answers to the sub-questions listed below:

- What AF tools are being used, and how they are being used? Not only did the research aim to determine which applications are used for Anti forensic purposes, but also how suspects use such software or tools. In addition, the research looked at the success rate of such tools in achieving the intended purpose and if any artefacts remained after the use of a particular tool. This research will identify which of the available AF tools are being used and for what purpose.
- Are South African DF practitioners able to identify AF tool use by the artefacts that such tools leave behind? As with many other computer applications, the actual use of an AF tool to remove forensic artefacts, will in itself leave trace evidence.
- How prevalent is AF tool use in the South African environment? This research will attempt to establish whether digital forensic practitioners experience anti forensic tool use on a regular basis.

3.2 Research Methodology and Proposed Model

A positivistic research philosophy was adopted for this research. A cross-sectional time-horizon is used, as the study will aim to understand the status of the situation at a particular point in time. The research used a deductive approach. To that end, a research model was developed as is shown in figure 1.

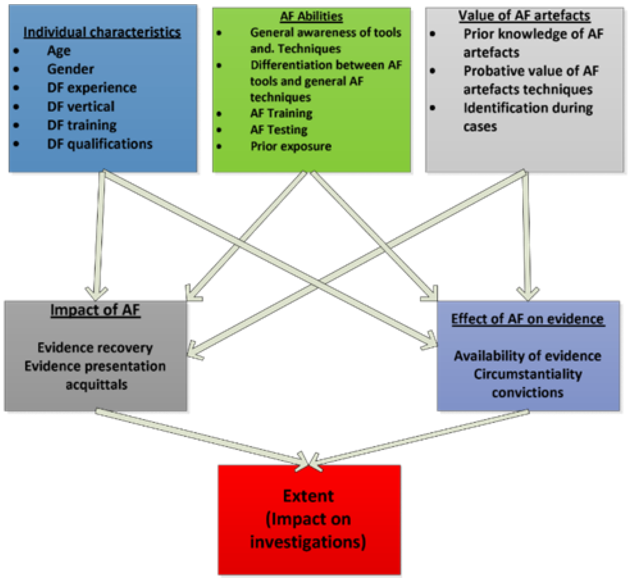

Figure 1. Proposed research model

Some of the constructs warrant further explanation. Under the Individual Characteristics, "DF" refers to the Digital Forensics experience and skills, including DF experience, formal DF training, any qualifications obtained and the industry environment in which they are deployed (DF *vertical*: civil, criminal or corporate environment).

The AF abilities refer to specific Anti-Forensic tool and method abilities. The value of AF artefacts refers to the knowledge of and ability to identify AF artefacts (i.e. evidence left behind by AF tools) including the knowledge of artefacts left behind by AF tools and techniques, the ability to identify AF tools by their artefacts and knowledge of the evidentiary value of the artefacts left by AF use.

The impact of AF is measured by evidence recovery (the DF practitioner's ability to recover useable evidence), evidence presentation (the DF practitioner's ability to present evidence of probative value) and acquittals (where AF leads to acquittals). The Impact of AF as part of all evidence refers to the impact AF has on electronic evidence when seen as part of the entire case and all other types of evidence presented and convictions refers to the impact of AF on convictions when seen as part of the entire case and all other types of evidence presented.

The sample size needed to test the model statistically, far exceeded the number of digital forensics practitioners in South Africa, which made testing the multiple relationships simultaneously impossible.

Instead, the model served as a guide for the development of constructs to include in the questionnaire, generating descriptive statistics and doing limited inferential statistical tests such as construct correlations and ANOVA.

3.3 Research Instrument and Sampling Approach

Collection of data was by means of a survey to assess the state of events as experienced by DF practitioners. A mostly original survey instrument was created. Due to the large number of constructs, usually only one question (test item) was formulated for each of the constructs.

South African DF practitioners were targeted to include practitioners that operate in criminal, civil, and corporate environments. The aim was to include practitioners that deal with evidence in traditional, mobile and internet / e-commerce forensics. Thus a probability-sample using the stratified random-sampling technique was used in order to identify forensic practitioners functioning across the strata. Figure 2 illustrates the employment sectors of the respondents.

