Forensic Auditing: A Guide for Practitioners

Prof. Dr Tamuka Maziriri

[PhD, CFA, FICTA, R.T.A(Z)]

ISBN: 9781073661916

Printed in United States of America
Edited & Printed by Amazon

Dedication

This book is dedicated to my wife, Beauty and our children who inspired me to write this book. Guys you made me proud of you. Despite my busy schedule sometimes, you kept on pushing me and sometimes taking much of your time to focus on this book.

FOREWORD

Many accountants and auditors find themselves investigating and testifying in a court of law only to be disappointed when courts throw away their cases for lack of evidence. Tremendous effort and time would have been used during the investigation process. This is so disappointing to the investigator and sometimes very humiliating as if the investigator is not a learned person. Sometimes the evidence would have been illegally acquired, sometimes the investigator would have failed to authenticate his evidence or the chain of custody also called the chain of possession would have been broken. All of these cause serious harm to the case under investigation. Courts use court rules and not accounting or auditing rules and it is therefore important that the investigator apply court rules as he investigates a case. Don't speak like an accountant in a court of law, but speak like a lawyer for that is the language that courts understand. Use court language and never the language of your profession for you are likely to be speaking to yourself. Don't speak to yourself, but speak to the jury for they are the ones that can decide on your case. Avoid pompousness and reduce technical jargon as much as you can, for you may spend the whole day being asked by the defense lawyer to define your jargons!

Many businesses are failing due to effects fraud having taken place unnoticed for quite some time. Fraud is a complicated crime to unearth, investigate and prosecute and as such, it takes a trained and professional person to investigate it. Inexperienced investigators end up contaminating the evidence making it inadmissible in a court of law. Some of them lack the technical competence to be treated as experts and this always weaken their cases and legal standing in a court of law.

It is the desire of the desire of this book to help accountants and other professionals that may be given a responsibility to investigate a case. The book, written in simple language, offers a step by step guide towards the journey of being a professional forensic accountant or expert witness. This however should not be taken as an event, but should be treated as a process of professional development.

TABLE OF CONTENTS

CHAPTER	TOPIC	PAGE
1	Introduction to Forensic Auditing	6
2	Investigation Techniques	10
3	Crime Scene Attendance	20
4	Evidence	26
5	Forensic Audit Report Writing	30
6	Expert Witness Testimony	32

CHAPTER 1

INTRODUCTION TO FORENSIC AUDITING

What is forensic auditing?

Forensic auditing is a part of the forensic family and is important for us to understand the meaning of the word forensic itself. The term "forensic[1]" means something to do with the courts of law. It relates to the scientific methods and techniques that are applied to the investigation of crimes. Crimes that may be investigated include murder, rape, fraud, etc. The person who investigates a case is called an expert witness[2] provided he possesses the necessary skills and knowledge in a particular field. There are so many experts that can be called experts like the engineers when it comes to engineering matters, pathologists when it comes to human deaths and also forensic auditors when it comes to financial matters not limited to fraud of course.

Forensic always involve an investigation to establish facts that answers what may be called the 6Ws. The 6Ws that must come out from the investigation are what happened, when did it happen, where did it happen, who is involved, why did it happen and how did it happen? These facts must come out when a case has been brought before a court of law. Most importantly to remember is why a person has been called by the court to assist in a certain case. Obviously, it means the case before the court is complex and usually beyond the knowledge and understanding of the jury and hence the need to call an expert to come and assist with the answering of the 6Ws. The jury are laymen in the case brought before it, but at the same time, it has a duty to deliver a verdict. One of the immediate worries of the court is to what extent the court should rely on the evidence that is being presented to it by the expert witness who could be a forensic auditor? There is a risk before the court that a wrong verdict can be passed as a result of a technical deficiency of the expert witness. Someone can be wrongfully jailed or hanged as a result of the evidence that has been brought by the expert witness. It is therefore important that the court protects itself from such shortcomings. The credibility of the expert witness must always be interrogated at the initial stages of testifying. His or her credentials must be asked such as his professional qualifications and to a less extent his education qualifications. For a person to be called an expert, he must belong to a recognised professional body that has a duty to supervise his technical competence[3]

[1] Forensic means something to do with the courts of law which is usually evidence.

[2] While a forensic auditor is an expert witness, it is important to note that in a court of law he is treated almost the same like any other witness. He is an expert only because of the specialised knowledge that he possesses, otherwise the court expects him to submit a witness statement in the ordinary way and not a report such as a forensic report. Courts always work with statements especially for Zimbabwean Courts.

[3] Competence relates either to technical competence, legal competence as well as resource competence. Legal competence is the right or permission to do the assignment. The legal competence may be enshrined in the laws of the land or a professional body may give the right to its members to do certain assignments. Employers or other private persons may also confer legal competence especially where a

throughout someone’s career. The professional body must also have the technical competence at minimum to supervisor its members and in some jurisdiction, the professional body must also have the legal competence to do so as well as the resource competence within its area of jurisdiction. This equally applies to the expert, that is, he must have the technical, legal and resource competence to carry out an investigation. In some cases, experience may be substituted for technical competence.

Forensic auditing is therefore a combination of investigation skills, legal or law skills and accounting or auditing as some may prefer to call it. The term forensic auditing may also be interchangeably called forensic accounting. A good forensic auditor is therefore one who is good at crime investigation, accounting and interpretation of the laws of the land which always supersede any standard or regulation. A forensic person must be conversant with the law of evidence, court procedures and the law pertaining to the crime under investigations especially the essential elements of that particular crime. He must be a good investigator in order to gather the evidence, apply good investigation techniques during investigation and have some good intelligence sources [4]to assist him in the collection of evidence. In a court of law, when everything is said and done, evidence must be given a chance to speak for itself. The investigator must be in a possession to authenticate his evidence throughout in order for the evidence to be considered credible. If evidence is not credible, then there is no case to talk about. If the forensic auditor is not credible, there is no case to talk about as he is our first piece of evidence at the commencement of any case that he brings before a court of law. As a rule, evidence must be credible in order for it to be admissible in a court of law.

What is a crime scene?

Generally, when an investigation commences, the area covered by the investigation should be treated as a crime scene by the investigator. Duties of the investigator at the crime scene include but not limited to crime scene protection, duty to protect the evidence which must always remain in the same state or in a state that is as close as possible as it was when the investigator arrived at the crime scene. ISO 27037[5] and the ACPO[6] Guidelines can be of great help to crime investigators.

The Locard’s Exchange Principle

In forensic science, **Locard's exchange principle** holds that the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence. Dr. Edmond Locard (13 December 1877 – 4 May 1966) was a

person wants to be represented by another person. Technical competence is associated with someone’s qualifications usually professional qualifications and experience may also be considered as part of technical competence. Resource competence relates to the means and resources which could be human capital and financial resources required to do a certain assignment.

[4] Intelligence sources include human intelligence (HUMINT), Technical Intelligence (TECHINT), Communication Intelligence (COMMINT), Electronic Intelligence (ELINT), Open Source Intelligence (OSINT), etc.

[5] ISO 27037 is a standard that relates to the Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. It is used mainly in conjunction with digital evidence.

[6] ACPO standards for the Association of Chief Police Officers of England and Wales. The Guideline is a Good Practice Guide for Digital Evidence which is used mainly by law enforcement agents of England and Wales.

pioneer in forensic science who became known as the Sherlock Holmes of France. He formulated the basic principle of forensic science as: "Every contact leaves a trace".

The Locard's Exchange Principle is also called by various names such as the exchange principle, CSI (Crime Scene Investigation) and also the contamination principle.

Paul L. Kirk expressed the principle as follows:

"Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it can diminish its value."

The Locard's Exchange Principle is the answer to every investigation. Whenever a crime is committed, there are always traces that the perpetrator leaves behind. This principle has been in existence for time immemorial. Law enforcement agents have been using this principle in murder and rape cases just to mention a few. The same applies when two or more computers communicate with each other; there are always traces that are left behind. These traces provide some invaluable evidence to an investigator when investigating digital crimes and cybercrimes.

