Computer Forensics – Past, Present And Future

EWA HUEBNER[*] DEREK BEM[**] AND OSCAR BEM[***]

Abstract

In this paper we examine the emergence and evolution of computer crime and computer forensics, as well as the crisis computer forensics is now facing. We propose new directions and approaches which better reflect the current objective of this discipline. We further discuss important challenges that this discipline will be facing in the near future, and we propose an approach more suitable to prepare for these challenges. We focus on the technical aspects, while at the same time providing insights which we believe would be helpful for the legal profession to better understand the unique issues related to computer forensic evidence when presented in the court of law.

Keywords: computer forensics, computer crime, electronic evidence

[*] Senior Lecturer, University of Western Sydney, School of Computing and Mathematics.
[**] Lecturer, University of Western Sydney, School of Computing and Mathematics.
[***] Student, University of Western Sydney, College of Law and Business.

1. Introduction

In this paper we present a brief overview of the historical emergence of computer crime, and propose its classification into three areas: activity targeting computer systems, computer assisted crime, and incidental computer crime. We also discuss how computer forensics emerged as a new discipline, what it has achieved in the first thirty or so years of its existence, and what challenges it is facing in the near future. New directions and approaches are proposed which better reflect the objectives of computer forensics today. We believe that the content may be useful for the legal profession, which lacks literature explaining computer forensics without excessive amount of technical terms and references. Other target readers for this paper are business professionals, computer forensic analysts and examiners, law enforcement personnel, system administrators and managers, and anyone involved in computer security.

It should be noted that **this paper describes international issues.** References to case law and statute law in different countries are an integral part of the paper, and should be seen as illustrative examples only. We endeavoured to balance the discussion and used, where appropriate, **examples from the USA, Australia, and Europe,** while at the same time not limiting the analysis of issues to any specific country. When quoting, the original spelling is retained, while Australian spelling is used in the remaining parts of the paper.

2. Computer Crime And The Emergence of Computer Forensics

Computer Forensics aims to solve, document and enable prosecution of computer crime. Computer crime is broadly understood as criminal acts in which a computer is the object of the offence or the tool for its commission.[1] Computers first started to appear in the mid 1940s, and rapid development of this technology was soon followed by various computer offences. In the mid 1960s Donn Parker noticed that: *"when people entered the computer center they left their ethics at the door"*.[2] The first criminally prosecuted case was recorded in Texas, USA in 1966[3] and resulted in a five year sentence. However many offences then and now are unreported, never prosecuted and subsequently unknown to the public at large. USA annual Computer Crime and Security Surveys conducted by the CSI/FBI[4] show that between 1999-2006 30% to 45% responders did not report computer intrusion, the main reason being fear of negative publicity. Australian surveys show much higher figures: in the 2006 AusCERT survey[5] a very high percentage of responders (69%) chose not to report attacks to any external party.

---

1 See, eg, 'Concepts and terms' (2005) *High Tech Crime Brief* <www.aic.gov.au/publications/htcb/htcb001.pdf> at 12 August 2006.

2 See Terrell Bynum, 'Computer Ethics: Basic Concepts and Historical Overview' (Winter 2001) *Stanford Encyclopedia of Philosophy* <http://plato.stanford.edu/archives/win2001/entries/ethics-computer/> at 12 January 2007.

3 Michael P. Dierks, 'Computer Network Abuse' (1993) Volume 6 Number 2 *Harvard Journal of Law & Technology*.

4 Lawrence A. Gordon et al, '2006 CSI/FBI Computer Crime and Security Survey' (2006)

5 *2006 Australian Computer Crime and Security Survey* (2006).

In the 1970s and 1980s relatively inexpensive personal computers became common, and individuals and businesses began to use them on a regular basis; subsequently law enforcement agencies noticed the emergence of a new class of crime: computer related crime.[6] The emergence of computer forensics was largely in response to a demand for service from the law. By the 1990s law enforcement agencies in every technologically advanced country were aware of computer crime, and had a system in place to investigate and to prosecute such activities. Many research centres and scientific groups were also formed, and the software industry started to offer various specialized tools to help in investigating computer crime.[7]

For the sake of clarity and to assist in the understanding of computer crime we propose the following classification:

- Computer centred crime: criminal activity targeting computer systems, networks, storage media, or other computer devices (e.g. breaking into a commercial Web site and changing its contents). This can be seen as new tools facilitating a new class of crime.
- Computer assisted crime: use of computer systems as tools to assist in a criminal activity where using computers is not strictly necessary (e.g. child pornography). This can be seen as new ways to commit conventional crimes.
- Incidental computer crime: criminal activity where using a computer system is incidental to the activity itself (e.g. computerized accounting used to keep records of drug trafficking). This can be seen as using new tools to replace conventional tools (e.g. a bookkeeping ledger in the form of a paper book replaced by accounting software).