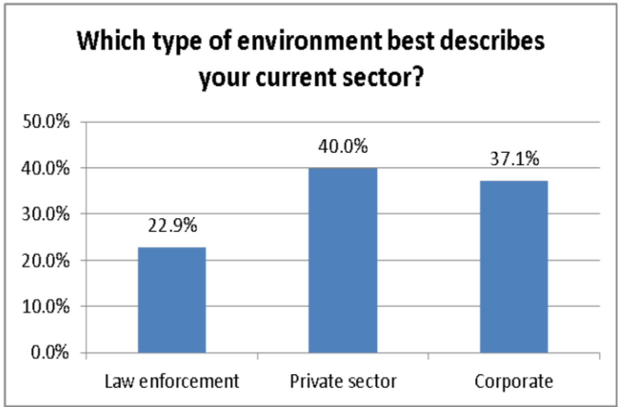

Figure 2. Employments sectors

A limitation is the relatively small size of the South African DF fraternity. The researchers have access to a large proportion of the South African digital forensics practitioners, since due to the small size of the group, practitioners tend to meet on a regular basis and it was felt that a representative sample was obtained.

No personal interviews were conducted and no personal information was collected about any of the practitioners or their places of employment.

4 DATA ANALYSIS

4.1 Demographic Profile of Respondents:

The majority (85.7%) of respondents were male and most fall in the 31-40 year age range. These sample characteristics are fairly representative of the DF practitioner community in South Africa.

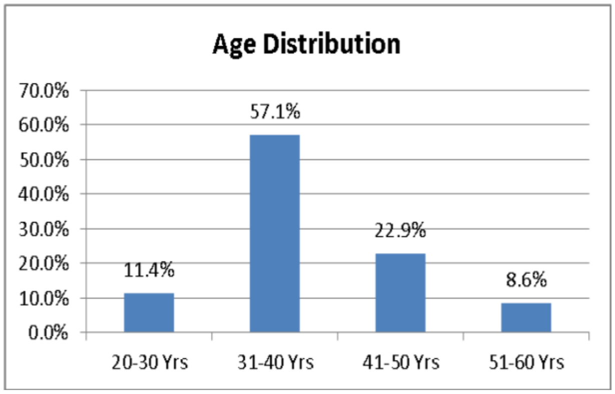

Figure 3. Age distribution of respondents

Most DF practitioners were practicing although nine respondents (25.7%) indicated that they were not practicing DF investigators. Six of these non-practicing AF investigators (67%) are in the corporate environment. It is possible that the 9 (25.7%) survey participants have branched into other areas of their organization, some even into managerial positions.

A wide spread of experience in DF was borne out by the respondents. In line with the stratified random-sampling method a satisfactory spread of employment sectors was achieved.

Table 1. DF qualifications

Education and training level	Yes	%(Yes)	No	%(No)
Do you have a Digital forensics qualification? (EnCe, ACE etc.)	3	33.33%	6	66.67%
Do you have a tertiary qualification?	8	88.89%	1	11.11%
Have you completed any Anti-forensic tool testing?	2	22.22%	7	77.78%
Have you had any Anti-forensics training?	5	55.56%	4	44.44%
Have you had any formal digital forensics training?	8	88.89%	1	11.11%

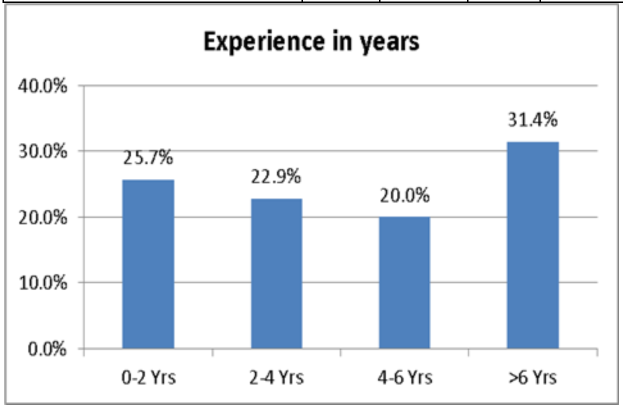

Figure 4. Experience.

Whilst most respondents (89%) indicated that they had received formal DF training, only a few respondents followed such training up with a qualification. However, on the other hand, 89% of them had a tertiary qualification.

More than half (56%) of respondents claim to have had training in AF techniques and tools. The same respondents who have completed AF training have also tested AF tools and techniques.

Most respondents rate their knowledge of AF tools and techniques as average to good but their prior exposure to AF was lower as can be seen in tables 2a &b. Very few respondents rate their prior exposure to AF as excellent.