According to Edmund Locard, it is very difficult for a perpetrator of a crime to commit a crime without leaving traces behind. It is these footprints that will lead to the apprehension of an offender. These footprints are a silent witness when a crime has been committed. It is therefore of paramount importance that the footprints that are left behind be protected by the investigator. Investigators must also be very careful so as not to contaminate the evidence as this will destroy the case they are investigating. An investigator has a duty to preserve everything, but is not allowed to change anything. This is particularly true in forensic science where the emphasis is on dead forensics as opposed to live forensics. If one is to do live forensics which is contrary to the general rules, one must be able to justify his actions and be able to give evidence to support such a move. A competent witness must be available to witness live forensics taking place otherwise the case will lose its value when it is brought before the courts of law.

Forensic Auditing Phases

1. Identification
2. Collection
3. Preservation
4. Examination
5. Analysis
6. Presentation/Report

Conclusion

Forensic auditing is the art of combining investigative skills, legal skills and accounting or auditing skills with a view of assisting the jury with aspects of a complicated case that falls outside its domain of knowledge. The expert must be independent, objective, honest and a person of confidentiality. He has a role to assist the court and is not allowed to tell falsehood. Forensic accountants have a duty to identify, collect, analyze and acquire evidence. Evidence must speak for itself and should be credible enough and equally, the expert must be credible in order for the evidence he brings in to be admissible in a court of law.

CHAPTER 2

INVESTIGATION TECHNIQUES

Introduction

A good forensic audit requires a thorough investigation. The forensic auditor must be a very good investigator. He should apply his investigative skills to a case that he is investigating. The purpose of an investigation is to collect and acquire evidence from a crime scene. Evidence so acquired must remain in the same state or in a state that is as close as possible to the one the investigator took over the case.

Sources of Intelligence

The forensic auditor should have good sources of intelligence at his disposal when investigating cases. It is however important to note that an evidence that is illegally acquired is generally inadmissible in a court of law in many jurisdictions and it is therefore important that legal means are used to acquire evidence.

Human Intelligence (HUMINT)

Human Intelligence commonly referred to as HUMINT within the intelligence community involves the use of human beings in acquiring intelligence that can lead to unveiling of the *modus operand*[7] of a crime or matter under investigation. So many techniques can be used under HUMINT and these include:

(a) **Undercover Operations**[8] **-** These are clandestine operations that plant a person in an organization who acts as an informant of the investigator. To be an undercover, it requires some special training otherwise the cover will be blown during the initial stages making future undercover operations difficult. Once a cover has been blown or is believed to have been blown, the undercover should be moved at the earliest to avoid further damage to the case.

[7] Modus operand is a latin word that means, method of operation.

[8] Undercover operations involve the planting of an investigator or informant within the organization with a role to report to his principals of the secret or illegal activities that will be taking place. Undercovers are generally deployed in problematic areas for example in the finance department, procurement, etc where the person is usually employed as a very junior person. The undercover can be a cleaner for example.

(b) **Physical Surveillance** – This usually involves tracking a suspicious person or person put under investigation. Trackers may be on foot, driving or wandering within the area of the victim. The investigator may be using a camera to take photographs which may be used as evidence during a criminal or civil proceeding. Such camera should be digital to the extent that it should be recording the date and time the photograph was taken.

(c) **Social Engineering** – This technique involves engineering the minds of the victims in order to get certain pieces of evidence. The technique exploits vulnerabilities of human beings such as trust, being helpful, greedy, etc. Hackers also use the same technique to attack their intended victims.

(d) **Penetration Testing** – This approach is also called ethical hacking within the hacking community or white-hat hacking. The technique involves the exploitation of existing vulnerabilities in order to acquire some pieces of evidence. Vulnerabilities may involve entering a building or office through the window, unlocked door or even through the roof. It is important to note that the illegal entrance may be considered criminal if no prior permission was given by the owner or a court.

(e) **Interviews** – These generally involve asking questions from the person under investigation in order to provide leads of the case under investigation. The investigator should make use of open-ended questions during the initial stages of the interview and latter one used closed questions that for example require a yes or no answer in order to close the interview. Accusatory language should be avoided as this may tantamount to an interrogation which generally is considered illegal in many jurisdictions.

(f) **Interrogations** – This technique make use of accusatory language and may involve the use of minimum force in order to get answers from the victim. Interrogations are generally considered illegal in many jurisdictions and as such, a confession made as a result of an interrogation is generally inadmissible in a court of law. Investigators are therefore discouraged from making use of this technique as it usually backfires and kills your case.

(g) **Dumpster Diving / Scavenging** – This technique involves the collection of documents from dumpsites of victims or persons under investigation with a view of getting clues of their illegal activities. The technique therefore gives clues to the investigator and these clues can be used as leads to a criminal or civil case.

(h) **Extortion** – This technique when used by investigators involves the use of threats to some extent as part of the negotiation deal. The threat may be disclosure of some very sensitive matter that the victim was a part of in the past. In exchange for not revealing such matter, the investigator negotiates for a voluntary disclosure of the facts of a matter under investigation.

Open Source Intelligence (OSINT)

Open Source Intelligence as the name suggests, relies on information and data that is readily available from the public domain. Such sources include internet searches, reading newspapers, watching television, fingerprint vetting, listening to the radio and visiting libraries in search of certain information. The cost of getting such information is usually next to zero and experienced investigators usually make use of this source of intelligence. Suppose the organization intends to recruit a manager for example, the investigator doing background checks may want to Google the applicant's name to find out more about him and this technique may provide invaluable information about the applicant that he normally is not willing to disclose. An applicant may want to hide his previous conviction for example, but good enough; the information is already available on the public domain.

Website Investigations

Website investigations make use of internet searches as well as visiting certain specialist websites. When visiting such sites, it is important that the investigator protects his identity on the internet otherwise he will be noticed and tracked by his victims. Free tools in the form of (Virtual Private Network) VPN are readily available on the internet that can protect the investigator. Examples of VPN include Cyberghost which is now a paid tool, Hidemyass, etc. These tools have the effect of changing the IP address[9] of the investigator to an obscured IP address which is randomly allocated from a pool of available IP addresses or the investigator may want to change the IP address to one of his choice. A website address such as https://www.whoishostingthis.com can be used to find the IP address of a website, the organization responsible for hosting the website and also the DNS[10] that are being used by the website. Websites generally make use of static IP address [11]and the opposite is dynamic IP address[12]. Details of the owner of a website can be obtained by enquiring the WHOIS information from many websites e.g. using www.whois.net. Some people for various reasons may want to hide their personal details on the

[9] IP stands for Internet Protocol and it is an address that is used by a computer to communicate with other computer across the world. A computer needs this IP address in order to communicate publicly with other computers. Websites make use of a static IP address and computers connecting to the internet are allocated with a dynamic IP address. IP addresses are owned and controlled by an organization called the ICANN (Internet Corporation for Assigned Names and Numbers).

[10] DNS stands for Domain Name System. Domain Name System (DNS) servers are the "phonebooks" of the Internet. They maintain directories that match IP addresses with registered domains and resolve the text that people understand (the domain name) into a format that devices understand (the IP address).

[11] "Static" IP addresses are permanently assigned to devices configured to always have the same IP address. A person, business, or organization maintaining a constant Internet presence, such as a Web site, generally requires a static IP address.

[12] "Dynamic" IP addresses are temporarily assigned from a pool of available addresses registered to an ISP. These addresses are assigned to a device when a user begins an online session. As a result, a device's IP address may vary from one logon session to the next.

internet regarding the ownership of a website using protection tools such as privacyprotect.org. When this tool is in operation, it is a bit difficult to discover the details of ownership of a website and it's a long process that the investigator will have to go through. It is much easier to investigate a website with a country level domain name as compared to an international level domain name. Country level domain names end with the country extension such as .co.za, .co.zw in which case the .za is associated with South Africa while the .zw is associated with Zimbabwe.

