I.T. FORENSICS: THE COLLECTION AND PRESENTATION OF DIGITAL EVIDENCE

Author:

Johann Hershensohn

Address:

Block D, 204 Rivonia Drive, Morningside, Johannesburg

P O Box 33641, Glenstantia, 0010

Contact numbers:

(w) 011 895 2000

(f) 011 895 2080

(c) 082 600 1175

Email:

johann.hershensohn@atosorigin.com

johann.hershensohn@csfs.co.za

ABSTRACT

This paper deals with the following concepts:

Digital evidence, IT forensics, the nature of digital evidence, the relevance of digital evidence, the digital audit trail, digital evidence and forensic science, the hearsay nature of digital evidence, documentary evidence and digital evidence, the best evidence rule, the role of digital evidence, the investigative framework, authorization to collect digital evidence, the acquisition of digital evidence, the analysis of digital evidence, reporting on digital evidence, the presentation of testimony relating to digital evidence.

INTRODUCTION

In starting this paper, I would like to refer to the following quote:

"As of this writing, most computers use magnetic media for their permanent storage. This media can be in the form of hard disks, floppy disks, or magnetic tape. What all of these have in common is that they are coated with a metallic oxide. Ferric (iron) oxide, which is the basic component of the coating of these media, and which is usually used in conjunction with cobalt or barium, is commonly called rust. Seizing this media, examining it, developing information from it and entering it into evidence at trial, is a process called computer forensics."[1]

In the past, when investigating a crime, or presenting evidence in a trial and or hearing, the traditional smoking gun was a letter, a jotted note on a piece of paper, or other paper based document.

Now days digital evidence such as e-mails, electronic documents, spreadsheets, databases, and other digital formats, form the crux of the evidence in a given dispute and or crime.

As a case example, in the *Duvenhage case*, a lady working for an insurance firm, was about to resign and take employ at a second insurance firm, along with her fiancé. Prior to leaving the employ of the first insurance firm, she accessed, and emailed sensitive information belonging to the first insurance firm, and which was crucial to their business. This was then forwarded to the email address of her fiancé, at the second insurance firm. She was arrested, and charged with

[1] US Department of Justice: FBI: Computer Analysis Response Team: Conducting searches in a computer environment Rev 2/21/97

contraventions of Sect 86(1) of the *Electronic Communications and Transaction Act 25 of 2002*. In this case the key aspects related to electronic data which was "stolen". [2]

It appears however that, in South Africa, we have not entirely kept up pace with these new developments, and today we find ourselves confronted with a situation where it appears that the South African courts are not adducing enough of these cases to provide us with a clear president of the law in this regard.

Fortunately we are able to draw on the vast experience of the United States of America, and the United Kingdom, when addressing this issue, and hence I will refer to some of the cases, documents procedures and policies that they have drafted in the recent past.

The main purpose of this paper is to provide a South African perspective on the collection, preservation and presentation of digital evidence in legal proceedings, as is evident from the title.

In order to achieve this, I will address the following aspects:

a) The nature of digital evidence

b) The Legal framework

c) The investigative process

THE NATURE OF DIGITAL EVIDENCE

What is digital evidence?

In order to standardize on a single definition of digital evidence I would like to use the following definition:

"Digital evidence is defined as any data stored or transmitted using a computer that support or refute a theory of how an offence occurred or address critical elements of the offence."[3]

[2] S v. ME DUVENHAGE 11/150/2003

[3] Digital evidence and computer crime 2nd ed E Cassy

The above definition is fine when addressing a criminal offence, however, Digital evidence may also be relevant in other matters, not of a criminal nature, and hence, I would like to adapt this definition as follows:

Digital evidence is defined as any data stored or transmitted, using a computer, that supports or refutes a theory of how an offence occurred or addresses critical elements of the offence, ***or prove a relevant aspect of the facts at issue****.*

As stated earlier, digital evidence is nothing more than rust, arranged in coherent and legible patterns, commonly represented by 1's and 0's in various combinations, commonly called *bits*. These *bits* are the building blocks of digital evidence, and in order to present this as evidence one must understand the very nature of how digital evidence is created, used, and stored.