Tables 2a & 2b. Knowledge of AF tools and techniques and prior exposure to AF

How would you rate your knowledge of anti-forensics tools and techniques?	%
Excellent	5.7%
Good	42.9%
Average	37.1%
Poor	11.4%
None	2.9%

How would you rate your prior exposure to anti-forensics?	%
Poor	34.3%
Average	28.6%
Good	28.6%
Excellent	8.6%

4.2 Interesting Correlations between Independent Variables

Possible correlations between demographic variables and other independent variables were investigated. For instance, there was a significant difference between the sectors in which an FP was employed and their investigation environments. FPs employed in the law-enforcement and private sectors tend to investigate computer/networks, internet/e-commerce whereas those in corporate environments tend to limit their investigations mainly to computer/network forensics and, to a lesser extent, internet/e-commerce (Chi-square χ^2 value=7.79, DF=2, p-value = 0.0203).

However, there was no statistical evidence to suggest that a difference exists between the knowledge, qualifications and training in Anti-Forensic investigators between the 3 employment sectors, or that they were exposed to different types of AF threats. Not surprisingly, there is a statistically significant correlation between completed AF tools training and a respondent's own rating of knowledge of anti-forensics tools and techniques (χ^2 value=8.241, DF=1, p-value=0.0041). In fact, respondents with AF tools Training completed are 8.4 times more likely to rate their knowledge of AF tools and techniques as "Good/Excellent".

Formal Forensics training, Digital Forensics Qualification and Tertiary Qualification show no association (or relationship) with respondent's prior exposure to AF. However, specific AF training" has an association (or relationship) with prior exposure to AF (χ^2 value=4.61, DF=1, p-value=0.0318) and persons with AF training are 4 times more likely to rate their prior exposure to AF as GOOD. Even more so, "specific AF tools testing" has an association with prior exposure to AF (χ^2 value=12.61, DF=1, p-value=0.0004) with those who have completed AF tools testing are 18.7 times more likely to have GOOD prior AF exposure.

This shows that *generic* formal digital forensics training is deficient in imparting AF-specific skills or knowledge. This should be remedied by addressing the curricula of (generic) forensics training courses.

On the whole, respondents seem to be familiar with the more common AF techniques i.e. data hiding and data destruction. The twelve (34%) respondents that rate their prior AF exposure as "poor" have hardly any familiarity with the AF techniques of data contraception, trail obfuscation, data fabrication and file system attacks, although half of them were exposed to data hiding and data destruction.

These respondents are familiar with an average of only 1.2 AF techniques whereas respondents who rate their prior exposure as average to excellent have an exposure to an average of 2.9 techniques.

Table 3. Familiarity with AF techniques.

Which Anti forensic techniques are you most familiar with?	%No	%Yes
Data Hiding	28.6%	71.4%
Data destruction	31.4%	68.6%
Trail obfuscation	68.6%	31.4%
Data fabrication	77.1%	22.9%
File System attacks	77.1%	22.9%
Data contraception	85.7%	14.3%
None of the above	88.6%	11.4%

As with AF techniques, most respondents appear to be familiar with the more commonly known AF tools such as data wiping and encryption.

Table 4. Familiarity with AF tools (all respondents)

Familiarity with AF Tools	No	%No	Yes	%Yes
Data wiping and history removal (CCleaner, Eraser etc.)	7	20.0%	28	80.0%
Encryption tools (Truecrypt etc.)	8	22.9%	27	77.1%
Steganography tools (Quickstego etc.)	21	60.0%	14	40.0%
Timestomp (by Metasploit)	25	71.4%	10	28.6%
Rootkits	31	88.6%	4	11.4%
Transmogrify (by Metasploit)	32	91.4%	3	8.6%
The complete A-Z of open source tools out there.	34	97.1%	1	2.9%

No relationship (association) were found between respondent's rating of the probative value of artefacts that AF tools leave behind, and their familiarity with AF tools. (Chi-Square tests performed). Neither is there a relationship (association) between respondent's rating of their efforts to actively identify anti-forensics as part of investigations, and their familiarity with AF tools. (Chi-Square tests performed)

The following graph summarizes respondent's view of AF techniques that most affected their cases. The more common techniques appear to be more prevalent, however respondents previously indicated that they are less familiar with the more complex techniques such as data contraception, which may indicate that such techniques are not identified.