While the public information displayed may give some leads into a case, it is important to note that most of the information shown of the owners of the websites and domain names is that information which is voluntarily entered by a domain applicant which is sometimes very misleading as ICANN has no capacity to verify the authenticity of the registrant information.

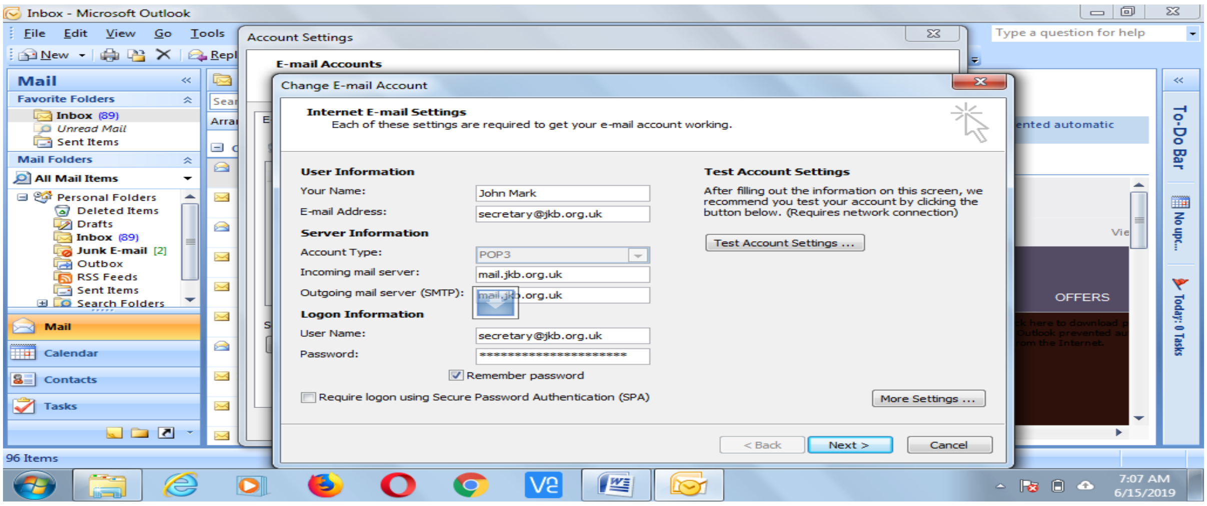
In short, further verification procedures must be performed before one can jump into a conclusion especially when dealing with digital information. The whole information acquired may be untrue.

Technical Intelligence (TECHINT)

Technical Intelligence makes use of exploiting technical vulnerabilities[13] of a system. An investigator may wish to exploit a vulnerability of an internet browser such as Firefox, Google Chrome, Explorer, etc in order to obtain passwords that are saved on the computer for the purpose of trying to access certain accounts that the victim would not ordinarily make available to the investigator. One may learn more about these technical vulnerabilities through open source intelligence for example. Old version of systems normally has these technical vulnerabilities and it is therefore important systems are patched in order to close technical vulnerabilities. Passwords with asterisk keys (********) can be revealed by may open source tools such as the Asterisk Key which can be downloaded for free from the internet.

Below is a screenshot that was taken from Outlook to demonstrate the use and applicant of the Asterisk Key.

[13] Vulnerability refers to the weakness of a system that can be exploited by one or more threats.



Change E-mail Account

Internet E-mail Settings
Each of these settings are required to get your e-mail account working.

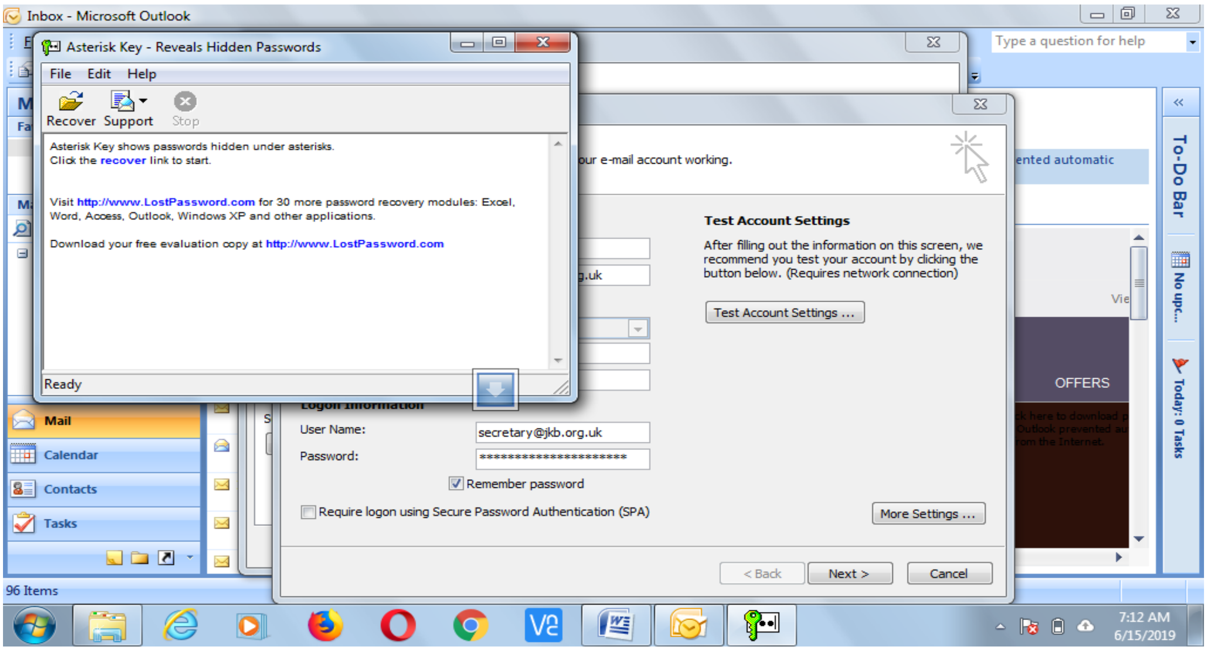
User Information
Your Name: John Mark
E-mail Address: secretary@jkb.org.uk

Server Information
Account Type: POP3
Incoming mail server: mail.jkb.org.uk
Outgoing mail server (SMTP): mail.jkb.org.uk

Logon Information
User Name: secretary@jkb.org.uk
Password: ********************
☑ Remember password
□ Require logon using Secure Password Authentication (SPA)

Test Account Settings
After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

In order to reveal the hidden password in asterisk key, the investigator should then open the Asterisk Key tool while the Outlook is also opened on the area with the hidden password (*******).


Inbox - Microsoft Outlook
Asterisk Key - Reveals Hidden Passwords
File Edit Help
Recover
Support
Stop
Ready
Test Account Settings ...
More Settings ...
< Back
Next >
Cancel

Asterisk Key shows passwords hidden under asterisks.
Click the recover link to start.

