The use of digital data as evidence in the South African Law

Mini-dissertation submitted in partial fulfilment of the requirements of the degree Magister Legum in Import- and Export law at the North-West University (Potchefstroom Campus)

By

Alma Nel

The use of digital data as evidence in the South African Law

Mini-dissertation submitted in partial fulfilment of the requirements of the degree Magister Legum in Import- and Export law at the North-West University (Potchefstroom Campus)

By

A Nel
12323977

Successfully completed modules: LLMI 874
LLMI 875
LLMI 876
LLMI 877
LLMI 884

Study supervisor: Prof SPLR de la Harpe

October 2005

Recognition

The research, hundreds of pages of print-outs and copies, hours on the internet, compilation and binding of this mini-dissertation was made possible by bursaries received from the WNNR/CSIR as well as the North-West University Potchefstroom Campus and its Faculty of Law Focus Area.

I would also like to thank Professor de la Harpe for all his guidance, time, patience and understanding.

A special thank you to my family and friends, who put up with me and always asked 'Are you done yet?' and if the answer was in the negative, just smiled, brought me some coffee and replied 'Good luck'.

Die gebruik van digitale data as bewyse in die Suid-Afrikaanse reg

Deur
Alma Nel

Die groeiende gebruik en wye strekking van tegnologie gedurende die afgelope paar jare, het 'n nuwe tipe bewysmateriaal geskep wat in beide siviele en kriminele sake gebruik word: sogenaamde digitale bewysmateriaal.

Soos tegnologie verander moet die reg ook verander. Die reg moet aanpas om by te hou met die konstante veranderinge van tegnologie. Weens die mens se daaglikse afhanklikheid van tegnologie, en die groter invloed daarvan in siviele en kriminele aangeleenthede, word besondere uitdagings geskep vir die tradisionele reëls van die hedendaagse Suid-Afrikaanse bewysreg. Die regulering, verkryging en bewaring van digitale bewysmateriaal veroorsaak 'n leemte in die bestaande Suid-Afrikaanse reg.

Om digitale data se gebruik as bewysmateriaal in 'n Suid-Afrikaanse hof te vergemaklik moet die Suid-Afrikaanse reg met verwysing na digitale data verander. Die effektiewe bewaring van digitale data, wat ook die integriteit en oorspronklikheid daarvan sal verseker, moet na gekyk word. Weens die aard van rekenaar-genereerde en digitale bewysmateriaal word dit as broos beskou. Dit kan maklik verander en onttrek word en is moeilik om 'n onderskeid te tref tussen die oorspronklike en kopieë daarvan. Die bewaring en dokumentering van digitale bewysmateriaal vereis daarom spesiale aandag. Nuwe tegnieke en prosedures word vereis en moet ontwikkel word sodat dit gebruik kan word om die behoud van die integriteit van die digitale data te kan verseker.

Die Suid-Afrikaanse reg met betrekking tot digitale bewysmateriaal word tans grotendeels gereguleer deur *die Elektroniese Transaksies en Kommunikasie Wet* 25 van 2002. Hierdie wetgewing is baie wyd geformuleer en bevat geen definisie van digitale bewysmateriaal nie. Die wetgewing skryf ook nie die nodige tegnieke en prosedures wat toegepas moet word om die integriteit van digitale bewysmateriaal te verseker voor nie.

Hierin word 'n studie gedoen van die reeds bestaande regsreëls en regulasies van toepassing op digitale bewysmateriaal in beide die Suid-Afrikaanse en Amerikaanse regstelsels. Die Amerikaanse regstelsel het verskeie wetgewing, regspraak en institusionele reëls en regulasies wat die gebruik van digitale data as bewysmateriaal vergemaklik. Hierdie wetgewing, regspraak en institusionele reëls en regulasies maak wel voorsiening vir spesifieke tegnieke en prosedures wat gevolg moet word gedurende 'n ondersoek na digitale bewysmateriaal deur rekenaar forensiese inspekteurs om die integriteit van die digitale data te verseker.

Daarna word 'n regsvergelyking gedoen tussen die twee regstelsels om moontlike oplossings te lewer vir die probleem wat tans ervaar word in Suid-Afrika met betrekking tot die gebruik van digitale data as bewysmateriaal in 'n Suid-Afrikaanse hof.

Table of contents

Chapter 1

Introduction

> Just think of all the paper that you see today, the source of nearly it all, is an electronic file.[1]

Cyberspace[2] can be seen as a community consisting of networked computer users around the world. In this digital world it would be ignorant to believe that the normal perils of lawlessness will have no effect on a network user.[3] Cyberspace has brought electronic merchants, on-line or networked educators, and even doctors meeting on-line with patients in offices around the world. Finding cyber criminals amongst network users is thus not surprising. As this digital world is so vast and stretches far beyond any national borders, the idea of a 'police man' to supervise all actions in this arena may be perceived as a notion created by a vivid imagination. Offenders can therefore maintain a level of anonymity only possible in this digital world.

The importance of the electronic era for international trade is that trade is boosted through the use of ever-changing digital technology. The rise in electronic contracts via the Internet is due to the fact that it is a much speedier, convenient and cost effective manner in which to conclude international contracts. All these Internet contracts will be in the form of digital data stored in files and e-mails that contain offers and acceptance agreements, confirmations thereof and confirmation of receipt of goods. It would be to the detriment of any

---

1 Richard 1999-2000 *Whittier Law Review* 463.

2 Cyberspace is also more commonly known as the Internet. It is described as the world of connected computers and the society that gathers around them. University of Georgia Office of Information Security [InfoSec] Enterprise Information Technology Services 'InfoSec Glossary of Terms' HYPERLINK http://www.infosec.uga.edu/glossary.php?question=nq 23 Sept.

3 The growth of the Internet has improved our economy, medicine and technology. Unfortunately, it has brought new opportunities for criminal activity, as well. Using computer technology, criminal types steal life savings and even identities of unsuspecting individuals, posing serious threats to the lives and the livelihoods of many individuals. See House of Representatives, Subcommittee on Crime, Committee on the Judiciary, Washington, DC Report 'Fighting Cyber Crime: Efforts by Federal Law Enforcement' 2001 HYPERLINK http://commdocs.house.gov/committees/judiciary/hju72616.000/hju72616_1.htm 11 Oct. p 88.

party to such agreements if he/she does not store evidence of these transaction or contracts. Therefore most of the information and data about these international transactions are most likely stored on computers in digital format.[4]

The widespread use of computers in recent years has led to a new type of evidence in both criminal and civil cases, namely digital evidence. Daily it becomes clearer that nearly every area of the law and legal practice can be affected by digital data. Therefore, as technology changes, so too must the law adapt in order to keep pace with constant change. Our reliance on digital technology and the use thereof in all spheres of life poses significant challenges for the traditional rules of the present day South African law of evidence. Therefore, in order to use digital data as admissible evidence, the South African law of evidence concerning digital data needs to change. Furthermore, the traditional procedures and techniques applied in the collection of admissible evidence in all litigious matters should change to accommodate digital evidence.[5] Central to these issues is the much needed requirement that the digital data must be preserved effectively to ensure its integrity and originality.[6]

---

4 In order for something to be referred to as digital it must comply with the definition of this term. Digital is data that has been created, transmitted, or stored as a string of signals coded as "1" (on) or "0" (off). Data in digital form (text, numbers, graphics, voice, video, etc.) can be stored and processed by computers and communicated at high speed over electronic networks with complete accuracy and reliability. Exact copies of digital data can be made in which the copy is indistinguishable from the original. See University of Georgia Office of Information Security footnote 2 above.

5 Provisions must be made to include digital evidence within the world of physical evidence. New techniques and procedures are required in response to the increasing number of criminal and civil cases that are based on digital evidence.

6 Due to the fragile nature of digital data and the strict evidential rules applied to determine admissibility of any evidence, the techniques and procedures followed when collecting and preserving or storing digital data from a suspect digital device must be effective and secure in such a manner as not to compromise the digital evidence further by possibly altering it during preservation or further searches through it. Simply turning on the subject computer or accessing a file will change critical information on the hard drive, particularly related to date/time stamps. In order to preserve electronic evidence, special procedures and tools should be utilized to make an exact image copy of the media – without altering a single byte of data. In this way, the chain of custody and forensic soundness of the electronic information is maintained. See Snyder JA and Morelock A 'Electronic Data Discovery: Litigation Gold Mine or Nightmare?' HYPERLINK http://www.mobar.org/journal/2002/janfeb/snyder.htm 11 Oct.

For most physical evidence investigations the use of Forensic Investigators are required. However, in today's day and age, the help of Computer Forensic Investigators is also required to investigate technological devices for digital evidence.[7] Digital evidence can *inter alia* be found on laptops, digital cameras, phones, and hard drives.[8] By using these devices a single file, credit card purchase or stray e-mail message can provide the proof that can clinch a case. Computer Forensics should be considered as a standard and routine practice in all legal matters. [9]

The law of evidence in South Africa must change in such a manner as not to attempt to force the products of modern technology into the rather limited categories of either real or documentary evidence.[10] In contrast to investigations into digital evidence, investigations of other physical evidence have existed for thousands of years. The experience from these investigations can and should be applied to the digital world.

Due to the fact that more criminal and civil cases will include investigations into digital evidence at some point, it is imperative that an acceptable process or

---

7 In situations where a technological device is suspected to have been part of or used in all matters of commerce and other aspects of life, both the computer forensic investigator and law enforcement officials should approach the device with caution. The prime objective of any computer forensic investigator should be to provide acceptable evidence with an assurance of integrity.

8 Hard drives are not the only place to turn for potential electronic evidence. Network servers, e-mail servers, backup tapes and other computerized storage should also be considered. In addition, electronic calendars, printers, fax machines and copiers are often sources of electronic evidence. See Snyder and Morelock footnote 6 above.

9 Computer Forensics is a relatively new concept in South Africa. Due to the fact that digital data is easily altered, and that it is difficult to distinguish between original data and copies, the extraction, securing and documenting thereof require special attention. Various procedures and techniques that computer forensic investigators can and should use when trying to extract digital data from these devices, in order to ensure the digital information's integrity and authenticity will be discussed.

10 The use of computers places the law of evidence under great strain. More so than any of its technological predecessors since computers work with data in a digital format that makes it susceptible to manipulation. The programmable and digital nature of the data on a computer, which allows its workings and output to be constantly modified by human intervention, strains the analogy with real evidence. Even though there are case law that admit computer print-outs as evidence, all digital evidence and digital documents cannot reside within the traditional concept of documentary evidence as there are more to these digital documents than can allow them to merely be seen as documents.

model for a digital investigation exists to ensure the integrity of the data.[11] The current rules, of discovery in civil litigation and collection through search and seizure in criminal litigation, and the principles of reliability and authenticity have all developed around traditional paper documents. They do however contain occasional patchwork in an effort to accommodate the products of photography, cinematography, audio and video magnetic tapes, mechanical data recording devices and the computer.[12] The present content and application of these rules to digital evidence is not recommended and is insufficient.

The law governing digital evidence lags behind the reality of cyber-crime and the use of digital data in all spheres of life. Few legal precedents exist to guide judges. It is also perceived that many judges[13] may not understand the digital technology and issues it raises.[14]

The nature of computer based evidence makes it inherently fragile. It is easily altered, extracted and it is difficult to distinguish between original data and

---

11 This process or model must also be able to easily interact with the investigations of other physical evidence.

12 See, for example, the *General Law Third Amendment Act* 129 of 1993 S 45 amended S 236 of the *Criminal Procedure Act* 51 of 1977 in order to for it to make provisions for the admissibility of computer printouts as accounting records. See also the *Marine Living Resources Act* 18 of 1998 in which S 75(1) provides for the use of Photographic evidence as follows: "If a photograph is taken of any fishing or related activity and the date and time on and position from which the photograph is taken are simultaneously superimposed upon the photograph, it shall be *prima facie* evidence that the photograph was taken on the date, at the time and in the position so appearing." See further the provisions in Ss 11-19 of the *Electronic Communications and Transactions Act* 25 of 2002 in which there are numerous sections providing for the use of computer evidence.

13 This may be said of judges who did not grow up working on, using, or learning about computers on almost a daily basis.

14 In most litigation where evidence is presented which is derived from technological devices, judges will most likely not have sufficient knowledge of the workings and operation of the device. An expert witness will have to testify on the workings of the device and the nature and composition of the information presented as evidence. In the opinion of the University of Dayton's Susan Brenner: "We have judges who did not grow up with computers and so many do not understand the technology and issues it raises", as referred to in Coren 'Digital evidence: Today's fingerprints. Electronic world increasingly being used to solve crimes' HYPERLINK http://www.cnn.com/2005/LAW/01/28/digital.evidence/index.html 10 March p 2. This is the case both in the USA and South Africa – as many of the presiding South African judges simply do not have the same technological experience that students today have, and may therefore be hesitant to trust digital evidence without requiring extensive evidence to prove its authenticity.

copies.[15] The securing and documenting of digital evidence requires special attention. In order for digital evidence to be admissible in a court of law, there is a need for new development in techniques and procedures presently applied to better or more accurately preserve the data integrity of digital evidence.[16]

In order to solve this problem, it is necessary to look for solutions and insights outside South Africa. The USA is one of the leaders in the world on the use of technology.[17] Therefore a comparative study of the American law with regard to the use of digital data as evidence will be done. The courts in the USA have Federal and State legislative provisions in this regard.[18] Even as early as the year 2000, it was standard practice in America for lawyers, engaged in criminal or civil cases, to request information that was created, stored, transmitted, discarded, or deleted electronically.[19]

Due to the extensive practical application of digital data as evidence in America, their investigative institutions,[20] legislature and case law have provided possible

---

15 For a further discussion on this see Chapter 2 paragraph *2.1.4 Computer Forensics Basics* of this mini-dissertation. See also Kerr 2005 *Columbia Law Review*.
If electronic files are produced only in printed form, there is important background information missing. This information, or metadata, provides such information as the file's location, creator, date created, date last accessed, etc. Electronic copies also provide file formatting, information about password and other forms of protection, notes embedded and hidden in the document, and certain version information. Paper copies are not an acceptable substitute. See in this regard Snyder and Morelock footnote 6 above.

16 There is a *lacuna*, in the law of evidence, which the regulation, collection and preservation of digital evidence pose in present-day South Africa. This is due to the South African law of evidence not keeping abreast of digital evidence, as it is based on paper based transactions and physical evidence.

17 America, is a country on the forefront of technological development (the home of one of the worlds larges IT companies Microsoft) and this is evident by a substantial amount of case law against cyber criminals and cyber terrorists.
The USA has specific legislation and investigative agencies such as the Federal Bureau of Investigation (with help from private agencies such as Microsoft) specializing in the collection of digital evidence and using it as admissible evidence. See also Anon. 'Anti-phishing 'posses' hunt criminals' *United Press International* October 05, 2005 HYPERLINK http://www.physorg.com/news6992.html 10 Oct.

18 These legislative provisions are not totally infallible, and are constantly being improved.

19 A search through digital data could recover a hidden document or deleted e-mail message, and the information thereof could lead to a favourable settlement or might even win a case.

20 Such as the Federal Bureau of Investigation (FBI) for national investigations, the Central Intelligence Agency (CIA) for international investigations that affect the USA and each of the separate States' Police Computer forensic divisions.

techniques and procedural steps that must be taken during the collection and use of digital data from technological devices. These procedures and techniques will ensure the integrity of the digital data in order for it to be admitted as digital evidence. These rules and regulations are applied without unreasonably compromising the citizen's Fourth Amendment rights or the rights protected in legislation specifically applicable to the use, search and seizure of digital evidence.[21]

To start with, the technical aspects applicable to digital data being applied as evidence, and the possible techniques and procedures that can be introduced and followed in South Africa to ensure the integrity, authenticity and admissibility of digital evidence will be discussed. Thereafter the present South African law of evidence will be discussed with particular reference to the use of digital evidence and the limitations imposed on the use thereof by rules of evidence.[22] In the next chapter the present American Federal and Texas State law of evidence will be discussed with particular reference to the use of digital evidence, and the possible limitations imposed on the use thereof by evidence rules similar to those discussed under the chapter on the South African law of evidence. Thereafter a comparative analysis of the American and South African law of evidence will be done. In conclusion, possible solutions and proposals to overcome the existing problems with regard to the use of admissible digital evidence in a South African court of law will be discussed.

---

21 See the discussion under paragraph *4.3.2 Federal Rules of Evidence* in Chapter 4 of this mini-dissertation. See also Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations' 2002 HYPERLINK http://www.cybercrime.gov/s&smanual2002.htm 11 Oct.

22 The rules of evidence discussed in this mini-dissertation are authenticity requirements, the best evidence rule, and the prohibition of hearsay evidence.

Chapter 2

The Phenomenon of Digital Evidence

Hidden on hard drives, diskettes and other forms of storage devices is a plethora of e-mail, draft documents, and confidential files.[1] In this chapter the various technical aspects with regard to the use of and collection of digital evidence, technical jargon and possible techniques and procedures that may be used to obtain admissible digital evidence is explained and discussed.

2.1 Preservation of digital evidence: techniques and procedures

2.1.1 Evidence in general

Evidence encompasses all the information obtained to establish the fact in question. The general rule, in both South African and American law, is that no evidence of any fact is admissible if it is immaterial or irrelevant.[2] As with other forms of evidence,[3] the form, prevalence, and existence of digital evidence will help clarify competing stories about the re-enactment of an event. Digital evidence is becoming a central focus in the investigation for and collection of evidence.[4]

---

1 Every day people strike at computer keyboards, typing up confidential e-mail messages or files that they do not want others to see. This is done on their private home or office computers. It is saved and with a single stroke of the delete key, it is believed that its existence is deleted. This is however not the case. All this digital data may be used as evidence in a trial before a court of law. For a list of terminology that will be encountered during a discussion concerning data storage and data storage devices see Annexure "A".

2 For South African authority see Schmidt *Bewysreg* 359-361 and also Vos 'Evidence Unlawfully Obtained' 2004 HYPERLINK http://www.deneysreitz.co.za/news/news.asp?ThisCat=2&ThisItem=539 21 Sept. For American authority see Kenneally 2001 *Virginia Journal of Law and Technology*. All evidence that is reliable and relevant to the facts that need to be proven, will be admissible unless it is prohibited by an evidence exclusionary rule. See *R v Schaube-Kuffer* 1969 2 SA 40 (RA) at 50B-C. See also Van der Merwe and Janse van Vuuren 'Internet Contracts' HYPERLINK http://www.cyberlawsa.co.za/cyberlaw/cybertext/chapter6.htm# 21 Sept.

3 Such forms as hair, blood, eyewitness accounts, or paper documents.

4 Due to an apparent hesitation by South African courts in allowing digital evidence to be admitted as evidence, legal representatives are faced with various problems in this field. The problem posed by digital evidence to legal representatives in South Africa lies in the fact that there exists very little legislation and case law which deals fully with this phenomenon. Neither case law, nor legislation specifies which techniques and procedures must be used to ensure the integrity and admissibility of digital evidence during the investigation for and collection thereof. The assurance of the authenticity and

2.1.2 Digital evidence[5] as a new phenomenon

Digital evidence can be regarded as:

- information stored or transmitted in electronic or magnetic form;[6]
- information stored or transmitted in binary form that may be relied upon in court.[7]

However, some authors also refer to the term 'Electronic evidence'[8] which has been defined as information and data of investigative value that is stored on or transmitted by an electronic device.[9] The term 'digital' refers to data that has been created, transmitted, or stored as a string of signals coded as '1' (on) or '0' (off).[10] Data in digital form[11] can be stored and processed by computers and communicated at high speed over electronic networks with complete accuracy and reliability.[12] Technically, documents and data are 'electronic' if they exist in a medium that can only be read through the use of computers.[13] On the other hand, information that is in a digital form will be

---

integrity of digital evidence is fundamental to ensure that it is accepted as admissible by South African courts. See Chapters 3 and 4 of this mini-dissertation for a comprehensive discussion on the problems faced by South African and American legal representatives respectively.

5 For purposes of this mini-dissertation reference will throughout only be made to digital evidence and not electronic evidence.

6 Chawki 'The Digital Evidence in the Information Era' 2004 HYPERLINK http://www.crime-research.org/articles/chawki1/ 25 Jul.

7 University of Georgia Office of Information Security [InfoSec] Enterprise Information Technology Services 'InfoSec Glossary of Terms' HYPERLINK http://www.infosec.uga.edu/glossary.php?question=nq 23 Sept.

8 In America the term 'electronic evidence' is used rather that 'digital evidence'. The collection and civil discovery requests for such evidence and the search applied to obtain such evidence is referred to as electronic discovery. Electronic documents include e-mail, web pages, word processing files, computer databases, and virtually anything that is stored on a computer. See Hedges 'Discovery of Digital Information' 2005 HYPERLINK http://www.roscoepound.org/new/updates/2005hedges.pdf 23 Sept. p 5.

9 See footnote 7 above. Because the description of digital evidence above includes provision for electronically stored information as digital evidence, to avoid confusion during this discussion only the term digital evidence will be used. This will therefore include the American concept of electronic evidence.

10 See footnote 7 above.

11 Such as text, numbers, graphics, voice, video, etc.

12 See footnote 7 above. The basic problem with information stored in this manner is that it has a fragile nature as exact copies of digital data can be made in which the copy is indistinguishable from the original.

13 Electronic data consists of zeros and ones created by electric polarity. Such data may be found on/in cache memory, magnetic disks (such as computer hard drives or floppy disks), optical disks (such as DVDs or CDs), and magnetic tapes. See Hedges footnote 8

present on many more devices than just computers.[14] Digital evidence can therefore be regarded as any electronic or digital information that can be generated by, stored or found on, *inter alia*, a computer or any other technological device such as mobile phones, laptops, digital cameras, and hard drives.[15]

2.1.3 Computer Forensics[16]

During this technological era in which we live, there is a need for the help of Computer Forensic Teams to investigate technological devices in order to obtain digital evidence. Computer forensics has been described as:

> The analysis of data processing equipment, typically a home computer laptop, server, or office workstation, to determine if the equipment has been used for illegal, unauthorized, or unusual activities. It can also include monitoring a network for the same purpose.[17]

---

above. This differs from digital evidence which can be present in all digital devices such as mobile phones and digital cameras, and also on computers.

14 Digital evidence may be present in all digital devices such as mobile phones and digital cameras, and not merely on computers as it is in the case of electronic evidence.

15 Also referred to as Hardware interface software, which is a program that works with the operating system to control hardware devices. See Wilson *Information Processing* 2002 275.
Hard drives are not the only place to turn for potential electronic evidence. Network servers, e-mail servers, backup tapes and other computerized storage should also be considered. In addition, electronic calendars, printers, fax machines and copiers are often sources of electronic evidence. See Snyder and Morelock 'Electronic Data Discovery: Litigation Gold Mine or Nightmare?' HYPERLINK http://www.mobar.org/journal/2002/janfeb/snyder.htm 11 Oct.

16 Computer forensics may be described as the science whereby experts extract data from computer media in such a way that it may be used in a court of law and to ensure the integrity of the information obtained. The science involved is computer science and some refer to it as Forensic Computer Science. Computer forensics may also be regarded as the autopsy of a computer hard disk drive. Computer forensics requires specialised software tools and techniques to analyse the various levels at which computer data is stored. See footnote 7 above.

17 Wikipedia 'The free encyclopaedia: Computer Forensics' HYPERLINK http://en.wikipedia.org/wiki/Computer_forensics 10 March. A server can be described as Computers used to store and service a network. See Wilson footnote 15 above p 281.
An office workstation can be described as the individual computers connected to a network. See Wilson footnote 15 above p 283.
A network can be described as two or more computers joined together for the purpose of transmitting and receiving data. See Wilson footnote 15 above p 277.

Computer forensics is typically a two-stage process:[18]

- the discovery, recovery, preservation and control of electronic data or documents.
- the analysis, verification and presentation of e-evidence in a court of law or investigations[19] for that purpose.

Computer forensics involves collecting, preserving, seizing, analyzing and the presentation of computer-related evidence by utilizing secure, controlled methodologies and auditable procedures.[20] The forensic specialist uses specialized software,[21] and the examination will enable him/her to:

- discover data that exists in a computer system;
- recover deleted, encrypted or damaged file information; and
- recover passwords to enable him/her to read certain documents.[22]

Any or all of this information found during the analysis can potentially be used during both criminal and civil litigation.[23] Computer forensic teams are required to recover data[24] from the technological device(s) of a suspect or in the course of civil litigation. Data recovery may be described as:

> The act of salvaging data stored on damaged media, such as magnetic disks and tapes (magnetic devices). There are a number of companies and software products that can help recover data damaged by a disk crash or computer virus. Of course, not all data is recoverable, but data recovery specialists can often restore a surprisingly high percentage of

---

18 Volonino 2003 *Communications of the Association for Information Systems* 8.

19 All investigations (for civil- and criminal matters) undergone with the purpose of finding digital evidence that may be used as admissible evidence in a court of law.

20 These examinations involve the examination of computer media, such as floppy disks, hard disk drives, backup tapes, CD-ROM's and any other media used to store data. See footnote 7 above.

21 This specialized software is not normally available to the general public.

22 See footnote 7 above.

23 See footnote 7 above. Computer forensics can be used to detect, trace, or prove a diverse range of crimes or aspects relevant in civil litigation, such as: Fraud, negligence, malpractice; Theft of trade secrets, intellectual property; Violations of non-competitive restraint on trade agreements; Safer design of a defective product; Privacy invasion, identity theft; Child pornography, violent crime; Money laundering, terrorist activity; Hacker activity, malware; Workplace harassment, discrimination, defamation; Examples of civil application may be situations in which e-agreements or Electronic Data Interface agreements have been concluded but one of the parties thereto have failed to comply therewith or are in breach of such an agreement. See footnote 18 above.

24 Any individual fact that can be input, stored, processed output and retrieved from a computer. See Wilson footnote 15 above p 272.

the data on damaged media. The ability to recover 'deleted' data is a problem when equipment used to store sensitive data is to be discredited.[25]

The help of computer forensic teams are often required to investigate technological devices in order to obtain and ensure admissible digital evidence. Therefore Computer forensic investigators will play an increasing important role.

2.1.4 Computer Forensics Basics: use, storage and deletion of digital information

2.1.4.1 Creation and storage of Documents[26]

When a document is created in Microsoft Word, three things happen:[27]

- the new document is displayed on the screen;
- a 'temporary' work file is created on the hard disk.[28] This file will be referred to as "Work File A." This file is invisible to the user;
- data begins to churn though the virtual memory file, which is a physical file on the hard disk.[29] This file will be referred to as the "VM file." This file is also invisible to the user.

When the author saves the document he/she is writing, a fourth thing happens:

- a file with a name given to it by the author is created on the computer's hard disk.[30] This file will be referred to as the "User Document." As the writer continues to write or update the document, changes occur within the User Document, these changes are reflected in "Work File A", and

---

25 See footnote 18 above. Magnetic devices can be described as storage which uses magnetic material to hold binary data. See Wilson footnote 15 above p 276. Software can be described as programs or sets of instructions that control the operation of the hardware. See Wilson footnote 15 above p 281.

26 The following discussion will use the Microsoft Word program to explain the basics of computer usage and the generation of digital information.

27 Burgess 'The Case for Electronic Discovery' HYPERLINK http://adr.forensic.e-symposium.com/computerforensics/whitepaper.pdf 23 Sept.

28 *Ibid.*

29 See footnote 27 above.

30 See footnote 27 above.

much of this data is written into the "VM file".[31] As the writer changes and updates the User Document, most of the previous edition is invisibly archived into the User File as well as into the other two files mentioned above.[32]

When the file is closed, "Work File A" is not saved as a document accessible to the user, but it continues to exist as a deleted file on the computer's hard disk.[33] When the User Document is opened again, a new temporary and invisible Work File is created[34] – referred to herein as "Work File B." There may be several iterations of the creation of a Work File on a given hard disk, one corresponding to each time the User File is opened and viewed and/or modified, and correspondingly named "Work File C," "Work File D," etc.[35] If the User Document is saved with a different name, the document is still maintained on the hard disk with its original names, as well as with the new name.[36]

2.1.4.2 Saving a File

When a document is named, it is saved. It may be saved with a name such as "Untitled" even if not given a unique name by the author.[37] When the file is saved, there are several attributes saved with it:

- the date the file was created;
- the date the file was last changed, or modified;
- the date the file was last accessed.[38]

---

31 See footnote 27 above.
32 See footnote 27 above.
33 See footnote 27 above.
34 See footnote 27 above.
35 See footnote 27 above.
36 E-mail and other documents behave in much the same way, although some of the specifics differ somewhat from program to program. Microsoft Outlook saves its email files somewhat differently that Microsoft Outlook Express, for instance. See footnote 27 above.
37 See footnote 27 above.
38 This information is kept as part of a file listing called a 'directory.' This file listing is viewed as a 'folder' by the computer user and the computer saves both a long version and a short version of the name as two adjacent directory listings. See footnote 27 above.