The increasing relevance of digital evidence

Digital evidence is encountered more and more each day by law enforcement, lawyers, investigators and the like, as a matter of fact, and it is as a result of this very phenomenon becoming more and more relevant in their every day work.

Key areas in which one now expects to find digital evidence are in amongst others, matters involving:

- **Computer intrusions**: - where the method of access, actions perpetrated by the offender, actions taken to hide or disguise the offender.

- **Fraud**: albeit where a computer is merely a repository for certain accounting or other relevant records, or as the actual instrument of the fraudulent transaction.

    - During the "Shaik" fraud and corruption trial, the prosecution presented a critical piece of evidence, a document which detailed how the accused attempted to solicit a bribe for a prominent politician. This evidence was presented to investigators on a floppy disk by a witness, and one of the challenges facing the investigators was to link the document back to the accused in some manner. Although no judgment has yet been made in this case, a large part of this specific evidence given in the trial revolved around the digital evidence.[4]

- **Identity theft**: where a computer is used to steal the digital identity of an individual so.

[4] S v. SHAIK Durban, South Africa, 2005

- Here one thinks back to 2002, when an individual gained access to a computer terminal, and using "spy ware", was able to steal the identities of individuals who used the terminal for internet banking. Once in possession of this information, the perpetrator was able to log on, and withdraw money from the victims bank accounts.

- **Intellectual property theft**: where the actual intellectual property is in a digital format, digital evidence may be required to prove that the IP was actually stolen by the perpetrator, or even in the possession of the perpetrator.

    - See Duvenhage case supra[5]

- **Child pornography**: where the offending material again is stored, or distributed, or manufactured in a digital format.

- **Sexual harassment:** where the actual harassment or offending material originates and was distributed in a digital form.

- **Violent crimes** such as for example murder, as per the following case example:

    - A Maryland woman named Sharon Lopatka told her husband that she was leaving to visit friends. However she left a chilling note that caused her husband to inform the police that she was missing. During their investigation the police found hundreds of e-mail messages between Lopatka and a man named Robert Glass about their torture and death fantasies. The contents of the e-mail led investigators to Glass' trailer in North Carolina, and hey found Lopatka's shallow grave nearby. Her hands and feet had been tied and she had been strangled. Glass pleaded guilty, claiming that he had killed Lopatka accidentally during sex.[6]

The digital audit trail and its challenges

As a form of physical evidence, Digital evidence inherently has several challenges that can hamper the investigator. These aspects may relate to the fact that digital evidence is:

- **Very messy** and slippery since for example the hard drive contains a messy amalgam of data, bits and pieces of information all mixed together, much of which will not be relevant to the matter at hand.

---

[5] S v DUVENHAGE 11/150/2003

[6] Marryland 1996

- Digital evidence **is typically an abstraction** of some event or a digital object. This raises the hearsay nature of digital evidence not only in South African Law, but also in the United States. I will discuss this aspect in more detail later in this paper.

- The fact that **digital evidence can be manipulated** so easily raises challenges to the investigator, during the collection, analysis and presentation of the evidence.

- Digital evidence **is usually circumstantial**, making it difficult to attribute computer activity to an individual. This being the case, it is more often than not easier to prosecute the computer rather than an individual!

    - In an investigation into the notorious online Wonderland Club, Grant argued that all evidence found in his home should be suppressed because investigators had failed to prove that he was the person associated with the illegal online activities in question. However the prosecution presented enough corroborating evidence to prove their case.[7]

Another aspect to be considered is the dynamic and distributed nature of networks, which makes it even more difficult to find, and collect all the relevant digital evidence.

Marrying digital evidence and forensic science:

What is Forensic Science? "*Forensic Science is the application of science to the investigation of, and prosecution of crime, or the just resolution of a conflict*."8

With the above definition in mind it becomes evident that in order to investigate digital evidence, one is required to use science to collect, analyze and present this evidence in court, so similarly to the employment of science around DNA to the identification of the perpetrator of a murder for example.