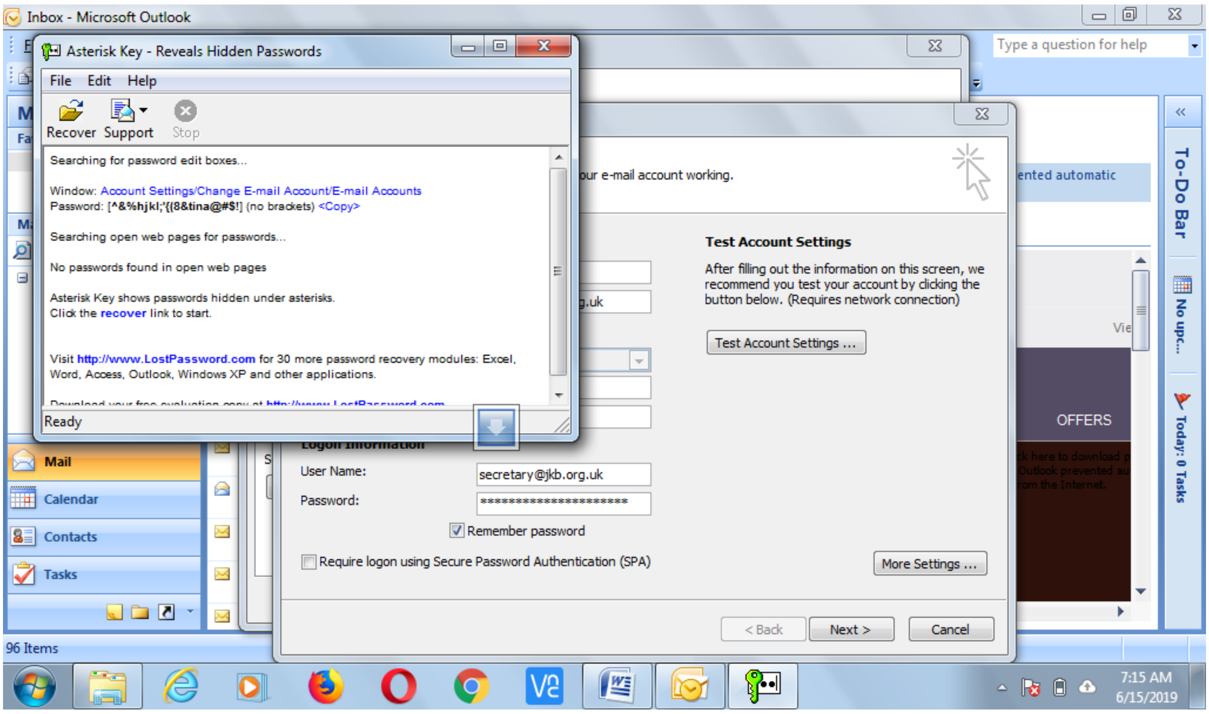
Visit http://www.LostPassword.com for 30 more password recovery modules: Excel, Word, Access, Outlook, Windows XP and other applications.

Download your free evaluation copy at http://www.LostPassword.com

User Name: secretary@jkb.org.uk
Password: ********************
☑ Remember password
□ Require logon using Secure Password Authentication (SPA)

To reveal the password, the investigator should then click on the link where it says, “click the recover link to start”

Let us now click it and see what would come out. See the result below.



Searching for password edit boxes...

Window: Account Settings/Change E-mail Account/E-mail Accounts
Password: [^&%hjkl;'{(8&tina@#$!] (no brackets) <Copy>

Searching open web pages for passwords...

No passwords found in open web pages

Asterisk Key shows passwords hidden under asterisks.
Click the recover link to start.

Visit http://www.LostPassword.com for 30 more password recovery modules: Excel, Word, Access, Outlook, Windows XP and other applications.

our e-mail account working.

Test Account Settings

After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

Logon Information

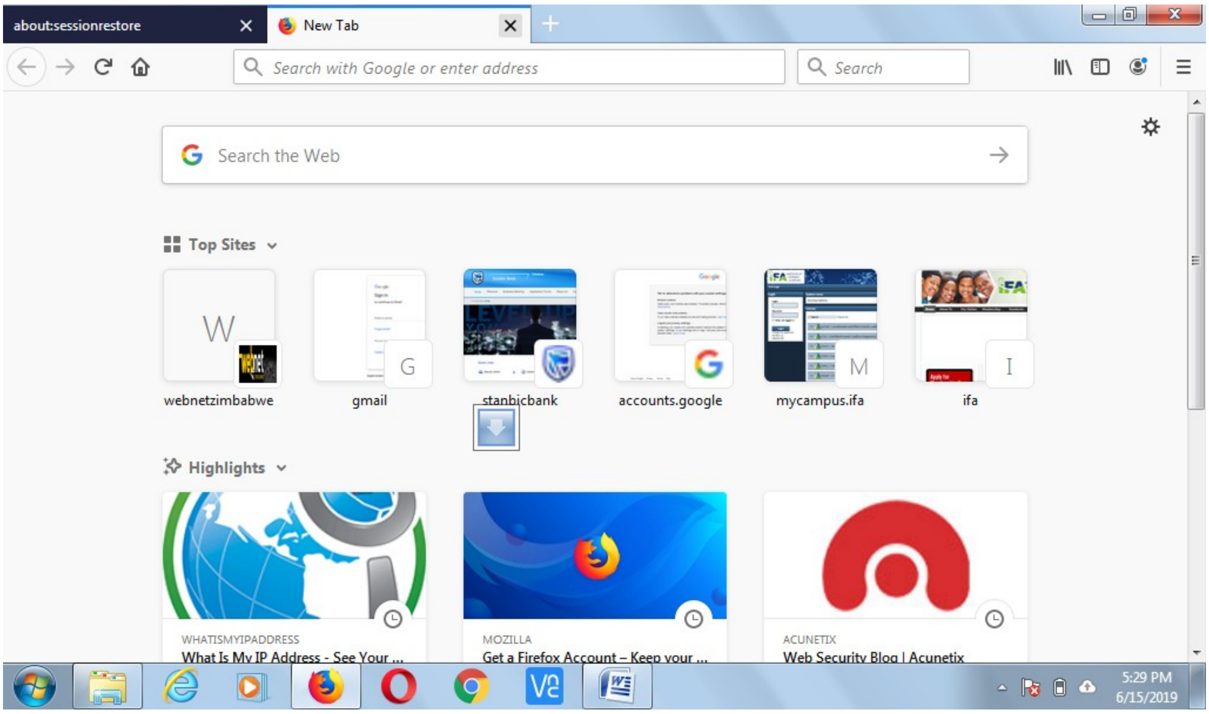
User Name: secretary@jkb.org.uk
Password: *********************
☑ Remember password
☐ Require logon using Secure Password Authentication (SPA)

The password is now being shown by the tool as ^&%hjkl;'{(8&tina@#$!
That is the password that the user is using for his or her emails and now that we have the password, it is now possible to open the person's emails by setting up the same emails using Outlook or opening them using Webmail for example which in this case is webmail.kjb.org.uk and this should be entered on a web browser. It would prompt you for a username which one should enter as the email account and the password as ^&%hjkl;'{(8&tina@#$!. Once that is done, the investigator can see all the emails going out and coming in. Legal authorisation is however required in order to use this technique which may be given by the owner of the asset under consideration or investigation. If it is a laptop, then the employer may give the legal competence to the investigator. Using the same password, the investigator is now in a position to try and access other accounts associated with the victim which could be his or her facebook account, Gmail account, Yahoo account, etc.