2.1.4.3 Deleting a File

When a file is deleted, the file does not simply go away. It remains invisible on the hard disk.[39] Furthermore, the deletion of the file does not affect the pre-existing Work Files, and has little one-to-one correspondence with any changes to the "VM file".[40] The computer keeps track of the physical locations to where a data file may be written. When a file is written, the computer[41] makes one or more entries into its index of file information that includes whether or not a specific spot on a hard disk contains a file.[42]

When a file is deleted, the computer marks the physical location of the file as available to be used, and it also changes the name of the file by altering its first character.[43] But until another file is saved to that directory, and saved at that spot in the directory, the file name is not overwritten.[44] Similarly, when a file is overwritten, much of the previous content of the file may remain intact. If, for instance, a file that took up 4 entire clusters is deleted, and another file that measures 256 bytes is written, then 3½ clusters or 7/8 of the original data is maintained and may be able to be recovered.[45] When a file is simply deleted, and not overwritten, it is fairly easy for a computer forensic examiner to recover, or recreate, the file.[46]

Whenever new data, files, or documents are written to the computer, there is a possibility that the data remaining from previously deleted files will be

---

39 See footnote 27 above.
40 See footnote 27 above.
41 Actually this is done by the operating system.
42 See footnote 27 above.
43 If a file was named, "Computer file," its name would change to "σomputer file"; therefore having the "σ" character at the beginning of its name tells the computer that this file listing is available to be overwritten. See footnote 27 above.
44 Furthermore, if the name of the new file that is written to the same location in the directory is shorter than the original name, only part of the original name is overwritten. For instance, if the original file were named "Computer file" and the new file were named "Joe," then while the directory entry would appear to the user to be "Joe'" the name actually in the directory listing would look something like "Joeputer file." See footnote 27 above.
45 See footnote 27 above. This is the kind of work a computer forensic examiner performs.
46 See footnote 27 above.

overwritten.[47] Overwritten data is not recoverable through any means available to most computer forensic examiners.[48]

Some e-mail programs work in a slightly different fashion. In Microsoft Outlook, all e-mails are kept in one large file. When e-mails are deleted and even when they are purged, the content of the deleted e-mail is not necessarily deleted from the large Outlook file.[49] Deleted e-mails may not necessarily be removed from that file, and may be recoverable by a manual process.[50]

2.1.4.4 Data recovery[51]

A myth in the electronic world is that a deleted message will be gone forever. However, deleted data is merely moved out of the way by computers. It is only 'removed' once new saved data takes over its place,[52] as it then becomes

---

47 See footnote 27 above.

48 The very act of starting up a computer, shutting it down, or even looking for files will alter the actual contents of the hard disk. The longer the computer is in use after a file has been written or deleted, the greater are the odds that data of interest will be spoiled or destroyed. See footnote 27 above.

49 These deleted e-mails may be recovered through a manual process. In Microsoft Outlook Express and other e-mail programs, such as Qualcomm Eudora Pro, each mailbox has its own file, and all e-mails from a given mailbox are kept in that one file. See footnote 27 above.

50 See footnote 27 above.

51 Data remanence is the residual physical representation of data that has been in some way erased. After storage media is erased there may be some physical characteristics that allow data to be reconstructed. Overwriting can also be an effective method of clearing data. For example, a single overwrite of a file (or all system storage, if the circumstance warrants such an action) is adequate to ensure that previous information cannot be reconstructed through a keyboard attack. Erasure is a process by which data recorded on storage media is removed. An Overwrite Procedure is a procedure to destroy data recorded on Automated Information System (AIS) storage media by recording patterns of unclassified data over the data stored on the media. AIS is an assembly of computer hardware, firmware, and/or software configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. AIS Storage Media is the physical substance used by an AIS system upon which data is recorded. Remanence is the residual information that remains on storage media after erasure. See In this regard Goldston 'A Guide to Understanding Data Remanence in Automated Information Systems' HYPERLINK http://www.finecrypt.net/datarem.html 23 Sept.

52 Computer files are not immortal, but the act of deleting a file does not destroy it. Nonetheless, the very act of using a computer overwrites computer files. Overwriting is the process of writing patterns of data on top of the data stored on a magnetic medium; Deleted Files are files that a subject deletes that in many instances a forensic examiner is able to recover all or part of the original data; Unallocated File Space is the content that remains when files are erased or deleted in DOS, Windows, Windows 95, Windows

inaccessible to the user. A lot can be learned from digital data. A simple search through digital evidence can recover a hidden document or deleted e-mail message. These can accelerate a favourable settlement or even win the case.[53] As a general rule, applicable to all data types, one can assume that if information was displayed at some time on a computer screen, it can generally be recovered from that computer.[54]

Data recovery is essentially the gathering of information. The information gathered during an investigation, in order to be used as evidence, can either be in hard copy form and/or in digital form. The evidence in hard copy would be any form of tangible evidence obtained from various sources during the course of an investigation.[55] Digital evidence consists of electronic documents which can be described as the entire range of information stored in or generated by digital devices and computers that can be reduced to a hardcopy printout, including e-mail,[56] documents created by a word

---

98 and Windows NT, and as a result, the data remains behind for discovery through the use of data recovery and/or computer forensics software utilities. See footnote 7 above.

53 Lewis 'Data Forensics – The smoking gun may be a click away' HYPERLINK http://www.forensicfocus.com/computer-forensics-smoking-gun.php 10 March.

54 See Lewis footnote 53 above with regard to the following explanation. If a user, for example, checks her account balance online, it is likely that information can be retrieved at a later date. Another example will be if a Microsoft Word document was created, as this processing system contains a plethora of information that is not displayed on the screen and not printed to the printer. A forensic examiner will be able to discover a wealth of additional information with regard to the document in what is called 'metadata'. Metadata is a description or definition of electronic data, or data about data, but can often only be accessed in certain viewing modes. It can include descriptive 'tags' and information about when a document was created, and what changes have been made on that document. Metadata is also referred to as Data about data. Metadata describes how and when and by whom a particular set of data was collected, and how the data is formatted. There are at least three types of metadata: semantic data, which gives the meaning of the "raw" data; formatting data which describes the appearance of the data on-screen or on-page; and intellectual property data which describes data ownership conditions. See also footnote 7 above.

55 Strydom 'Computer Evidence' HYPERLINK http://www.crimeinstitute.ac.za/2ndconf/papers/strydom.pdf 10 March.

56 Electronic mail is a method of sending messages using the internet or other networks. See Wilson footnote 15 above p 273.
E-mail messages are the most commonly investigated digital data. To non-computer experts, e-mail is a relative simple concept: a computer user will open an e-mail program, type in an e-mail address, then a message, and will hit a key to send the message. Seconds later, an icon will appear on the recipient user's screen to alert him/her of this message. The mail can then be opened and read. All of which can be done in a few minutes. Bester and Matthew 1998 *Commercial Law Conspectus* 76.

processor,[57] database,[58] or spreadsheet,[59] digitised video or audio,[60] voice mail, computer programs, and data files[61].[62]

2.1.4.5 Digital signatures[63] and encryption[64]

Digital signatures[65] can be used to verify that an e-mail message is really from the person who supposedly sent it and that it has not been changed.[66] Digital signatures are generated through the use of a mathematical algorithm in order to combine the information in a key with the information in the message.[67] This process will result in a random-looking string of letters and numbers, which tells you that this particular person wrote this message.[68] These types of signatures indicate that changes have not been made to the content since it

---

57 Application program for the entry, editing and manipulation of text. See Wilson footnote 15 above p 283.

58 A collection of related records organised and stored so that information may be obtained by the user. See Wilson footnote 15 above p 272.

59 Programs used to manipulate numeric data and display data in text and graphical form. See Wilson footnote 15 above p 282.

60 Obtained by using a digital camera, which is a device used to collect and digitise still images or moving images. See Wilson footnote 15 above p 273.

61 A file is a block of related data stored under a single name. See Wilson footnote 15 above p 274.

62 See footnote 53 above.

63 A Digital Signature is a type of electronic signature that is generally considered the most reliable and secure. Digital signatures use public key infrastructure (PKI) to authenticate the sender and verify the information contained in the document. With the passage of the electronic signatures act, digital signatures are expected to become increasingly popular for exchanging information, conducting transactions and signing contracts over the Internet. See footnote 7 above.
A digital signature is a way to ensure that the information received was actually sent from whom it purports to have been sent, and that it has not been changed or altered in any way. Any alteration to the signed message will cause the signature to break. This means that any change to the 'document' will interrupt the signature code and it will fragment, causing a different code which will indicate to the user that the originally sent document had in fact been altered.

64 Encryption is the coding of data to stop unauthorised users who access data from understanding the data. The authorised user is able to decode what they need. See Wilson footnote 15 above p 274.
Encryption is therefore the process of encoding data to prevent unauthorized access, especially during transmission. See footnote 7 above.

65 A form of encryption attached to electronic documents by firms that want added security which includes a private and a public key that must match to authenticate the message. See Wilson footnote 15 above p 273.

66 McDowell and Householder 'US-CERT National Cyber Alert System ST04-018-Understanding Digital Signatures' HYPERLINK http://www.UnderstandingDigital Signatures.htm 15 March.

67 *Ibid.*

68 See footnote 66 above.

was sent, as any changes would cause the signature to break.[69] A digital signature can be regarded as the electronic equivalent of a handwritten signature,[70] used to verify the authenticity of electronic documents. In fact, digital signatures may provide even more security than their handwritten counterparts.[71]

More often than not a digital signature uses a system of public key encryption to verify that a document has not been altered.[72] Public key encryption[73] uses a system of two keys:

- a private key, which only one individual uses;[74] and
- a public key, which other people use and are often stored on public key servers.[75]

A document that is encrypted with one of these keys can be decrypted only with the other key in the pair.[76] Digital signatures often use a PKE-system.[77] For example, before encrypting the message to Steve, Susan can sign the message using her private key; when Steve decrypts the message, he can verify the signature using her public key.[78]

---

69 See footnote 66 above.

70 This is however not the case for all legislation. For example, the *Electronic Communications and Transactions Act* 25 of 2002 does not enforce this view on all legal aspects. This view is especially excluded in the law of succession and specifically for the legal requirements of testamentary signatures, in which digital signatures are presently not acceptable and therefore not an equivalent to hand written signatures.

71 Buchanan 'Digital Signatures and Public Key Encryption' 2002 HYPERLINK http://afongen.com/essays/pke/ 23 Sept.

72 *Ibid.*

73 Also herein after referred to as PKE.

74 This private key must be protected with a well-chosen, carefully protected pass phrase.

75 See footnote 71 above.

76 For example, let's say that Susan wants to send a message to Steve using PGP (a popular public key encryption system). She encrypts the message with Steve's public key and sends it using her favourite email program. Once the message is encrypted with Steve's public key, only Steve can decrypt the message using his private key. Even major governments using supercomputers would have to work for a very long time to decrypt this message without the private key. See footnote 71 above.

77 Consider Susan and Steve again: how can Steve be sure that it was really Susan who sent the message, and not the criminally-minded Nicky pretending to be Susan? See footnote 71 above.

78 Refer to footnote 76 above.

It works as follows:[79]

1. Susan creates a digest of the message — a sort of digital fingerprint. If the message changes, so does the digest;
2. Susan then encrypts the digest with her private key. The encrypted digest is the digital signature;
3. The encrypted digest is sent to Steve along with the message;
4. When Steve receives the message, he decrypts the digest using Susan's public key;
5. Steve then creates a digest of the message using the same function that Susan used;
6. Steve compares the digest that he created with the one that Susan encrypted. If the digests match, then Steve can be confident that the signed message is indeed from Susan. If they don't match, then the message has been tampered with — or is not from Susan at all.[80]

A digital signature is basically a way to ensure that a digital document[81] is authentic[82] and can be used anywhere that a system for authenticating data is necessary, i.e. anywhere a handwritten signature could be used but can not or should not for some reason.[83] A system of digital signatures and encryption is used in e-commerce all the time, to protect confidential information.[84]

Another way in which e-mail users and some companies use to protect the confidentiality of electronically transferred messages is by encryption. Encryption is a good way to protect sensitive information as it ensures that only an authorised person who has access to the key[85] and data can read it.[86]

---

79 See footnote 71 above.

80 See footnote 71 above. If this sounds complicated, rest assured that the software makes it easier.

81 Electronic or digital documents for example, e-mail, spreadsheet, text file, etc.

82 Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it. See Anon. How Stuff Works 'How do digital signatures work?' HYPERLINK http://computer.howstuffworks.com/computer-channel.htm 23 Sept.

83 For example, in situations of online banking or payroll transactions, or web registration for college courses. See footnote 71 above.

84 See footnote 71 above.

85 A Key is a symbol or sequence of symbols (or electrical or mechanical correlates of symbols) applied to text in order to encrypt or decrypt. See footnote 7 above.

The only way to read an encrypted message is by using the correct key. Otherwise the message will merely be seen as a random series of letters, numbers, and characters.[87] Digital signatures rely on certain types of encryption to ensure authentication. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode.[88] These two processes work hand in hand for digital signatures.

Encryption differs from digital signatures, as its purpose is confidentiality. The purpose of digital signatures is integrity[89] and authenticity.[90] Although these two concepts can be used independently, a person can also sign an encrypted message. A further difference is that when a message is signed by

---

Keys are used to create digital signatures and for encryption of messages. For every signature, there is a public key and a private key. A private key is the portion of the key you use to actually sign an e-mail message. This private key is protected by a password, and you should never give your private key to anyone. A public key is the portion of the key that is available to other people. Whether you upload it to a public key ring or send it to someone, this is the key other people can use to check your signature. A list of other people who have signed your key is also included with your public key. Their identity will only be seen if you already have their public keys on your key ring. A key ring contains public keys. The computer will have a key ring that contains the keys of people who have sent you their keys or whose keys you have received from a public key server. A public key server contains keys of people who have chosen to upload their keys. See footnote 66 above.

Private Key Cryptography is an encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret. This methodology is usually only used by a small group; Public Key Cryptography on the other hand is a coding system in which encryption and decryption are done with public and private keys, allowing users who do not know each other to send secure or verifiable messages. Suppose Fred wants to send a message. He would encrypt it with his private key, which no one else knows; then, the recipient would decrypt it using Fred's publicly available key, thus verifying that the message came from Fred. Alternately, suppose Fred wants to receive an encrypted message. The sender would encrypt the message with Fred's public key, and only Fred would be able to decrypt it, using his private key. This method, also known as dual-key cryptography, contrasts with the older secret-key or symmetric cryptography, in which the sender and recipient must agree on and use the same private key for encryption and decryption; Public Key Infrastructure (PKI) is a system for securely exchanging information within a company, group or worldwide that includes a method for publishing the public keys used in public key cryptography and for keeping track of keys that are no longer valid. Different industry and technical groups are developing PKI technology, and the National Institute for Standards and Technology (NIST - America) is working to make sure those technologies are compatible. See footnote 7 above.

86 See footnote 66 above.

87 See footnote 66 above.

88 See footnote 66 above.

89 Data stored in information systems needs to be accurate, consistent and up to date. This is known as data integrity. See Wilson footnote 15 above p 273.

90 McDowell and Householder 'US-CERT National Cyber Alert System ST04-019-Understanding Encryption' HYPERLINK http://www.UnderstandingDigital Signatures.htm 15 March.

an individual, a private key is used, and anybody who has this individuals' public key can verify that the signature is valid. However, when a message is encrypted, the public key for the person it is sent to is used. His/her private key is then used to decrypt the message.[91]

In recent years it has become clear that traditional encryption as discussed above is not specifically used as such by terrorist organisations or informed cyber criminals. It has come to the attention of Federal investigators at the Federal Bureau of Investigation[92] in America that these cyber criminals and terrorists also use digital images.[93]

It works as follows:

Each image[94] is created by a series of dots. Inside the dots are a string of letters and numbers that computers read to create the image. A coded message or another image can be hidden in those letters and numbers.[95] Even if these images are found, the encrypted message or image is

---

91 This person should be the only one who is able to view the information See footnote 53 above.

92 Herein after referred to as the FBI.

93 These images may contain much more than just a family picture. Hidden in the X-rated pictures on several pornographic Web sites and the posted comments on sports chat rooms may lay the encrypted plans of the next terrorist attack against America or its allies. It sounds farfetched, but American officials and experts say it is the most commonly used method of communication being used by terrorists to outsmart law enforcement. US and foreign officials say that Osama Bin Laden (Indicted in the bombing in 1998 of two U.S. embassies in East Africa and as the responsible party for the 9/11 Attacks on the World Trade Centre in New York) and others are hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites. U.S. officials and militant Muslim groups say terrorists began using encryption — which scrambles data and then hides the data in existing images — from the mid 1990's. See Kelly 'Terror groups hide behind Web encryption' 2001 HYPERLINK http://www.usatoday.com/tech/news/2001-02-05-binladen.htm 10 Oct.

94 This image may be a picture or a map.

95 These messages can be hidden by using free encryption Internet programs made available by privacy advocacy groups. The programs scramble the messages or pictures into existing images. The images can only be unlocked using a 'private key,' or code, selected by the recipient. Otherwise, they are impossible to see or read. Some officials are even of the opinion that you could have a photograph and image with the time and information of an attack sitting on your computer, and you would never know it because it will look no different than a photograph exchanged between two friends or family members. See Kelly footnote 93 above.

impossible to read without cracking the encryptions' code.[96] Some academics are also of the opinion that it is not surprising that the FBI wants all encryption programs to file what amounts to a 'master key' with a federal authority that would allow them, with a judge's permission, to decrypt a code in a case of national security.[97]

Encryption standards must therefore be monitored and updated as code breakers' computing power increases and to keep pace with new methods of encryption.

2.1.4.6 Devices on which data can be stored[98]

Various storage mediums exist, each developed for a specific type of information, stored by using a specific software program and device and with a specific size limit. These mediums also differ in that certain types thereof will be insufficient for use by Computer forensic investigators, due to their size limitations, content restrictions[99] and their possible overwriting of other valuable data when being used to store information. A floppy disk for example is sufficient to store small amounts of data, but they are limited for forensic use due to their small storage space.[100] All devices that are found at an investigation site that are capable of storing digital data, including the digital device[101] itself, will be studied by computer forensic investigators in order to extract digital evidence.

---

96 A senior US Defence Department mathematician has said that cracking a code often requires lots of time and the use of a government supercomputer. See Kelly footnote 93 above.

97 Civil liberties groups, which offer encryption programs on the Web to further privacy, have vowed to fight this. See Kelly footnote 93 above.

98 See also 'Annexure A' to this mini-dissertation for the different forms of storage devices.

99 Restrictions such as to whether audio/visual files only or also data files can be stored.

100 Even using and connecting other storage mediums such as a removable device like a USB (Universal serial bus) or Fire-wire drive is not advised seeing as this could change the system state. Attaching a hard drive would be the first device you think of next, however attaching it cannot be done without shutting down the machine. See Kornblum 'Preservation of fragile digital evidence by first responders' HYPERLINK http://www.dfrws.org/dfrws2002/papers/Papers/Jesse_Kornblum.pdf 10 March.

101 Digital devices such as a computer, PDA, mobile phone or digital camera.

2.1.5 Developments and/or devices required for the preservation of digital evidence

To ensure the protection of digital evidence by the first investigator thereof[102] he/she needs to be equipped with a tool[103] developed with the following primary goals in mind:

a) the forensic integrity of the system must be maintained;
b) the tool should handle all evidence without any intervention from the user;
c) the tool should gather all of the pertinent information that might be lost either during examination or transportation of the evidence;
d) the tool should provide the first responder with enough information to determine if an incident has occurred.[104]

A computer forensic investigators' goal must be to modify as little information as possible on the machine. However, it is also accepted that by doing any kind of analysis of a system there are going to be changes to some extent. The goal is to keep these to a minimum.[105] In order to guarantee that the digital evidence has not been tampered with, the tool should not leave any of the handling of digital evidence to the first responder. The evidence and first responder should be physically separated from each other.[106] The goal of this tool is to gather and protect the information that can be easily lost.

---

102 Also referred to as the first responder. The first responder is a term referring to the first investigation officer or law enforcement official coming into contact with the crime scene and/or the computer suspected of being part of or used to commit a crime.

103 A tool is a component or device used by forensic investigators to extract information or evidence from a possible crime scene – such as a pair of pliers will be used by a normal crime scene investigator to collect hair samples, so too must a specifically designed tool be used by digital forensic experts in order to collect the evidence stored on the computer. The tool will be a device or software program that the investigator can use to extract the digital information safely and at the same time it will ensure the limitation of human interference with the evidence.

104 See Kornblum footnote 100 above.

105 See Kornblum footnote 100 above.

106 See Kornblum footnote 100 above.

2.1.6 Proposed procedures for Digital Forensic Investigations

Data forensics should be considered as a standard and routine practice in legal matters of all types. Failure to analyse digital data is inexcusable.[107] In situations where a technological device is suspected to have been part of or used to initiate steps to commit a crime, or is relevant in civil litigation, both the investigator and law enforcement officials should approach the device with caution.[108] Computer investigations are not as clear as when only physical evidence is present. This is so because the existence of digital evidence may not be obvious upon first examination.[109] In order to uncover any digital evidence an investigator must perform a full forensic analysis of the computer.[110]

In all cases where digital evidence could be found on computers at crime scenes, investigators should know of and take care in preserving the types of fragile digital evidence, which are described as:

> Transient data: Information that will be lost at shutdown, such as open network connections, memory resident, programs, etc.
> Fragile data: Data that is stored on the hard disk, but can easily be altered, such as last accessed time stamps.
> Temporarily accessible data: Data that is stored on the disk, but that can only be accessed at certain times.[111]

As can be concluded from the above description of transient data, the danger facing it is that it will be lost if the machine is turned off. Within this definition we can also include data that will simply end over time - seeing as network

---

107 In technological devices is a plethora of digital data that could be used as digital evidence; the collection, preservation and use of which can win or lose a case. If all the best possible evidence that exists and can be used is not used by legal practitioners (either by negligently excluding the digital information or due to insufficient knowledge on the use of digital data as evidence), this will mean that the legal representative did not act in the best interest of his/her client and this will be sufficient grounds for a complaint or even a case of ineffective legal assistance against the legal practitioner. See also footnote 53 above.

108 This cautious approach will also be required in investigations for digital evidence required to be provided in civil matters. See Chapter 5 of this mini-dissertation for a comparative analysis between SA and USA procedures currently followed by law enforcement officials.

109 See Kornblum footnote 100 above.

110 See Kornblum footnote 100 above.

111 See Kornblum footnote 100 above.

connections are closed or timeout, users log out, and cached data[112] expires.[113]

Several factors should be considered when determining whether or not a computer hard drive should be preserved and analysed:

a) a likelihood must exist that the hard drive does contain information of value to the investigation;
b) the number of drives to be preserved and analysed usually translates directly into a linear increase in the overall cost of both litigation and investigation;
c) internet logs may also provide valuable evidence.[114]

It has to be remembered that, in these types of investigations and/or seizures, one should never use the same machine from which the original data is being collected to analyse the data connected with the suspected incident under investigation. The safest approach would be to make forensically sound copies[115] of all data storage devices – primarily hard drives. Care must be taken not to use too much memory[116] while information is being transferred, as this could lead to the use of virtual memory overwriting data on the disk. The best method for extracting data will be via the network connection.[117]

---

112 Stored in cache memory – a high-speed storage that can be quickly accessed by the central processing unit. See Wilson footnote 15 above p 271.

113 All of these data types could hold potential digital evidence. See Kornblum footnote 100 above.

114 See footnote 53 above.

115 A Forensic Copy is an exact bit-by-bit copy of the entire physical hard drive of a computer system, including slack and unallocated space. See Hedges footnote 8 p 7 above.

116 Hardware that stores data. See Wilson footnote 15 above p 277.
There are two main categories of memory: primary memory and secondary memory. Primary memory stores data required for the operation of the computer and consists of many different forms of memory including ROM (Read-only memory whose contents may be retrieved but not altered by the user. See Wilson footnote 15 above p 280), and RAM (Random-access memory - Stores data and programs while they are in use by the system, that is, volatile memory. See Wilson footnote 15 above p 280). Another form of non-volatile memory is Flash memory (Special silicon chips that are non-volatile. These chips are embedded on cards that can be installed into many portable devices. See Wilson footnote 15 above p 274), which, when the computer crashes or the power is switched off, will retain their data. Used in many portable devices such as modems, mobile phones and some personal computers. See Wilson footnote 15 above p 274.

117 This may also strangely be the same path used by an intruder to invade the 'victim' device.

Once a possible incident is discovered it would be wise to disconnect the 'victim' from the network, this will protect the system from further attack and keep the existence of the investigation private.[118] The computer can instead be connected to a private hub[119] and the collected data sent to another machine on the same hub.[120]

Seizure of the computer can pose a significant problem, as the computer is usually turned off and moved to a laboratory. When this takes place, all of the data on it that is not saved to the hard drive will be lost. However, evidence may also be destroyed if the computer is not turned off and is still connected to the network,[121] as an individual could delete evidence.[122] Data could further be erased by an individual's instruction via a computer programme to erase information without any human interaction. The first data sent to the receiver should be the contents of the suspected computers' memory, done in small batches to avoid overwriting the remainder of memory.[123] Once the RAM is transferred, other data can be transferred without regard to size limits.[124]

---

118 See Kornblum footnote 100 above.

119 A private and specially set up connection between the 'victim' computer and the computer forensic investigator's computer or stand alone hard drive in order to copy the fragile digital data safely.

120 By collecting the computer to a private hub the investigator will usually make use of a LAN (Local Area Network). A LAN is a computer communications system limited to no more than a few miles and using high-speed connections (2 to 100 megabits per second). A short-haul communications system that connects ADP devices in a building or group of buildings within a few square kilometres, including workstations, front-end processors, controllers, switches, and gateways; The following network may also be used but it is not recommended – a WAN (Wide Area Network) is a physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks. See footnote 7 above.
A LAN will ensure more as the computers connected to this network may be controlled by the person(s) connecting the LAN. In this manner the investigator will be able to download or copy files from the 'victim' computer in such a manner that will not expose the computer data to a larger (uncontrolled) public network. See Kornblum footnote 100 above.

121 Two or more computers joined together for the purpose of transmitting and receiving data. See Wilson footnote 15 above p 277.

122 An intruder could erase log files or a legitimate user could cause data to be written to the system that overwrites evidence of a crime. See .Jackson 'Justice issues guidelines for handling digital evidence' HYPERLINK http://www.gcn.com/vol1_no1/daily-updates/26961-1.html 10 March.

123 See Kornblum footnote 100 above.

124 See Kornblum footnote 100 above.

Data stored on a hard drive can be regarded as fragile if it can be easily altered,[125] especially by a first responder trying to determine if an incident has occurred.[126] Once altered, there is no way to recover the original data. The prime objective of any computer forensic investigator is digital evidence preservation and presentation for the purpose of any legal process. Due to the fragile nature[127] of digital data, the extraction, securing and documenting of digital evidence requires special attention.[128]

In order for computer forensic investigators to analyse the machine as completely as possible, the following procedure is proposed:

a) Any information which can be gained by examining the applications[129] currently open from an active machine should be recorded.

- This is especially necessary if information is stored in RAM as it will be lost if it is not recovered before the machine is powered down, or switched off[130].

b) A machine should be powered down or switched off in exactly the same way as the suspects would power it down.

- This is critical when the machine is powered off, especially if data is normally stored only in memory,[131] wiped from the drive after booting,[132] and is only committed back to disk. Modern machines – after shut down - must be physically removed from

---

125 For example, this includes access dates on files or temporary files.

126 See Kornblum footnote 100 above.

127 It is easily altered, difficult to distinguish between original data and copies.

128 See Kornblum footnote 100 above.

129 Contained in application software – applications are programs written to solve a user's problem. See Wilson footnote 15 above p 270.

130 The best way to switch the computer off – as used by general computer users – is to: Save the work one has been doing on a stiffy or on the hard disk; Close down all the programs/applications; Click with the mouse on Start in the bottom left corner; Click just above Start on Shut down; Click on Yes; Take out the stiffy and any other disk; and When the message appears on the screen that it is safe to turn off the computer, one presses the Power button to switch the electricity off – Note: the latest Pentiums switch themselves off. See Du Toit *Basic Computer Skills* 7.

131 Hardware that stores data. See Wilson footnote 15 above p 277.

132 Booting the computer is the starting of the computer. Making sure there is no disk or stiffy in the disk drive, one switches the computer on/boot the computer by pressing the Power button on the Central Processing Unit (CPU). See Du Toit footnote 130 above.

the power supply and one must wait 30 seconds before they are really 'off'.

c) The chassis[133] must be inspected for traps, intrusion detection mechanisms, and self-destruct mechanisms.

- This can be done by inserting an illuminated Fibre-scope through a hole in the chassis to inspect the inside of the machine. The investigator should look specifically for large capacitors or batteries, non-standard wiring around the drives, and possible incendiary or explosive devices. One should specifically look for a wire running from anything to the CMOS battery or 'CMOS clear' jumper. The CMOS memory can be used to store data on the motherboard itself, and if power is removed from it the contents will be lost.

d) After determining that the case is safe to open, the investigator can proceed to remove the cover.

e) Thereafter the configuration of the system must be fully documented.

- This should be done by completely photographing the entire configuration of the system. Special attention must be paid to the order in which the hard drives are wired – as this indicates boot order – which is further necessary to reconstruct a RAID[134] array[135].

f) Hard drives must then be duplicated.

- By using a stand-alone hard-drive duplicator or a similar device, this can be done in order to completely duplicate the entire hard drive. Rather than duplicating the file system one must make a

---

133 The frame, casing or box in which the computer is stored. Also referred to as the CPU tower.

134 Redundant array of independent storage disks – systems that use many disk drives within a single system box. See Wilson footnote 15 above p 280.

135 Organised set of data of the same type. See Wilson footnote 15 above p 270.

bit-stream[136] copy of every part of the hard drive, which can physically store data.

- Notes should also be made as to which physical drive each image corresponds. Original drives can then be removed to secure storage and prevent tampering with it.

These procedures need to be adjusted according to the circumstances of each investigation and comply with local laws and rules of evidence. These procedures will also have to be proven to ensure the integrity of the digital data before a court of law will admit the digital evidence.

2.2 Conclusion

Digital data is inherently fragile. It is therefore critical for the first responder to ensure that the evidence is gathered and preserved in a simple, secure, and forensically sound manner.

The following must always be kept in mind when dealing with digital evidence:

- when a document is written, multiple files are created;
- when a document is deleted, the original is not destroyed, and none of the additional, invisible files may be affected at all;
- continued use of the computer(s) in question in the case investigated is likely to spoil evidence;
- a computer forensic specialist can make identical copies of the hard disks in question without disrupting the data on the computer. These copies may then be properly examined in a lab;
- a computer forensic specialist is likely to be able to produce relevant documents or portions thereof by examining the hard disk copies.