THE LEGAL FRAMEWORK

If one was to write solely on the law of evidence, relating to the collection of and presentation of forensic evidence, one could write volumes, since this is a vast topic. In this section I will attempt to

---

[7] United States v. Grant 2000

[8] Cassey: Digital evidence and computer crime 2nd edition 2004

stay focused on these areas specifically relevant to digital evidence, the collection of such evidence, the analysis of such evidence, and finally the presentation of such in court.

The hearsay nature of digital evidence:

As an overview, van der Merwe states: "*We teach students of the law of evidence that evidence may be brought before the court either as oral or viva voce evidence, real evidence or documentary evidence. Traditionally, and at present, mostly in criminal cases, oral evidence has been the rule. A witness usually gives testimony orally, under oath, and is the subjected to cross examination. The oath is intended to help to prevent deliberate untruths in the course of the evidence being given, while the cross examination helps to guarantee both the lack of deliberate untruths, as well as honest mistake, on the part of the witness. For this reason, hearsay evidence has usually been held as inadmissible, since the person making the statement was not under oath while making the statement and since, not being present before the court where his statement is being repeated, cross examination is impossible*." [9]

In this regard, it has long been the view that documentary evidence be considered as hearsay evidence, unless it has been authenticate – in most cases by the author who will testify to its authenticity *viva voce*. This raised many questions on how and when documentary evidence was presented in a particular case, and what the weight attached to that evidence should have been.

But what does documentary evidence and hearsay evidence have to do with digital evidence? Well the statutory definition attached to hearsay evidence as in section 3(4) of the *Law of evidence amendment Act*[10], hearsay evidence is "*evidence whether oral or in writing, the probative value of which depends upon the credibility of any person other than the person giving such evidence*", which is obviously very relevant to documentary evidence.

If one delves further and asks what is a document, our courts have in *Seccombe and Others v Attorney General*[11] defined a document as "*a very wide term and includes everything that contains written or pictorial proof of something*". This could then quite understandibly include digital evidence.

The question now arises, when is digital evidence seen as hearsay, and when is it seen as real evidence?

The distinction lies in how the evidence is tendered, in other words, either testimonially, or circumstantially. In *Weintraub v Oxford Brickworks (Pty) Ltd*[12] the court held "*A letter is only*

---

[9] Documentary evidence (with specific reference to hearsay) Obiter 1994

[10] Act 45 of 1988

[11] 1919 TPD 270

evidence of the fact that it was written by the person who wrote it, and that that person said what the letter contains. It is not evidence that what he said is true."

In his article, van der Merwe[13] states that on the basis of *Mdani v Allianz Insurance ltd*[14], it seems that if a statement is not tendered to prove the truth of its contents, it does not amount to hearsay.

To conclude on this point, if documentary evidence is tendered to prove the truth of its content, it may amount to hearsay. In this regard, it remains circumstantial and hearsay, until supported by evidence tendered *viva voce* in its support. This will become specifically relevant when we look at the types of digital evidence and how it is presented in court.

The best evidence rule

According to Hoffman and Zefferet[15], any party who wishes to rely upon statements contained in a document, must ordinarily comply with three general rules:

- Subject to various exceptions, the contents of a document may be proved only by production of the original (best evidence rule).
- Evidence is normally required to satisfy the court of the documents authenticity, also subject to various exclusions.
- A document may have to be stamped in accordance with the Stamp Duties Act 1968

This potentially creates problems around digital evidence, since how does one prove the original evidence, when a print out of such is not the original. Fortunately the legislature in South Africa has come to the rescue, an we can avoid the above debate relating to digital evidence and the above criteria.

In terms of section 15 of the *Electronic Communications and Transactions Act 25 of 2002*, it is provided that the rules of evidence must not be applied to deny the admissibility of a data message purely because it is constituted by a data message, or on the grounds that it is not in its original form, if it is the best evidence that the person adducing it can obtain.