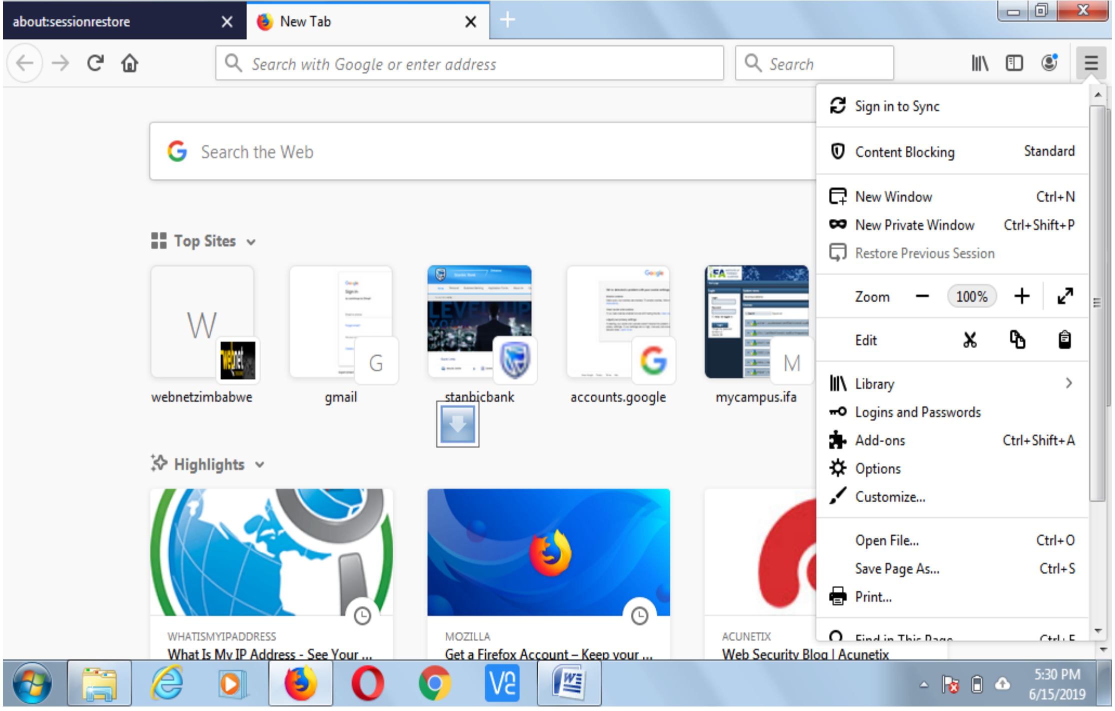
Internet Web Browser Exploitation of Technical Vulnerabilities

In this segment, we are going to exploit technical vulnerabilities of the Firefox web browser. This vulnerability is associated with the saving of passwords on the browser when a computer asks a user to remember his or her password. Once a password is saved, it can be retrieved by anyone who is interested in getting it.

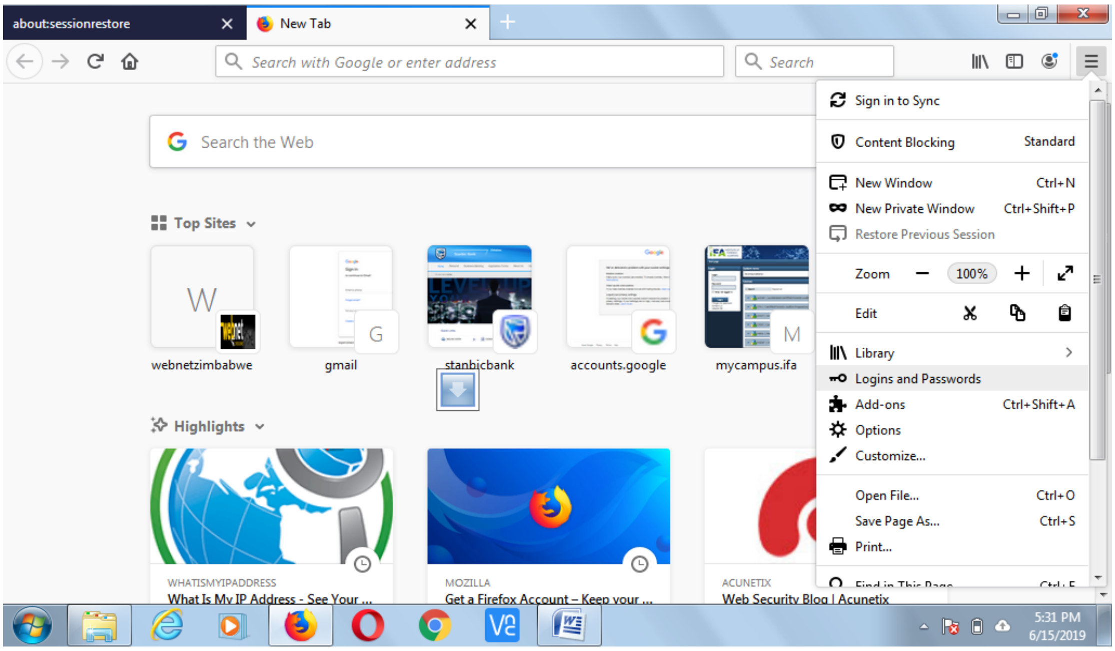
Open a new firefox browser and go the far right of the blank page and click on this symbol ≡.



Once the ≡symbol is clinked, various items will be displayed and go to where it says *logins and passwords*. This is the location where passwords and login details of the user are stored if the computer is given the permission to remember passwords. It is risky to store passwords on a computer as hackers can exploit this vulnerability to the detriment of the user. Sensitive information can be accessed which could harm the image and reputation of the user.

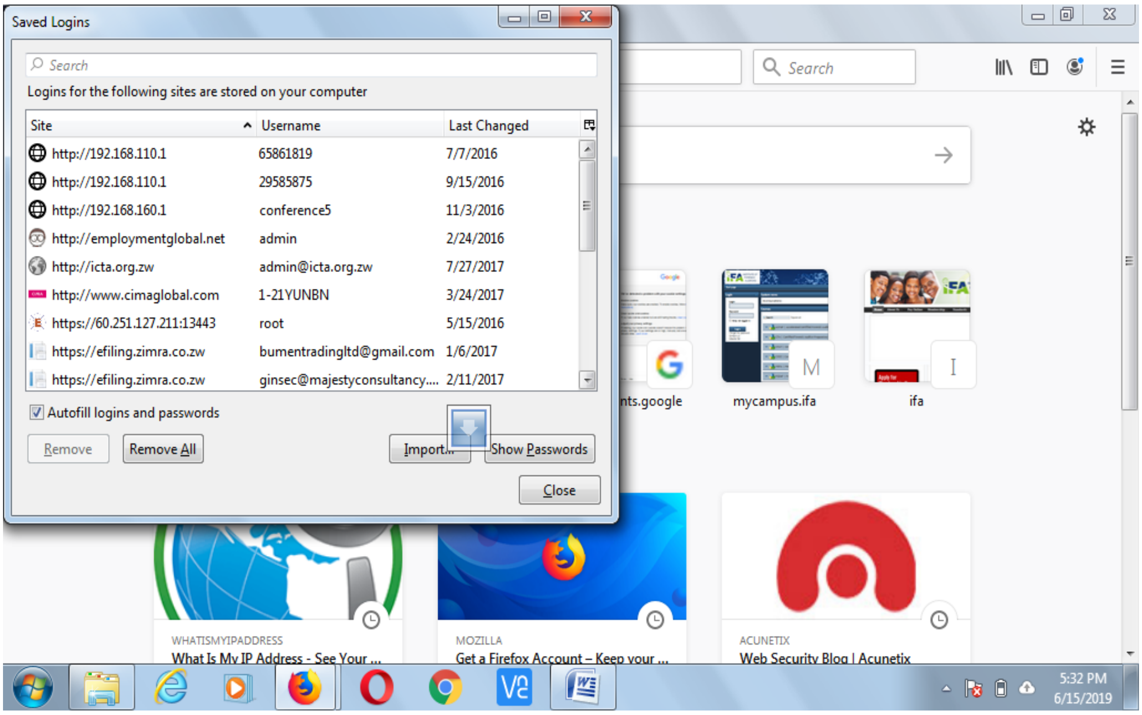


Opening the logins and Passwords option will reveal the user name and password and also the URL[14] pointing to the accessed location.



Below is the information that will be displayed when the logins and password option is clicked.

[14] URL stands for the Uniform Resource Locator usually the http://www..... Or the https://www.... HTTP stands for the Hyper Text Transfer Protocol while the HTTPS stands for the Hyper Text Transfer Protocol Secure. The HTTPS means that the website is secure and that security is obtained through installation of the SSL certificates from many vendors such as Thwart, etc.