South Africa needs computer forensic investigators that can ensure, and be able to prove, that they apply techniques and procedures that will ensure the integrity and authenticity of digital data during their investigations.

---

[136] A bit is a binary digit – a 1 or 0 in the binary system. See Wilson footnote 15 above p 270.

Chapter 3

South African Law on Digital Evidence

3.1 Introduction

Evidential requirements in the South African law of evidence for admission of evidence in a court of law are found in the rules of the common law as interpreted by the courts and in legislation.[1] With technological advancements it becomes clear that new situations raised by this will not fit within the rules and regulations set for more traditional analogous evidence material.[2]

The traditional procedures and techniques applied in the collection of admissible evidence for any legal matter must change to accommodate digital evidence[3] in response to the increasing number of criminal and civil cases that are based on digital evidence.[4] The applicable legislation[5] with regard to digital evidence is very broadly formulated and there are very little South African court precedents that give sufficient guidance as to which techniques and procedures need to be followed when computer forensic investigators obtain digital evidence in order to ensure its admissibility.

In this chapter a study will be done of the South African common law, legislation and case law with regard to the admissibility of digital evidence.

---

1 In the event of conflict with the common law, the conflicting legislation will take precedence. See Harris 2000 *National Archives of South Africa.*

2 Fahey 2004 *SANS Institute* 3. The products of modern technology should not be forced into the traditionally limited categories of either real or documentary evidence. The current evidential prerequisites of reliability and authenticity are based on traditional paper documents.

3 As opposed to physical evidence.

4 Electronic evidence is fragile. Simply turning on the subject computer or accessing a file will change critical information on the hard drive. In order maintain the chain of custody and forensic soundness of the electronic information and to preserve electronic evidence, special procedures and tools should be utilized to make an exact image copy of the media – without altering a single byte of data. Due to the strict evidential rules applied to determine admissibility of any evidence, the techniques and procedures followed when collecting and preserving or storing digital data from a suspect digital device must be effective and secure in such a manner as not to compromise the digital evidence further. See Snyder and Morelock 'Electronic Data Discovery: Litigation Gold Mine or Nightmare?' HYPERLINK http://www.mobar.org/journal/2002/janfeb/snyder.htm 11 Oct.

5 The legislation presently applicable to regulate the use of digital evidence is the *Electronic Communications and Transactions Act* 25 of 2002 specifically Ss 11-19. Herein after referred to as the ECT Act.

3.2 Common law

In South Africa, concentrating on rules pertaining to paper based record keeping, very few guarantees with regard to the authenticity and reliability of digital data are provided for.[6] The South African law of evidence is mainly regulated by the common-law and statutory provisions specifically providing for aspects with regard to admitting evidence in civil and criminal cases.

The *Civil Proceedings Evidence Act*[7] regulates the admission of evidence in civil cases.[8] So too are the common-law provisions applicable to evidence in criminal cases regulated by the *Criminal Procedure Act*[9].[10] Both civil and criminal matters, with regard to evidence in general are also regulated by the *Law of Evidence Amendment Act*[11].[12] Aspects with regard to the use of digital evidence in both civil and criminal matters are regulated by the *Electronic Communications and Transactions Act.*[13]

3.2.1 Evidence in general: Digital Evidence v Physical Evidence

In general, evidence should provide the grounds to enable a finding with regard to a point that is factually in dispute.[14] Evidence is provided by information obtained in a legal investigation that can establish the fact in question.[15]

---

6 The common-law poses a significant problem to the use of digital evidence as it was formulated over the years to be applicable to only physical evidence and does not specifically contain rules and regulations directly applicable to digital evidence. The South African law of evidence is mainly regulated by the common-law, which consists of Roman law, Roman-Dutch law and English law. The common law has been further developed by our courts over time. There are however, various provisions for the admission of documentary evidence. These have been reformulated over the years to attempt to incorporate computer print-outs as admissible evidence and can still further be reformulated to act as the basic grounds for allowing digital evidence. See Schmidt *Bewysreg* 12-15. See also Hoffmann and Zeffertt *The South African Law of Evidence* 4.

7 *Civil Proceedings Evidence Act* 25 of 1965.

8 See Hoffmann and Zeffertt footnote 6 above p 16.

9 *Criminal Procedure Act* 51 of 1977.

10 See Hoffmann and Zeffertt footnote 6 above p 16.

11 *Law of Evidence Amendment Act* 45 of 1988.

12 See Hoffmann and Zeffertt footnote 6 above p 16.

13 *Electronic Communications and Transactions Act* 25 of 2002 specifically Ss 11-19.

14 See Schmidt footnote 6 above p 2. See also Hoffmann and Zeffertt footnote 6 above p 5.

15 See Schmidt footnote 6 above p 3. See also Hoffmann and Zeffertt footnote 6 above p 5 and p 21. See further S 210 of the *Criminal Procedure Act* 51 of 1977.

In the South African law of evidence, the concept of relevance is regarded as the basic criterion of admissibility.[16] Also, as long as evidence is material and relevant[17] it is admissible, unless there is some other rule of evidence which excludes it.[18] Evidence will be relevant if it can be used to prove either primary or secondary facts in question.[19]

The court will require a high degree of relevance before it will receive evidence which involves a lengthy investigation of collateral issues or is likely to cause prejudice or confusion, or raise difficult questions of credibility.[20] On the other hand, the court must consider all material which may assist it to reach a proper conclusion.[21]

3.2.1.1 Documentary Evidence

The present definition of a document is 'any writing or printing capable of being made evidence', to which can be added that it does not matter on what

---

16 See Schmidt footnote 6 above p 360. See also Hoffmann and Zeffertt footnote 6 above p 21.

17 Evidence that has no weight can have no probative value and is irrelevant. It will be relevant if the facts which it is used to prove can contribute to proving or disproving the existence of the facts in dispute. See Schmidt footnote 6 above p 359. See also Hoffmann and Zeffertt footnote 6 above p 21.

18 See *R v Schaube-Kuffer* 1969 2 SA 40 (RA) at 50B-C. See Schmidt footnote 6 above p 361. Exclusionary rules that will be discussed in this chapter are the prohibition of hearsay evidence and the application of the best evidence rule, along with requirements for establishing the authenticity of the proposed evidence.
See also Hoffmann and Zeffertt footnote 6 above p 23 and p 26.

19 See Schmidt footnote 6 above p 363. When for example the content of a document must be proven, the document itself (if available) must be produced. The document itself is 'primary evidence' of its contents and any other evidence is 'secondary evidence.' Secondary evidence will for example be that which proves the status of the relationship resulting from the document. Primary facts are required for a finding in favour of one of the opposing parties. The secondary facts support a finding, but are not necessary – the finding can also be acquired by another means. See Schmidt footnote 6 above p 323.

20 See *Delew v Town Council of Springs* 1945 TPD 128. See also Hoffmann and Zeffertt footnote 6 above p 24.

21 See Hoffmann and Zeffertt footnote 6 above p 24. See also *Shabalala v The Attorney General of Transvaal & The Commissioner of the South African Police; Gumede v The Attorney General of Transvaal* 1995 1 SACR 88 (T). Here the court held that: "...the applicants *in casu* are entitled to invoke section 23 (of the *Constitution of the Republic of South Africa*, 1993 – right to access to information) for the purpose of obtaining access to all information held by the Attorney General in so far as such information is required for the exercise or protection of their right to a fair trial and in particular, to adduce and challenge evidence." This may be grounds enough for an argument to include digital evidence that will be relevant to the facts in issue. If this digital evidence is not admitted, and if it is the best evidence available to prove or disprove a fact in question, by not including or admitting it into evidence one may be prevented from having a fair trial.

type of material the writing or printing appears.[22] Even though a photo and a product of a device are defined as a document for purposes of some legislation, it must be remembered that there are important differences between a true document and the product of a device such as a photo, or a print-out from a computer.[23]

Any party who wishes to rely upon statements that may be contained in a document will be required to comply with three general rules, which are: [24]

- the contents of a document may only be proved by production of the original;
- where the original is not available, the court will generally accept any other evidence of the document if it is satisfied that the original in fact existed and a reasonable explanation for its non-production has been given; and
- evidence is normally required to satisfy the court of a document's authenticity.

In terms of the common-law, the following will be the only circumstances in which a party will be allowed to adduce secondary evidence of the contents of a document:[25]

- the original document has been destroyed or cannot be found after proper search;
- it would be impossible or highly inconvenient to bring the original to court;

---

22 See Schmidt footnote 6 above p 315. See also *Secombe and Others v Attorney-General and Others* 1919 TPD 270 at 277 where it was stated that "The word 'document' is a very wide term and includes everything that contains the written or pictoral proof of something. It does not matter of what material it is made." See also the case of *Protea Assurance v Waverley Agencies* 1994 3 SA 247 (C) at 249H-I where the court held that: "The word 'document' is a word which is linguistically capable of encompassing a very wide variety of things." See also Zeffertt et al *The South African Law of Evidence* p 685.

23 See Schmidt footnote 6 above p 316. See also the case of *Protea Assurance v Waverley Agencies* 1994 3 SA 247 (C) at 250A where the court held that: "If pictures and frescoes are capable of being regarded as documents, it seems to me that photographs should be similarly regarded in this day and age."

24 See Harris footnote 1 above. These general rules do however, only deal with the circumstances in which the court will receive evidence to prove what a document contains. See also Hoffmann and Zeffertt footnote 6 above p 389.

25 See Hoffmann and Zeffertt footnote 6 above p 394-399.

- the original is in the possession of the opposite party;
- the document is in the possession of a third party who refuses to produce it;
- the document is a public document as provided for in section 234(1) of the *Criminal Procedure Act*[26] and section 20(1) of the *Civil Proceedings Evidence Act*[27];
- other statutory provisions such as bankers' books;[28] and
- intermediary hearings.[29]

The following exceptions entail that a document does not have to be identified by a witness or be proven to be authentic:[30]

- when the opposing party admits the contents of the document and requests its submission to the trial or hearing;[31]
- when judicial notice is taken thereof;[32]
- when the opposing party recognises its authenticity;[33]
- when the document is admissible by submission in accordance with legislation;
- documents from another state.[34]

---

26 S 233(1) of the *Criminal Procedure Act* 51 of 1977 provides that the contents of any book or document which is of such a public nature as to be admissible upon its mere production, may be proved by means of an examined copy or exact, or what purports to be signed and certified as a true copy or exact by the office to whose custody the original is entrusted.

27 *Civil Proceedings Evidence Act* 25 of 1965.

28 In criminal proceedings entries in the accounting records of a bank are *prima facie* proof of their contents upon the mere production of an affidavit which alleges that it has been sworn to by a person in the service of the bank, that the records are the ordinary records or documents of the bank. See Schmidt footnote 6 above p 330.

29 See Schmidt footnote 6 above p 327-330.

30 See Schmidt footnote 6 above p 321. See also *Howard & Decker Witkoppen Agencies and Fourways Estates (Pty) Ltd v De Sousa* 1971 3 SA 937 (T) at 940G.

31 See *Supreme Court Rule* 35(10), and also *Magistrates' Court Rule* 23(4).

32 For example the statutory provisions that require the notice of the content of a *Government Gazette* in both criminal and civil matters.

33 See *Supreme Court Rules* 35(9) and 36(10) and also *Magistrates' Court Rule* 24(10).

34 These documents can be proven in the normal way, but the *Supreme Court Rule* 63 makes the proof thereof easier, by providing that if these documents are authenticated in the other state they may be admitted in the court without additional proof. See Schmidt footnote 6 above p 322.
This will be especially beneficial if digital evidence is required from another state that has less stringent evidence authentication requirements than in South Africa. This will be very helpful when proving e-commerce transactions between a South African and a citizen of another state, and also to acquire evidence of a cyber crime committed or with effects felt in South Africa of which the evidence is acquired outside South Africa.

The originality requirement is sufficiently provided for in section 14 of the *Electronic Communications and Transactions Act.*[35] However, to provide proof of authenticity and originality, any party who keeps, wants to keep or is required by law to keep records, must put systems and procedures into place which promote and protect the authenticity of records in their care.[36]

3.2.1.2 Digital Evidence

Computer-generated evidence shows characteristics of both documentary evidence and evidence provided by a device or apparatus.[37] Real evidence consists of things which are examined by the court as a means of proof.[38] Real evidence is seldom of much assistance unless it is supplemented by the testimony of witnesses.[39] The testimony of such a witness will only be admitted if it can be of real assistance to the court[40] and if the court is satisfied that the witness possesses sufficient skill, training or experience to assist the court.[41] Computer-generated evidence will more readily be admitted as real evidence if it has been generated without human intervention.[42]

This dualism of computer-generated evidence does however bring three potentially problematic areas into play – the provision against hearsay

---

35 *Electronic Communications and Transactions Act* 25 of 2002. The provisions of which will be discussed under paragraph '3.4.2.1 The ECT Act in general' below.

36 This is especially important when originals of these records are not available and when copies are being used the parties must show that these copies were produced in the ordinary course of business and were produced subject to stringent control mechanisms. See Harris footnote 1 above.

37 See Schmidt footnote 6 above p 346. See also Hoffmann and Zeffertt footnote 6 above p 404-405.

38 See Hoffmann and Zeffertt footnote 6 above p 405.
The use of an object as evidence is known as the use of 'real evidence.' The following are some types of real evidence: an object such as a knife or clothing, and even an animal, recognised by a witness as an exhibit of evidence and handed in to the court as such. See Schmidt footnote 6 above p 305.

39 See Hoffmann and Zeffertt footnote 6 above p 405. See also *S v Peake* 1962 4 SA 288 (C) at 291A-B where the court held that there must be proof that the evidence has to be what it purports to be, and that there must be evidence *aliunde* establishing its accuracy. See also Hoffmann and Zeffertt footnote 6 above p 408.
The principal method of adducing evidence is by the oral testimony of competent witnesses. A witness is competent if he/she may lawfully give evidence. See Hoffmann and Zeffertt footnote 6 above p 369.

40 See Hoffmann and Zeffertt footnote 6 above p 98.

41 See Hoffmann and Zeffertt footnote 6 above p 100.

42 This will happen when for example an ATM machine prints a clients' bank statement. See Zeffertt footnote 22 above p 712.

evidence,[43] the authenticity requirement[44] and the reliability of the computer[45] and computer system or –program applied by it.[46]

3.2.1.3 Authenticity

When a party tenders a document, he/she may usually be required to produce evidence to satisfy the court of its authenticity.[47] This could be done in various ways. The most commonly used are:

- for the writer to identify the document; or
- to tender the evidence of someone who saw him/her sign or write it; or
- who can identify his/her handwriting. [48]

If the authenticity of a document is not proved or admitted, its contents will not be allowed to be used either as evidence or for the purpose of cross-examination. A qualification does exist that the authenticity of the document may be proved at a stage of the trial that is later than the cross-examination.[49]

---

43 When common-law provisions are applied to computer evidence, the rule against hearsay evidence immediately comes to mind. If there is a person or persons who can deliver original evidence about the information that is processed or stored in the memory of the device, the hearsay rule will not come into play. See Schmidt footnote 6 above p 346.

44 Proof of authenticity requires in these situations that somebody must be able to identify the print-out or information used and displayed on the screen of the device. See Schmidt footnote 6 above p 346.
A witness may have acquired special knowledge or skill on a particular subject without necessarily being an expert in the generally accepted sense of the word. See Hoffmann and Zeffertt footnote 6 above p 98.

45 This does not require a technical exposition of how the device or system works, but it does require proof and evidence of experience with the device. This must prove to the court that both the hardware and software used by the computer or digital device is reliable – therefore that it probably was functioning normally and correctly. See Schmidt footnote 6 above p 346.
The opinion of an expert witness is admissible whenever, by reason of their special knowledge and skill, they are better qualified to draw inferences than the judicial officer. See *Goliath v Fedgen Insurance* 1994 2 PHF 31 (E). See also Hoffmann and Zeffertt footnote 6 above p 97.

46 See Schmidt footnote 6 above p 346.

47 See Schmidt footnote 6 above p 318. The evidence has to be tendered by a witness who can prove its authenticity and that it is what it purports to be. Documents can be tendered by: a) The author, dictator or signee; b) The witness; c) Someone that can identify the handwriting; d) Someone that found the document in the possession or under the control of the opposing party; e) Someone under whose legal guardianship and control the document was held. See also Hoffmann and Zeffertt footnote 6 above p 399.

48 See Zeffertt footnote 22 above p 694.

49 Such as during the re-directing question phase or when required to answer questions posed by the presiding judicial officer. See Zeffertt footnote 22 above p 695.

Documentary, modular or pictoral evidence may not be introduced into evidence without the leave of the court, or the consent of the other parties to the action, unless the opposing party has been given notice to admit it – in which case a failure to object thereto amounts to an admission thereof.[50]

Even though one cannot generalise digital evidence as digital documents, by using these methods of proving documentary authenticity, and sufficiently adapting them, they along with the provisions of Section 14 of the *Electronic Communications and Transactions Act,*[51] may be used to support the admission of digital evidence.[52]

Digital evidence may be of a fragile nature,[53] but the metadata contained in the files created when digital data is stored[54] will be able to prove (or disprove) the authenticity of the digital data and support the admission of

---

50 In practice a party to a civil action can usually avoid having to prove the authenticity of documents by serving a notice to admit their proper execution and authenticity upon his/her opponent before trial. See *Supreme Court Rule* 35(9). If the required admission is not forthcoming the opponent will have to prove the document. See Zeffertt footnote 22 above p 694-695.

51 S 14 of the *Electronic Communications and Transactions Act* 25 of 2002 provides for the assessment of the integrity of data messages. See footnote 111 below.

52 In *S v Harper* 1981 1 SA 88 (D) (This is a case with application to criminal matters) the Court held that computer print-outs are 'documents' in the ordinary meaning of that expression. In terms of Section 221(5) of the *Criminal Procedure Act* 51 of 1977, the definition of a document will also include a device through which information is stored or recorded. See Schmidt footnote 6 above p 347.

53 As this type of data is easy to alter or overwrite.

54 See the discussion in Chapter 2 under paragraph *2.1.4 Computer Forensics Basics: use, storage and deletion of digital information* of this mini-dissertation. In Microsoft Word when a document or file is saved, there are several attributes saved with it: a) the date it was created; b) the date it was last changed, or modified; c) the date it was last accessed. This information is kept as part of a file listing called a 'directory.' This file listing is viewed as a 'folder' by the computer user and the computer saves both a long version and a short version of the name as two adjacent directory listings. This information is also known as Metadata and can be obtained by computer forensic investigators, which will be able to prove or disprove the authenticity of digital evidence. See Burgess 'The Case for Electronic Discovery' HYPERLINK http://adr.forensic.e-symposium.com/computerforensics/whitepaper.pdf 23 Sept.
Metadata is also referred to as Data about data. Metadata describes how and when and by whom a particular set of data was collected, and how the data is formatted. There are at least three types of metadata: semantic data, which gives the meaning of the 'raw' data; formatting data which describes the appearance of the data on-screen or on-page; and intellectual property data which describes data ownership conditions. See University of Georgia Office of Information Security [InfoSec] Enterprise Information Technology Services 'InfoSec Glossary of Terms' HYPERLINK
http://www.infosec.uga.edu/glossary.php?question=nq 23 Sept.

digital evidence. Computer forensic investigators will be able to extract the required information[55] with relative ease. This information can then be used to prove authenticity of the digital evidence. If the computer or other digital or electronic device is capable of providing the required information that will be used as evidence without human intervention, it may be regarded as real evidence and will not be subject to the prohibition of hearsay evidence.[56]

3.2.1.4 Admissibility of digital evidence

There are no common-law rules that explicitly refer or specifically apply to digital evidence. As a starting point, the prerequisites for the admissibility of documentary evidence could be applied to determine the admissibility of digital evidence. These common-law admissibility requirements can then be used to compile a set of basic requirements to be incorporated into the techniques and procedures applied to ensure the admissibility of digital evidence.

Overly,[57] is of the opinion that the admissibility of digital evidence revolves around three questions:[58]

1. Can the evidence be properly authenticated?
2. Does the Best Evidence Rule require the original of the document to be produced?[59]

---

55 Metadata with regard to by whom and when data was created and stored or when and by whom it was altered.

56 See Zeffertt footnote 22 above p 712.

57 The opinion of M Overly as discussed in Strydom 'Computer Evidence' HYPERLINK http://www.crimeinstitute.ac.za/2ndconf/papers/strydom.pdf 25 March.

58 *Ibid.*

59 The best-evidence rule applies only when the content of a document is directly in issue. In its widest form, this rule requires that only the best evidence of a fact in question was admissible, and accordingly that the best evidence thereof will always be admissible. See Schmidt footnote 6 above p 366. See also Hoffmann and Zeffertt footnote 6 above p 114.
The view of various South African legal scholars however is that the best evidence rule can and is no longer applied in the South African legal system. See Schmidt footnote 6 above p 369.
There is no rule today that provides that oral evidence about a thing is inadmissible if the thing itself could have been produced, or that circumstantial evidence is excluded when direct evidence could have been obtained. With one or two possible exceptions, the only survival is the rule requiring production of original documents. This will however, not pose too many problems for digital evidence due to the provisions contained in S 14 of

3. Is the document hearsay and not subject to an exception?[60]

Overly[61] goes even further and states that admissibility could further be ensured by establishing:[62]

- who created the document?
- its contents;
- how it was created; and
- that it has not been altered, either intentionally or unintentionally.[63]

---

the *Electronic Communications and Transactions Act* 25 of 2002. See also Hoffmann and Zeffertt footnote 6 above p 115.
This is due to the fact that, apart from the rule that secondary evidence of a document may only be tendered if the original is no longer available. There are no existing regulations that require that the best evidence of a fact will *always* be admissible, or that weaker evidence than the best evidence will *never* be admissible. See Schmidt footnote 6 above p 369. See also Hoffmann and Zeffertt footnote 6 above p 115.

60 Hearsay evidence is evidence of something that a person other than the witness said or did. The witness says or writes what he/she heard or read. This type of evidence is explicitly regulated by legislation and is excluded as evidence by a court because it is simply weak or unreliable evidence that can mislead the court. See Schmidt footnote 6 above p 443. See also Hoffmann and Zeffertt footnote 6 above p 623.
In terms of S 3 of this act the common-law of hearsay no longer applies. See also Hoffmann and Zeffertt footnote 6 above p 126.
In terms of S 3 of the *Law of Evidence Amendment Act* 45 of 1988 hearsay evidence is defined and may in principle not be admitted. S 3 (1) of the *Law of Evidence Amendment Act* 45 of 1988 provides that 'subject to the provisions of any other law, hearsay evidence may not be admitted as evidence at criminal or civil proceedings, unless:
(a) each party against whom the evidence is to be adduced agrees to the admission thereof as evidence at such proceedings; (b) the person upon whose credibility the probative value of such evidence depends, him or herself testifies at such proceedings; or (c) the court, having regard to: (i) the nature of the proceedings; (ii) the nature of the evidence; (iii) the purpose for which the evidence is tendered; (iv) the probative value of the evidence; (v) the reason why the evidence is not given by the person upon whose credibility the probative value of such evidence depends; (vi) any prejudice to a party which the admission of such evidence might entail; and (vii) any other factor which should in the opinion of the court be taken into account, is of the opinion that such evidence should be admitted in the interests of justice.'
Hearsay evidence may be provisionally admitted under S 3(1) of the *Law of Evidence Amendment Act* 45 of 1988 if the court is satisfied that the person upon whose credibility the probative value of such evidence depends, will him/herself testify in such proceedings. Should this person not testify, the hearsay evidence must be left out of account unless admitted under S 3(1) (a) or (c). See also S 3(3) of the *Law of Evidence Amendment Act* 45 of 1988.
In terms of S 3(1) (c) the court has a discretion to allow hearsay evidence if it will, within the court's judgement, be in the interests of justice to allow it. See Schmidt footnote 6 above p 447. See also *Hlongwane and Others v Rector, ST Francis Colledge, and Others* 1989 3 SA 318 (D) at 324E-F.

61 The opinion of M Overly as discussed in Strydom footnote 57 above.

62 See footnote 57 above.

63 These factors that must be proven are similar to the common-law factors required to prove the authenticity of documents.

Digital evidence falls within the definition of real evidence and it will remain real evidence even though it is digital.[64] Therefore, common-law requirements set for the admissibility of real evidence can be applied to digital evidence.[65]

3.2.2 Rules of Evidence that restrict the use of digital evidence

3.2.2.1 The Prohibition of Hearsay Evidence

The largest stumbling block for an increased acceptance of digital evidence in South African law, is the question of whether or not digital evidence constitutes hearsay evidence?

What is then the effect of section 15(1) of the ECT Act in possibly alleviating, removing or freeing such evidence from exclusion on the basis of hearsay? Furthermore, what is its effect on other statutory exceptions, such as section 3 of the *Law of Evidence Amendment Act,*[66] sections 221 and 222 of the *Criminal Procedure Act* [67] and section 34 of the *Civil Proceedings Evidence Act*?[68]

It must be kept in mind that the ECT Act refers to 'data messages' as to include electronic representations of information in any form, which are 'generated, sent, received or stored by electronic means.' This could mean that it is no longer necessary to produce a print-out of the information, when a device which is able to reflect its stored data would suffice.[69]

---

64 This is also required by S 15(1) of the *Electronic Communications and Transactions Act* 25 of 2002 providing for this type of evidence to be admitted if it is the best evidence of the facts in question. See also Hoffmann and Zeffertt footnote 6 above p 405.

65 The judge is entitled to rely upon his/her own perceptions and to draw such inferences as may reasonably be drawn without the need for expert qualifications. See Hoffmann and Zeffertt footnote 6 above p 405. However, most judges are unfamiliar with digital evidence. Therefore this digital evidence will have to be supported by the testimony of an expert witness or at least a person with sufficient knowledge of the workings of the techniques and procedures used to collect and preserve the digital evidence.

66 *Law of Evidence Amendment Act* 45 of 1988.

67 *Criminal Procedure Act* 51 of 1977.

68 *Civil Proceedings Evidence Act* 25 of 1965. See Zeffertt footnote 22 above p 394.

69 See Zeffertt footnote 22 above p 395.

Section 15 of the ECT Act appears to be expansive. Its purpose is to free as much computer-generated evidence from the hearsay rule,[70] as can be justified. [71]

The problem with the use of data messages as evidence can be explained by looking at the situation that may exist if the evidence were not in the form of a data message. If one regards it as direct oral evidence, given by the person upon whose credibility the probative value of this evidence depends, it will not be regarded as hearsay and will be admissible.[72] However, if one regards it as evidence given by a witness, other than the person upon whose credibility its probative value depends, it will be hearsay and will only be admissible if the requirements of section 3 of the *Law of Evidence Amendment Act*[73] are satisfied or some other exception to the hearsay rule can be applied.[74] The problem is that the wording of the ECT Act section 15(1) does not indicate which of the above approaches one should follow.[75]

Only in exceptional circumstances may computer-generated evidence be admitted as hearsay evidence and only if provided for in section 221 of the *Criminal Procedure Act*.[76] However, if it is inadmissible under any of the provisions it may, depending on the circumstances, be admitted as real evidence – this will be the case if it were generated without the intervention of the human mind.[77] If the evidence was derived in part or in whole from a statement made by a person, then hearsay considerations would once again come into play and the statutes mentioned above would be the only routes of possible admissibility.[78]

---

70 Without infringing upon the values served by this exclusionary rule.
71 See S 15(3) and (4) in footnote 120 below.
72 See Zeffertt footnote 22 above p 394.
73 *Law of Evidence Amendment Act* 45 of 1988.
74 Such as Ss 221 and 222 of the *Criminal Procedure Act* 51 of 1977. See also Zeffertt footnote 22 above p 394.
75 See Zeffertt footnote 22 above p 395.
76 *Criminal Procedure Act* 51 of 1977. See also Zeffertt footnote 22 above p 712.
77 See Zeffertt footnote 22 above p 712.
78 See Zeffertt footnote 22 above p 712.

3.2.2.2 The Best Evidence Rule

With regard to the use of digital evidence, section 15(1)(b)[79] of the *Electronic Communications and Transactions Act*[80] expressly states that 'In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.' Even though the use of digital evidence as the best evidence of a fact in dispute is provided for in this legislation, the view of Schmidt[81] and other legal scholars is that the best evidence rule is no longer applied in the South African legal system.[82]

3.3 Case Law[83] on the admission of digital evidence

South African courts of law hesitate to admit digital evidence. This leads to the assumption that new legal requirements need to be developed with regard to the collection and preservation of digital data to ensure the integrity and originality thereof.

In *Ex Parte Rosch*[84] the court held that during the interpretation on the evidentiary import of computer evidence that one may consider such an interpretation at two levels.

---

79 S 15 of the *Electronic Communications and Transactions Act* 25 of 2002.

80 *Electronic Communications and Transactions Act* 25 of 2002.

81 In Schmidt footnote 6 above.

82 See Schmidt footnote 6 above p 368.

83 This is a short discussion on the most influential case law on the use of digital evidence or computer-generated evidence. Other relevant case law that may provide guidance on the use of digital evidence and is not specifically mentioned under this paragraph but also have specific application to proving the authenticity or set requirements for admissibility or application of the exclusionary rules of evidence will be discussed in the footnote explanations to such points of relevance.

84 *Ex Parte Rosch* 1998 1 All SA 319 (W). This is a case with application to the admission of digital evidence as real evidence. The court stated that the provisions of the *Law of Evidence Amendment Act* 45 of 1988 regarding hearsay evidence were also not applicable as the computer was not a "person" as contemplated in S 3(4) of the *Law of Evidence Amendment Act* 45 of 1988. The Court found that the print-out was real evidence in the sense that it came about automatically and not as a result of any input or information by a human being. There was therefore no room for dishonesty or human error. *Ex Parte Rosch* 1998 1 All SA 319 (W) at 321.