This classification, like many others, should be seen only as an aid to understand the area it is describing. One can imagine a scenario where certain criminal activities may span more than one area, or are difficult to classify as fitting into any of the three areas just described.

Computer crime led directly to attempts to combat it. In the early days various tools or tests were used by courts to help determine the scientific merits of the evidence presented. In 1993 a legal precedent was set by the U.S. Supreme Court regarding the admissibility of expert witnesses' testimony, which came to be known as the Daubert test, the Daubert standard, or just *Daubert*.[8] The *Daubert* test largely replaced previously used standards (Frye, Federal Rules of Evidence[9]). In the *Daubert* ruling the U.S. Supreme Court suggested four criteria for determining whether science was reliable and, therefore, admissible:[10]

---

6 Richard E. Overill, 'Computer crime - an historical survey' (1998) <http://www.kcl.ac.uk/orgs/icsa/Old/crime.html> at 20 December 2006.

7 See Michael G. Noblett, Mark M. Pollitt and Lawrence A. Presley, 'Recovering and Examining Computer Forensic Evidence' (2000) Volume 2 Number 4 *Forensic Science Communications.*

8 *Daubert* U.S. Supreme Court Ruling issued on 28 June, 1993 has been described in many sources. See assessment of its impact by The Project on Scientific Knowledge and Public Policy ('SKAPP') coordinated by the Tellus Institute here: 'Daubert:The Most Influential Supreme Court Ruling You've Never Heard Of' (Tellus Institute, 2003).

9 See Richard Saferstein, *Forensic Science Handbook* (2001).

10 Daubert, above n 8.

- Is the evidence based on a testable theory or technique?
- Has the theory or technique been peer reviewed?
- In the case of a particular technique, does it have a known error rate and standards controlling its operation?
- Is the underlying science generally accepted?

In short, *Daubert* helps to decide what is 'good' science and what is 'bad' science. However, when dealing with complex technical issues it can only be seen as a general guide. Thus while it helps to assess the suitability of computer forensic evidence, it still leaves many questions unanswered.

3. First Period Leads to First Definitions

For early investigators involved in computer related crimes it became immediately obvious that if their response and findings were to be of any use as court evidence they had to comply with the same rules as any other, more conventional investigations. The first thing every investigator has to be aware of is Locard's Exchange Principle: *"Anyone or anything entering a crime scene takes something of the scene with them, or leaves something of themselves behind when they depart"*.[11] It also became clear that when investigating computer related crime the same basic rules applied as in a non-computer related crime scene investigation. The investigation process includes phases of physical scene preservation, survey, search and reconstruction using collected evidence, all of which is formally documented. This process is described in detail in many books, manuals and guides, with Fisher[12] being a useful example.

Soon it also became apparent that computer related crime is sufficiently different to justify defining a separate field of knowledge, now commonly referred to as 'computer forensics'.

The field of investigating computer related crimes not only lacks one commonly agreed upon definition, but even the area itself is referred to differently across the field. While the term 'computer forensics' appears to be most widespread, some other names are also used, such as 'forensic computing',[13] or 'digital forensics'.[14] The broader term 'digital forensics' typically refers to digital evidence which is understood to be *"any information of probative value that is either stored or transmitted in a digital form"*.[15] Thus digital evidence refers not only to computers, but also to digital audio, digital video, digital fax machines, and similar devices. One would expect to see even broader terms like 'electronic forensics' or 'e-forensics' covering all electronic digital and analogue devices and media, but those terms are rarely used. It appears that by 2007 the term 'computer forensics' became

---

11 Saferstein, above n 9.

12 Barry A.J. Fisher, *Techniques of Crime Scene Investigation* (7 ed, 2003).

13 See one of the first Australian sources which defines computer forensics: Rodney McKemmish, 'What is Forensic Computing?' (Australian Institute of Criminology, 1999).

14 *Digital Forensic Research Workshop (DFRWS)* <http://www.dfrws.org/ > at 22 April 2005.

15 Carrie Morgan Whitcombe, 'An Historical Perspective of Digital Evidence: A Forensic Scientist's View' (Spring 2002) Volume 1(Issue 1) *International Journal of Digital Evidence.*

commonly accepted, and often used in a broader sense in relation to devices which are, strictly speaking, not computers.