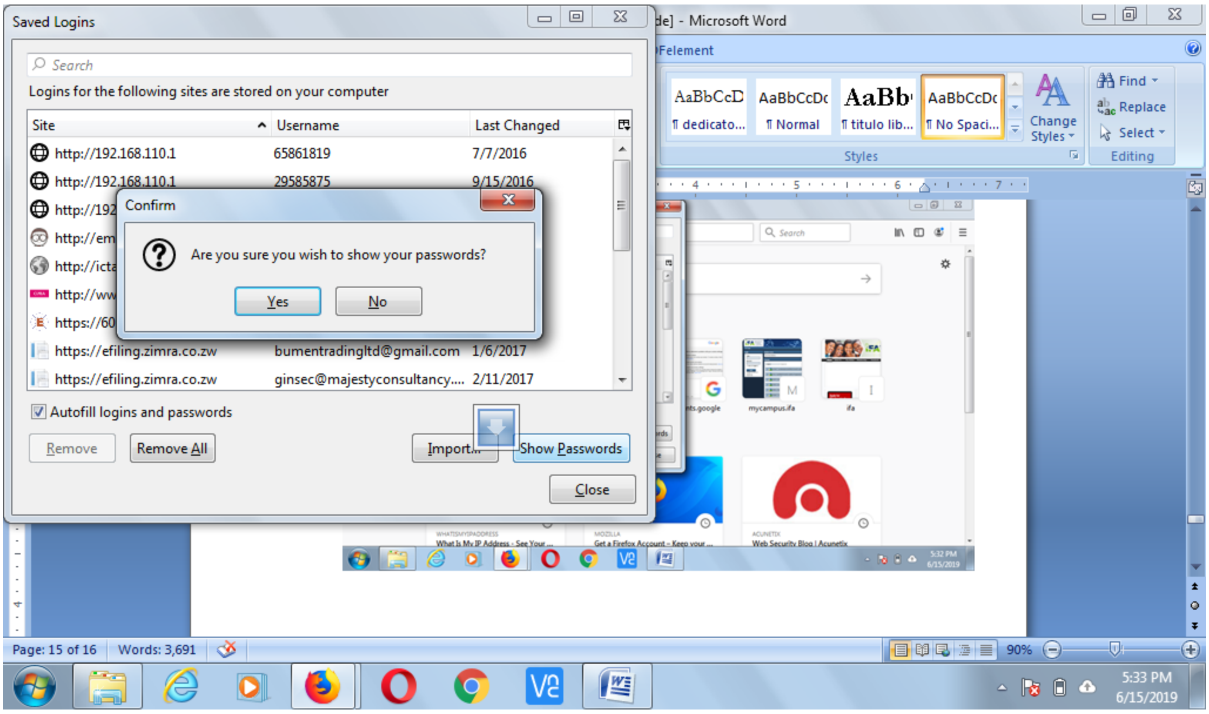
Saved Logins

Logins for the following sites are stored on your computer

Site	Username	Last Changed
http://192.168.110.1	65861819	7/7/2016
http://192.168.110.1	29585875	9/15/2016
http://192.168.160.1	conference5	11/3/2016
http://employmentglobal.net	admin	2/24/2016
http://icta.org.zw	admin@icta.org.zw	7/27/2017
http://www.cimaglobal.com	1-21YUNBN	3/24/2017
https://60.251.127.211:13443	root	5/15/2016
https://efiling.zimra.co.zw	bumentradingltd@gmail.com	1/6/2017
https://efiling.zimra.co.zw	ginsec@majestyconsultancy....	2/11/2017

☑ Autofill logins and passwords

Clicking the yes option below will reveal the saved passwords.



Confirm

Are you sure you wish to show your passwords?

Communication Intelligence (COMMINT)

This technique involves the interception of communication on the sender or receiver’s end. The interception could be of a signal in which case it is referred to as signal intelligence (SIGINT) or it can be an interception of an electronic communication in which case it is called electronic intelligence (ELINT).

Interception tools that can be used range from free spyware to paid tools. Some of these tools include E-Detective, Keyloggers, etc. The legality of these tools may be considered illegal in certain jurisdictions and it is important that consent is given by the owners of an asset that falls within the jurisdiction of an investigation.

All Source Intelligence (ALSINT)

All source intelligence encompasses the collection of evidence from any available source. This may include consulting sangomas[15], man of God (prophets), gossiping and rumours going around, whatsapp communication, facebook posts, etc. Study has shown that some of these sources provide accurate information and such sources should not be underrated by an investigator.

Conclusion

A sound investigation largely depends on the investigator's sources of intelligence that provide some leads into a case under investigation. The sources of intelligence are the foundation of obtaining evidence to substantiate a case and are the objective of many investigations.

[15] A sangoma is a traditional healer mostly found in Africa and the term is common in South Africa, Zimbabwe, Zambia and Botswana.

CHAPTER 3

CRIME SCENE ATTENDANCE

Introduction

A crime scene is any place where a crime would have taken place and the investigator has a responsibility to protect the crime scene so that the necessary evidence remains intact. The investigator has other duties that include the identification, collection, acquisition and preservation of evidence. Evidence must be preserved throughout the investigation process and this duty is relinquished when the evidence has been returned to its rightful owner. A chain of custody must be maintained throughout the investigation process. Whether the investigator is an auditor, police officer or other person tasked with a responsibility to investigate a case, these duties applies to all investigators.

Crime scene attendance involves a practical application of the Locard's Exchange Principle that states that whenever two things come into contact with each other, there is a trace that is always left behind. This is particularly true with relationship to rape cases where semen is left on the victim's private parts. It is this semen that should be collected including any hairs left behind that should be matched with those of the suspected perpetrator of that crime. Similarities of the hairs and semen provide circumstantial evidence as to the culprit to be implicated. The fingerprint approach follows the same principle in identifying suspects. In the event of a house breaking or burglary case, the culprits leave behind the scent which the police dogs can sniff and follow the criminals. From all these scenarios, it is important that crime scenes are attended timely while the evidence is still fresh otherwise it will get contaminated and the sniff dogs in the burglary case won't be in a position to track down the criminals once they encounter other scents than the one they were tracking.

What to take to a crime scene

The following is a suggested list of equipment that might be of value during crime scene attendance in terms of the ACPO Guideline (2009). This basic tool-kit should be considered for use in the proper dismantling of digital systems as well as for their packaging and removal:

- Property register;
- Exhibit labels (tie-on and adhesive);
- Labels and tape to mark and identify component parts of the system, including leads and sockets;
- Tools such as screw drivers (flathead and crosshead), small pliers, and wire cutters for removal of cable ties;

- A range of packaging and evidential bags fit for the purpose of securing and sealing heavy items such as computers and smaller items such as PDAs and mobile phone handsets;
- Cable ties for securing cables;
- Flat pack assembly boxes - consider using original packaging if available;
- Coloured marker pens to code and identify removed items;
- Camera and/or video to photograph scene in situ and any on-screen displays;
- Torch;
- Forensically sterile storage material.

In addition, the following items may be useful when attending scenes to retrieve CCTV:

- Laptop with USB and network connectivity. A selection of proprietary replay software could be installed, to enable the downloaded data to be checked;
- External CD/DVD writer;
- USB hard drives.

Records to be kept

To comply with ACPO Principle 3, records must be kept of all actions taken in relation to digital evidence or other evidence, for example:

- ✓ Sketch map/photographs of scene and digital equipment;
- ✓ Record location and contact details;
- ✓ If a business, record opening hours;
- ✓ Details of all persons present where digital equipment is located;
- ✓ Details of digital items - make, model, serial number;
- ✓ Details of connected peripherals;
- ✓ Remarks/comments/information offered by user(s) of equipment;
- ✓ Actions taken at scene showing exact time;
- ✓ Notes/photographs showing state of system when found.

Seizure steps:

1. Secure and take control of the area containing the equipment;

2. Move people away from any computers and power supplies and do not allow any interaction with digital devices by suspect;

3. Photograph or video the scene and all the components including the leads in situ. If no camera is available, draw a sketch plan of the system and label the ports and cables so that system/s may be reconstructed at a later date;

4. Allow any printers to finish printing.

If switched off:

5. Do not, in any circumstance, switch the computer on;

6. Make sure that the computer is switched off, by moving the mouse – some screen savers may give the appearance that the computer is switched off, but hard drive and monitor activity lights may indicate that the machine is switched on;

7. Be aware that some laptop computers may power on by opening the lid. Remove the battery from the laptop. Seize any power supply cables for future use.