In the first instance, the Court distinguished computer evidence which amounts to 'real evidence'. In this regard, the Court opined that computer print-outs amount to real evidence if the information in the print-out came about automatically and not without mediation by a human agency. Thus the court would consider evidence with the view on how it was generated.[85] On the other hand, the Court further opined that different rules apply where the information in the print-out did not come about automatically. It is under such circumstances that the *Computer Evidence Act*[86], according to the Court, used to apply.[87]

No case law exist which provides guidance on what techniques and procedures should be followed by computer forensic investigators when collecting digital evidence to ensure its authenticity and admissibility.

3.4 Legislation

Most of the case law with regard to the admissibility of computer-generated evidence was decided in terms of the *Computer Evidence Act*.[88] The *Electronic Communications and Transactions Act*[89] repealed this act and came into force on 30 August 2002. The ECT Act is a relatively new act, and very little case law has been decided on how this act will be practically applied.[90] This act also makes sufficient provision for both civil and criminal digital evidentiary matters.

---

85 The court also gave the following opinion: "A court would be failing in its duty if it ignored the realities of modern science and technology in the production of evidence. The admissibility of such evidence would not affect the weight to be attached thereto: it would still be open to the other party to rebut the evidence so admitted. In the instant case, the trustworthiness of the documents was supported by the fact that there had been no complaints by subscribers of the telephone company regarding the telephone records generated by its computer, as well as by the fact that the evidence recorded manually in the first set of exhibits was almost identical to that recorded by the computer." *Ex Parte Rosch* 1998 1 All SA 319 (W) at 321.

86 *Computer Evidence Act* 57 of 1983.

87 Today the *Electronic Communications and Transactions Act* 25 of 2002 will be applied in order to support the allowance and admission of any digital evidence, and not only computer print-outs.

88 *Computer Evidence Act 57* of 1983. This act mainly found application only in civil matters. See Zeffertt footnote 22 above p 393.

89 *Electronic Communications and Transactions Act* 25 of 2002.

90 There are very few South African court precedents that give sufficient guidance on how the legislation with regard to digital evidence must be practically applied. The courts also

3.4.1 Legislation with regard to digital evidence in general

The following legislation had profound effects in the use of computer-derived evidence in the past:

- Section 221 of the *Criminal Procedure Act*;[91]
- Part VI of the *Civil Proceedings Act*;[92]
- The *Documentary Evidence from Countries in Africa Act*.[93]

---

do not give guidance as to which techniques and procedures need to be followed when computer forensic investigators obtain digital evidence in order to ensure its admissibility.

91 *Criminal Procedure Act* 51 of 1977. According to S 221, the definition of a document will also include a device through which information is stored or recorded. S 221(5) of the *Criminal Procedure Act* 51 of 1977. See Schmidt footnote 6 above p 347.
A Computer is clearly such a device, but the computer itself cannot be regarded as a document. A computer print-out will surely fall hereunder and as such will be admissible as evidence if it also complies with the other requirements set by S 221. See Schmidt footnote 6 above p 347. See also *S v Harper* 1981 1 SA 88 (D) 95E-H.
This legislative provision is however limited to criminal matters and documents that are (business) records or part of a record. It is further limited to having the information supplied by a person with personal knowledge thereof and the computer must itself have noted or stored the information, not merely processed it. See Schmidt footnote 6 above p 347.

92 *Civil Proceedings Act* 25 of 1965. S 34(1) of the Act prescribes when a statement 'made by a person' in a document, and such statement is direct oral evidence of such fact, will become admissible evidence. S 34(4) of the Act provides that a statement in a document is not deemed to have been made by a person unless the document was written, made, or produced by him 'with his own hand' or was 'signed' or 'initialled' by him or otherwise recognised by him in writing as one for the accuracy of which he is responsible. However, the court found in the case of *Narlis v South African Bank of Athens* 1976 2 SA 573 (A) at 577H that this legislation will not be applicable to computer-generated evidence for the simple reason that it requires the statement that 'is made by a person in a document', and a computer is not a person.

93 The *Documentary Evidence from Countries in Africa Act* 62 of 1993. The Act is important owing to its extensive definition of a 'document', which includes transcribed computer print-outs produced by any mechanical or electronic device and any device by means of which information is recorded or stored. See S 1 of the *Documentary Evidence from Countries in Africa Act* 62 of 1993 in which it is provided that a 'document' includes any affidavit, certificate, record, photograph, book, map, plan, drawing and any documentary recording or transcribed computer printout produced by any mechanical or electronic device and any device by means of which information is recorded or stored. Due to the Internet domain stretching far beyond the national borders of South Africa, this act is especially important. This act, along with the provisions of Chapter XIII of the *Electronic Communications and Transactions Act* 25 of 2002, will apply to cases where the digital evidence is connected with and required to prove a crime committed in South Africa, is situated in another African country. This will help to alleviate the traditional jurisdictional restrictions created by legal rules that find application to physical evidence.

3.4.2 The Electronic Communications and Transactions Act[94]

The ECT Act is a positive step towards ensuring that the law in general is effectively enforced also in cyberspace.[95] Unlike, for example America, where different issues are often addressed by means of separate laws,[96] this law proposes to deal with issues with regard to writing and signature requirements, authentication, accreditation, safety and security, national strategy, e-government, access to electronic services, consumer protection, domain name administration and cyber crime, all in one piece of legislation.[97]

Even though there are provisions in the act relating to the search of a building in order to seize a 'suspect' device or computer,[98] it does not provide for specific steps to be taken in the handling of such a 'suspect' device in order not to compromise the digital data contained therein.

3.4.2.1 The ECT Act in general

To achieve the objective of legal certainty, the ECT Act ensures that electronic transactions will be legally binding and further provides for the criminal punishment of cyber-criminals.[99] The ECT Act, therefore, provides a

---

94 *Electronic Communications and Transactions Act* 25 of 2002. In accordance with the pre-amble to this act it was enacted to provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for the Republic; to promote universal access to electronic communications and transactions and the use of electronic transactions by SMMEs; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and to provide for matters connected therewith.

95 The *Electronic Communications and Transactions Act* 25 of 2002 does this by allowing for the admission of evidence in digital or electronic format by requiring that these types of evidence should not be excluded merely because they are in a digital or electronic form.

96 The United States of America has two separate laws, The *Uniform Electronic Transactions Act* 1999 for regulation of electronic transactions in general, and *The Federal Electronic Signature in Global and National Commerce Act* 2000 directed specifically at e-signatures.

97 Coetzee 2004 *STELL LR* 502.

98 See S 82 of the *Electronic Communications and Transactions Act* 25 of 2002.

99 The promotion of public confidence in electronic transactions requires a regulatory and supervisory framework where security is a key issue. See footnote 97 above p 503. See also the Chapter XIII provisions of this Act on Cyber-crime.

legal framework for the legality of data messages, electronic signatures and electronic and digital evidence.[100]

Chapter III provides for the facilitation of electronic transactions. Starting with Section 11 which provides for the legal recognition of data or electronic messages in general, and continuing with a legal framework for issues such as writing,[101] signatures,[102] copies,[103] originals,[104] admissibility and evidential weight of data messages,[105] retention,[106] notarisation, acknowledgement and certification.[107]

Chapter XIII of the ECT Act provides for the first statutory provisions on cyber crime in South Africa,[108] which is a welcome addition to South African legislation. It has theoretically[109] given South Africa the means by which to combat, regulate and prosecute offenders of cyber-crime.[110]

A functional equivalent for the concept of originality was introduced in section 14[111] of the ECT Act. Section 14 requires that the integrity of the information should be assessed in regard to whether it is complete and unaltered, and

---

100 See footnote 97 above p 503.

101 S 12 of the *Electronic Communications and Transactions Act* 25 of 2002.

102 S 13 of the *Electronic Communications and Transactions Act* 25 of 2002.

103 S 19(1) of the *Electronic Communications and Transactions Act* 25 of 2002.

104 S 14 of the *Electronic Communications and Transactions Act* 25 of 2002.

105 S 15 of the *Electronic Communications and Transactions Act* 25 of 2002.

106 S 16 of the *Electronic Communications and Transactions Act* 25 of 2002.

107 S 18 of the *Electronic Communications and Transactions Act* 25 of 2002.

108 See footnote 97 above p 508.

109 The practical application by South African courts of law of the Act is limited.

110 S 87 of the *Electronic Communications and Transactions Act* 25 of 2002 provides for the criminal prohibition and outlawing of extortion, fraud and forgery committed by using the Internet as a means to an end, and is a welcome addition to South African legislative provisions.

111 S 14 of the *Electronic Communications and Transactions Act* 25 of 2002 states that:
'1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if-
a. the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and
b. that information is capable of being displayed or produced to the person to whom it is to be presented.
2) For the purposes of subsection 1(a), the integrity must be assessed:-
a. by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display; b. in the light of the purpose for which the information was generated; and c. having regard to all other relevant circumstances.'

also that the information should be capable of being displayed or reproduced.[112] The requirement of originality will be satisfied if a document originated from a computer and can be reproduced in either electronic or paper format.[113]

Section 17[114] of the ECT Act provides for certain requirements to ensure that the integrity of the information contained in a document or data message is maintained. Evidence provided in paper or electronic form will therefore be admissible if the requirements are met by proving that the relevant circumstances existed at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document.

In terms of the ECT Act a court must not discriminate against evidence due to it being in electronic format. However, the manner in which the electronic evidence was collected and retained will still have an effect on the evidential value thereof.[115] This is extremely important because the ECT Act contains no provisions that state how this evidence should be collected or retained to ensure its reliability and authenticity. The required techniques and procedures

---

112 See footnote 97 above p 512.

113 This will have the practical effect of making the requirement for production of an original document (and also computer print-outs) as evidence redundant. S 14 of the *Electronic Communications and Transactions Act* 25 of 2002 now enables one to produce the data on a screen or in a viewable format, permitted that it is proven to be relevant and authentic, as an original of such evidence.

114 S 17 of the *Electronic Communications and Transactions Act* 25 of 2002 states that:
'(1) Subject to section 28, where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information, and if-
a. considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and b. at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference.
(2) For the purposes of subsection (1), the integrity of the information contained in a document is maintained if the information has remained complete and unaltered, except for-
a. the addition of any endorsement; or b. any immaterial change, which arises in the normal course of communication, storage or display.'

115 Leggat 'Hackers have a free ride in SA' HYPERLINK http://estrategy.co.za/article.asp?pklArticleID=2542&pklIssueID=346&pklCategoryID.htm 10 Feb. p 3.

that must be applied in order to prove these requirements are not expressly provided for in legislative provisions, or in case law. The ECT Act does, however, provide a broad legislative regulation of the issues relating to the admissibility of digital evidence.

Various opinions have been raised concerning the application of the ECT Act in practice. For example that of Buys,[116] when he said that:

> The ECT Act defines most recognised cyber crimes, but does not give guidelines on how the evidence should be collected.[117]

Another opinion also given during this period is that of Silber[118] who stated that the ECT Act was designed to cater for those cases where it is difficult to prove that physical access had been gained to a computer and that:

> The ECT Act is broad, and we do need some practical application of how it is to be used.[119]

These opinions are well-founded if one considers the apparent lack of practical application of the ECT Act and its provisions concerning digital evidence in South African courts. Neither the ECT Act or case law provide guidance on how law enforcement officials, must proceed during their investigations for digital evidence and do therefore not provide practical examples of the techniques and procedures that must be applied to ensure admissible digital evidence.

3.4.2.2 Section 15 on the admissibility and evidential weight of data messages

Section 15[120] provides for the use of and admissibility of data messages[121] as evidence. Section 15(1)[122] of the ECT Act provides that rules of evidence

---

116 Reinhardt Buys of the South African IT law firm Buys Incorporated. A statement given by him prior to the settlement of the ABSA Fraud Case. See Vecchiatto 'Lawyers lick lips over ABSA Fraud Case' HYPERLINK http://www.itweb.co.za/sections/internet/2003/0307291128.asp?S=IT%20in%20Banking&A=ITB&O=S 11 Feb.

117 See Vecchiatto footnote 116.

118 Opinion by Michael Silber an Independent electronic law lawyer. See Vecchiatto footnote 116.

119 See Vecchiatto footnote 116.

must not be applied to deny the admissibility of a data[123] message purely because it is constituted by a data message,[124] or on the grounds that it is not in its original form, if it is the best evidence that can be obtained.

The ECT Act does, however, not give a definition of what constitutes digital evidence. Data and data messages are however defined. Digital evidence has been defined in American law as 'Information stored or transmitted in binary form that may be relied upon in court.'[125] In accordance with this definition, digital evidence can be included in the definition of a data message as it is also generated, sent, received or stored by electronic means and a stored record.[126] Accordingly, it is not necessary to produce a print-out of the

---

120 S 15 of the *Electronic Communications and Transactions Act* 25 of 2002 provides as follows: '(1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence:-
a. on the mere grounds that it is constituted by a data message; or b. if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form;
(2) Information in the form of a data message must be given due evidential weight;
(3) In assessing the evidential weight of a data message, regard must be given to:-
a. the reliability of the manner in which the data message was generated, stored or communicated; b. the reliability of the manner in which the integrity of the data message was maintained; c. the manner in which its originator was identified; and d. any other relevant factor.
(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.'

121 Defined in S 1 of the *Electronic Communications and Transactions Act* 25 of 2002 and means 'data generated, sent, received or stored by electronic means and includes (a) voice, where the voice is used in an automated transaction; and (b) a stored record.'

122 See S 15(1) in footnote 120 above.

123 The act defines data as electronic representations of information in any form and does not require any technology to secure the data.

124 The term 'Data messages' is defined in S 1 of the *Electronic Communications and Transactions Act* 25 of 2002 as meaning 'data generated, sent, received or stored by electronic means and includes (a) voice, where the voice is used in an automated transaction; and (b) a stored record.'

125 See University of Georgia footnote 54 above.
Including this American legal definition of digital evidence into the definitions of data and data messages in the *Electronic Communications and Transactions Act* 25 of 2002 will however have to be done by interpretation of the provisions of this act by the courts. In order to facilitate such an interpretation a party may inform the court of this definition and application thereof in America. The applicable rules and regulations with regard to digital evidence in America will however only have persuasive effect in a South African court and the court may take this foreign law into consideration in interpreting the South African legislation. Fundamental rights to access to information contained in S 32 of the *Constitution of the Republic of South Africa*, 1996 was given statutory effect in the

information as the production of a device which is capable of reflecting the stored data will suffice.[127]

Section 15(3)[128] further gives guidance on how the evidential weight of data messages should be treated. Factors such as the author of the message, the reliability of the manner in which the message was generated, stored, communicated, and how its integrity is maintained must be considered.[129] These factors are reminiscent of the common-law requirements for documentary evidence discussed above. This shows that theoretically, the use of digital evidence and data messages as evidence is broadly provided for in the provisions of the ECT Act and these forms of evidence could more readily be admitted in the South African courts of law. The practical application is however lacking.

The possible reason for the broad formulation of the ECT Act could be to allow for future technological change so that the legislature will not have to adopt new legislation every time technology develops beyond a narrow legislative regulation. The ECT Act does therefore give broad legislative guidance on what has to be proven in order to ensure that digital evidence is admitted as proof of a fact in question in a court of law. The relevant rules and regulations with regard to the applicable techniques and procedures that have to be applied by computer forensic investigators to collect and ensure admissible digital evidence must be provided for by case law in the future. However for the time being, these rules and regulations will have to be developed and lawfully implemented by computer forensic investigators and the South African Police Services.

Promotion of Access to Information Act 2 of 2002 specifically S 50(1) (a), which requires such access to be 'Reasonably required for exercise or protection of right' – see in this regard *Davis v Clutchco (Pty) Ltd*, 2003 3 All SA 561; 2004 1 SA 75 (C).
See also further S 34 of the *Constitution of the Republic of South Africa*, 1996 in which the fundamental right to a fair and impartial hearing is contained.

127 See Zeffertt footnote 22 above p 395.

128 See S 15(3) in footnote 120 above.

129 See footnote 97 above p 512.

3.4.2.3 Other provisions of the ECT Act that have an effect on the admissibility of digital evidence

a) The Cyber Inspector

The ECT Act makes express provision for a person to be appointed as a cyber inspector to enforce South African legislation concerning digital data, digital evidence or any suspected cyber crimes. The legislative provisions for such an office require effective procedures to be in place in order for this inspector to do his/her job in such a manner so as not to cause unnecessary exclusion of digital evidence in a trial.[130]

The cyber inspector has express powers of inspection, search and seizure.[131] This section provides that he/she may:[132]

- enter and search a premises, person and information system;
- take extracts and copy books, documents and records;
- demand production of and inspection of licences and registration certificates; and
- inspect business facilities including ones linked and/or associated with the one under investigation.

Any statutory body with investigative powers may apply for assistance from the cyber inspector in an investigation provided they apply to the Department and get authorisation.[133] This will supply investigators, such as the South African Police Services, to acquire the digital evidence in the safest possible manner as to ensure its authenticity and acceptance as evidence in a court.

---

130 See footnote 97 above p 507. See Chapters 2 and 5 of this mini-dissertation for a discussion on possible procedures that should be followed in the collection of digital evidence to ensure its inclusion as evidence in a court hearing.

131 As is provided for in S 82 (subject to S 83) of the *Electronic Communications and Transactions Act* 25 of 2002.

132 See footnote 97 above p 507.

133 See footnote 97 above p 507.

b) Privacy issues connected with digital evidence[134]

The ECT Act provides for the protection of personal information[135] in Chapter VIII sections 50[136] and 51[137]. Section 50 limits the scope of this protection to

---

134 The provisions in Ss 50 and 51 of the ECT Act (to protect the constitutional right to privacy contained in S 14 of the 1996 Constitution) provide similar protection to privacy rights as those provided for in the American *Electronic Communications Privacy Act* 1986 (to protect the individuals constitutional 4th Amendment right not to be unreasonably searched and have property seized by the government). These requirements have to be met as not to unreasonably infringe upon the basic privacy rights of individuals as provided for in S 14 of the *Constitution of the Republic of South Africa*, 1996 when also applying the functions of the Cyber Inspector provided for in S 82 to perform searches and seize property or information found during such investigations. S 14 of the *Constitution of the Republic of South Africa*, 1996 provides that: 'Everyone has the right to privacy, which includes the right not to have—(*a*) their person or home searched; (*b*) their property searched; (*c*) their possessions seized; or (*d*) the privacy of their communications infringed.'

135 S 1 of the *Electronic Communications and Transactions Act* 25 of 2002 provides that personal information means: 'information about an identifiable individual, including, but not limited to-
a. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual; b. information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; c. any identifying number, symbol, or other particular assigned to the individual; d. the address, fingerprints or blood type of the individual; e. the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual; f. correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; g. the views or opinions of another individual about the individual; h. the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and i. the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than 20 years.'

136 S 50 of the *Electronic Communications and Transactions Act* 25 of 2002 provides that: '(1) This Chapter only applies to personal information that has been obtained through electronic transactions. (2) A data controller may voluntarily subscribe to the principles outlined in section 51 by recording such fact in any agreement with a data subject. (3) A data controller must subscribe to all the principles outlined in section 51 and not merely to parts thereof. (4) The rights and obligations of the parties in respect of the breach of the principles outlined in section 51 are governed by the terms of any agreement between them.'

137 S 51 of the *Electronic Communications and Transactions Act* 25 of 2002 provides that: '(1) A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law. (2) A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required. (3) The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored. (4) The data controller may not use the personal

information contained or produced as a result of an electronic transaction. Section 51 sets requirements that must be complied with before personal information may be requested and used by a data controller.[138]

3.5 Conclusion

The ECT Act has aimed at the elimination of much of the legal uncertainty that previously prevailed in South African law and one of its purposes is to place electronic transactions on the same footing as traditional paper-based transactions.[139] It theoretically gives legal recognition to data messages and records for evidential purposes and gives legal force to electronically concluded contracts.[140] It further caters for the rights of individuals by providing for consumer protection, protection of personal information, as well as security measures in regard to data messages and electronic signatures, and the regulation of cyber crime.[141]

An example of how digital evidence has been treated practically by some magistrates in South Africa can be found in a briefing undergone in April 2000 by Harris during a gathering of magistrates from around the country on archival and related law.[142] Harris took the opportunity to question the magistrates on their experience with electronic evidence, where it became

---

information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law. (5) The data controller must, for as long as the personal information is used and for a period of at (cast one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected. (6) A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject. (7) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed. (8) The data controller must delete or destroy all personal information which has become obsolete. (9) A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.'

138 S 1 of the *Electronic Communications and Transactions Act* 25 of 2002 defines a data controller as: 'any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject.'

139 See footnote 97 above p 520.

140 See footnote 97 above p 520.

141 See footnote 97 above p 521.

142 See Harris footnote 1 above.

apparent that both experience and perspective were widely divergent.[143] The slow pace at which the law changes, and the lack of technical knowledge of older judges, prevents the SA legal system from sufficiently regulating the effects of the technological advancements brought to South Africa by the computer age.

The ECT Act is broadly formulated in order to be able to apply to digital evidence stored on or generated by most digital devices. It does not specifically provide computer forensic investigators with the required techniques and procedures that must be applied to ensure the admissibility of digital evidence.[144] For the moment, and in order to prove the authenticity of the proposed digital evidence, a witness will have to testify as to what techniques and procedures were followed when investigating and collecting the digital evidence and that these procedures and techniques were correctly applied to ensure the authenticity of the digital evidence.

The law of evidence in South Africa must change in such a manner as not to attempt to force the products of modern technology into the rather limited categories of either real or documentary evidence. While some changes should and are likely to come from the courts, more can be expected from legislation and investigation departments that are able to offer new and creative approaches to the problem posed by the use of digital data as evidence.

Having legislation such as the ECT Act to regulate this matter is a great advantage. The lack of detail provisions as to how digital evidence should be obtained, stored and reproduced is a constraining factor.

---

143 At one extreme was a magistrate who claimed never to have admitted electronic evidence – in every one of about a dozen cases – his reason being that the deponent had failed to satisfy the requirements for authentication. At another extreme was a magistrate who expressed "no problems" with electronic evidence - she confessed to testing the reliability of an e-mail message produced in a particular case by doing a few manipulation exercises on e-mails stored on her own Personal Computer. See Harris footnote 1 above.

144 These techniques and procedures will have to be developed by computer forensic laboratories and by law enforcement.

Chapter 4

American Law on the Use of Digital Evidence

The view in America is that the law governing digital evidence lags behind the reality of cyber-crime,[1] and that America has few legal precedents to guide judges.[2] It has also become standard practice in America for legal representatives[3] to request digital and electronic information during litigation proceedings.[4] Therefore, digital evidence[5] investigations have become more common.[6] However, physical investigations have existed for thousands of years and the procedures followed and techniques used during these investigations can provide guidance to the world of digital evidence investigations.[7]

This Chapter will attempt to show that the USA has tried and tested Federal and State legislative provisions with regard to digital evidence.[8]

---

1 Coren 'Digital evidence: Today's fingerprints. Electronic world increasingly being used to solve crimes' HYPERLINK http://www.cnn.com/2005/LAW/01/28/digital.evidence/index.html 10 March p 2.

2 In the opinion of the University of Dayton's Susan Brenner: "We have judges who did not grow up with computers and so many do not understand the technology and issues it raises", as referred to in footnote 1 above p 2.

3 Volonino 2003 *Communications of Association for Information Systems* 17.

4 See footnote 3 above p 17.

5 The rule of thumb is that if information was displayed at some time on a computer screen, it can generally be recovered from that computer. This rule can be applied to data of all types. See Lewis 'Data Forensics – The smoking gun may be a click away' HYPERLINK http://www.forensicfocus.com/computer-forensics-smoking-gun.php 10 March.

6 The Martha Stewart trial and ongoing investigations at Enron and WorldCom reveal the importance of computer forensics. See Lewis footnote 5 above.
The outcome of many corporate cases turns on evidence obtained through computer forensics, for example and most prominently those concerning Enron, Chase, Imclone, and Microsoft. In some of these computer forensics investigations, deliberate attempts to obstruct justice by destroying evidence, which is a criminal offence, was revealed. See footnote 3 above p 8.

7 Most criminal and civil investigations will include computers at some point in the case. It is for this reason imperative that a process model for a digital evidence investigation exists and that it will easily interact with pre-existing physical investigation procedures. See Carrier and Spafford 2003 *International Journal of Digital Evidence.*

8 The American legislation with regard to digital evidence is not totally infallible, and it is constantly being improved.

4.1 Evidence in general

The evidence is the foundation of every case.[9] It is classified into three categories:[10]

- real or physical evidence, which consists of tangible objects that can be seen and touched;[11]
- testimonial evidence, where the testimony of a witness can be given during a trial, based on a personal observation or experience;[12]
- circumstantial evidence, which is based on a remark, or observation of realities that tends to support a conclusion, but not to prove it.

4.1.1 Civil- and Criminal matters[13]

In criminal litigation, the burden of proof is always on the state, which must prove that the defendant is guilty.[14] In criminal litigation, the state must prove that, beyond a reasonable doubt, the defendant has satisfied each element of the statutory definition of the crime and the defendant's participation therein.[15]

---

9 Evidence can be generally defined as something that tends to establish or disprove a fact. See Chawki 'The Digital Evidence in the Information Era' 2004 HYPERLINK http://www.crime-research.org/articles/chawki1/ 25 Jul p 1.

10 See Chawki footnote 9 above.

11 Physical evidence is a tangible item such as, for example, a murder weapon, a firewall log or a hard disk containing data. See Shinder 'Preserving Digital Evidence to Bring Hackers and Attackers to Justice' 2005 HYPERLINK http://www.computerworld.com/securitytopics/security/story/0,10801,102157,00.html 11 Oct.

12 Evidence can be witness testimony from a person who has personal knowledge of facts pertaining to the crime. See Shinder footnote 11 above.

13 The Federal Rules of Evidence apply to both criminal and civil cases. Nevertheless, a number of rules recognise a distinction between civil and criminal trials, either explicitly or by implication. Similarly, a number of rules, due to their subject matter, apply only in civil cases. For example, Rule 407 (subsequent remedial measures) and Rule 411 (liability insurance). Further differences in applicability in criminal and civil proceedings arise because the Rules of Evidence generally do not codify constitutional principles. See also Anon. 'Discussion on Contents of *Understanding Evidence'* 2003 HYPERLINK http://www.lexisnexis.com/lawschool/study/outlines/word/evid05.doc 11 Oct.

14 This must be done due to the defendant being assumed to be innocent.

15 Standler 'Computer Crime' 1999/2002 HYPERLINK http://www.rbs2.com/ccrime.htm 11 Oct.

In civil litigation, the burden of proof is initially on the plaintiff. However, there are a number of technical situations in which the burden shifts to the defendant.[16] In civil litigation, the plaintiff wins if the preponderance of the evidence favours the plaintiff.[17] A few tort claims[18] require that the plaintiff prove his/her case at a level of 'clear and convincing evidence', which is a standard higher than preponderance, but less than beyond a reasonable doubt. [19]

There are no differences between civil and criminal cases in the procedures and techniques used during an investigation for digital evidence. The differences will come into play where the digital evidence is requested in civil cases to be made available to the opposing party[20] by using a subpoena. In criminal cases there will be an investigation for possible digital evidence after a warrant to search and seize has been granted by a judge that would legally allow such investigations in or on the premises of the suspect. There are however situations in which a search and seizure warrant or a judge's permission will not be required.[21]

---

16 For example, when the plaintiff has made a prima facie case, the burden shifts to the defendant to refute or rebut the plaintiff's evidence.

17 For example, if the jury believes that there is *more than a 50%* probability that the defendant was negligent in causing the plaintiff's injury, the plaintiff wins. This is a very low standard, compared to criminal law.

18 Tort claims such as, for example fraud.

19 In addition to any criminal penalties, victim(s) of computer crimes can sue the perpetrator in tort. There is also the possibility of a class action by corporate and personal victims against a person who wrote and initially released a computer virus. There is another remedy in civil law, besides damages awarded in tort litigation: a victim can get a temporary restraining order, then an injunction, that enjoins continuance of wrongs (e.g., disclosure of proprietary or private data) that will cause irreparable harm or for which there is no adequate remedy at law. See footnote 15 above.

20 This is also referred to as a discovery request and must be done within the boundaries of legislation regulating a persons' basic right of access to information.

21 These are regulated by legislation and usually when there is a suspicion that the suspect will destroy the evidence before a warrant can be obtained; when the evidence is in plain sight; or even when the suspect gives his/her permission to the judicial officer to enter the premises and to search it.

4.1.2 Rules of Evidence

Evidence must be relevant, competent, and material to the case at hand.[22] The Federal Rules of Evidence[23] and case law provide standards applied by trial courts to determine whether evidence that is scientific, technical or of a specialized nature[24] may be admitted.[25]

Digital data poses a problem due to it being somewhat less tangible than most physical evidence. Therefore digital data falls within the category of fragile evidence.[26] In fact, the very act of collecting or examining digital data can change it.[27] This is a problem because in order for evidence to be admissible, the party introducing it must prove that it has not been tampered with or modified since it was collected at the crime scene.[28] In order for the party introducing the digital evidence to prove its authenticity, he/she must therefore show that the scientific or forensic techniques and procedures applied to collect it are scientifically sound, and in accordance with the *Daubert*[29]-test.

Daubert v. Merrell Dow Pharmaceuticals[30] is seen as the leading case in which guidelines for evidentiary reliability was established.[31] The guidelines from this

---

22 This is the basic legal doctrine with regard to the admission of any type of evidence. See Kenneally 2001 *Virginia Journal of Law and Technology*.

23 See discussion under paragraph *4.3 Legislation* below of this Chapter of this mini-dissertation.

24 Such as the computer science applicable to digital evidence.

25 See Kenneally footnote 22 above. See also the discussion on the case of *Daubert v. Merrell Dow Pharmaceuticals*, 509 US 572 (1993).