---

[12] 1948 1 SA 1090 (T) 1093

[13] Documentary evidence ((with specific reference to hearsay) Obiter 1994

[14] 1991 1 SA 184 (A)

[15] The South African law of evidence 4th edition

Thus this information, albeit in the form of a data message, must be given due evidential weight, having regard to:

1. the reliability of the manner in which the data message was **generated,** stored or communicated;

2. the reliability of the manner in which the **integrity of the data** message was maintained;

3. the manner in which its **originator was identified**; and

4. any other relevant factor.

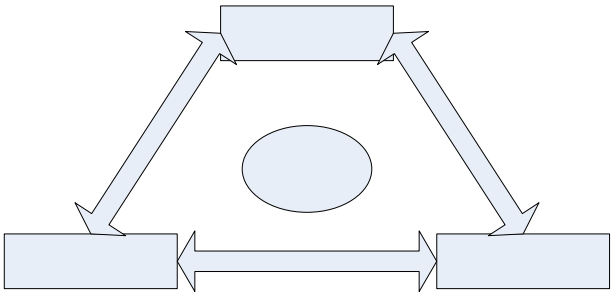
It is also finally stated that a data message made in the ordinary course of business, or a copy or print out correctly certified to be correct is on its mere production admissible in evidence and is rebuttable proof of the facts contained in such record, copy, printout or extract.

The role of digital evidence

We now know that digital evidence could be hearsay – if tendered to prove its content, since there is no one who testifies as to the truth of its contents. We also know that if a data message is made in the ordinary course of business, it is admissible in evidence and is rebuttable proof of the facts contained in such a record.

This leads us to the point that the role of digital evidence can vary, and so too the reason that it is sought.

According to Lochard's exchange principle, anyone, or anything entering a crime scene takes something of the crime scene with them, and leaves something of themselves behind when they leave.



In the digital realm, similar exchanges of evidence occur. As an example, data from an offender's computer is recorded by a web server and/or data from web servers is stored on the offenders computer when the offender visits a specific web page.

From the above, we can conclude that digital evidence may take the form of content which has been created by an author, and the truth of which has to be supported by witness testimony *viva voce* (e.g. the content of a letter, an email, or the like), or it may be in the form of a data message, or record produced in the ordinary course of business, such as a web log, Automatic Number Identification (ANI) logs, date and time stamp, automated transactional record, and so on.

Although we may distinguish between these two types of digital evidence, the investigative methodology applied, the manner of collection, and finally its presentation in court will remain constant.

THE INVESTIGATIVE PROCESS

Casey[16] has defined 12 key processes relating to the investigation of an event. Since we are dealing not only with digital evidence in relation to crime but also in the context of a dispute of another nature, I would like to focus on the following key aspects:

- **Authorisation** to collect the evidence: What is the legal authority on which the evidence is collected?

- **Acquisition** of evidence: The evidence should be acquired in a manner that preserves the evidence in its original form, for future analysis.

- **Authentication** of the evidence: The ability to enable one to authenticate that the evidence being presented is in fact that evidence in its original form.

- **Analysis** of the evidence: Analysis in a manner as free from bias as possible, and the results of which can be validated by another party.

- **Reporting** on the findings: The ability to portray the actions taken by the investigator, as well as his findings of an analysis in a coherent manner.

---

[16] Digital evidence and computer crime 2nd edition 2004

- **Testimony:** The ability of an investigator to present his report, and to testify to its content viva voce in court.

Authorisation:

A final legal point worth discussing is the collection of the digital evidence. In order to be admissible in court, the collection of the digital evidence has to take place in a legal manner. Digital evidence may legally be collected by:

- Receiving the permission of the owner thereof to collect such, such as the written permission of the owner to collect such, or by mutual consent as detailed in a contract.

- By means of an order of court, such as an Anton Pillar order often issued in cases involving copyright and other intellectual property disputes.

- By means of a search warrant issued by a court.

- By means of an interception directive issued

The point I wish to make here is that there has to be a legal basis for the collection of the evidence before such takes place. Ignoring this foundational fact will almost surely result in the inadmissibility of the digital evidence.