If switched on:

8. Record what is on the screen by photographing it and by making a written note of the content of the screen;

9. Do not touch the keyboard or click the mouse. If the screen is blank or a screen saver is present, the investigator should be asked to decide if they wish to restore the screen. If so, a short movement of the mouse should restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph or video it and note its content. If password protection is shown, continue as below, without any further touching of the mouse. Record the time and activity of the use of the mouse in these circumstances. (For games consoles, or tablet computers, the equivalent would be moving the controller joystick or touching the touchscreen);

10. If the system may contain valuable evidence in its current state (for example, if it is currently displaying a relevant document or an instant message conversation), seizing officers should seek expert advice from their local digital forensic unit as this may be lost if the power is lost. This is especially important if the suspect is a technically knowledgeable user who may be using encryption, as there may be no way to retrieve evidence stored in encrypted volumes once the power is lost;

11. Consider advice from the owner/user of the computer but make sure this information is treated with caution;

12. Remove the main power source battery from laptop computers. However, prior to doing so, consider if the machine is in standby mode. In such circumstances, battery removal could result in avoidable data loss. This is normally evident by a small LED (light) lit on the casing. In this case, officers should seek advice from their local digital forensic unit;

13. Unplug the power and other devices from sockets on the computer itself (i.e. not the wall socket).

14. When removing the power supply cable, always remove the end connected to the computer, and not that attached to the socket. This will avoid any data being written to the hard drive if an uninterruptible power supply is fitted. If the equipment was switched on, do not close down any programs or shut down the computer, as this will cause changes to the stored data and may trigger wiping software to run, if this is installed;

15. Ensure that all items have signed and completed exhibit labels attached to them. Failure to do so may create difficulties with continuity and cause the equipment to be rejected by the digital forensic unit;

16. Search the area for diaries, notebooks or pieces of paper with passwords on them, often attached or close to the computer;

17. Ask the user about the setup of the system, including any passwords, if circumstances dictate. If these are given, record them accurately;

18. Allow the equipment to cool down before removal;

19. Track any cables that can be seen as they made lead you to other devices in other rooms.

Mobile devices

This includes mobile phones, smartphones, and other devices which may have wireless connectivity/communications capability such as tablet computers, personal digital assistants (PDAs), personal media players and satellite navigation systems.

1. Secure and take control of the area containing the equipment. Do not allow others to interact with the equipment;

2. Photograph the device in situ, or note where it was found, and record the status of the device and any on-screen information;

3. If the device switched on, power it off. It is important to isolate the device from receiving signals from a network to avoid changes being made to the data it contains. For example, it is possible to wipe certain devices remotely and powering the device off will prevent this.

   However, in exceptional circumstances the decision may be made to keep the device on. Timely access to the handset data is critical the decision may be made to leave the device switched on. Consideration may be given to place the handset in a Faraday environment to further prevent signal reception. In such circumstances advice should be sought from the DFU.

4. Seize cables, chargers, packaging, manuals, phone bills etc. as these may assist the enquiry and minimise the delays in any examination;

5. Packaging materials and associated paperwork may be a good source of PIN/PUK details;

6. Be aware that some mobile phone handsets may have automatic housekeeping functions, which clear data after a number of days. For example, some Symbian phones start clearing call/event logs after 30 days, or any other user defined period. Submit items for examination as soon as possible.

Handling and transporting digital evidence

Digital Devices

Handle with care. If placing in a car, place upright where it will not receive serious physical shocks. Keep away from magnetic sources (loudspeakers, heated seats & windows and police radios).

Hard disks

As for all digital devices protect from magnetic fields. Place in anti-static bags, tough paper bags or tamperevident cardboard packaging or wrap in paper and place in aerated plastic bags.

Removable storage

Floppy disks, memory sticks, memory cards, CDs/DVDs) Protect from magnetic fields. Do not fold or bend.

Do not place labels directly onto floppy disks or CDs/DVDs. Package in tamper-force approved packaging to avoid interaction with the device whilst it is sealed.

Other items

Protect from magnetic fields. Package correctly and seal in plastic bags. Do not allow items to get wet.

Other Considerations

1. If fingerprints or DNA evidence are likely to be required, always consult with the investigator;

2. Using aluminium powder on electronic devices can be dangerous and result in the loss of evidence.

Before any examination using this substance, consider all options carefully.

The equipment should be stored at normal room temperature, without being subject to any extremes of humidity and free from magnetic influence such as radio receivers. Dust, smoke, sand, water and oil are also harmful to electronic equipment. Some devices are capable of storing internal data (such as the time and date set on the system) by use of batteries. If the battery is allowed to become flat, internal data will be lost. It is not possible to determine the life expectancy of any one battery. However, this is an important consideration when storing a device for long periods before forensic examination and should be addressed in local policy.

CHAPTER 4

EVIDENCE

Introduction

Evidence is what we are looking for in order to authenticate our case. Without evidence, there is no case to talk about. The rules of evidence must be observed and any violation weakens the case which becomes a nullity. Evidence may be digital or documentary regardless of its format, the same rules are applied. However for the purposes of our discussion, the book focuses on digital evidence. In this regard, we are guided by the ACPO Guideline, ISO 27037 and other sources which of course do not have a force of law, but good enough to persuade the jury to decide along these international best practices. The basics of evidence are constant across both physical and cyber/digital. Digital/ Electronic evidence is extremely volatile. Once the evidence is contaminated it cannot be de-contaminated! The courts acceptance is based on the best evidence principle. With computer data, printouts or other output readable by sight, and bit stream copies adhere to this principle. Chain of Custody is crucial.

SECTION 2 – THE PRINCIPLES OF DIGITAL EVIDENCE (ACPO Guideline)

2.1 PRINCIPLES

2.1.1 **Principle 1:** No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

2.1.2 **Principle 2:** In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

2.1.3 **Principle 3:** An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

2.1.4 **Principle 4:** The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

2.2 EXPLANATION OF THE PRINCIPLES

2.2.1 All digital evidence is subject to the same rules and laws that apply to documentary evidence.

2.2.2 The doctrine of documentary evidence may be explained thus: the onus is on the prosecution to show to the court that the evidence produced is no more and no less now than when it was first taken into the possession of law enforcement.

2.2.3 Operating systems and other programs frequently alter, add and delete the contents of electronic storage. This may happen automatically without the user necessarily being aware that the data has been changed.

2.2.4 In order to comply with the principles of digital evidence, wherever practicable, proportionate and relevant an image should be made of the device. This will ensure that the original data is preserved, enabling an independent third party to re-examine it and achieve the same result, as required by principle 3.

2.2.5 This may be a physical / logical block image of the entire device, or a logical file image containing partial or selective data (which may be captured as a result of a triage process). Investigators should use their professional judgement to endeavour to capture all relevant evidence if this approach is adopted.

2.2.6 In cases dealing with data which is not stored locally but is stored at a remote, possibly inaccessible location it may not be possible to obtain an image. It may become necessary for the original data to be directly accessed to recover the data. With this in mind, it is essential that a person who is competent to retrieve the data and then able to give evidence to a court of law makes any such access. Due consideration must also be given to applicable legislation if data is retrieved which resides in another jurisdiction.

2.2.7 It is essential to display objectivity in a court of law, as well as the continuity and integrity of evidence. It is also necessary to demonstrate how evidence has been recovered, showing each process through which the evidence was obtained. Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a court.

2.2.8 It should be noted that the application of the principles does not preclude a proportionate approach to the examination of digital evidence. Those making decisions about the conduct of a digital investigation must often make judgements about the focus and scope of an investigation, taking into account available intelligence and investigative resources. This will often include a risk assessment based on technical and non-technical factors, for example the potential evidence which may be held by a particular type of device or the previous offending history of the suspect. Where this is done it should be transparent, decisions should be justifiable and the rationale recorded.