In 1999 Farmer and Venema[16] defined computer forensics as the process of:

> *"gathering and analysing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system"*

To comply with conventional investigative methods they also suggested a series of stages a computer forensics investigator should follow:[17]

- Secure and isolate.
- Record the scene.
- Conduct a systematic search for evidence.
- Collect and package evidence.
- Maintain chain of custody.

While the above set is quite accurate and logical, depending on the specific focus some of the points could perhaps be expanded further.

Another more computer specific definition of computer forensics was offered in 1999[18] by the Australian Institute of Criminology:

> *"the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable"*

The same guide also defines four key elements of this process:

- Identification.
- Preservation.
- Analysis.
- Presentation.

The guide also recommends that this process should comply with a series of basic rules:

- Minimal handling of the original.
- Account for any change.
- Comply with the rules of evidence.
- Do not exceed your knowledge.

Subsequently various researchers offered similar, often more detailed descriptions of the computer forensics process. For example Mandia, Prosise and Pepe[19] describe seven components of incident response:

> 1. Pre-incident preparation.

---

16 Dan Farmer and Wietse Venema, *Forensic Discovery* (1st ed, 2005).

17 Dan Farmer and Wietse Venema, 'Murder on the Internet Express' (6 August 1999) <http://www.porcupine.org/forensics/> at 15 June 2006.

18 McKemmish, above n 13.

19 Kevin Mandia, Chris Prosie and Matt Pepe, *Incident Response & Computer Forensics, Second Edition* (2nd ed, 2003).

2. Detection of incident.
3. Initial response.
4. Formulate response strategy.
5. Investigate the incident: data collection followed by data analysis.
6. Reporting.
7. Resolution (security measures, lessons learned, long-term solutions).

All definitions of computer forensics have the following features in common:

1. They are based on the conventional crime handbook approach, which in turn follows Locard's Exchange Principle. Rationale: such compliance is necessary if the findings are to be used as evidence in court.
2. They formally describe detailed steps, often including decision charts or additional procedures, thus creating rather long lists and sets of steps to follow. Rationale: to make the process less error prone, and to demonstrate that sound forensic rules were adhered to, thus the results are valid and admissible in court.
3. The definitions are broad and not uniquely matched to a computing environment. If one were to remove computing specific terms, the definitions would remain valid. The definitions do not clearly indicate that they are dealing with the computing field.
4. Some definitions miss the necessary link between "forensics" in computer forensics, and "suitable for use in court". It does not matter how well computer forensics is defined if it misses a statement saying in effect: "all evidence must be collected and presented *in a manner that is legally acceptable*". Rationale: a definition should reflect that computer forensic experts are agents of the court.

4. Computer Forensics as a Separate Science Discipline

The first criminally prosecuted computer crime case (as mentioned before) took place in 1966. The first computer forensics training course appeared around 1989 (University of North Texas), the first International Law Enforcement Conference on Computer Evidence was hosted in 1993 (and in 1996 in Australia), and the first specialized software tools were developed in the mid-1980s.[20] Yet today (early 2007) there is still no agreement on what is the precise meaning of various terms, and many definitions are missing or are inadequate. In summary, the standards are still not developed and the body of knowledge is not precisely defined.

Computer forensics is a unique discipline of science, and in many areas it requires a different approach, different tools, as well as specialised education and training. While the distinctive position of computer forensics is generally accepted, the formal recognition of computer forensics as a section of forensic science has not yet eventuated. As an example, at the time of writing, there are three forensics institutes in Australia:

---

[20] Whitcombe, above n 15.

- National Institute of Forensic Science ('NIFS')[21]
- Senior Managers of Australian and New Zealand Forensic Laboratories ('SMANZFL')[22]
- The Australian And New Zealand Forensic Science Society ('ANZFSS')[23]

While these organisations are aware that computer forensics exists, none of them formally recognises it as a separate, distinct scientific discipline.

As a result the Australian courts use the general Supreme Court Rules[24] to determine the suitability of a person to be a computer expert witness or an independent computer expert:

> *"Expert means a person who has specialised knowledge based on the person's training, study or experience."*

An expert witness has to demonstrate the appropriate qualifications and experience, and has to present clear and logically arranged documentation. Still no formal accreditation to become an expert is required or even possible to obtain. Some private institutions offer computer forensics training,[25] and many offer vendor specific software training.[26] While such training is often useful it can not be seen as leading to a recognized certification. A similar situation is prevalent in other technologically advanced countries.[27], [28]

5. The Beginning of Computer Forensics

The first period in computer forensics history is characterized by dealing with relatively small capacity storage devices and a relatively small amounts of information.[29] This allowed for the complete hard disk to be copied to another disk, the copy used to analyse the contents, and search for evidence. During this period computer networks (two or more computers linked together) became easier to use, inexpensive, and gained popularity even in the home environment. The Internet started to spread rapidly, and today many households as well as most workplaces use it extensively.