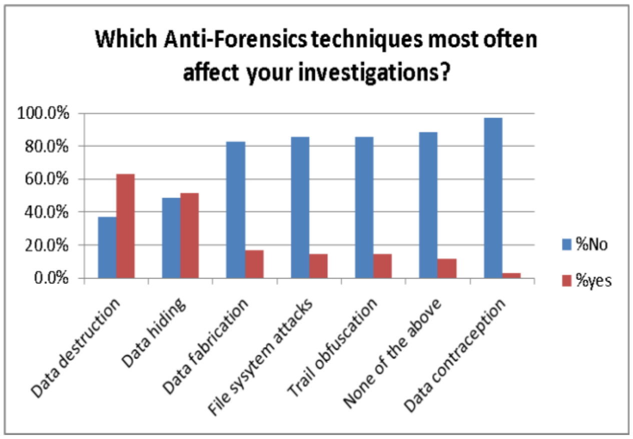

Figure 5. AF Techniques that most affect investigations

As with the AF techniques, respondents feel that the commonest AF tools are most prevalent during their investigations. Data destruction and Data-hiding are the most common AF techniques that respondents experience. Data contraception, Trail obfuscation, System file attacks and data fabrication are the least seen AF techniques.

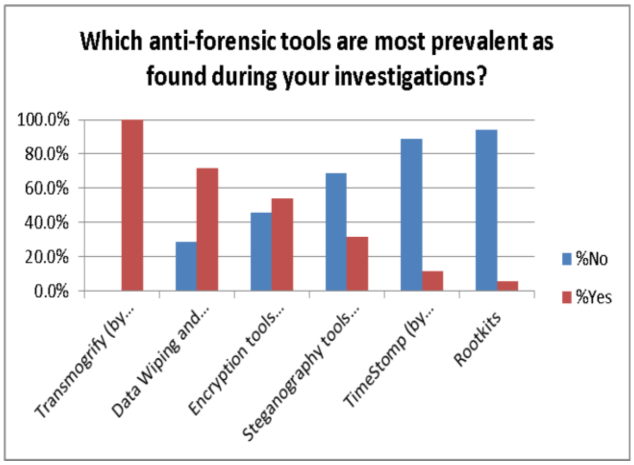

Figure 6. AF tools most prevalent in investigations

4.3 Respondents Rating of Their AF Abilities

Respondents were asked to rate their own Anti-Forensics abilities by means of three questions: their own knowledge of AF, their prior exposure to AF and their ability to counteract the use of AF tools. The 3 items were considered as a single construct as they logically represent respondent's abilities to investigate AF.

The items were subjected to a reliability analysis to determine the internal consistency between items to measure a single construct. The overall Cronbach Alpha was 0.825 which is considered a very good reliability. A mean score of approximate 2.8 for this construct was achieved

The influence of the biographical profile of respondents, employment sector, and type of forensic investigation participation, education and training level was tested using ANOVA. In the absence of normality, a non-parametric test (Mann-Witney U test for 2 groups and Kruskal-Wallis for more than 2 groups) was performed. If the variances of the scores of the groups are unequal, the result of the Welch test is reported.

The male respondents rate themselves significantly more highly in AF ability than their female counterparts (Welch test p = 0.0361). The age groups 31-40 and 41-50 years also rated themselves significantly higher than the two other (smaller) age groups i.e. those younger than 31 or above 50 years old (Welch test p = 0.0088).

Respondents who are practicing digital forensic investigators rate themselves significantly higher than those who are currently not practicing (Welch test p = 0.0385). Finally, respondents with more than 2 years of experience rate their AF abilities higher than the group with 2 or less years' experience (p = 0.0355)

However, there was *no* significant correlation between the AF ability of the respondent and:

the sector in which employed, the type of forensic participation or the respondent's training and education level.

4.4 The Impact of Anti-Forensics upon Investigations

Figure 7 summarizes the responses to the questions related to the impact of AF on investigations.