26 Digital evidence is regarded as fragile evidence due to its fragile nature - as it can so easily be altered or destroyed. Another example of fragile evidence is for example footprints in snow. See Shinder footnote 11 above.

27 See Shinder footnote 11 above. See also the discussion under Chapter 2 of this mini-dissertation.

28 See Shinder footnote 11 above.

29 This test for reliability was formulated by the American court in the case of *Daubert v. Merrell Dow Pharmaceuticals*, 509 US 572 (1993).

30 *Daubert v. Merrell Dow Pharmaceuticals*, 509 US 572 (1993). This case involved challenges to the admission of scientific evidence, and was aimed to bring clarity to the reliability requirements provided for in the Federal Rules of Evidence. In this case the issue concerned the admissibility of scientific evidence (expert testimony based on epidemiological evidence) supporting the claim that the drug Bendectin caused birth defects.

case require that courts consider the following factors to determine the admissibility of scientific evidence:

- has the scientific theory or technique been empirically tested; or, is it falsifiable?
- has the theory or technique been subjected to peer review and publication?
- what is the known or potential error rate?
- is the theory or technique generally accepted within the relevant scientific community?[32]

In this manner[33] the court defines reliability as "something that can be validated by testing and supported by more than subjective beliefs or unsupported speculation."[34]

The *Kumho Tire v. Carmichael*[35] case extended the *Daubert*[36] guidelines to non-scientific evidence.[37] This gives trial judges the discretion to determine which criteria should be applied in order to determine reliability, and whether those criteria are in fact satisfied.[38] The Court interpreted the reliability requirement of

---

31 These criteria are seen as the court's attempt to meet the standard of evidentiary reliability and are done by ensuring that technical evidence is grounded in knowledge derived from the methods and procedures of science. See Kenneally footnote 22 above.

32 See footnote 30 above *Daubert*-case at 593-595. Other factors that may be relevant to the consideration include: the relationship of technique to methods established as reliable; the non-judicial uses of the method; the logical or internal consistency of the hypothesis; the consistency of hypothesis with accepted theories; and, the precision of hypothesis or theory.

33 This can be done by connecting the validity of the knowledge to the underlying scientific methodology.

34 See footnote 30 above *Daubert*-case at 590.

35 *Kumho Tire v. Carmichael*, 526 U.S. 137, 147-49 (1999).

36 *Daubert v. Merrell Dow Pharmaceuticals*, 509 US 572 (1993).

37 This ruling appears to be valuable to make standards of reliability for non-scientific evidence clear. However, the court assumed that the four factors used to measure the reliability of scientific evidence may be applied just as effectively in order to evaluate technical or specialized evidence. It must be remembered that if knowledge is based on experience or subjective interpretations that are not susceptible to validation through testing, those factors do not provide assistance in evaluating the reliability of that knowledge. See Kenneally footnote 22 above.

38 In *Kumho Tire v. Carmichael*, 526 U.S. 137, 147-49 (1999) the court concedes that, on its face, *Daubert* limited its discussion to evaluating the admissibility of scientific knowledge; however, the court explains here that as a matter of language, Rule 702 applies to all

Federal Rule of Evidence 702 to apply to the word 'knowledge,' instead of 'scientific, technical or other specialized.'[39] To establish reliability, a party must therefore demonstrate that the method used by an expert to reach his/her conclusions is derived from valid methodology. The trial judge must determine at the outset, pursuant to Rule 104(a), whether an expert proposes to testify to relevant 'knowledge'.[40]

The technical knowledge that may accompany the introduction of some forms of digital evidence generally represents a complex and uncharted territory for judges.[41]

---

matters within its scope, i. e. scientific, technical, or other specialized knowledge. *See Kumho*, 526 U. S. at 147-49. The Court specifically held here that a judge's broad 'gate-keeping' discretion extends to all expert testimony. Therefore, when presented with any expert, a judge must evaluate the reliability of the methodology used to reach a conclusion and the relevance or 'fit' of the proffered evidence to a fact in issue. See Harris and Gotell 'Preparing Experts with Kumho in Mind' 2000 HYPERLINK http://www.lowenstein.com/new/kuhmo.html 15 Oct. See also footnote 25 above.

39 In other words, expert testimony can be based on non-scientific knowledge in a particular field in order to meet the standard of evidentiary reliability. See the *Kumho*-case footnote 35 and also footnote 30 above *Daubert*-case at 509. As also referred to by Kenneally - footnote 22 above.

Rule 702 states that "[i]f scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise." See Harris and Gotell footnote 38 above.

40 *See Kumho Tire v. Carmichael*, 526 U.S. 137, 147-49 (1999) at 149. If a party cannot establish the validity of an expert's methodology, the expert's proffered testimony is merely a subjective belief or unsupported speculation rather than 'knowledge' as required under Rule 702. See also Harris and Gotell footnote 38 above.

41 This uncharted territory and the fact that the claimed expertise by some judges may have come from an experience-based body of knowledge, may mean that the discretion used by these judges to allow such technical evidence to go before a jury might be less predictable. See Kenneally footnote 22 above.

In American law, during the pre-trial phase, the presiding judge will determine what proposed evidence will be admissible. If this evidence is allowed, the jury will be required to take it into consideration in making their finding. If a judge is not familiar with the particular technological device from which the digital evidence was collected, or the technological expertise applied to acquire the proposed digital evidence, this unfamiliar territory may possibly lead the judge to use his/her discretion and then not allow the digital evidence. In this regard see footnote 2 above.

4.1.2.1 Admissibility and Authenticity

Generally there are three requirements for evidence to be admissible in a court:

(a) authentication - the showing of a true copy of the original;

(b) the best evidence rule - means presenting the original; and

(c) exceptions to the hearsay rule - the allowable exceptions are when confessions, business, or official records are involved.[42]

In addition, US courts of law require the legality[43] of the evidence.[44]

In terms of Rule 401 of the Federal Rules of Evidence, evidence is defined as:

> Having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.[45]

It must further be kept in mind that the basic prerequisites of admissibility[46] are relevance,[47] materiality,[48] and competence[49].[50] If evidence complies herewith, and is not barred by an exclusionary rule, it is admissible.[51]

---

42 Authentication appears to be the most commonly used rule, but experts disagree over what is the most essential, or most correct, element of authentication in practice. See Chawki footnote 9 above.

43 The legality requirement means that the digital evidence must be obtained in accordance with the laws governing search and seizure, including laws expressed in the US and state legislations. See Chawki footnote 9 above.

44 See Chawki footnote 9 above.

45 See Chawki footnote 9 above.

46 These requirements for admissible evidence are considered by a judge during the preliminary determinations of the case before him/her. The initial screening during preliminary determinations by the presiding judge is required to ensure that the evidence complies with a basic reliability; upon which a jury can then decide what weight that evidence should carry in resolving the issue at hand. See Kenneally footnote 22 above.
These preliminary determinations occur in accordance with Rule 901 of the Federal Rules of Evidence. This rule requires that 'the matter in question is what it is claimed to be' or that it is authentic.
Another rule that must be used during the preliminary determinations is Rule 702 which requires proof of reliability. Rule 702 of the Federal Rules of Evidence provides that in order for a witness to be qualified as an expert, the expert must be shown to have "knowledge, skill, experience, training, or education" regarding the subject matter involved. The testimony of this witness will have to prove that the techniques and procedures used to collect the evidence can be regarded or shown to be reliable – thus adding the methods reliability to the evidence obtained through the use thereof. See Kenneally footnote 22 above.

Physical evidence is usually authenticated by the sworn testimony of one or more persons who can verify that it is what it purports to be.[52] It appears that this authentication rule is also applied to digital evidence, because computer-derived data has gained admission upon the basic proof or showing that the computer process or -system produces accurate results when used, that it was operated properly, and that it was so employed when the evidence was generated.[53]

Federal Rule of Evidence 901 grants a presumption of authenticity to evidence such as x-rays, photographs, tape recordings, computer-generated records or scientific surveys produced by an automated process - if these are shown to

---

47 Evidence is *relevant* when it has any tendency in reason to make the fact that it is offered to prove or disprove either more or less probable - Federal Rules of Evidence 401. To be relevant, a particular item of evidence need not make the fact for which it is offered certain, or even more probable than not. All that is required is that it has some tendency to increase the likelihood of the fact for which it is offered. See DiCarlo 'A Summary of the Rules of Evidence: The Essential Tools for Survival in the Courtroom' HYPERLINK http://www.dicarlolaw.com/RulesofEvidenceSummary.htm 25 Jul.
It must pertain to the actual case. For example, evidence showing that a person hacked into a different computer system 10 years ago generally would not be admissible in a trial to determine his guilt or innocence in an attack that occurred 10 months ago. See Shinder footnote 11 above.
Rule 402 of the Federal Rules of Evidence provides that if evidence is not relevant it is not admissible - 'All relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority.' See Chawki footnote 9 above.

48 The evidence must prove or disprove facts that impact the question before the court - which is usually: "Did the defendant commit the crime with which he's charged". See Shinder footnote 11 above.

49 The evidence must be proved to actually be what it purports to be. Proving its competence is called authentication of the evidence. See Shinder footnote 11 above.

50 See DiCarlo footnote 47 above.

51 Federal Rule of Evidence 402. As referred to by DiCarlo footnote 47 above.

52 For example, the network administrator who checked the firewall logs immediately following an attack can testify that the log data presented in court matches the data he saw in the logs on that date and time. The police officer who arrived on the scene can testify that he packaged up the computer containing the log files and delivered them to the evidence lab. The computer forensics technician who took possession of the computer can testify that he received it from that officer and that he used standard forensics methods to make a bit level copy of the disk containing the logs. See Shinder footnote 11 above.

53 It must be remembered that authenticity standards are meant to ensure that evidence is what it purports to be. The rigour of the foundation required to make this finding will depend on the existence of something that can be tested. This is primarily accomplished through the testimony of a witness who can speak to the identity and accuracy of the computer-derived evidence. The rationale is that the availability of a witness who can be cross-examined about the actual event and its link to the digital exhibit is a sufficient guarantee of authenticity. See Kenneally footnote 22 above.

render accurate results.[54] This presumption of reliability has been extended to software performing data storage, -collection or -retrieval functions.[55]

When the question arises for authenticating computer-derived or digital evidence, it is recommended that a higher standard apply than that used for photographs, whereas others advocate that mere judicial notice of the authenticity of computer-derived evidence under Federal Rule of Evidence 901(b) (9) should be allowed.[56]

4.1.2.2 Best Evidence Rule

The best evidence rule basically requires that the best or highest form of evidence[57] available to a party must be presented in evidence.[58]

The Uniform Federal Rules of Evidence establish the criteria for producing records that can be admitted into evidence.[59] Rule 1002[60] thereof specifies the requirement for original records as follows:

---

54 See Federal Rule of Evidence 901. For example, when photographs are used as evidence, a witness familiar with the picture must testify that it is a fair and accurate portrayal of the scene. See also Kenneally footnote 22 above.

55 Computer-derived evidence has been extended a similar presumption of authenticity by some courts, provided that a computer operator, who is familiar with the process undertaken by the software, testifies. See Kenneally footnote 22 above.

56 Rule 901(b) (9) governs authentication of evidence describing a process or system. Rule 901(b) (9) of the Uniform Rules of Evidence reflects what the criteria for introducing records into evidence are. The rule provides that records or other evidence can be admitted in evidence if the proponent provides evidence describing a process or system used to produce a result and shows that the process or systems produces an accurate result. Each form of record must be viewed based upon the accuracy of the process or system used to produce the record. See also Kenneally footnote 22 above.

57 Anon. 'The Best Evidence Rule is Dead' HYPERLINK http://www.irch.com/articles/articl11.htm 25 Jul.

58 For example, a party cannot rely solely on the testimony of an individual who knows something about a subject when another individual is available who is thoroughly familiar with the facts of the matter. The Best Evidence Rule originally was developed to ensure that the courts considered the best evidence related to a particular matter. This rule therefore permits records to be introduced as a primary form of evidence, but also specifies that original records are preferred. Therefore, when given a choice between two forms of the same records such as the originals versus duplicates, the court will normally require production of the original paper records. See footnote 57 above.

59 Some of the major provisions found in these laws include making the record at or near the time of the event, obtaining information for the record by or from somebody with knowledge, producing the record in the regular course of business and providing a custodian or other qualified person as a witness to testify regarding the methods used to create the records.

> To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required except as otherwise provided in these rules or by statute.[61]

The requirements of the best evidence rule, however, can no longer be upheld in the real world of technology. Modern record technology[62] systems usually differ in establishing processes or systems that produce accurate results.[63] One might argue that the best evidence rule should be changed to indicate that accurate records, regardless of form, can be introduced in evidence.[64] With various safeguards that can be built into today's modern record technology systems, the

---

Where once live testimony was the only form of evidence, now live testimony and records serve as primary forms of evidence. Some judges even believe that records might be a better form of evidence than live testimony since peoples' memory changes and weakens over time while records preserve the information in the same form in which it was originally recorded. See footnote 57 above.

In these rules there is however a preference for original records. See DiCarlo footnote 47 above.

60 The best evidence rule provides that, where writing is offered in evidence, a copy or other secondary evidence of its content will not be received in place of the original document unless an adequate explanation is offered for the absence of the original - Federal Rules of Evidence 1002. See also DiCarlo footnote 47 above.

61 Although Rule 1003 permits the introduction of duplicate records, the requirement of Rule 1002 clearly establishes a preference for the original unless other conditions in the rule have been satisfied. Most jurisdictions will still have a restatement of the best evidence rule related to originals in either the Uniform Rules of Evidence or other equivalent statutes or rules of evidence. See also footnote 57 above.

62 Every day more and more records of transactions or business records are stored technologically in for example digital format. Records technology may be regarded as various software applications implemented by companies and civilians to facilitate a more sufficient digital system of record keeping. By using records technology the immense space and expenses incurred by documentary or paper based record keeping can be substantially lessened by storing all required information in digital format – as most businesses are required to store business records for a pre-determined period in the USA. See footnote 57 above.

63 The quality of records produced by records technology systems may surprise most legal purists. They have continually argued that since information can be manipulated during reproduction or within a computer system, the records are inherently less reliable. This view, however, is not always correct. Modern record technology systems can produce records that are more accurate than paper-based systems. Most systems prohibit fraud and detect unauthorized attempts at information manipulation. Most systems will also include audit trails and audits of data accuracy (such as Metadata information) to ensure the overall integrity of the system. Paper records systems can be manipulated by even the most unsophisticated person in the organization. Even janitors can selectively steal or destroy paper-based information without a trace. See footnote 57 above.

64 See footnote 57 above.

best evidence may not only be the product of a particular technology but also the result of a trustworthy process or system used to produce the records.[65]

4.1.2.3 The Hearsay Rule

A basic evidentiary doctrine governing admissibility determinations is that there are circumstantial guarantees of trustworthiness[66] to ensure some reliability so that a jury is not unduly confused or prejudiced by a given piece of evidence.[67] Hearsay is generally not allowed because it violates this doctrine.

Federal Rule of Evidence 801(c)[68] defines hearsay as:

> A statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.[69]

The prohibition against hearsay is a barrier and standard to which courts have subjected computer-derived evidence.[70] It is accepted that computer programs

---

65 See footnote 57 above.

66 Factors such as routine reliance on records kept within the normal course of business, lack of motives to fabricate those records, and the non-adversarial nature within which they were created, converge to create circumstantial guarantees of trustworthiness. As an example it can be noted that paper-based business records are occasionally found to be inadmissible if the source of information or the method or circumstances of preparation indicate a lack of trustworthiness; and that computers may produce different results based on different assumptions of programmers, however, which can only be directly determined by looking at the source code. See Kenneally footnote 22 above.

67 See Kenneally footnote 22 above.

68 Federal Rule of Evidence 801(c), 1996.

69 The 'declarant-focused' definition highlights the underlying policy of the hearsay rule. There is, however, a competing definition, an 'assertion-focused' definition: Hearsay is an out-of-court statement offered for the truth of its assertion. In most cases, the same result is reached under either definition but not always. The Federal Rules adopt the latter definition. See footnote 13 above.

70 Various business records exceptions have been codified, see for example Federal Rule of Evidence 803(6). The following is not excluded by the hearsay rule: 'A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness ... unless the source of information or the method or circumstances of preparation indicate a lack of trustworthiness.' See Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations' 2002 HYPERLINK

that contain out-of-court statements by declarants[71] and which are offered to prove the truth of the matter, violate the hearsay rule.[72] Nonetheless, some federal courts have applied the business records exception[73] to a wide variety of computer-based information.[74]

Alternatively, proponents of computer-derived evidence may by-pass the hearsay exception by convincing the court that such digital evidence constitutes a product of a device that performed pre-programmed tasks on admissible data input, as for example with a radar gun or a calculator.[75]

It is dangerous to immunise certain computer records from the hearsay rule just because they appear to be the product of a mechanical process that cannot produce hearsay.[76] It would be persuasive to argue that computer logs, for example, are merely the tangible result of the computer's internal operations, which do not rely on human observations or reports, and are made concurrently with the capturing of data.[77]

Questions about how complete the data capture is and how the logging software decides what should be captured and processed can only be done by examining

---

http://www.cybercrime.gov/s&smanual2002.htm 11 Oct.

71 Declarants can be computer operators, programmers, or data entry personnel.

72 See Kenneally footnote 22 above.

73 Contained in Federal Rule of Evidence 803(6).

74 It was held in *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990) that computer data compilations are admissible as business records under Federal Rule of Evidence 803(6) if a proper foundation as to the reliability of the records is established. The Senate Committee's report on the Federal Rules of Evidence also implicitly recognized that computer-based records fall under the Rule 803(6). As cited in *United States v. Jackson* 7th Circuit No. 99-2223. See also Kenneally footnote 22 above.

75 See Kenneally footnote 22 above. Computerised printouts of phone traces, for example, were not hearsay in one case because they did not rely on the assistance, observations, or reports of a human declarant, and it was found that the printouts were merely the tangible result of the computer's internal operations. See also *State v. Armstead*, 432 So. 2d 837, 839-41 (La. 1983) in which the court held that computerised records of phone traces were not hearsay and that such records were computer-generated data to be distinguished from computer-stored declarations.

76 See Kenneally footnote 22 above.

77 Unlike phone trace records and calculators, however, the software producing the logs is programmed to capture and process data deemed to be relevant to its programmed function from many computers over a network. See Kenneally footnote 22 above.

the underlying source.[78] If digital evidence is admitted without uncovering the assumptions that underlie its function,[79] it would lead to the resolution of claims based on a very small quantity of reliable evidence.[80]

4.2 Case Law on the admission of digital evidence

It appears that, in America, some judges have restricted the conduct of computer forensic searches by law enforcement, insisting that certain procedures or methods must be followed.[81] Police and prosecutors argue that a judge can only issue a search or seizure warrant, not dictate its terms.[82] It is clear that questions about privacy infringement and the sanctity of personal data loom because digital technology is inextricably linked to our daily lives during which personal information is given and recorded for various reasons.[83]

In the case of *Zubulake v UBS Warburg*[84] the courts, when addressing the burden and expense issues associated with electronic discovery, recognised five categories of stored data:[85]

---

78 See Kenneally footnote 22 above.

79 Such assumptions are of the credibility of the program used to create and store the digital information, the possibilities of a malfunctioning of the program going undetected and possibly altering the digital information created by the program.

80 See Kenneally footnote 22 above.

81 See footnote 1 above p 2.

82 See footnote 1 above p 2.

83 This can lead to the conclusion that there is a need to revisit the laws designed during an earlier, simpler age. This is also the view of Susan Brenner (as referred to in footnote 2 above). See footnote 1 above p 2.

84 *Zubulake v UBS Warburg* S.D.N.Y. May 13, 2003. This case is generally considered the first definitive case in the United States on a wide range of electronic discovery issues. These issues include: a) The scope of a party's duty to preserve electronic evidence during the course of litigation; b) Lawyer's duty to monitor their clients' compliance with electronic data preservation and production; c) Data sampling; d) The ability for the disclosing party to shift the costs of restoring "inaccessible" back up tapes to the requesting party; e) The imposition of sanctions for the spoliation (or destruction) of electronic evidence.
The *Zubulake* decisions are of particular interest in the United States in the light of Judge Scheindlin's knowledge of the subject and due to the opinions arising from the influential Southern District of New York, both of which have provided American lawyers with new best practices relating to both the legal and technical aspects of electronic discovery. See Legal Resources 'Zubulake v. UBS Warburg' 2005 HYPERLINK http://www.krollontrack.co.uk/legalresources/zubulake.asp 15 Oct.

85 See footnote 3 above p 12.

- active, online data;[86]
- near-line data;[87]
- offline storage or archives;[88]
- backup tapes;[89]
- erased, fragmented, or damaged data.[90]

Perhaps the most important case on the fact that American courts are requiring specific techniques and procedures to be followed by law enforcement when collecting digital evidence is that of *In re Search of 3817 W. West End.*[91] In this case the judge refused the government's request for a warrant to search a home computer unless the government first agreed to abide by pre-approved computer search protocol outlining the steps that would be taken to locate the evidence stored on the hard drive.[92] The reasoning behind this condition[93] set by the judge was to ensure that the search was constitutionally reasonable.[94]

---

86 This is data in an 'active' stage and is available for access as it is created and processed. Storage examples include hard drives or active network servers. See footnote 3 above p 12.

87 This data is typically housed on removable media, with multiple read/write devices used to store and retrieve records. Storage examples include optical disks or magnetic tape. See footnote 3 above p 12.

88 This category represents data that is offline on tape or other removable computer storage medium. Offline storage of electronic records id traditionally used for disaster recovery or for records considered "archival" in that their likelihood of retrieval is minimal. See footnote 3 above p 12.

89 Data stored on backup tapes is not organized for retrieval of individual documents or files, because the organization of the data mirrors the computer's structure, not the human records management structure. Data stored on backup tapes is also typically compressed, allowing storage of greater volumes of data, but also making restoration more time-consuming and expensive. See footnote 3 above p 12.

90 This data was tagged for deletion by a computer user, but may still exist somewhere on the free space of the computer until it is overwritten by new data. Significant efforts are required to access this data. See footnote 3 above p 12.

91 *In re Search of 3817 W. West End,* 321 F. Supp. 2d. 953 (N.D. Ill. 2004.) This is a recent Chicago case, which suggests that some judges are taking bolder steps. The court found the government's argument unpersuasive and distinguished the two requirements based on the existence of certain tools allowing the search of computer information to be more targeted than a search of hard copy documents. The court stated that these tools afforded the government the ability to limit its search by date range, key words, specific files, and specific software programs. Based on this, the court held the search protocol was necessary in order to meet the particularity requirement of a constitutional search warrant. See also Forensicon 'Court Orders Government to Submit Search Protocol Prior to Examining Seized Computer' HYPERLINK http://www.forensicon.com/casesummaries/cs-3817.asp 15 Oct.

92 The judge refused to allow the search without a specific judge-approved search protocol on the basis that doing so would grant the investigators a licence to roam through everything in

4.2.1 The Hearsay rule

The evidentiary issues raised by the admission of digital and computer records should depend on what kind of computer records are requested to be admitted.[95] For example, computer records that contain text often can be divided into two categories: computer-generated records,[96] and records that are merely computer-stored.[97] The difference depends upon whether a person or a machine created the contents of the records.

As with any other testimony or documentary evidence containing human statements, computer-stored records must comply with the hearsay rule. If the records are admitted to prove the truth of the matter they assert, the party offering the records must show circumstances indicating that the human statements contained in the record are reliable and trustworthy and that the records are authentic.[98]

Unlike computer-stored records, computer-generated records do not contain human statements, but only the output of a computer program designed to process input following a defined algorithm.[99] However, the fact that a computer rather than a human being has created the record alters the evidentiary issues

---

the computer. The judge justified this condition on four practical concerns: a) the fact that computers are seized first and searched at a later time; b) the likelihood that evidence of crime was co-mingled with unrelated and innocent files; c) the fact that computers can store a large amount of information; and d) the existence of technical methods to refine searches. See Kerr 2005 *Columbia Law Review* 316.

93 The condition of compelling pre-approval of the search methods.

94 See Kerr footnote 92 above p 316.

95 See Computer Crime footnote 70 above.

96 Computer-generated records contain the output of computer programs, untouched by human hands. Log-in records from Internet service providers, telephone records, and ATM receipts tend to be computer-generated records. See Computer Crime footnote 70 above.

97 Computer-stored records refer to documents that contain the writings of some person or persons and happen to be in digital or electronic form. E-mail messages, word processing files, and Internet chat room messages provide common examples. See Computer Crime footnote 70 above.

98 See Computer Crime footnote 70 above.

99 Of course, a computer program can direct a computer to generate a record that mimics a human statement: an e-mail program can announce "You've got mail!" when e-mail arrives in an inbox, and an ATM receipt can state that $100 was deposited in an account at 2:25 pm. See Computer Crime footnote 70 above.

that the computer-generated records present.[100] The evidentiary issue is no longer whether a human's out-of-court statement was truthful and accurate,[101] but instead whether the computer program that generated the record was functioning properly[102].[103]

A third category of computer records exists. This category contains the computer records that are both computer-generated and computer-stored.[104] The party seeking the admission of the record should address both the hearsay issues implicated by the original input and the authenticity issues raised by the computer processing.[105]

Federal case law shows that the admission of computer records generally raises two distinct issues:

- first, there must be an establishment of the authenticity of all computer records, by providing the evidence sufficient to support a finding that the matter in question is what its proponent claims;[106]
- second, if the computer records are computer-stored records that contain human statements, it must be shown, that those human statements are not inadmissible hearsay.[107]

There are exceptions to the prohibition of hearsay evidence; the Due Process Clause is one of these and it may require the admissibility of hearsay in limited

---

100 See Computer Crime footnote 70 above.
101 This is regarded as a question of hearsay.
102 This is regarded as a question of authenticity.
103 See *People v. Holowko*, 486 N.E.2d at 878-79. See also Computer Crime footnote 70 above.
104 For example, a suspect in a fraud case might use a spreadsheet program to process financial figures relating to the fraudulent scheme. A computer record containing the output of the program would derive from both human statements (the suspect's input to the spreadsheet program) and computer processing (the mathematical operations of the spreadsheet program). These types of records combine the evidentiary concerns raised by computer-stored and computer-generated records. See also Computer Crime footnote 70 above.
105 See Computer Crime footnote 70 above.
106 See Federal Rule of Evidence 901(a). See also Computer Crime footnote 70 above.
107 In both instances this prove must be given by the party seeking to use this evidence. See Computer Crime footnote 70 above.

circumstances.[108] The leading case on this aspect is *Chambers v. Mississippi*.[109] In this case the Supreme Court held that state evidentiary rules that precluded the admission of critical and reliable evidence denied the defendant due process. One of the rules in this case that made the defence evidence inadmissible was the hearsay rule.[110]

The trial judge decides the admissibility of hearsay evidence under Rule 104 (a) and failure to raise the hearsay objection in a timely manner is regarded as a waiver of the objection,[111] and the evidence may then be considered by the jury.[112]

The reported decisions primarily relate to admissibility of routine business computer records under the business record exception to hearsay. For example, in *United States v. Glasser*,[113] computer printouts of transactions relating to mortgage bank accounts were admitted into evidence under the business record exception.[114] Also worth mentioning is the case of *United States v. Scholle*,[115] in which printouts of a computer retrieval system relating to information on drug evidence was admitted under the business record exception.[116]

---

108 See Anon. footnote 13 above.

109 *Chambers v. Mississippi*, 410 US 284, 302 (1973).

110 *Chambers v. Mississippi*, 410 US 284, 302 (1973). According to the court, in these circumstances (where constitutional rights directly affecting the ascertainment of guilt are implicated) the hearsay rule may not be applied mechanistically to defeat the ends of justice.

111 This can be found in the Federal Rule of Evidence 103.

112 *Bourjaily v. United States*, 483 US 171, 175 (1987).

113 *United States v. Glasser*, 773 F.2d 1553 (11th Cir. 1985).

114 *United States v. Glasser*, 773 F.2d 1553 (11th Cir. 1985) at 1558-59. See also Stoner 1999 HYPERLINK http://researchnotebook.com/FoleyLardner.pdf 15 Oct. 2005 p 7.

115 *United States v. Scholle*, 553 F.2d 1109, 1123-25 (8th Cir. 1977).

116 Importantly, *Glasser, Scholle* and other cases to date have been clear that electronic evidence is not deemed to be inherently less reliable or trustworthy than paper records. See also *United States v. Young Bros., Inc.*, 728 F.2d 682, 693-94 (5th Cir. 1984) where the court rejected an argument by defendant that computer records are inherently less reliable because of potential software and data entry problems. See also Stoner footnote 114 above p 7.

In the Seventh Circuit court's decision in *United States v. Briscoe*,[117] the court held that a proper foundation for computer records is generally established if the party presenting the computer records:

> Provides sufficient facts to warrant a finding that the records are trustworthy and the opposing party is afforded an opportunity to inquire into the accuracy thereof and how the records were maintained and produced.[118]

These decisions have in common the fact that the party seeking admission of the computer records was not required to prove beyond all doubt the accuracy of its records.[119] Rather, enough evidence initially was required to satisfy the inquiry under Federal Rule of Evidence 803(6), and thereafter the burden apparently shifted to the opponent to prove that the computer system was unreliable.[120]

4.2.2 Authenticity

A party must show that the evidence or digital evidence is authentic before he/she may request the admission thereof.[121] The standard for authenticating computer records is the same for authenticating other records.[122] For example,

---

117 *United States v. Briscoe*, 896 F.2d 1476 (7th Cir. 1990).