General Principles of Evidence

- **Repeatability** – refers to repeating the same process using the same tools used before and the results obtained should be similar to the first results. If the differ, it means our evidence lacks credibility and is no longer admissible in a court of law.

- **Reproducibility** – refers to the use of a different tool but an alternative of the first tool used and we expect results to be the same under normal circumstances. If results differ, then the case loses its credibility and the evidence is no longer admissible for court purposes.

- **Audibility** – this is a review of the documentation and other processes applied and the reviewer is expected to arrive at the same results as those arrived by the investigator. The reviewer is an independent person.

- **Justifiability** – In the event of going contrary to the normal rules of forensic science, an investigator is required to justify his actions for example where an investigator goes for live forensics as opposed to dead forensics.

Methods of Authenticating Evidence

There are basically three (3) ways that are used to authenticate evidence namely:-

- ✓ **Documentation** – The investigator should record key processes, take photographs of the crime scene, maintain a chain of custody, maintain working papers, write notes and other forms of documentation. This is another way to authenticate evidence.

- ✓ **Use of tools** – Recognised tools should be used in forensic auditing or investigation. These tools should have been peer reviewed and the investigator should know the tool's degree of error if any exists.

- ✓ **Hashing** – A mathematical algorithm that produces a unique value (128 Bit, 512 Bit). Common hash keys used are SHA-1, MD5, SHA-256, etc. These checksums are used to check whether evidence has not been changed and is still what it was when it was collected by the investigator. Hashing is only used when dealing with digital evidence. Developed in 1994, MD5 is a one-way hash algorithm that takes any length of data and produces a 128 bit value, which is a "fingerprint" or "message digest". This value is "non-reversible"; it is "computationally infeasible" to determine the data based on the value. This means someone cannot figure out your data based on its MD5 value.

  Example: **Hash Keys for ACPO Good Practice Guide for Digital Evidence v5.pdf**

  MD5: B33FE391BDC4B5016957E098D6D196D7

SHA-1: 5E733DDAE6039E2E1A8812A3DE9FE171D7215DB9

SHA-1 has 40 characters and MD5 has 32 characters. The above algorithms should remain the same for as long as the guideline has not been modified by its authors.

The 6 Principles of Digital Forensics are:

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
2. Upon seizing digital evidence, actions taken should not change that evidence.
3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
5. An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.
6. Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

Conclusion

Evidence is so crucial to the determination and outcome of a case. Care should be taken so as not to contaminate the evidence as decontaminating it is impossible. Difficulty is with digital evidence which is fragile and volatile to some extent. Investigators must be experienced when dealing with digital evidence.

CHAPTER 5

FORENSIC AUDIT REPORT WRITING

Introduction

The report writing is the final stage of an audit and is guided by the rules of the court if it is a criminal case and if it's an administrative matter, the administrative procedures of the organization should guide the investigator accordingly and it is not the purpose of this chapter to dwell on administrative issues. Generally the administrative report has a section for recommendation and conclusions drawn by the investigator. For court purposes, the investigator should never include such areas as it is the court's responsibility to recommend and conclude on a particular case. It is entirely up to the court to sentence a person or decline to prosecute.

A forensic auditor is a witness though classified as an expert witness. It is in this regard that the rules affecting witnesses in a particular jurisdiction be applied accordingly as the report / statement will end up in a court of law where the court applies its rules and not accounting or auditing rules for example. The format of the report should be a format that is acceptable in a court of law.

In many jurisdictions, the report takes the format of a Witness Statement and not the structure of a traditional report format. For administrative purposes, yes, it usually takes the traditional format where a recommendation and a conclusion are included. For administrative purposes, the objective of a forensic audit is to take corrective action so that recurrence of a case is prevented, but in a criminal context, the objective is to punish the wrongdoer as a way of protecting members of the public against such criminal elements. The state has a laid down template for criminal elements in our society and the court has that jurisdiction to decide the nature of punishment for the wrongdoer.

The 6Ws

When writing the report or statement as the case may be, the writer should answer the 6Ws namely:

1. What happened?
2. Who did it?
3. Where did it happen?
4. When did it happen?
5. Why did it happen?
6. How did it happen?

Report writing strategy

The report should avoid being accusatory, but try by all means to address the 6Ws. It is more of a story telling exercise than anything else. The court wants to be assisted with answers to the 6Ws so that they can come up with an opinion on a matter before it. It must decide on that complex matter in an unbiased manner that brings out fair justice to all the parties involved.

Technical jargon should be avoided as much as possible and it's not about impressing the court, but it is about making the judge understand the complex matter you have brought before him. Not all judges are accountants or auditors. Some do not even have a legal background and it is therefore important that the matter is simplified as much as possible to allow a layman to understand. Many cases lose value because of the jargon that writers use. Don't forget your primary role as an expert witness!

The report should be supported by facts and evidence. Facts must clearly come out of the report. A report without facts has no place in a court of law as a matter of principle.

At the end of your report, it should be signed by you. Include the date and place where the report was written.

If the case is criminal, do the report yourself and get less assistance from the police officer. The police do not have much time to write a very long report say for example, your case has 200 counts of fraud committed on 200 different days. They will usually try to summarise the case and this is not good enough for court purposes as far as the answering of the 6Ws is concerned.

Remember you are another piece of evidence that must be credible and as you write your report, tell us about your professional qualifications and probably experience. The investigator should possess the requisite professional qualifications or certifications relating to the nature of the investigation. For forensic auditing, the investigator needs to possess the necessary certifications such as Certified Forensic Auditor (CFA), Certified Fraud Examiner (CFE), etc. In your report, the investigator can even tell us about his professional association and his or her membership number and also whether he is a member in good standing or not.

Conclusion

The objective of a report is to address the key questions posed by the requester of it. You need to understand his needs and expectations. The report should therefore be written so as to help the requester of it so that he can decide on the matter. For the courts, it's usually about punishing the wrongdoer and for workplace reports, it is about taking a corrective action. The requester should be given enough room to decide on his own without much input from the writer though there is nothing wrong in making recommendations for administrative purposes. It is entirely up to the requester of a report to listen to the recommendation or not.

CHAPTER 6

EXPERT WITNESS TESTIMONY

Introduction

The final by-product of a report is appearing or testifying in a court of law or an administrative court. Appearance of the investigator helps in clarifying some pertinent questions that the court is in need of. The court is interested in cross examining the witness so that the truth can clearly come out and the court should also verify the credibility of the expert witness before putting reliance on his or her work. This is important to do in the best interest of delivering justice to all interested parties involved. Falsehood should be avoided when testifying and once summoned to appear in a court of law; the witness must comply as it is criminal to disobey a court order. Failure to appear in a court can cause the arrest of a witness with a view of securing his or her attendance in a court of law and is usually released once he or she has testified.

The Dos

- ✓ Arrive early at the Courts
- ✓ Always tell the truth and nothing more
- ✓ Dress professionally
- ✓ Limit technical jargon to exceptional cases
- ✓ Avoid falsehood
- ✓ Don’t rehearse your report
- ✓ Answer questions clearly and avoid creating your own questions
- ✓ Don’t get angry and manage your temper
- ✓ Don’t give the defense more information than required of you
- ✓ Where you make a mistake, always correct yourself while in the court
- ✓ Where you don’t know certain facts, just say l don’t know as this adds to your credibility
- ✓ Address all questions through the judge and not your opponent
- ✓ Work on good public speaking skills
- ✓ Feel relaxed when in a court of law and avoid being nervous; at least don’t show everyone that you are nervous
- ✓ Be confident of what you are saying
- ✓ Always do a thorough investigation and make sure your evidence is authenticated.
- ✓ Don’t think, but say the truth!

Conclusion

A successful prosecution largely depends on a good expert witness testimony. Poor testimonies always discredit the case than anything else.