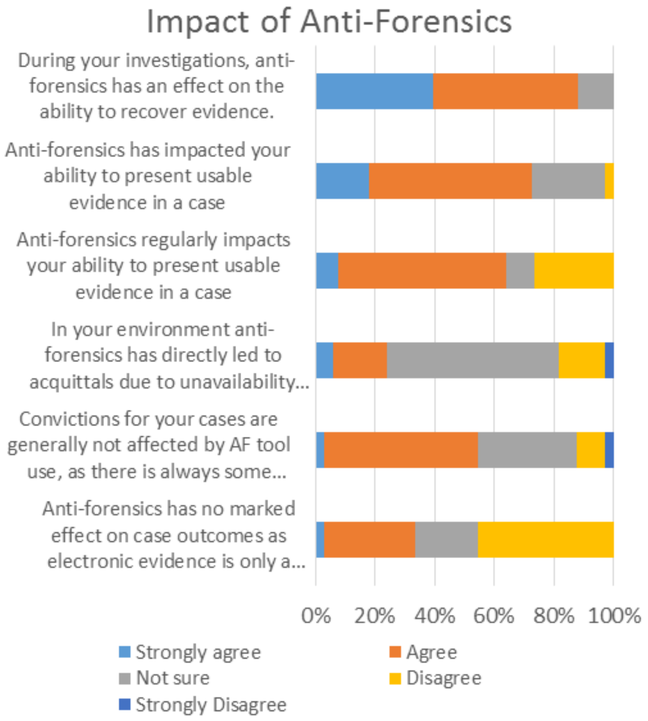

Figure 7. Impact of Anti-Forensics

Factor analysis was performed on the above test items to see if the five statements can be summarized into meaningful constructs. This was done using Principal Component extraction and Varimax (orthogonal) rotation techniques.

The factor analysis yielded 2 underlying constructs (factor loadings > 0.4), although item 4 ("Anti-forensics regularly impacts your ability to present usable evidence in a case") is ambiguous as it loads strongly upon both factors.

Two new constructs were created: the *Effect of AF on evidence*, which was composed of four test items (Cronbach Alpha of the resulting construct was 0.8433) and the *Impact of AF*.

The influence of: Biographical profile of respondents, Employment sector, Type of forensic investigation participation, Education and training level, Knowledge of AF tools and techniques (own rating), Prior exposure to AF (own rating), Familiarity with various AF techniques, Exposure to various AF Tools upon the constructs (Impact of AF and Effect of AF upon evidence) was investigated using Analysis of Variance (ANOVA) since the mean scores derived from the Likert scale statements can be viewed as continuous variables and their distributions were found to be roughly normally distributed.

Table 5. Construct creation after factor analysis.

Test Item (Question)	Factor 1	Factor 2
During your investigations, anti-forensics has an effect on the ability to recover evidence.	0.9132	0.0582
Anti-forensics has impacted your ability to present usable evidence in a case	0.8727	0.2216
In your environment anti-forensics has directly led to acquittals due to unavailability of evidence	0.7331	0.3592
Anti-forensics regularly impacts your ability to present usable evidence in a case	0.5583	0.5489
Convictions for your cases are generally not affected by AF tool use, as there is always some usable digital evidence.	0.3488	0.6433
Anti-forensics has no marked effect on case outcomes as electronic evidence is only a portion of the evidence presented to court or legal proceeding.	0.0301	0.9433

However, only one factor was found to exert a significant influence and that was one particular type of forensic participation that significantly influences the mean score of the Impact of AF, namely *mobile device investigations* (χ^2 statistic=4.26, DF=1, p-value =0.039). It is possible that this is an artefact of the data or small sample size.

5 DISCUSSION AND CONCLUSION

The main purpose of this research was to establish the impact of AF on DF investigations in a South African context.

Contextual factors and individual characteristics did *not* show a significant influence of respondent's rating of their knowledge of AF tools and techniques. More surprisingly, neither the respondent's familiarity with the various AF tools and techniques, nor their exposure to AF appeared to affect score for Effect of AF upon evidence or their score for impact of AF.

Perhaps contradictorily, although practitioners rate the value of AF artefacts highly, they don't make an effort to identify them as part of their investigations, as can be seen in table 6a & b below.

Table 6a & 6b. Probative value of AF artefacts and relative effort used to identify AF.

Rating of probative value of artefacts that AF tools leave behind	N	Mean
Critically valuable	6	2.61
Very valuable	12	2.44
Valuable	14	3.02
Moderately valuable	2	4.33
Useless	1	4
Rating of efforts to actively identify anti-forensics as part of investigations	N	Mean
Always	4	2.91
Often	12	2.38
Sometimes	13	2.97
Rarely	4	3.16
Never	2	4.16

The concern is that investigators who do not place a high value on AF artefacts and do not employ significant efforts to identify AF as part of their investigations could potentially be overlooking evidence of AF use, or indeed the opportunity to recover usable evidence.

Whilst the current research attempted to understand the impact of Anti-forensics on evidence, a troubling trend emerged as part of this research. Whilst most respondents (89.9%) list their knowledge of AF tools and techniques as average to good, it appears that that exposure is limited to certain types of AF tools and techniques.

From the findings, it is clear that investigators are quite familiar with the more common AF techniques such as data hiding and data destruction, but much less familiar with the more complex techniques such as data contraception amongst others.