118 *United States v. Briscoe*, 896 F.2d 1476 (7th Cir. 1990) at 1494-95. Briscoe followed the earlier decision in *United States v. Croft*, 750 F.2d 1354 (7th Cir. 1984), in which the Seventh Circuit upheld the admissibility of computer print-outs of payroll records - In the *Croft*-case at 1363-64. The panel was persuaded by the facts that (i) the opposing party was given the opportunity to thoroughly inquire into the accuracy of the computer and the input procedures, and (ii) the un-controverted evidence showed that the payroll information entered into the computer was subject to periodic reviews and audits throughout the year, which should have picked up any errors in the entry of such information. *United States v. Croft*, 750 F.2d 1354 (7th Cir. 1984) at 1364-65. The Court also was influenced by the fact that the computer print-outs were relied on for completing tax forms for the Internal Revenue Service. See also Stoner footnote 114 above p 7-8.

119 See Stoner footnote 114 above p 8.

120 See Stoner footnote 114 above p 8.

121 That is, the party must offer evidence that will be sufficient to support a finding that the computer record or other evidence in question is what its proponent claims. See Federal Rule of Evidence 901(a). See also *United States v. Simpson*, 152 F.3d 1241, 1250 (10th Cir. 1998).

122 The degree of authentication does not vary simply because a record happens to be, or was at one point, in digital or electronic form. See *United States v. Vela*, 673 F.2d 86, 90 (5th Cir. 1982); and *United States v. DeGeorgia*, 420 F.2d 889, 893 n.11 (9th Cir. 1969). See also Computer Crime footnote 70 above.

witnesses who testify to the authenticity of computer records need not have special qualifications.[123] Instead, the witness must simply have first-hand knowledge of the relevant facts to which he/she testifies.[124]

Challenges to the authenticity of computer records often take on one of the following forms:

- parties may challenge the authenticity of both computer-generated and computer-stored records by questioning whether the records were altered, manipulated, or damaged after they were created;[125]
- parties may question the authenticity of computer-generated records by challenging the reliability of the computer program that generated the records;[126]or
- parties may challenge the authenticity of computer-stored records by questioning the identity of their author. [127]

---

123 The witness does not need to have programmed the computer himself, or even need to understand the maintenance and technical operation of the computer. See *United States v. Salgado*, 250 F.3d 438, 453 (6th Cir. 2001).

124 See Computer Crime footnote 70 above.

125 The courts have responded with considerable scepticism to unsupported claims that computer records have been altered. Absent specific evidence that tampering occurred and the mere possibility of tampering does not affect the authenticity of a computer record. See *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988) and *United States v. Glasser*, 773 F.2d 1553, 1559 (11th Cir. 1985). See also Computer Crime footnote 70 above.

126 The authenticity of computer-generated records sometimes implicates the reliability of the computer programs that create the records. For example, a computer-generated record might not be authentic if the program that creates the record contains serious programming errors. If the program's output is inaccurate, the record may not be 'what its proponent claims' according to Federal Rule of Evidence 901. The courts have indicated that these challenges can be overcome so long as the party wanting to use the digital evidence provides sufficient facts to warrant a finding that the evidence is trustworthy and the opposing party is afforded an opportunity to inquire into the accuracy thereof. See *United States v. Briscoe*, 896 F.2d 1476, 1494-95 (7th Cir. 1990). In most cases, the reliability of a computer program can be established by showing that users of the program actually do rely on it on a regular basis, such as in the ordinary course of business. See, e.g., *United States v. Salgado*, 250 F.3d at 453 – where the court held that evidence that the computer was sufficiently accurate that the company relied upon it in conducting its business was sufficient for establishing trustworthiness. See also Computer Crime footnote 70 above.

127 Computer-stored records consist of a long string of zeros and ones that do not necessarily identify their author. This is a particular problem with Internet communications, which offer their authors an unusual degree of anonymity. When prosecutors seek the admission of such computer-stored records against a defendant, the defendant may challenge the

The case of *United States v. Weatherspoon*,[128] involved the presentation of thorough, all-encompassing evidence of computer input procedures for admissibility of computer printouts. In *Weatherspoon*[129] the U.S. Government provided evidence of its input procedures, as well as the accuracy thereof,[130] its monthly testing for internal programming errors, and its use and maintenance of the printouts in the ordinary course of business activities.[131] The panel in *Briscoe*,[132] however, noted that an extensive showing such as that in *Weatherspoon*[133] is not required in every case as a prerequisite to admitting computer records.[134]

---

authenticity of the record by challenging the identity of its author. Circumstantial evidence generally provides the key to establishing the authorship and authenticity of a computer record. For example, in *United States v. Simpson*, 152 F.3d 1241 (10th Cir. 1998), prosecutors sought to show that the defendant had conversed with an undercover FBI agent in an Internet chat room devoted to child pornography. The government offered a printout of an Internet chat conversation between the agent and an individual identified as "Stavron," and sought to show that "Stavron" was the defendant. The district court admitted the printout in evidence at trial. On appeal following his conviction, Simpson argued (at 1249) that "because the government could not identify that the statements attributed to [him] were in his handwriting, his writing style, or his voice," the printout had not been authenticated and should have been excluded. The Tenth Circuit rejected this argument (at 1250), noting the considerable circumstantial evidence that "Stavron" was the defendant. For example, "Stavron" had told the undercover agent that his real name was "B. Simpson," gave a home address that matched Simpson's, and appeared to be accessing the Internet from an account registered to Simpson. Further, the police found records in Simpson's home that listed the name, address, and phone number that the undercover agent had sent to "Stavron." Accordingly, the government had provided evidence sufficient to support a finding that the defendant was "Stavron," and the printout was properly authenticated. See also *United States v. Siddiqui,* 235 F.3d 1318, 1322-23 (11th Cir. 2000) - holding that e-mail messages were properly authenticated where messages included defendant's e-mail address, his/her nickname, and where he/she followed up messages with phone calls. See also Computer Crime footnote 70 above.

128 *United States v. Weatherspoon*, 581 F.2d 595 (7th Cir. 1978).

129 *United States v. Weatherspoon*, 581 F.2d 595 (7th Cir. 1978).

130 The accuracy was shown to be within two percent.

131 *United States v. Weatherspoon*, 581 F.2d 595 (7th Cir. 1978) at 598. See also Stoner footnote 114 above p 8.

132 *United States v. Briscoe*, 896 F.2d 1476 (7th Cir. 1990).

133 *United States v. Weatherspoon*, 581 F.2d 595 (7th Cir. 1978).

134 *United States v. Briscoe*, 896 F.2d 1476 (7th Cir. 1990) at 1494. The *Croft* panel made a similar comment. *United States v. Croft*, 750 F.2d 1354 (7th Cir. 1984) at 1365. See also Stoner footnote 114 above p 8.

4.2.3 The best evidence rule[135]

Agents and prosecutors occasionally express concern that a mere print-out of a computer-stored electronic file may not be an original for the purpose of the best evidence rule. After all, the original file is merely a collection of 0's and 1's. In contrast, the print-out is the result of manipulating the file through a complicated series of electronic and mechanical processes.[136]

Fortunately, the Federal Rules of Evidence have expressly addressed this concern. Rule 1001(3) states that:

> [i]f data are stored in a computer or similar device, any print-out or other output readable by sight, shown to reflect the data accurately, is an original.[137]

An accurate print-out of computer data will therefore satisfy the best evidence rule.[138]

4.3 Legislation

4.3.1 Federal Rules of Evidence[139]

The Federal Rules of Civil Procedure govern discovery, and the process of pre-trial information sharing during a civil suit. According to Rule 26(b) (1) of these rules, discovery may be made of any matter which is not privileged, that likely will lead to discoverable evidence.[140] Rule 34 of the Federal Rules of Civil Procedure was amended to address changing technology and communication.[141]

---

135 See Federal Rule of Evidence 1002. See also Computer Crime footnote 70 above.
136 See Computer Crime footnote 70 above.
137 Federal Rule of Evidence 1001(3).
138 See Computer Crime footnote 61 above.
139 The specific Federal Rules of Evidence applicable to the existing evidentiary rules have already been discussed under paragraph *4.1.1 Rules of Evidence* of this mini-dissertation above. The following is only a discussion of those rules that did not specifically reside under the above discussed topics.
140 See footnote 3 above p 5.
141 See footnote 3 above p 6. This rule made electronically stored information subject to 'subpoena and discovery' for use in legal proceedings.

Another rule worth mentioning here is Rule 26 of the Federal Rules of Discovery, in accordance with which each company has the duty to preserve documents that may be relevant in a case, including computer-stored[142] and computer-generated[143] records.[144]

The Federal Courts appear to treat digital evidence as documents[145] that carry the same burden of proof of authenticity as other documents do.[146] However, digital evidence carries a further burden because copies are allowed, and because digital evidence is easy to alter in discreet ways if not handled properly.[147] Furthermore digital evidence must meet strict court approvals.[148] The data stored in a computer or similar device as well as any print-out or other output readable by sight, must be shown to reflect the data accurately, and must be considered an 'original'.[149]

There are many federal statutes in the USA that can be used to prosecute computer criminals.[150] The law governing digital evidence in criminal

---

142 This category includes active data, replicated data, residual data, backup data, and legacy data.

143 This category includes cache files, cookies, Web logs, and embedded data or metadata.

144 See footnote 3 above p 6.

145 See Federal Evidence Rule 901(a). See Anon. 'Digital Forensics Legal Summary: Federal Evidence Rule 901(a)' HYPERLINK http://dfc.cs.uri.edu/resources/LegalSummary.html 25 Jul.

146 *Ibid.*

147 See Anon. footnote 145 above.

148 See Federal Evidence Rule 1001. See also Anon. footnote 145 above.

149 Forensically obtained bit stream copies are considered original. Digital signatures are used by digital forensics specialists to prove authenticity and originality. Printouts of digital data, although considered original, lose 'meta data' - data about the time of creation, location of the data on the media, etc. Forensic digital copies maintain all metadata. See Anon. footnote 145 above.

150 These include the following - 15 USC § 1644, prohibiting fraudulent use of credit cards; 18 USC § 1029, prohibiting fraudulent acquisition of telecommunications services; 18 USC § 1030, prohibiting unauthorized access to any computer operated by the U.S. Government, financial institution insured by the U.S. Government, federally registered securities dealer, or foreign bank; 18 USC § 1343, prohibiting wire fraud; 18 USC § 1361-2, prohibiting malicious mischief; 18 USC § 1831, prohibiting stealing of trade secrets; 18 USC § 2314, prohibiting interstate transport of stolen, converted, or fraudulently obtained material; does apply to computer data files *U.S. v. Riggs,* 739 F.Supp. 414 (N.D.Ill 1990); 18 USC § 2319 and 17 USC § 506(a), criminal violations of copyright law; 18 USC § 2510-11, prohibiting interception of electronic communications; 18 USC § 2701, prohibiting access to communications stored on a computer (i.e., privacy of e-mail); 47 USC § 223, prohibiting interstate harassing telephone calls. See also footnote 15 above.

investigations has two primary sources: the Fourth Amendment to the American Constitution, and the codified statutory privacy laws.[151]

In addressing data retention and preservation issues the *Sarbanes-Oxley Act*[152] was signed into law in 2002.[153] Arising from the Enron and Arthur Andersen fraud cases, this law mandates the retention of electronic documents; mandates that companies produce their electronic records and other documents when summoned by the Oversight Board; and imposes strict criminal penalties for altering or destroying records, including those kept in electronic form.[154]

The most important federal statutes affecting computer forensics are the *Electronic Communications Privacy Act*,[155] the *Wiretap Statute*,[156] the *Pen/Trap Statute*[157] and the *USA PATRIOT Act*[158].[159]

---

151 Statutory privacy laws codified at 18 U.S.C. §§ 2510-22, 18 U.S.C. §§ 2701-12, and 18 U.S.C. §§ 3121-27. Although constitutional and statutory issues overlap in some cases, most situations present either a constitutional issue under the Fourth Amendment or a statutory issue under these three statutes. See also Computer Crime footnote 70 above.

152 *Sarbanes-Oxley Act* of 2002 (SOX).

153 See footnote 3 above p 5.

154 See footnote 3 above p 5.

155 *Electronic Communications Privacy Act* 1986. Herein after referred to as ECPA. The ECPA was promulgated due to Congress feeling that information stored on a network deserved varying levels of privacy protection, depending on how important or sensitive the information was. Accordingly, in Title 18, Section 2703 of the U.S. Code, the ECPA created five categories of sensitivity. The more sensitive the category, the greater the justification the government must show in order to obtain the information from a third party (usually the system administrator). The most sensitive information consists of the content of un-retrieved communications such as e-mail that has resided in electronic storage for 180 days or less. See also Wegman 'Computer Forensics: Admissibility of Evidence in Criminal Cases' HYPERLINK http://www.cbe.uidaho.edu/wegman/Computer%20Forensics%20AA%202004.htm 11 Oct.

156 *Wiretap Statute* 1986. While the ECPA regulates government access to stored computer information in the hands of third parties, the *Wiretap* statute deals with direct surveillance or real-time interception of electronic communications by government agents. Before the government may use a wiretap, a court order must be obtained. Court orders vary widely in the amount of justification that must be demonstrated for their issuance. Section 2518 of the Wiretap statute requires a substantial amount of justification. This includes a demonstration of probable cause to believe that the interception will produce evidence relating to a felony; that normal investigative procedures have either failed, are unlikely to succeed, or are too dangerous; that the computer or other electronic/digital device is being used in the commission of a crime; and finally, that the surveillance will be conducted in a manner that will minimize the interception of innocent communications. See Wegman footnote 155 above.

4.3.2 State Rules of Evidence[160]

Each of the American states has its own set of evidential rules and own state court cases to which it must adhere. The federal rules of evidence will be applied in every state as a general guideline.

Texas law originally applied the Rules of Evidence into separate rules for civil and criminal proceedings. The Rules were revised and promulgated as a single set, the Texas Rules of Evidence on March 1, 1998.[161] The Rules of Evidence govern the Law of Evidence in Federal and State of Texas' courts and are perceived as the codification of the common law of evidence.[162] The text of the Texas Rules of Evidence is very similar to the Federal Rules of Evidence.[163]

---

157 *Pen/Trap Statute,* 2001, 18 United States Code Sec. 3121-3127. The *Pen/Trap* statute provides for a less intrusive form of government surveillance than the *Wiretap* statute. This statute authorizes the installation of pen registers and trap-and-trace devices. A pen register records only dialing, routing and addressing information regarding *outgoing* electronic communications. Electronic communications include telephone, computer, telegraph and telex communications. Perhaps the most controversial provision of the Patriot Act is the so-called "sneak and peek" authority conveyed in Section 213 of the Act. This Section provides delayed notification to the targets of searches. The Act modifies the U.S. Criminal Code, Title 18, Sections 3103a and 2705. These modifications allow the government to delay notification of physical searches for up to 90 days. Extensions may be given for good cause. See Wegman footnote 155 above.

158 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act - USA PATRIOT Act* 2001.

159 See Wegman footnote 155 above.

160 For purposes of this discussion, the State Evidence laws of Texas will be used.

161 See Murr 'How to Offer and Exclude Evidence: Conduct, Character, Remedial Measures: Common Relevancy Problems' HYPERLINK http://www.bmpllp.com/CM/Publications-Articles/How%20to%20Offer%20and%20Exclude%20Evidence.pdf 27 Sept. p 4.

162 Citations or reference to the "Rules of Evidence" apply to both civil and criminal cases unless otherwise specified. See footnote 161 above.

163 With a few notable exceptions, mainly Rule 407 regarding subsequent remedial measures and Federal Rules of Evidence 413 through 415, which do not have counterparts in the Texas Rules. See footnote 161 above p 4.

4.3.3 Privacy issues connected with digital evidence

The most important federal legislation with regard to privacy issues are the provisions for the rights of citizens contained in the Fourth Amendment[164] and the provisions contained in the *Electronic Communications Privacy Act.*[165]

The ECPA regulates how the government can obtain stored account information from network service providers such as Internet Service Providers.[166] Whenever agents or prosecutors seek stored e-mail, account records, or subscriber information from a network service provider, they must comply with ECPA.[167] The stored communication portion of the ECPA, creates statutory privacy rights for customers and subscribers of computer network service providers.[168]

In a broad sense, the ECPA 'fills in the gaps' left by the uncertain application of the Fourth Amendment protections to cyberspace.[169] If law enforcement investigators want to obtain the contents of a network account or information about its use, they do not need to go to the user to get that information. [170]

---

164 Amendment IV of the United States Constitution, guards against unreasonable searches and seizures, and came into operation on December 15, 1791. It states as follow: '*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*' See Wikipedia 'Fourth Amendment' HYPERLINK http://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution 25 Jul.

165 *Electronic Communications Privacy Act (ECPA)*, 18 U.S.C. Sec. 2701-2712 (1986).

166 See Computer Crime footnote 70 above.

167 See Computer Crime footnote 70 above.

168 See Computer Crime footnote 70 above.

169 To understand these gaps, consider the legal protections American citizens have in their homes. The Fourth Amendment clearly protects their homes in the physical world. If special circumstances are absent, the government must first obtain a warrant before it searches there. When people use a computer network such as the Internet, however, they do not have a physical 'home'. Instead, they typically have a network account consisting of a block of computer storage that is owned by a network service provider such as America Online. See Computer Crime footnote 70 above.

170 See Computer Crime footnote 70 above.

Instead, the government can obtain the information directly from the service provider.[171]

The balance between the individuals' right of privacy and the governments' right to violate that privacy by searching and seizing property is defined by the Fourth Amendment to the U.S. Constitution.[172] The Amendment interposes a magistrate as an impartial arbiter between the defendant and the police[173] or between the opposing parties to a civil matter[174].[175]

Although the Fourth Amendment generally requires the government to obtain a warrant to search a home, it does not require the government to obtain a warrant to obtain the stored contents of a network account.[176] Instead, the Fourth Amendment generally permits the government to issue a subpoena to a network provider ordering the provider to divulge the contents of an account.[177] The ECPA addresses this imbalance by offering network account holders a range of statutory privacy rights against access to stored account information held by network service providers.[178] In some cases the ECPA[179] is the controlling legal authority, rather than the Fourth Amendment. Typically this occurs when

---

171 See Computer Crime footnote 70 above.

172 It is in frequent use in law enforcement today, as police searches and seizures must comply with its requirements. See Wegman footnote 155 above.

173 The officer must prepare an affidavit that describes the basis for probable cause, and the affidavit must limit the area to be searched and evidence searched for. The warrant thus gives the police only a limited right to violate a citizen's privacy. If the police exceed that limited right, or if a warrant is required but the police have not first obtained one, then any evidence seized must be suppressed. Suppressed evidence may not be used in court. In many cases the criminal charges will be dismissed, even though the guilt of the defendant is clear. However, if other, untainted evidence exists supporting conviction, the defendant may be convicted on the strength of that evidence. The magistrate may issue a search warrant if he/she is convinced that probable cause exists to support a belief that evidence of a crime is located at the premises. See Wegman footnote 155 above.

174 In these civil matters a judge will determine whether the requesting party is entitled to the other party complying with his/her discovery request fro evidence in the opposing party's possession.

175 See Wegman footnote 155 above.

176 See Computer Crime footnote 70 above.

177 See Computer Crime footnote 70 above.

178 See Computer Crime footnote 70 above.

179 *Electronic Communications Privacy Act (ECPA)*, 18 U.S.C. Sec. 2701-2712 (1986).

information is transmitted to a network and is then stored under the control of a network administrator.[180]

No warrant is needed when the target consents to a search of his/her computer and no warrant is needed where a third party[181] consents to the search, so long as the third party has equal control over the computer.[182] Furthermore, no warrant is required when probable cause exists but there is an 'emergency' situation, leaving no time or opportunity to obtain a warrant.[183]

As noted above, a search warrant gives only limited authority to the police to search. The search should be no more extensive than is absolutely necessary, as justified by probable cause.[184] If the police wish to seize a computer and analyze it at a later time, the probable cause statement should demonstrate the impracticality or danger of examining the computer on the premises hence the need to confiscate it and analyze it off-site.[185]

Forensic investigators should understand that before they seize a computer or other electronic hardware they must consider whether the Fourth Amendment requires a search warrant.[186] They should be aware that if they wish to access stored electronic communications, they will need to comply with the ECPA.[187] If they wish to conduct real-time electronic surveillance, they will need to obtain a wiretap order from a judge.[188]

---

180 See Wegman footnote 155 above.
181 Such as a spouse, parent, employer or co-worker.
182 See Wegman footnote 155 above.
183 An example is *U.S. v. David*, 756 F. Supp. 1385 (1991), where agents observing the target deleting files immediately seized the computer. See also Wegman footnote 155 above.
184 Thus, if the probable cause indicates that the contraband is located in a file on a CD, this would not justify seizing every computer and server on the premises. The extent of the search is tailored to the extent of the probable cause. See Wegman footnote 155 above.
185 See Wegman footnote 155 above.
186 See Wegman footnote 155 above.
187 *Electronic Communications Privacy Act (ECPA)*, 18 U.S.C. Sec. 2701-2712 (1986).
188 See Wegman footnote 155 above.

4.4 Procedures to be followed during the collection of digital evidence

4.4.1 Procedures Followed in Practice

Computer forensics experts have developed a detailed set of procedures that forensic analysts ordinarily follow when they seize and analyse a targets' computer:[189]

- first, the detectives ordinarily seize the computer and bring it back to a government forensic laboratory for analysis;[190]
- back at the lab, the analyst begins by generating a "bit-stream" or "mirror" image of the hard drive;[191]
- the analyst then performs his work on the copy rather than the original to ensure that the original will not be damaged or altered by the analyst's investigation;[192]
- the analyst may try a range of techniques to locate the evidence sought;[193]
- assuming the suspect was not tipped off to the investigation and has not permanently erased the relevant files, the analyst may find master

---

189 See Kerr footnote 92 above p 288.

190 This is necessary because the forensic process is very time consuming; computer experts normally cannot find the evidence on a hard drive in the time that would allow the search to occur on site. See Kerr footnote 92 above p 288.

191 The bitstream copy is an exact duplicate, not just of the files, but of every single bit and byte stored on the drive. In order to determine whether or not to preserve and analyse a computer hard drive, several factors must be considered:
1) There must be the likelihood that the hard drive does contain information of value - If an event allegedly occurred in 2002 and a new computer is purchased in 2004, it is highly unlikely that any information of value will be contained on the new computer unless older data was copied to it. See Lewis footnote 5 above.
2) Cost must be considered as it is a determining factor since most data forensics firms bill by the hour and the number of drives to be preserved and analysed usually translates directly into a linear increase in the overall cost – See Lewis footnote 5 above. See also Kerr footnote 92 above p 288.

192 See Kerr footnote 92 above p 288.

193 For example, the examiner may begin by executing string searches for particular extensions, phrases, or textual fragments that relate to the evidence justifying the search. Alternatively, he may open all files with particular characteristics or sample from the files until he finds the evidence linking the suspect to the crime. See Kerr footnote 92 above p 288.

passwords, records, and other evidence linking the computer and its owner to the crime.[194]

The difference in activities between physical and digital forensics has led to the concept of a digital 'crime' scene. Therefore, instead of treating the computer as a substance that needs to be identified, it must be treated as a secondary 'crime' scene.[195]

A persons' first tendency upon discovering that the network has been breached may be to open the log files, shut down the system, etc.[196] However, if there is a chance that the case will be presented for litigation, as little as possible must be done beyond disconnecting the system from the network and protecting the scene.[197]

The following must be adhered to:

- do not turn off the system;[198]
- do disconnect the system from the network;[199]

---

194 See Kerr footnote 92 above p 289.

195 When seen this way, the same principles that are used to process a room where jewellery was stolen can be used to process a server where credit card numbers were stolen – although the technology required to perform the process will be different. A computer itself is only one piece of physical evidence, but it can be processed to identify thousands of pieces of digital evidence and each of these can be analysed to identify ownership, location, and timing. The digital evidence can thus be analysed to produce similar characteristics as physical evidence. This is also due to the presumption that the investigation of billions of bytes of digital data is similar to the investigation of a house where an investigator must look at thousands of objects, fibres, and surface areas and use his/her experience to identify potential evidence that should be sent to a lab for analysis. See Carrier and Spafford footnote 7 above p 2.

196 See Shinder footnote 11 above.

197 This must be done to ensure that nobody else changes anything until computer forensic personnel arrive. See Shinder footnote 11 above.

198 Data that is in volatile memory (RAM) will be lost. See Shinder footnote 11 above.

199 If it stays connected, a hacker could cover his tracks by deleting log files and other evidentiary data. See Shinder footnote 11 above.
The best way to preserve digital evidence in its original state is to connect the computer to another computer onto which the digital information can be copied. This has already been discussed in Chapter 2. Just to recap, this can be done through a private network connection between the two computers. Data can be transferred over an Ethernet connection between the two computers (by connecting them both to a private hub that is not connected to any other network) or through a serial or USB connection. The contents of the original (source)

- do not use the system to do anything;[200]
- do not open files to examine them as this modifies the date/time stamp.[201]

4.4.2 The Perfect Tool

Computer tools that work with digital evidence must be shown to be accurate and not to modify the original evidence.[202] As with all scientific evidence, a computer tool must demonstrate (*Daubert*-test[203]) that it:[204]

- can be tested;
- has been subject to peer review/publication;
- has a known error rate;
- is generally accepted in the community.

Digital forensic techniques and tools must meet basic evidentiary and scientific standards to be allowed as evidence in legal proceedings.[205] In America, the American Society for Crime Lab Directors/Lab Accreditation Board[206] is the official body that accredits crime labs.[207] The board has developed standards

---

computer's memory should be transferred to the second (target) computer first. Transfer the memory contents in small increments so as not to overwrite what is already in memory. The contents of the source computers' hard disk should be copied to the target computer as a bit level image. That means the image is an exact copy of all information on the source disk, including slack space. It is best to use software designed specifically for forensic purposes. Programs used by law enforcement forensics experts include EnCase, made by Guidance Software (which offers a graphical interface) and the command line tools made by New Technologies Inc. (NTI). Some investigators also use programs such as Symantec's Ghost, which can make bitstream images using the "ir" or "image raw" switch. See Shinder footnote 11 above.

200 No programs should be run. Evidentiary data could inadvertently be overwritten. In some cases, the hacker might have planted a program that will erase data when triggered by some event (such as opening or closing a program). See Shinder footnote 11 above.

201 See Shinder footnote 11 above.

202 See Anon. footnote 145 above.

203 As compiled by the court during the *Daubert*-case footnote 30 above.

204 See Anon. footnote 145 above.

205 Craiger et al 'Law Enforcement and Digital Evidence' 2005 HYPERLINK http://csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf 11 Oct.

206 Herein after referred to as ASCLD/LAB.

207 See footnote 205 above p 1.

relating to establishing the validity and acceptability of forensic techniques, tools, and accreditation of individual crime labs.[208]

In the context of digital forensics labs there is a standard requirement that software and hardware must be validated prior to its use in examinations.[209] In the context of digital evidence, the Scientific Working Group for Digital Evidence[210] defines the term validation as 'an evaluation to determine if a tool, technique or procedure functions correctly and as intended.'[211]

The National Institute for Standards and Technology's[212] Computer Forensics Tool Testing division[213] is one government entity that formally tests computer forensics software.[214]

Forensic tools acquire data from a device in one of two ways: physical acquisition or logical acquisition:[215]

- physical acquisition implies a bit-by-bit copy of an entire physical store;[216]

---

208 ASCLD/LABs criteria for accreditation consist of standards covering crime lab management and operations, personnel, and physical plant. Each standard is labelled as desirable, important, or essential, depending upon its importance and requirement for meeting ASCLD/LAB specifications. Labs seeking accreditation must meet 100% of the essential criteria, 75% of the important criteria, and 50% of desirable criteria. See footnote 205 above p 1.

209 Tools, techniques and procedures should be validated prior to initial use in digital forensic processes. See footnote 205 above p 19.

210 Herein after referred to as SWGDE.

211 Software validation has long been an important component of software design and development. However, it plays a crucial role in digital forensics because there exists the potential consequence of denying a defendant's constitutional rights to life and liberty. Validation testing is critical to the outcome of the entire examination process and validation, based on sound scientific principles, is required to demonstrate that examination tools (hardware and software), techniques and procedures are suitable for their intended purpose. See footnote 205 above p 19.

212 Herein after referred to as NIST.

213 Herein after referred to as CFTT.

214 CFTT performs extremely rigorous scientific tests to validate software tools used in digital forensic examinations. See footnote 205 above p 21.

215 Ayers and Jansen 2004 *National Institute of Standards and Technology Interagency Report* 6.

216 For example, a disk drive or RAM chip.

- while logical acquisition implies a bit-by-bit copy of logical storage objects[217] that reside on a logical store[218].[219]

In general, physical acquisition is preferable, since it allows any data remnants present[220] to be examined, which otherwise would go unaccounted in a logical acquisition.[221] Physical device images are generally more easily imported into another tool for examination and reporting.[222] However, a logical acquisition provides a more natural and understandable organization of the information acquired, and thus it is preferable to do both types of acquisition, if possible.[223]

4.4.3 US Agencies that provide assistance

The US National Association of Securities Dealers[224] and other government agencies issued new regulations and guidelines that expand existing e-record retention requirements.[225] Agents and prosecutors who need more detailed advice on how to handle digital evidence can rely on several resources for further assistance.[226]

The Office of International Affairs provides expertise in the many computer crime investigations that raise international issues and the Office of Enforcement Operations provides expertise in the wire-tapping laws and other privacy

---

217 For example, directories and files.
218 For example, involving several disk drives.
219 The difference lies in the distinction between memory as seen by a process through the operating system facilities (i.e., a logical view), versus memory as seen by the processor and other related hardware components (i.e., a physical view). See footnote 205 above p 6.
220 For example unallocated RAM or unused file system space.
221 See footnote 205 above p 6.
222 See footnote 205 above p 6.
223 See footnote 205 above p 6.
224 Herein after referred to as NASD.
225 See footnote 3 above p 5.
226 At the federal district level, every United States Attorney's Office has at least one Assistant U.S. Attorney who has been designated as a Computer and Telecommunications Coordinator ("CTC"). Every CTC receives extensive training in computer-related crime, and is primarily responsible for providing expertise relating to the topics covered in this manual within his/her district. Further, several sections within the Criminal Division of the United States Department of Justice in Washington, D.C., have expertise in computer-related fields. See Computer Crime footnote 70 above.

statutes.[227] Also, the Child Exploitation and Obscenity Section provide expertise in computer-related cases involving child pornography and child exploitation.[228]

Finally, agents and prosecutors can always contact the Computer Crime and Intellectual Property Section directly both for general advice and specific case-related assistance.[229]

4.5 Conclusion

With the vast majority of documents being created on computer systems, and with so many written communications taking place electronically, attorneys now have both the luxury of easily and quickly validating a controversy and the responsibility of doing so.[230] This is why practising attorneys and law students must have thorough knowledge of information technology law.