Acquisition of the evidence:

There are a vast quantity of documents laying down international standards and best practices for the acquisition of digital evidence. I would like to mention a few of the ones that I have found useful:

- The good practice guide for computer based electronic evidence by the ACPO

- The European convention on Cyber Crime

- The G8 proposed principles from the 13th INTERPOL Forensic Science Symposium, Lyon, France

- The US Department of Justice: Electronic Crime Scene Investigation: A First Responders Guide

- The US Department of Justice Electronic Evidence Search and Seizure Manual

The above documents all focus around the following principles relating to the acquisition of digital evidence, which were formalized at the 13th INTERPOL Forensic Science Symposium:

- When dealing with digital evidence, all of the general forensic and procedural principles must apply.

- Upon seizing digital evidence, actions taken should not change that evidence.

- When it is necessary for a person to access original digital evidence, that person should be trained for that purpose.

- 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 whilst the digital evidence is in their possession.

- Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

Authentication:

The word Authentication was mentioned earlier in this article, with specific reference to documentary evidence. The US perspective on authentication is probably worth mentioning here.

"*Authentication means satisfying the court that (a) the contents of the record have remained unchanged, (b) that the information in the record does in fact originate form its purported source, whether human or machine, and (c) that extraneous information such as the apparent date of the record is accurate. As with paper records, the necessary degree of authentication may be provided through oral and circumstantial evidence, if available, or via technological features in the system or record.*"[17]

In the South African context, we again refer to the provisions of section 15 of the *Electronic Communications and Transactions Act 25 of 2002*, which sets out the 4 requirements for a data message to be afforded due evidential weight.

[17] Reed 1990-91

Analysis

Once the digital evidence has been acquired and authenticated, an analysis phase takes place, where the investigator will analyze the data at his disposal, and draw certain conclusions. Typically the analysis phase should include amongst others the following sub categories:

- **Assessment:** the evaluation of digital data objects to try to determine factors such as means, motivation, and opportunity

- **Experimentation:** A generic term meaning the use of unorthodox or previously untried methods and techniques that may be required during an investigation. It is crucial that the experimental process be documented vigorously so that it may be tested by the scientific community and the courts.

- **Fusion and correlation:** in all likelihood, digital evidence alone will not tell the whole story, thus digital evidence with traditional evidence and investigation methods to gain the full story. To head straight for the digital evidence, and to ignore the fingerprint on the keyboard is the mistake one is inclined to make.

- **Validation:** the output or results from the analysis phase, which are put to the courts or other decision makers as "positive proof".

Reporting:

Cassey[18] puts it very well: "(Reporting means) *To provide a transparent view of the investigative process, final reports should contain important details from each step, including reference to protocols followed and methods used, to seize, document, collect, preserve, recover, reconstruct, organize and search key evidence*."

The aim of the report is to document and detail each process followed by the investigator, including even alternative theories, thus demonstrating the independence, and objectivity, of the investigator, and his investigation.

Testimony:

It inevitably becomes necessary that the investigator present his findings to a court or other forum, and he will have to be able to firstly convey his findings and report to the court, by giving testimony *viva voce*, and secondly to stand the scrutiny of cross examination on his report, findings, and testimony.

---

[18] Digital evidence and computer crime 2nd edition 2004

The problem the investigator has with digital evidence is that although he may be very well versed in his field, he has to be able to translate these facts which are some times of a very technical nature, to the court, who is very often, not technical minded. he is well advised to keep the evidence concise, and understandable.

CONCLUSION

In conclusion, digital evidence can be exceptionally relevant in any criminal investigation, or legal dispute for that matter, however if one intends using this evidence successfully, it is prudent to understand the legal rules of evidence, and how they are employed in the investigative process to ensure acceptance of the evidence, and the application of the appropriate evidential weight thereto.

Digital evidence should also not be viewed as the holy grail of evidence, but should be considered in the light of the other evidence in the given case.

Although the South African courts have not had much opportunity to litigate around this topic, we are fortunate in that we can look to the United States of America, and the United Kingdom, for rulings, which in many cases will apply to the scenarios at hand.

Finally, the forensic investigator tasked with reviewing and analyzing digital evidence, should be process driven, and should familiarize himself with the various good practice guides readily available. Should he fail to do this, his elaborate investigation may be worthless.