Correspondingly, respondents were much more familiar with the tools related to data wiping and encryption than they are with the more complex tools such as steganography, rootkits and data contraception. This trend is also supported by the finding that most respondents feel that their cases are affected mainly by the more common AF techniques such as data destruction and data hiding.

The risk is that DF investigators are not properly versed in the more complex techniques and tools, and as such does not have the skills to identify the use of such tools and may be ignorant of their presence and effect on the cases that they participate in. This combined with the results that show a lack of active identification of AF as part of investigations, due to the low value placed on AF artefacts leaves a potential gap for usable evidence of probative value to be overlooked, as the AF technique or tool used to destroy or misrepresent that evidence is not identified.

The main contributions of this paper to the body of academic knowledge is the application of a model-driven empirical investigation as well as a number of findings which partly collaborate and partly extend current knowledge. For the practitioner community, it is clear that additional effort and resources must be deployed to inform and educate practitioners about common anti-forensic tools and activities.

Apart from further empirical research to establish comparative baselines in other countries or, longitudinally, one or two years into the future, we also strongly recommend additional in-depth research into the advanced AF techniques and tools to establish the actual effect of these advanced techniques in investigations.

6 REFERENCES

[1] R. Harris, “Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem,” Digital Investigation, 2006, 3(Supplement 1), pp. 44-49.

[2] M. Pollitt, “Applying traditional forensic taxonomy to digital forensics” in Advances in Digital Forensics IV (pp. 17-26), New York: Springer, 2008.

[3] E. Casey, Handbook of digital forensics and investigation (Non Trans.), San Diego, California: Elsevier, 2010.

[4] Verizon, “Data breach investigations report”, Retrieved 05/14, 2012, from http://www.verizonbusiness.com/resources/reports/rp_data-breachinvestigations-report-2012_en_xg.pdf

[5] E. Casey, Digital evidence and computer crime. Burlington: Elsevier, 2004.

[6] K.M. Hess, Criminal investigation (9th ed.). New York: Delmar, Cengage Learning, 2009.

[7] B. Carrier, File system forensic analysis. Addison Wesley Professional, 2005.

[8] G.C. Kessler, “Anti-forensics and the digital investigator,” paper presented at the Proceedings of the 5th Australian Digital Forensics Conference, 2007, 1(1) 5. Retrieved from http://scissec.scis.ecu.edu.au/proceedings/2007/forensics/00_Forensics2007_Complete_Proceedings.pdf

[9] B. Blunden, The rootkit arsenal escape and evasion is the dark corners of the system, Wordware Publishing, 2009.

[10] D. Forte, “Dealing with forensic software vulnerabilities: Is anti-forensics a real danger?” Network Security, 2008(12), 18.

[11] H. Sencar, M. Rankukar, & A. Akansu, Data hiding fundamentals and applications. San Diego, California: Elsevier, 2005.

[12] A. Philipp, D. Cowen, D., & C. Davis, C., Hacking exposed computer forensics, second edition: Computer forensics secrets & solutions (Second Ed.) New York: McGraw-Hill Osborne Media, 2009.

[13] P. Wayner, Disappearing cryptography, second edition: Information hiding: Steganography & watermarking. The Morgan Kaufmann series in software engineering and programming, New York: Morgan Kaufman, 2003.

[14] J. Pan, H. Huang, L. Jain, & W. Fang, Intelligent multimedia data hiding. New York: Springer, 2007.

[15] H/ Nemadi, & L. Yang, Applied cryptography for cybersecurity and defense: Information encryption and cyphering. Hershey, PA: Information Science Reference, 2011.

[16] L. Roy, “Lockdown: Secure your files with TrueCrypt”, Makeuseof.com.

[17] D.O. Kennedy, J. Gorman, & M. Aharoni, Metasploit: The penetration tester's guide. No Starch Press, 2011.

[18] D. Behr, “Anti-forensics – what it is what it does what you need to know,” New Jersey Lawyer Magazine, 2008, 255, 4-5.

[19] D. Forte, & R. Power, “A tour through the realm of anti-forensics,” Computer Fraud & Security, 2007(6), 18-20.

[20] M. Kedziora, “Anti-forensics overview,” retrieved 16/02, 2011, from http://www.forensics-research.com

[21] D. Maynor, Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research, San Diego, California: Elsevier, 2011.

[22] M. Geiger, “Counter-forensic tools: Analysis and data recovery,” 18th Annual FIRST Conference, Maltimore, Maryland, 25-30 June 2006.