Electronic and digital data discovery is a potent tool that litigators are using at an accelerating pace. Numerous evidentiary objections are available in seeking to exclude the evidence. Care must therefore be taken in the extraction, preservation and presentation of electronic data to overcome the common objections.

The decision of the judge in the case *In re Search of 3817 W. West End*[231] could be used in South Africa to promote the inclusion of digital evidence in litigation. As required by the court in this American case, a South African court may also impose the requirement that the government must first agree to abide by pre-

---

227 See Computer Crime footnote 70 above.
228 See Computer Crime footnote 70 above.
229 See Computer Crime footnote 70 above.
230 See Lewis footnote 5 above.
231 *In re Search of 3817 W. West End,* 321 F. Supp. 2d. 953 N.D. Ill. 2004. See also Kerr footnote 92 above 316.

approved computer search protocol outlining the steps that would be taken to locate the evidence stored in the hard drive.[232]

America has extensive Federal and State case law with regard to the procedures to be followed in obtaining digital data and the use of digital evidence in courts of law. This legislation appears to work effectively. The American legislation has compiled with the Fourth Amendment right as starting point. This allows for the effective regulation of possible search and seizure infringements to the citizens' Fourth Amendment right, all the while ensuring enough legal room for the investigators to search for and seize all the necessary digital devices and digital evidence that may be required to win a case.

A complete incorporation of American evidence rules, and the techniques and procedures applied by their computer forensic investigators in searching for and seizing digital evidence, will not be recommended or fit within the South African legal context. They may however provide a basic guideline for the formulation of new South African legal rules and regulations by law enforcement and computer forensic investigators. The use of expert testimony as to the reliability and security of the application of these legal rules and regulations will comply with the admissibility requirement of proving the authenticity of the evidence, and will also provide for the judicial recognition of these procedures and digital evidence.

A point of concern to all those reading this document should be, as Jessen[233] explained:

> It is not a question any more if your client is going to be asked to provide electronic media and data in litigation…it's a question of when.[234]

---

232 If a South African court recognises and applies this American courts' pre-condition to collecting digital evidence, the application can serve as a basic guide to the development of new South African rules and regulations for the collection of admissible digital evidence.

233 American electronic evidence expert John Jessen.

234 Richard 1999-2000 *Whittier Law Review* 477.

Chapter 5
Comparative analysis

In this chapter a comparative analysis will be made between the South African Law of Evidence and the position in the American law, in particular those legal matters concerned with the use of digital evidence.

Due to the similarities between these two legal systems, the possibility of applying the American rules and regulations with regard to the collection and preservation of admissible digital evidence within the South African law of evidence by South African computer forensic investigators, should not pose too many problems. The two legal systems are historically different, and yet so many similarities exist between the applied laws of evidence.

5.1 Basic rules of evidence

The general rule in both legal systems is that the evidence presented must be relevant to the facts in question and that irrelevant evidence will not be admissible Therefore as long as evidence is material and relevant[1] it is admissible, unless there is some other rule of evidence which excludes it.[2] Evidence will be relevant if it can be used to prove either primary or secondary facts in question.[3]

It can be classified into three categories:[4]

- real or physical evidence, which consists of tangible objects that can be seen and touched;

---

1 Evidence that has no weight can have no probative value and is irrelevant.
2 See *R v Schaube-Kuffer* 1969 (2) SA 40 (RA) at 50B-C. See Schmidt *Bewysreg* 361.
3 See Schmidt footnote 2 above p 363. Primary facts are required for a finding in favour of one of the opposing parties. The secondary facts support a finding, but are not necessary – the finding can also be acquired by another means.
4 See Chawki 'The Digital Evidence in the Information Era' 2004 HYPERLINK http://www.crime-research.org/articles/chawki1/ 25 Jul p 1.

- testimonial evidence, where the testimony of a witness can be given during a trial, based on a personal observation or experience;
- circumstantial evidence, which is based on a remark, or observation of realities that tends to support a conclusion, but not to prove it.

In essence therefore, these two legal systems basic rules with regard to evidence are very much the same.

5.1.1 Admissibility

In both legal systems there are similar rules for determining admissibility of evidence. When a party tenders a document, he/she will usually be required to produce evidence to satisfy the court of its authenticity.[5] The basic prerequisites of admissibility are relevance,[6] materiality, and competence.[7]

The admissibility of electronic evidence revolves around three questions:[8]

- Can the evidence be properly authenticated?
- Does the Best Evidence Rule require the original of the document to be produced?
- Is the document hearsay and not subject to an exception?

In order to answer the question of the admissibility of the digital evidence, it must be established.[9]

- Who created the document or electronic file/information;
- Its contents;

---

5 See Schmidt footnote 2 above p 318. The evidence has to be tendered by a witness who can prove its authenticity and that it is what it purports to be.

6 Evidence is *relevant* when it has any tendency in reason to make the fact that it is offered to prove or disprove either more or less probable - Federal Rules of Evidence 401. See DiCarlo 'A Summary of the Rules of Evidence: The Essential Tools for Survival in the Courtroom' HYPERLINK http://www.dicarlolaw.com/RulesofEvidenceSummary.htm 25 Jul.

7 See DiCarlo footnote 6 above.

8 The opinion of M Overly as discussed in Strydom 'Computer Evidence' HYPERLINK http://www.crimeinstitute.ac.za/2ndconf/papers/strydom.pdf 25 March.

9 The opinion of M Overly as discussed in Strydom footnote 8 above.

- How it was created;
- That it has not been altered, either intentionally or unintentionally.

In both systems, the strictness, with which the reliability requirement is applied to software-derived evidence, should rest on its importance as evidence and the extent to which its probative value depends on its accurate and unchanged condition.

South African courts and legislation provide the basic factors that must be proven to ensure the admissibility of digital evidence. The courts and legislation does however, not provide investigators with specific rules and regulations as to what techniques and procedures must be used to ensure the integrity and admissibility of digital evidence.

However, American case law does exist that specifically prescribes what requirements must be met by the techniques and procedures used to collect digital evidence. The case law also requires that the techniques and procedures applied should have been judicially approved by a judge before it may be used to collect digital evidence.

In both systems it is shown that the standards for authenticating computer records are the same as for authenticating other records. The degree of authentication does not vary simply because a record happens to be, or has been at one point, in digital or electronic form. For example, witnesses who can testify to the authenticity of computer records need not have special qualifications. The witness does not need to have programmed the computer himself, or even need to understand the maintenance and technical operation of the computer. Instead, the witness simply must have first-hand knowledge of the relevant facts to which he/she testifies.[10]

[10] See Standler 'Computer Crime' 1999, 2002 HYPERLINK http://www.rbs2.com/ccrime.htm 11 Oct.

Therefore, the authenticity common-law requirements set for documentary evidence may be interpreted and used by a party wishing to introduce digital evidence of statements contained on a digital device. The party will fulfil the above requirements by supplying evidence as to the correct and effective workings of the digital device. This can be done by an expert or at least a person that is familiar with the workings of and storage of data on the digital device. The testimony of such a witness must show that the device on which the digital evidence was stored and obtained from was working correctly and effectively, and that the techniques and procedures followed with regard to the collection and preservation of the digital evidence are sufficient to ensure the integrity of digital evidence.

5.1.2 The Hearsay Rule

This evidentiary rule is very much defined and applied in the same manner in both legal systems. Both systems have legislative definitions of hearsay that codify the common-law hearsay rules. Both systems' regulation of this aspect is very similar, and both systems provide for exclusions to this rule.[11] If these exclusionary situations exist, the evidence may still be admitted even if it is hearsay.

---

[11] In SA the prohibition against hearsay is regulated by S 3 of the *Law of Evidence Amendment Act* 45 of 1988. In terms of section 3(1)(c) the court has a discretion to allow hearsay evidence if it will, within the court's judgement, be in the interests of justice to allow it - See *Hlongwane and Others v Rector, ST Francis Colledge, and Others* 1989 3 SA 318 (D) at 324E-F.
In the USA, the prohibition against hearsay is a barrier and standard to which courts have subjected computer-derived evidence. Various business records exceptions have been codified, see for example Federal Rule of Evidence 803(6). "Computer data compilations are admissible as business records under Federal Rule of Evidence 803(6) if a proper foundation as to the reliability of the records is established" - *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990). See also Kenneally 2001 *Virginia Journal of Law and Technology*.
Alternatively, proponents of computer-derived evidence may have bypassed the hearsay exception by convincing the court that such digital evidence constitutes a product of a device that performed pre-programmed tasks on admissible data input, as for example with a radar gun or a calculator. Computerised printouts of phone traces, for example, were not hearsay in one case because they did not rely on the assistance, observations, or reports of a human declarant, and it was found that the printouts were "merely the tangible result of the computer's internal operations." See also *State v. Armstead*, 432 So. 2d 837, 839-41 (La. 1983).

5.1.3 The best evidence rule

Both legal systems have similar definitions of the best evidence rule. In its widest form, this rule requires that only the best evidence of a fact in question is admissible, and accordingly that the best evidence thereof will always be admissible.[12]

The views of some South African legal scholars however is that the best evidence rule can and is no longer applied in the South African legal system.[13] These views are supported by the fact that, apart from the rule that secondary evidence of a document may only be tendered if the original is no longer available, there are no existing regulations that require that the best evidence of a fact will always be admissible, or that weaker evidence than the best evidence will never be admissible.[14]

In the USA the Uniform Federal Rules of Evidence establish the criteria for producing records that can be admitted into evidence.[15] The best evidence rule thus permits records to be introduced as a primary form of evidence, but also specifies that original records are preferred.[16]

This position of the best evidence rule in America, however, can also no longer be upheld in the real world of technology. Modern record technology systems usually differ in establishing processes or systems that produce accurate

---

12 For example, a party cannot rely solely on the testimony of an individual who knows something about a subject when another individual is available who is thoroughly familiar with the facts in the matter.

13 See Schmidt footnote 2 above p 369.

14 See Schmidt footnote 2 above p 369.

15 Some of the major provisions found in these laws include making the record at or near the time of the event, obtaining information for the record by or from somebody with knowledge, producing the record in the regular course of business and providing a custodian or other qualified person as a witness to testify regarding the methods used to create the records. Anon. 'The Best Evidence Rule is Dead' HYPERLINK http://www.irch.com/articles/articl11.htm 25 Jul.

16 In the Uniform Federal Rules of Evidence there is a preference for original records. Rule 1002 thereof specifies the requirement for original records as follows: 'To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required except as otherwise provided in these rules or by statute.'

results.[17] One might argue that the best evidence rule should be changed to indicate that accurate records, regardless of form, can be introduced in evidence.

5.2 Techniques and procedures to ensure the admissibility of digital evidence

5.2.1 South African case law in comparison with American case law

Digital evidence poses a significant problem to legal representatives in South Africa. The specific legislation with regard to digital evidence is very broadly formulated and there are very few South African court precedents that give sufficient guidance as to which procedures need to be followed when computer forensic investigators obtain digital evidence in order to ensure its admissibility.

Both legal systems provide or have definitions of the word 'document' that make provisions for digital documents,[18] computer print-outs and other computer-generated or digital device –generated information.[19] As long as the information or data can be reproduced in a manner that will not affect its integrity and authenticity, and can be examined or read in paper-document form or displayed on a screen, it will comply with the definition.

The SA court will require a high degree of relevance before it will receive evidence which involves a lengthy investigation of collateral issues or is likely to

---

17 The quality of records produced by records technology systems may surprise most legal purists. They have continually argued that since information can be manipulated during reproduction or within a computer system, the records are inherently less reliable. This view, however, is not always correct. Modern record technology systems can produce records that are more accurate than paper-based systems. See Anon. footnote 15 above.

18 As from the 1st of January 1996, the Illinois Supreme Court Rule 201 defined the word 'documents' as including all retrievable information in computer storage.

19 In SA the court held in *S v Harper* 1981 (1) SA 88 (D) that computer print-outs are 'documents' in the ordinary meaning of that expression. According to legislation, for example Section 221(5) of the *Criminal Procedure Act* 51 of 1977, the definition of a document will also include a device through which information is stored or recorded. See also Schmidt footnote 2 above p 347.

cause prejudice or confusion, or raise difficult questions of credibility.[20] On the other hand, the court must consider all material which may assist it to reach a proper conclusion.[21]

However, the view in both legal systems is also that the law governing digital evidence lags behind the reality of cyber-crime,[22] and that both systems have few legal precedents to guide judges.[23] It also appears from both legal systems that the courts treat digital evidence as documents that carry the same burden of proof of authenticity as other documents do. The data stored in a computer or similar device as well as any print-out or other output readable by sight, must however be shown to reflect the data accurately, and must be considered an 'original'.[24]

In both legal systems the parties wishing to introduce digital evidence will be able to prove its authenticity by providing the testimony of a witness who can speak to the identity and accuracy of the computer-derived evidence. The witness who testifies to the authenticity of computer records need not have special

---

20 See *Delew v Town Council of Springs* 1945 TPD 128. See also Hoffmann and Zeffertt *The South African Law of Evidence* 24.

21 See Hoffmann and Zeffertt footnote 20 above p 24. See also *Shabalala v The Attorney General of Transvaal & The Commissioner of the South African Police; Gumede v The Attorney General of Transvaal* 1995 1 SACR 88 (T). Here the court held that: '...the applicants *in casu* are entitled to invoke section 23 (of the Constitution, 1993 – right to access to information) for the purpose of obtaining access to all information held by the Attorney General in so far as such information is required for the exercise or protection of their right to a fair trial and in particular, to adduce and challenge evidence.' This may be grounds enough for an argument to include digital evidence that will be relevant to the facts in issue. If this digital evidence is not admitted, and if it is the best evidence available to prove or disprove a fact in question, by not including or admitting it into evidence one may be prevented from having a fair trial.

22 Coren 'Digital evidence: Today's fingerprints. Electronic world increasingly being used to solve crimes' HYPERLINK http://www.cnn.com/2005/LAW/01/28/digital.evidence/index.html 10 March p 2.

23 Judges often have little experience in the ever-changing world of digital technology. See footnote 22 above p 2.

24 Forensically obtained bit stream copies are considered original. Digital signatures are used by digital forensics specialists to prove authenticity and originality. Print-outs of digital data, although considered original, lose 'meta data' - data about the time of creation, location of the data on the media, etc. Forensic digital copies maintain all metadata.

qualifications.[25] Instead, the witness must simply have first-hand knowledge of the relevant facts to which he/she testifies.[26]

No South African case law exist which provide guidance on what techniques and procedures should be followed by computer forensic investigators when collecting digital evidence to ensure its authenticity and admissibility. In America, however, some judges have restricted the conduct of computer forensic searches by law enforcement, insisting that officers follow certain procedures or methods.[27]

Two very important cases with regard to the use of digital evidence and the requirements set by American courts for authenticating such evidence are *United States v. Weatherspoon*[28] and *In re Search of 3817 W. West End.*[29]

The case of *United States v. Weatherspoon*,[30] involved the presentation of thorough, all-encompassing evidence of computer input procedures for admissibility of computer print-outs. In this case, the U.S. Government provided evidence of its input procedures, the accuracy of its input procedures,[31] its monthly testing for internal programming errors, and its use and maintenance of the printouts in the ordinary course of business activities.[32] The panel in the

---

25 The witness does not need to have programmed the computer himself, or even need to understand the maintenance and technical operation of the computer. See *United States v. Salgado*, 250 F.3d 438, 453 (6th Cir. 2001).

26 See Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations' 2002 HYPERLINK http://www.cybercrime.gov/s&smanual2002.htm 11 Oct.

27 See Coren footnote 22 above p 2. In *In re Search of 3817 W. West End,* 321 F. Supp. 2d. 953 N.D. Ill. 2004 a judge refused the government's request for a warrant to search a home computer unless the government first agreed to abide by pre-approved computer search protocol outlining the steps that would be taken to locate the evidence stored on the hard drive. The judge refused to allow the search without a specific judge-approved search protocol on the basis that doing so would grant the investigators a license to roam through everything in the computer. See also Kerr 2005 *Columbia Law Review* 316.

28 *United States v. Weatherspoon*, 581 F.2d 595 (7th Cir. 1978).

29 *In re Search of 3817 W. West End,* 321 F. Supp. 2d. 953 N.D. Ill. 2004. See Kerr footnote 27 above p 316.

30 *United States v. Weatherspoon*, 581 F.2d 595 (7th Cir. 1978).

31 The accuracy was shown to be within two percent.

32 *United States v. Weatherspoon*, 581 F.2d 595 (7th Cir. 1978) at 598. See also Stoner 1999 HYPERLINK http://researchnotebook.com/FoleyLardner.pdf 15 Oct. p 7.

Briscoe-case,[33] however, noted that an extensive showing such as in *Weatherspoon*[34] is not required in every case as a prerequisite to admitting computer records.[35]

The decision of the judge in the case *In re Search of 3817 W. West End*[36] could be used in South Africa to promote the inclusion of digital evidence in litigation. The court in this case set specific requirements to be complied with before a search and seizure warrant would be issued for a computer search. Such specific requirements that must first be agreed to and abided by, or pre-approved computer search protocol that outline the steps that would be taken to locate the evidence stored in the hard drive may also be applied in and by a South African court.

If a South African court recognises and applies this American courts' pre-condition to collecting digital evidence, the application can serve as a basic guide to the development of new South African rules and regulations for the collection and preservation of admissible digital evidence.

It is therefore very important to note that America does actually have case law providing for the application of specific procedures and techniques when collecting digital evidence.

5.2.2 South African legislation in comparison with American legislation

Both systems have similar privacy rights[37] protection, and also have similar provisions on expert witness[38] testimony.

---

33 *United States v. Briscoe*, 896 F.2d 1476 (7th Cir. 1990).

34 *United States v. Weatherspoon*, 581 F.2d 595 (7th Cir. 1978).

35 *United States v. Briscoe*, 896 F.2d 1476 (7th Cir. 1990) at 1494. The *Croft* panel made a similar comment. *United States v. Croft*, 750 F.2d 1354 (7th Cir. 1984) at 1365. See also Stoner footnote 32 above p 8.

36 See footnote 29 above.

37 S 14 of the *Constitution of the Republic of South Africa*, 1996 and Ss 50 and 51 of the *Electronic Communications and Transactions Act* 25 of 2002. The most important American

In SA the most important legislation with regard to the use of digital evidence is the *Electronic Communications and Transactions Act*[39] which has application to both civil and criminal matters. SA does not have specific laws of evidence for each province, but only adheres to national laws. There is however the possibility of each provincial Police department having and applying their own legally admissible investigation techniques and procedures to collecting evidence. Sadly, some police departments in South Africa are very ill-equipped to sufficiently deal with digital evidence.

The ECT Act does not provide a definition of digital evidence. Data and data messages are however defined. In accordance with this definition, digital evidence can be included to that of a data message as it is also generated, sent, received or stored by electronic means and a stored record.[40] The ECT Act provides a broad regulation with regard to the use of digital evidence by providing guiding factors that have to be proven on which the evidential weight of data

---

federal legislation with regard to privacy issues are the provisions and rights of citizens contained in the Fourth Amendment and the provisions of the *Electronic Communications Privacy Act* 18 U.S.C. §§ 2701-2712 (herein after referred to as ECPA).

38 Rule 702 of the Federal Rules of Evidence provides that in order for a witness to be qualified as an expert, the expert must be shown to have "knowledge, skill, experience, training, or education" regarding the subject matter involved. The testimony of this witness will have to prove that the techniques and procedures used to collect the evidence can be regarded or shown to be reliable – thus adding the methods reliability to the evidence obtained through the use thereof.

39 *Electronic Communications and Transactions Act* 25 of 2002. Herein after referred to as the ECT Act.

40 Including this American definition of digital evidence into the definitions of data and data messages in the *Electronic Communications and Transactions Act* 25 of 2002 will however have to be done by interpretation of the provisions of this act by the courts. In order to facilitate such an interpretation a party may inform the court of this definition and application thereof in America. The applicable rules and regulations with regard to digital evidence in America will however only have persuasive effect in a South African court and the court may take this foreign law into consideration in interpreting the South African legislation. Fundamental rights to access to information contained in S 32 of the *Constitution of the Republic of South Africa*, 1996 was given statutory effect in the *Promotion of Access to Information Act* 2 of 2002 S 50(1) (a), which requires such access to be 'Reasonably required for exercise or protection of right' – see in this regard *Davis v Clutchco (Pty) Ltd*, 2003 3 All SA 561; 2004 1 SA 75 (C). See also further the right to a fair and impartial hearing contained in S 34 of the *Constitution of the Republic of South Africa*, 1996.

messages will depend, and it also has made provision for the protection of privacy rights during these searches and seizures.

Even though there are provisions in the act relating to the search of a building in order to seize a 'suspect' device or computer,[41] it does not provide for specific steps to be taken in the handling of such a 'suspect' device in order not to compromise the digital data contained therein. The ECT Act does however give broad legislative guidance on what has to be proven in order to ensure that digital evidence is admitted as proof of a fact in question in a court of law. The relevant rules and regulations with regard to the applicable techniques and procedures that have to be applied by computer forensic investigators to collect and ensure admissible digital evidence will have to be provided for by case law in the future. However for the time being, these rules and regulations will have to be developed by computer forensic investigators and the South African Police Services.

In America, on the other hand, the law of evidence is regulated by the Federal Rules of Evidence and each separate state has its own rules and regulations with regard to the law of evidence, most of which are very similar to the Federal Rules.[42] The American legislation makes sufficient provision for the requirements that must be complied[43] with during the application of the techniques and procedures necessary for the effective collection and preservation of admissible digital evidence.

---

41 See S 82 of the *Electronic Communications and Transactions Act* 25 of 2002.

42 Each of the US states has their own set of evidential rules and their own state court cases to which they must adhere. The federal rules of evidence will be applied in every state as a general guideline.

43 For example, see Rule 901(b) (9) of the Uniform Rules of Evidence reflects what the criteria for introducing records into evidence are. The rule provides that records or other evidence can be admitted in evidence if the proponent provides evidence describing a process or system used to produce a result and shows that the process or system produces an accurate result. The accuracy of the process or system used to produce the result will determine the legal acceptance of the records.

5.2.3 Current South African investigations in comparison with current American investigations

The techniques used in South Africa are mostly based on those applied to physical investigations. The few investigators that come into contact with possible digital evidence also may not have sufficient knowledge of how to ensure that the device and information contained in it are not compromised. Those that do must have sound knowledge of computer forensics, and are appointed as computer forensic investigators. The techniques and procedures applied by these computer forensic investigators appear to have originated in America.[44] Apart from the fact that financially our police force is unable to have computer crime labs at every police station, the officers will most likely not have the required knowledge or know-how to secure the integrity of digital evidence.

To overcome these obstacles, in America provision is made for specific agencies that provide assistance to investigators, field agents and prosecutors who need detailed advice and guidance on how to handle digital evidence.[45] Incorporating a similar system in South Africa will provide the skilled assistance that is needed for law enforcement officials and investigators that may not have extensive experience with the collection and preservation of digital evidence.

Computer forensics experts in America and around the world have developed a detailed set of procedures that forensic analysts ordinarily follow when they seize and analyse a target's computer:

- First, the detectives ordinarily seize the computer and bring it back to a government forensic laboratory for analysis;
- Back at the lab, the analyst begins by generating a "bitstream" or "mirror" image of the hard drive;

---

44 Such as those followed by the South African Scorpions' computer crime investigation unit. The official name of the Scorpions is the Directorate of Special Operations.

45 See footnote 26 above.

- The analyst then performs his work on the copy rather than the original to ensure that the original will not be damaged or altered by the analyst's investigation;
- The analyst may try a range of techniques to locate the evidence sought;
- Assuming the suspect was not tipped off to the investigation and has not permanently erased the relevant files, the analyst may find master passwords, records, and other evidence linking the computer and its owner to the crime.

In America, computer searches may be executed in a variety of ways. A similar method applied may be applied in the formulation of a corresponding South African system. For the most part, there are four possibilities:[46]

- search the computer and print out a hard copy of particular files at that time;
- search the computer and make an electronic copy of particular files at that time;
- create a duplicate electronic copy of the entire storage device on-site, and then later recreate a working copy of the storage device off-site for review; and
- seize the equipment, remove it from the premises, and review its contents off-site.

Computer tools that work with digital evidence must be shown to be accurate and not to modify the original evidence.[47] As with all scientific evidence, a computer tool must demonstrate that it:[48]

- can be tested;
- has been subject to peer review/publication;

---

46 See footnote 45 above.

47 See Anon. 'Digital Forensics Legal Summary: Federal Evidence Rule 901(a)' HYPERLINK http://dfc.cs.uri.edu/resources/LegalSummary.html 25 Jul.

48 *Ibid.*

- has a known error rate;
- is generally accepted in the community.

Digital forensic techniques and tools must meet basic evidentiary and scientific standards to be allowed as evidence in legal proceedings.[49]

5.2.4 Proposed techniques and procedures

A possible basis to work from for formulating a procedure to be used to support the authenticity of digital evidence could be similar to the following formulated by the International Hi Tech Crime Conference in 1999:[50]

- upon seizing digital evidence, action should not change that evidence;
- when it is necessary for a person to access original digital evidence, that person must be forensically competent;
- all activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review;
- an individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession;
- any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

A proposed process model for digital investigations must meet the following requirements:[51]

- it must be based on the existing theory for physical investigations;
- it must be practical and follow the same steps that an actual investigation would take;

---

49 Craiger et al 'Law Enforcement and Digital Evidence' 2005 HYPERLINK http://csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf 11 Oct.

50 See Shinder 'Preserving Digital Evidence to Bring Hackers and Attackers to Justice' 2005 HYPERLINK http://www.computerworld.com/securitytopics/security/story/0,10801,102157,00.html 11 Oct.

51 *Ibid.*

- it must be general with respect to technology and not be constrained to current products and procedures;
- it must be specific enough that general technology requirements for each phase can be developed;
- it must be abstract and apply to law enforcement investigations, corporate investigations, and incident response.

Searches for data and software must be examined in two groups:

(1) searches where the information sought is on the computer at the search scene; and

(2) searches where the information sought has been stored off-site, and the computer at the search scene is used to access this off-site location.[52]

When investigators deal with smaller networks, desktops personal computers and workstations, an attempt to justify the taking of the whole system should be based on the following criteria:[53]

- when an entire organization is pervasively involved in an ongoing criminal scheme, with little legitimate business, (in non-essential services); and
- evidence of the crime is clearly present throughout the network, an entire system seizure might be proper.[54]

Various models from which to launch a digital investigation have been proposed.[55] However the following model may be regarded as the most complete

---

52 See Chawki footnote 4 above.

53 In small desktop situations, investigators should seize the whole system, after requesting to do so in the affidavit, and should justify it by wording their affidavits in such a way so as to refer to the computer as a 'system', dependant on set configurations to preserve 'best evidence' in a state of original configuration. This can and often does include peripherals, components, manuals, and software. In addition to the above, investigators should make every effort to lessen the inconvenience of an on-site search. Some estimates of manual data search and analyses are 1 megabyte for every 1hour of investigation work. Based on this equation, a 1-Gigabyte hard drive can take up to 1000 hours to fully examine. This equation assumes that each piece of data is decrypted, decoded, compiled, read, interpreted and printed out. See Chawki footnote 4 above p 2.

54 See Chawki footnote 4 above p 2.

55 See footnote 50 above p 3.

and best option due to it incorporating the most necessary aspects from other models:[56]

An Abstract Process Model[57] which provides:

- Identification: Detect the incident or crime;
- Preparation: Prepare the tools, techniques, and obtain approval;
- Approach Strategy: Develop a strategy to maximize the collection of evidence and minimize the impact on the victim;
- Preservation: Isolate and secure the physical and digital evidence;
- Collection: Record the physical crime scene and duplicate digital evidence;
- Examination: Search for evidence relating to the suspected crime;
- Analysis: Determine significance and draw conclusions based on the evidence found. Repeat examination until a theory has been supported;
- Presentation: Summarise and provide an explanation of the final conclusions and theory;
- Return evidence: Return the evidence that was removed from the scene back to the owner.

5.3 Conclusion

The proposed way forward is based on the following key aspects:

- In essence both legal systems are very similar;
- The American law has developed a bit further and can provide guidance to South Africa, especially with regard to techniques and procedures that must be applied to ensure the integrity of digital evidence;

---

56 Researchers at the U.S. Air Force identified the common traits that various models had and incorporated them into an abstract process model. See footnote 50 above p 4.

57 Compiled by the U.S. Air Force. The Abstract Process Model provides a general framework that can be applied to a range of incidents, and it uses the examination and analysis phases to identify and collect digital evidence. See footnote 50 above p 4.

- Witness testimony must be used to testify about the techniques and procedures applied during investigations for digital evidence;
- If the witness testimony is accepted, this may lead to the recognition and application of American-based techniques and procedures for the collection of admissible digital evidence in South Africa.

In terms of both legal systems, a court must not discriminate against evidence due to it being in electronic format. However, the manner in which the electronic evidence has been collected and retained will still have an effect on the evidential value thereof.

Applying the techniques and procedures in South Africa, that are practically applied with very good results in America, as basis for developing our own rules and regulations with regard to the collection and preservation of admissible digital evidence, we will be able to provide greater legal certainty to those litigating parties who must rely on digital evidence.

The workings and partial application of another country's legislation, rules and regulations can merely facilitate a new approach to the present laws applicable in South Africa on this subject.

Chapter 6
Conclusion

Changes in technology often trigger changes in the law. By substituting the collection of physical evidence and eye witness testimony with the gathering of digital evidence, investigations involving computers and other digital devices will replace traditional mechanisms of search and seizure with different forms of surveillance, collection and new forms of forensic analysis.

Not only must computer forensic and cyber- investigators discover admissible digital evidence they must also do it in a lawful manner. Therefore all types of investigators must have a working knowledge of legal issues involved in computer forensics. They must know what constitutes a legal search of a stand-alone computer as opposed to a network; what laws govern obtaining evidence and securing it so that the chain of evidence is not compromised; what telecommunications may lawfully be intercepted or examined after they have been received; and what legally protected privacy rights employees and other individuals possess.

Because computer forensics is a relatively new field, investigative and legal norms are just now emerging. Little has been written about the legal requirements for admissibility of computer forensic evidence, or about the regulatory issues related to this new field. Computer and data forensics was all but unknown just a few years ago, but today it must be considered a standard and routine practice in all legal matters.

Digital evidence collection and -analysis is becoming an increasingly routine and essential part of criminal and civil investigations. Society's reliance on computers combined with the differences between physical evidence and digital evidence generates a need for re-thinking the techniques and procedures applied during

physical evidence investigations and these must be adjusted to sufficiently and effectively be applicable to digital evidence.

The South African Legislator has done its part by introducing the *Electronic Communications and Transactions Act* 25 of 2002 and with it new computer crimes law. It is however still more difficult to track down and prosecute those who intrude into our networks and steal our data, than catching and punishing those who break into individuals' homes or offices. One reason is the nature of digital evidence. To obtain a criminal conviction or win a civil case, evidence must be presented in court. However, in order to be admissible in a South African court of law, this evidence must be preserved and handled to ensure that it has not been altered in any way. Unfortunately, uninformed law enforcement personnel who are first responders and come into contact with a suspected device often inadvertently destroy the evidence - and along with it, any chance of winning or ensuring a strong case.

The largest obstacles preventing the admission of digital evidence are a lack of knowledge of digital evidence and a lack of guidance with regard to the techniques and procedures that must be followed by computer forensic investigators to secure and guarantee the authenticity of the digital evidence. Legal practitioners, forensic investigators, law enforcement as well as law students need sufficient knowledge of information technology law and the law of evidence with regard to the use of legally admissible digital evidence, simply because the world is becoming increasingly dependent upon modern technology and computer systems like the Internet.

American investigative institutions, legislation, and case law have provided procedural steps that must be taken with regard to the collection and use of digital data. These steps are put into place to ensure the integrity of the evidence, without unreasonably compromising the citizen's Fourth Amendment right or the rights protected in legislation specifically applicable to the use, search and seizure of digital evidence.

A complete incorporation of American evidence rules, and the techniques and procedures applied by their computer forensic investigators in collecting digital evidence, is not recommended nor will it be specifically suited within the South African legal context. The American procedures and techniques may however be used as basic guidelines for the formulation and incorporation of new South African legal rules applicable to digital evidence.

The South African legislator has provided, in the ECT Act, broad evidentiary requirements or factors that must be proven in order to admit digital evidence. The lack of practical application thereof, by the South African judiciary, with regard to which techniques and procedures must be followed to ensure compliance with these legislative factors and ensure the admissibility of digital evidence, has caused a *lacuna* within the South African law of evidence. The ECT Act is still a relatively young piece of legislation. In time, the courts will most likely supply South African legal practitioners and law enforcement with the guidelines needed to ensure the application of effective techniques and procedures to secure the integrity and admissibility of digital evidence.

Digital evidence will be admissible in a court of law if it can be proven to be authentic and relevant to prove the facts in question. However, this must be done by applying evidentiary rules that were not formulated with digital evidence in mind, and which were originally applied to traditional paper based or physical evidence.

For the time being, the best way to proceed is to provide expert evidence as to the reliability and security of the presently applied techniques and procedures during investigations to collect and preserve digital evidence. It must also be proved that these procedures ensure the integrity of the digital evidence, and that the digital evidence therefore complies with the authenticity requirement for admission of the evidence.

Although the basic rules of the law of evidence do not exclude the use of digital data as evidence in South Africa, digital data is not often used as evidence in South African courts. Digital data is a valuable source of evidence. The use thereof will increase in the future.

The use of digital data as evidence will be placed on a more secure footing if generally accepted rules and procedures exist that can ensure the originality and authenticity of digital data. The provisions of the American law can give assistance in this regard. This can happen either by the courts referring to the American position or specific rules and procedures being promulgated by the legislature to ensure the originality and authenticity of digital data.

Chapter 7
Bibliography

Books

D

Du Toit *Basic computer skills*

Du Toit A *Basic computer skills 2000 and beyond* 2nd edition (Exclusive Training Development Auckland Park 2000)

H

Hoffmann and Zeffertt *The South African Law of Evidence*

Hoffmann LH and Zeffertt DT *The South African Law of Evidence* 4th edition (Butterworths Durban 1989)

S

Schmidt *Bewysreg*

Schmidt CWH *Bewysreg* 3rd edition (Butterworths Durban 1989)

W

Wilson *Information Processing*

Wilson C *Information Processing & Technology: The preliminary Course* (Cambidge University Press 2002)

Z

Zeffertt et al *The South African Law of Evidence* 2003

Zeffertt DT, Paizes AP and Skeen A St Q *The South African Law of Evidence (formerly Hoffmann and Zeffertt)* (LexisNexis Butterworths Durban 2003)

Articles

Ayers and Jansen 2004 *National Institute of Standards and Technology Interagency Report*

Ayers R and Jansen W "PDA Forensic Tools: An Overview and Analysis" August 2004 *National Institute of Standards and Technology Interagency Report* (4) 1-67.

Bester and Matthew 1998 *Commercial Law Conspectus*

Bester A and Matthew J "Wreck on the Info-Bahn: Electronic Mail and the Destruction of Evidence" 1998 *Commercial Law Conspectus* Vol.6 75-88.

Carrier and Spafford 2003 *International Journal of Digital Evidence*

Carrier B and Spafford EH "Getting Physical with the Digital Investigation Process" Fall 2003 *International Journal of Digital Evidence* Vol.2(1) 1-20.

Coetzee 2004 *STELL LR*

Coetzee J "The Electronic Communications and Transactions Act 25 of 2002: Facilitating Electronic Commerce" 2004 *STELL LR* Vol.3 501-521.

Fahey 2004 *SANS Institute*

Fahey D "Electronic Discovery & Computer Forensics" January 22, 2004 - *SANS Institute* (as part of GIAC practical repository).

Harris 2000 *National Archives of South Africa*

Harris V "Law, evidence and electronic records: A strategic perspective from the global periphery" 2000 *National Archives of South Africa* April (The core research for this paper was conducted between July 1999 and January 2000. The writing was completed in April 2000.).

Kenneally 2001 *Virginia Journal of Law and Technology*

Kenneally EE "Gatekeeping Out of the Box: Open Source Software as a Mechanism to Access Reliability for Digital Evidence" Fall 2001 *Virginia Journal of Law and Technology* Vol.6(13).

Kerr 2005 *Columbia Law Review*

Kerr OS "Digital Evidence and the new Criminal Procedure" January 2005 *Columbia Law Review* Vol.105(279) 279-318.

Richard 1999-2000 *Whittier Law Review*

Richard KD "Electronic Evidence: To Produce or Not to Produce, That is the Question" 1999-2000 *Whittier Law Review* Vol.21 463-491.

Volonino 2003 *Communications of the Association for Information Systems.*

Volonino L "Electronic Evidence and Computer Forensics" October 2003 *Communications of Association for Information Systems.* Vol.12(Article 27) 1-24.

Legislation

SA

Civil Proceedings Evidence Act 25 of 1965

Computer Evidence Act 57 of 1983

Constitution of the Republic of South Africa, 1993

Constitution of the Republic of South Africa, 1996

Criminal Procedure Act 51 of 1977

Documentary Evidence from Countries in Africa Act 62 of 1993

Electronic Communications and Transactions Act 25 of 2002

General Law Third Amendment Act 129 of 1993

Law of Evidence Amendment Act 45 of 1988

Marine Living Resources Act 18 of 1998

Promotion of Access to Information Act 2 of 2002

Court Rules Applicable to this mini-dissertation:
Magistrates' Court Rule 23(4)

Magistrates' Court Rule 24(10)

Supreme Court Rules 35 (9) and (10)

Supreme Court Rule 36(10)

Supreme Court Rule 63

USA

Amendment IV of the United States Constitution of 1791 (Amendment IV of the United States Constitution came into operation on December 15, 1791)

Cyberspace Electronic Security Act of 1999 (CESA)

Electronic Communications Privacy Act (ECPA), 18 U.S.C. Sec. 2701-2712 (1986)

Federal Rules of Evidence

Sarbanes-Oxley Act of 2002 (SOX)

State Evidence Laws of Texas

Statutory Privacy Laws codified at: (U.S.C is the abbreviation for United States Code)
18 U.S.C. §§ 2510-22
18 U.S.C. §§ 2701-12
18 U.S.C. §§ 3121-27

Statutory Computer Crime Laws codified at:
15 U.S.C § 1644
17 U.S.C § 506(a)

18 U.S.C § 1029
18 U.S.C § 1030
18 U.S.C § 1343
18 U.S.C § 1361-2
18 U.S.C § 1831
18 U.S.C § 2314
18 U.S.C § 2319
18 U.S.C § 2510-11
18 U.S.C § 2701
47 U.S.C § 223

The Federal Electronic Signature in Global and National Commerce Act 2000

The Pen/Trap Statute 2001 - 18 USC Sec. 3121-3127

The Uniform Electronic Transactions Act 1999

The Wiretap Statute 1986 - Title III, amended 1986 (The Wiretap statute is commonly known as Title III, because it was first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 United States Code Sec. 2510-2522, amended in 1986)

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act - USA PATRIOT Act 2001

Case law

SA

Davis v Clutchco (Pty) Ltd, 2003 3 All SA 561; 2004 1 SA 75 (C)

Delew v Town Council of Springs 1945 TPD 128

Ex Parte Rosch 1998 1 All SA 319 (W)

Goliath v Fedgen Insurance 1994 2 PHF 31 (E)

Hlongwane and Others v Rector, ST Francis Colledge, and Others 1989 3 SA 318 (D)

Howard &Decker Witkoppen Agencies and Fourways Estates (Pty) Ltd v De Sousa 1971 3 SA 937 (T)

Narlis v South African Bank of Athens 1976 2 SA 573 (A)

Protea Assurance v Waverley Agencies 1994 3 SA 247 (C)

R v Schaube-Kuffer 1969 2 SA 40 (RA)

S v Harper and Another 1981 1 SA 88 (D); *S v Harper* 1981 2 SA 638 (D).

Secombe and Others v Attorney-General and Others 1919 TPD 270

Shabalala v The Attorney General of Transvaal & The Commissioner of the South African Police; Gumede v The Attorney General of Transvaal 1995 1 SACR 88 (T)

USA

Bourjaily v. United States, 483 US 171, 175 (1987)

Chambers v. Mississippi, 410 US 284, 302 (1973)

Daubert v. Merrell Dow Pharmaceuticals, 509 US 572 (1993)

In re Search of 3817 W. West End, 321 F. Supp. 2d. 953 (N.D. Ill. 2004)

Kumho Tire v. Carmichael, 526 U.S. 137, 147-49 (1999)

People v. Holowko, 486 N.E.2d at 878-79

State v. Armstead, 432 So. 2d 837, 839-41 (La. 1983)

United States v. Bonallo, 858 F.2d 1427, 1436 (9th Cir. 1988)

United States v. Briscoe, 896 F.2d 1476, 1494-95 (7th Cir. 1990)

United States v. Croft, 750 F.2d 1354 (7th Cir. 1984)

United States v. David, 756 F. Supp. 1385 (1991)

United States v. DeGeorgia, 420 F.2d 889, 893 n.11 (9th Cir. 1969)

United States v. Glasser, 773 F.2d 1553, 1559 (11th Cir. 1985)

United States v. Jackson 7th Circuit No. 99-2223

United States v. Riggs, 739 F.Supp. 414 (N.D.Ill 1990)

United States v. Salgado, 250 F.3d 438, 453 (6th Cir. 2001)

United States v. Scholle, 553 F.2d 1109, 1123-25 (8th Cir. 1977)

United States v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000)

United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998)

United States v. Vela, 673 F.2d 86, 89-90 (5th Cir. 1982)

United States v. Weatherspoon, 581 F.2d 595 (7th Cir. 1978)

United States v. Young Bros., Inc., 728 F.2d 682, 693-94 (5th Cir. 1984)

Zubulake v UBS Warburg S.D.N.Y. May 13, 2003

Websites

Anon. October 05, 2005 Anti-phishing 'posses' hunt criminals *United Press International* [Found on Internet] HYPERLINK http://www.physorg.com/news6992.html [Date of use 10 October 2005]

Anon. Digital Forensics Legal Summary: Federal Evidence Rule 901(a) [Found on Internet] HYPERLINK http://dfc.cs.uri.edu/resources/LegalSummary.html [Date of use 25 July 2005]

Anon. 2003 Discussion on Contents of *Understanding Evidence* LexisNexis Area of Law Summary [Found on Internet] HYPERLINK http://www.lexisnexis.com/lawschool/study/outlines/word/evid05.doc [Date of use 11 October 2005]

Anon. How do digital signatures work? How Stuff Works [Found on Internet] HYPERLINK http://computer.howstuffworks.com/computer-channel.htm [Date of use 23 September 2005]

Anon. The Best Evidence Rule is Dead...Except in the Mind of the Law! [Found on Internet] HYPERLINK http://www.irch.com/articles/articl11.htm [Date of use 25 July 2005]

Buchanan S March 2002 Digital Signatures and Public Key Encryption [Found on Internet] HYPERLINK http://afongen.com/essays/pke/ [Date of use 23 September 2005]

Burgess SG The Case for Electronic Discovery [Found on Internet] HYPERLINK http://adr.forensic.e-symposium.com/computerforensics/whitepaper.pdf [Date of use 23 September 2005]

Chawki M March 10, 2004 The Digital Evidence in the Information Era Computer Crime Research Centre [Found on Internet] HYPERLINK http://www.crime-research.org/articles/chawki1/ [Date of use 25 July 2005]

Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice July 2002 Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations [Found on Internet] HYPERLINK http://www.cybercrime.gov/s&smanual2002.htm [Date of use 11 October 2005]

Coren M Digital evidence: Today's fingerprints. Electronic world increasingly being used to solve crimes [Found on Internet] HYPERLINK http://cnn.law.printthis.clickability.com/pt/cpt?action=cpt&title=CNN.com+-+Digitalevidence [Date of use 10 March 2005]

Craiger JP, Pollitt M and Swauger J 4 January 2005 Law Enforcement and Digital Evidence (To appear in H. Bidgoli (Ed.), Handbook of Information Security. New York: John Wiley & Sons) [Found on Internet] HYPERLINK http://csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf [Date of use 11 October 2005]

DiCarlo V A Summary of the Rules of Evidence: The Essential Tools for Survival in the Courtroom [Found on Internet] HYPERLINK http://www.dicarlolaw.com/RulesofEvidenceSummary.htm [Date of use 25 July 2005]

Forensicon Court Orders Government to Submit Search Protocol Prior To Examining Seized Computer [Found on Internet] HYPERLINK http://www.forensicon.com/casesummaries/cs-3817.asp [Date of use 15 October 2005]

Goldston JK A Guide to Understanding Data Remanence in Automated Information Systems [Found on Internet] HYPERLINK http://www.finecrypt.net/datarem.html [Date of use 23 September 2005]

Harris DL and Gotell LS November 2000 Preparing Experts with Kumho in Mind (This article is reprinted with permission from the November 2000 issue of *The Practical Litigator*. © 2000 NLP IP Company) [Found on Internet] HYPERLINK http://www.lowenstein.com/new/kuhmo.html [Date of use 15 October 2005]

Hedges RJ May 16, 2005 Discovery of Digital Information [Found on Internet] HYPERLINK http://www.roscoepound.org/new/updates/2005hedges.pdf [Date of use 23 September 2005]

House of Representatives, Subcommittee on Crime, Committee on the Judiciary, Washington, DC Report 12 June 2001 Fighting Cyber Crime: Efforts by Federal Law Enforcement [Found on Internet] HYPERLINK http://commdocs.house.gov/committees/judiciary/hju72616.000/hju72616_1.htm [Date of use 11 October 2005]

Jackson W Justice issues guidelines for handling digital evidence [Found on Internet] HYPERLINK http://www.gcn.com/vol1_no1/daily-updates/26961-1.html [Date of use 10 March 2005]

Kelly J 2 May 2001 Terror groups hide behind Web encryption USA Today [Found on Internet] HYPERLINK http://www.usatoday.com/tech/news/2001-02-05-binladen.htm [Date of use 10 October 2005]

Kornblum J Preservation of fragile digital evidence by first responders [Found on Internet] HYPERLINK http://www.dfrws.org/dfrws2002/papers/Papers/Jesse_Kornblum.pdf [Date of use 10 March 2005]

Legal Resources 2005 Zubulake v. UBS Warburg [Found on Internet] HYPERLINK http://www.krollontrack.co.uk/legalresources/zubulake.asp [Date of use 15 October 2005]

Leggat H Hackers have a free ride in SA [Found on Internet] HYPERLINK http://estrategy.co.za/article.asp?pklArticleID=2542&pklIssueID=346&pklCategoryID.htm [Date of use 10 February 2005]

Lewis PG Data Forensics – The smoking gun may be a click away [Found on Internet] HYPERLINK http://www.forensicfocus.com/computer-forensics-smoking-gun.php [Date of use 10 March 2005]

McDowell M and Householder A US-CERT National Cyber Alert System ST04-018-Understanding Digital Signatures [Found on Internet] HYPERLINK http://www.UnderstandingDigital Signatures.htm [Date of use 15 March 2005]

McDowell M and Householder A US-CERT National Cyber Alert System ST04-019-Understanding Encryption [Found on Internet] HYPERLINK http://www.UnderstandingDigital Signatures.htm [Date of use 15 March 2005]

McGraw-Hill, Plummer WA, Hudson H and Morceau G Cheyney University of Pennsylvania Glossary of Computer Terms [Found on Internet] HYPERLINK http://www.cheyney.edu/documents/pdf/glossarycomputerterms.pdf [Date of Use 23 September 2005]

Murr GB How to Offer and Exclude Evidence: Conduct, Character, Remedial Measures: Common Relevancy Problems [Found on Internet] HYPERLINK http://www.bmpllp.com/CM/Publications-Articles/How%20to%20Offer%20and%20Exclude%20Evidence.pdf [Date of use 27 September 2005]

Shinder D June 2005 Preserving Digital Evidence to Bring Hackers and Attackers to Justice [Found on Internet] HYPERLINK http://www.computerworld.com/securitytopics/security/story/0,10801,102157,00.html [Date of use 11 October 2005]

Snyder JA and Morelock A Electronic Data Discovery: Litigation Gold Mine or Nightmare? [Found on Internet] HYPERLINK http://www.mobar.org/journal/2002/janfeb/snyder.htm [Date of use 11 October 2005]

Standler RB 1999, 2002 Computer Crime [Found on Internet] HYPERLINK http://www.rbs2.com/ccrime.htm [Date of use 11 October 2005]

Stoner BH 1 January 1999 Admissibility of Electronic Records Foley & Lardner [Found on Internet] HYPERLINK http://researchnotebook.com/FoleyLardner.pdf [Date of use 15 October 2005]

Strydom L Computer Evidence [Found on Internet] HYPERLINK http://www.crimeinstitute.ac.za/2ndconf/papers/strydom.pdf [Date of use 10 March 2005]

University of Georgia Office of Information Security [InfoSec] Enterprise Information Technology Services InfoSec Glossary of Terms [Found on Internet] HYPERLINK http://www.infosec.uga.edu/glossary.php?question=nq [Date of use 23 September 2005]

Van der Merwe M and Janse van Vuuren F Internet Contracts Cyberlaw@SA – Chapter 6 [Found on Internet] HYPERLINK http://www.cyberlawsa.co.za/cyberlaw/cybertext/chapter6.htm# [Date of use 21 September 2005]

Vecchiatto P Lawyers lick lips over ABSA Fraud Case [Found on Internet] HYPERLINK http://www.itweb.co.za/sections/internet/2003/0307291128.asp?S=IT%20in%20Banking&A=ITB&O=S [Date of use 11 February 2005]

Vos A 18 October 2004- 2005 Evidence Unlawfully Obtained Deneys Reitz Inc. [Found on Internet] HYPERLINK http://www.deneysreitz.co.za/news/news.asp?ThisCat=2&ThisItem=539 [Date of use 21 September 2005]

Wegman J Computer Forensics: Admissibility of Evidence in Criminal Cases [Found on Internet] HYPERLINK http://www.cbe.uidaho.edu/wegman/Computer%20Forensics%20AA%202004.htm [Date of use 11 October 2005]

Wikipedia The free encyclopaedia Computer Forensics [Found on Internet] HYPERLINK http://en.wikipedia.org/wiki/Computer_forensics [Date of use 25 July 2005]

Wikipedia The free encyclopaedia Fourth Amendment to the United States Constitution [Found on Internet] HYPERLINK http://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution [Date of use 25 July 2005]

Annexure A*

The following terminology will be encountered during a discussion concerning data storage and data storage devices:

- **Back Up** - The action of copying (or mirroring) important data to a second location or onto removable media Information given to you when you log into or otherwise access a system.[1]
- **Cache Memory** – High-speed storage that can be quickly accessed by the central processing unit (CPU[2]).[3]
- **CD-R** – Compact disk – recordable. WORM – disks (write once, read many times.) A CD burner is needed to write the data that is then permanent.[4]
- **CD-RW** – Compact disk – rewritable – a drive that can read and write to the CD-RW disk and read a CD-ROM.[5]
- **CD-ROM (Compact disk read-only memory) -** An acronym derived from compact disk-read only memory. A form optical **storage.** One compact disk can hold up to 250,000 text pages; it can also be used to store graphics, sound, and video.[6]
- **Data compression** - A procedure for reducing the volume of **data** so as to shorten the time needed to transfer the data.[7]

---

* This annexure contains definitions in addition to those discussed in the footnotes of this mini-dissertation and should not be regarded as a complete list of computer and data terminology.

1 University of Georgia Office of Information Security [InfoSec] Enterprise Information Technology Services 'InfoSec Glossary of Terms' HYPERLINK http://www.infosec.uga.edu/glossary.php?question=nq 23 Sept.

2 A CPU is Electrical circuits that control the movement of data, carry out instructions sent from peripheral devices, change the data according to the instructions and send instructions to peripheral devices. See Wilson *Information Processing* 271.

3 See Wilson footnote 2 above p 271.

4 See Wilson footnote 2 above p 271.

5 See Wilson footnote 2 above p 271.

6 McGraw-Hill, Plummer, Hudson and Morceau 'Cheyney University of Pennsylvania Glossary of Computer Terms' HYPERLINK http://www.cheyney.edu/documents/pdf/glossarycomputerterms.pdf 23 Sept. p 3.

7 See footnote 6 above p 5.

- **Disk -** A random-**access,** magnetically coated storage medium used to store and **retrieve** information.[8]
- **Disk drive** - The component of a **computer** into which a **disk** is inserted so that it can be reads or written on. [9]
- **Diskette -** A small, no rigid **disk** with limited **storage** capacity. Also know as a floppy disk.[10]
- **DRAM** – Dynamic random access memory.[11]
- **DVD** - Digital video disc (predicted to replace the CD-ROM).[12]
- **EDO RAM** – Extended data-out random-access memory.[13]
- **Emergency Disk** - Floppy disk that contains an unaffected copy of operating system.[14]
- **EPROM** – Erasable programmable read-only memory – variation of ROM chips that can have instructions altered or erased by the manufacturer.[15]
- **Flash memory** – Special silicon chips that are non-volatile. These chips are embedded on cards that can be inserted into many portable devices.[16]
- **Hard disk** - A rigid type of magnetic medium that can store large amounts of information.[17]
- **Hard disks** – Large capacity, inexpensive magnetic storage.[18]
- **Memory Cards** - Removable electronic storage devices, which do not lose the information when power is removed from the card. It may even be possible to recover erased images from memory cards. Memory cards can store hundreds of images in a credit card-size module. Used in a variety of devices, including computers, digital cameras, and Personal Data

---

8 See footnote 2 above p 6.
9 See footnote 6 above p 6.
10 See footnote 6 above p 6.
11 See Wilson footnote 2 above p 273.
12 See footnote 6 above p 7.
13 See Wilson footnote 2 above p 273.
14 See footnote 1 above.
15 See Wilson footnote 2 above p 274.
16 See Wilson footnote 2 above p 274.
17 See footnote 6 above p 9.
18 See Wilson footnote 2 above p 275.

Assistants (PDAs). Examples are memory sticks, smart cards, flash memory, and flash cards.[19]

- **Mirror image backups** - Backups that involve the backup of all areas of a computer hard disk drive or another type of storage media, e.g., Zip disks, floppy disks, Jazz disks, etc and exactly replicate all sectors on a given storage device. Thus, all files and ambient data storage areas are copied. Such backups are sometimes referred to as bit stream backups or 'evidence grade' backups and they differ substantially from standard file backups and network server backups.[20]
- **RAID** – Redundant array of independent storage disks – systems that use many disk drives within a single system box.[21]
- **RAM** – Random-access memory. Stores data and programs while they are in use by the system, that is, volatile memory.[22]
- **SRAM** – Static random-access memory.[23]
- **Storage -** The **memory** of a **computer.**

  External storage: A magnetic medium such as a **disk, diskette**, or tape used to store information; can be removed from the **computer.**

  Internal storage: An integral component of a **computer**; cannot be removed.

  Store: To place information in memory for later use.[24]

There are several ways to authenticate a person or information on a computer:

- **Checksum** - Probably one of the oldest methods of ensuring that data is correct, checksums also provide a form of authentication since an invalid

---

19 See footnote 1 above.
20 See footnote 1 above.
21 See Wilson footnote 2 above p 280.
22 See Wilson footnote 2 above p 280.
23 See Wilson footnote 2 above p 282.
24 See footnote 6 above p 17.

checksum suggests that the data has been compromised in some fashion.[25]

- **Cyclic Redundancy Check**[26] - CRCs are similar in concept to checksums. Polynomial division is used to determine the value of the CRC, which are usually 16 or 32 bits in length.[27]
- **Digital certificates** - To implement public key encryption on a large scale, such as a secure Web server might need, requires a different approach. This is where digital certificates come in. A digital certificate is essentially a bit of information that says the Web server is trusted by an independent source known as a Certificate Authority.[28]
- **Password** - The use of a user name and password provide the most common form of authentication.[29]
- **Private key encryption** - Private key means that each computer has a secret key or code that it can use to encrypt a packet of information before it is sent over the network to the other computer.[30]

---

25 A checksum is determined in one of two ways. Let's say the checksum of a packet is 1 byte long, which means it can have a maximum value of 255. If the sum of the other bytes in the packet is 255 or less, then the checksum contains that exact value. However, if the sum of the other bytes is more than 255, then the checksum is the remainder of the total value after it has been divided by 256. See Anon. How Stuff Works 'How do digital signatures work?' HYPERLINK http://computer.howstuffworks.com/computer-channel.htm 23 Sept.

26 Herein after referred to as CRC.

27 The good thing about CRC is that it is very accurate. If a single bit is incorrect, the CRC value will not match up. Both checksum and CRC are good for preventing random errors in transmission, but provide little protection from an intentional attack on your data. The encryption techniques below are much more secure. See Anon. footnote 25 above.

28 The Certificate Authority acts as the middleman and is trusted by the connected computers. It confirms that each computer is in fact that which it says it is. It then provides the public keys of each computer to the other. As an example of such an agency reference may be had to The Digital Signature Standard (DSS) which is based on a type of public key encryption method that uses the Digital Signature Algorithm (DSA). DSS is the format for digital signatures that has been endorsed by the US government. The DSA algorithm consists of a private key that only the originator of the document (signer) knows and a public key. See Anon. footnote 25 above.

29 The name and password are entered when prompted by the computer. The pair is checked against a secure file to confirm. If either the name or password does not match, no further access is allowed. See Anon. footnote 25 above.

30 The private key requires which computers will talk to each other and install the key on each one. Private key encryption is essentially the same as a secret code that the two computers must each know in order to decode the information. The code would provide the key to decoding the message. Think of it like this. A coded message is created to send to a friend where each letter is substituted by the letter that is second from it. So "A" becomes "C" and "B" becomes "D". A trusted friend has already been told that the code is "Shift by 2". The

- **Public key encryption** - Public key encryption uses a combination of a private key and a public key. The private key is known only to your computer while the public key is given by your computer to any computer that wants to communicate securely with it.[31]

message is received and decoded. The message seen by others will appear to be nonsense. See Anon. footnote 25 above.

[31] To decode an encrypted message, a computer must use the public key provided by the originating computer and its own private key. The key is based on a hash value. This is a value that is computed from a base input number using a hashing algorithm. The important thing about a hash value is that it is nearly impossible to derive the original input number without knowing the data used to create the hash value. Public key encryption is much more complex than this example but that is the basic idea. Public keys generally use complex algorithms and very large hash values for encrypting: 40-bit or even 128-bit numbers. A 128-bit number has a possible 2^{128} different combinations. That's as many combinations as there are water molecules in 2.7 million Olympic size swimming pools. Even the tiniest water droplet imagined has billions and billions of water molecules in it! See Anon. footnote 25 above.