---

21 <http://www.nifs.com.au/> at 12 April 2006.

22 < http://www.nifs.com.au/SMANZFL/SMANZFL.html?index.asp&1> at 20 April 2006.

23 <http://www.anzfss.org.au/> at 12 April 2004.

24 Supreme Court Rules 1970 - SECT 1.8 Interpretation.

25 See, eg, one of the leading Australian information and communications technology companies: *Volante* <http://www.volante.com.au/> at April 2005.

26 EnCase from GuidanceSoftware is a leading computer forensics product in the law enforcement community. See, eg, one of many training providers: *Dimension Data Guidance (EnCase) Training Courses* <http://www.ddls.com.au/VendCourse/GSI.htm> at 20 January 2007.

27 See, eg, U.S.A. source, Craig Ball, 'Finding the Right Computer Forensic Expert' (2004) <www.craigball.com> at 23 October 2005.

28 See, eg, U.K.source, Illena Armstrong, 'Computer Forensics Detecting the Imprint' (2002) *SC Magazine*

29 See, eg, *A Brief History of the Hard Disk Drive* <http://www.pcguide.com/ref/hdd/hist-c.html> at 28 November 2005.

Many books dealing with digital evidence were written during the last decade,[30] and computer forensics methodology was well developed to handle simple, typical cases. A good example of the development of a consistent methodology is a series of publications from the U.S. Department of Justice, the National Institute of Justice (NIJ).[31] The NIJ publications are probably the most complete set of materials to come from a single source, and can be collected to form a small library which covers all main areas of interest to personnel involved in all aspects of digital forensics. Some areas covered are:

- "A Guide for First Responders",[32] for use by first responders who have the responsibility for protecting an electronic crime scene and recognizing, collecting, and preserving electronic evidence.
- Follow up publications: "Forensic Examination of Digital Evidence: A Guide for Law Enforcement"[33] and "Investigations Involving the Internet and Computer Networks",[34] are resources for individuals responsible for investigations involving all sorts of digital evidence, the Internet and computer networks.
- "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors"[35] covers all aspects of collecting, handling and presenting the evidence in a way which complies with court admissibility rules.

The NIJ also tests and publishes the test results of various tools, for example disk imaging tools and write blockers (devices that prevent writing to storage media).[36]

When the need to perform an in-depth analysis of computer systems and media emerged there were no special tools available, and early investigators relied on various collections of existing utilities which they considered appropriate to the task at hand. One of the most useful tools was a hex editor, which allowed for the underlying structure of computer media to be looked at. Some software developers noticed the potential of the new emerging field and developed their products in this direction. A good example is the German company X-Ways, which many years ago offered free hex editor software. This software is now further

---

30 *University of Western Sydney Computer Forensics, Books And Journals* University of Western Sydney, Australia <http://www.scm.uws.edu.au/compsci/computerforensics/Books%20And%20Journals/index.php> at 20 January 2007.

31 *National Institute of Justice* <http://www.ojp.usdoj.gov/nij/> at 20 January 2007.

32 John Ashcroft, 'Electronic Crime Scene Investigation: A Guide for First Responders' (July 2001), U.S. Department of Justice Office of Justice Programs, Technical Working Group for Electronic Crime Scene Investigation <http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm>.

33 Sarah V. Hart, 'Forensic Examination of Digital Evidence: A Guide for Law Enforcement' (April 2004), U.S. Department of Justice Office of Justice Programs, Technical Working Group for Electronic Crime Scene Investigation <http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm>.

34 David W. Hagy, 'Investigations Involving the Internet and Computer Networks' (January 2007), U.S. Department of Justice Office of Justice Programs, Technical Working Group for Electronic Crime Scene Investigation <http://www.ojp.usdoj.gov/nij/pubs-sum/210798.htm> at 20 January 2006.

35 David W. Hagy, 'Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors' (January 2007), U.S. Department of Justice Office of Justice Programs, Technical Working Group for Electronic Crime Scene Investigation <http://www.ojp.usdoj.gov/nij/pubs-sum/211314.htm>.

36 *National Institute of Justice* <http://www.ojp.usdoj.gov/nij/> at 20 January 2007.

developed to offer more functionality, and the company also created a range of dedicated computer forensics tools.[37] Since the 1990s many other companies developed software tools aimed at the forensic market, and there are also many free and open source tools.[38]

6. Emerging Problems

The current philosophy and the state of digital crime investigations faces a problem, which can be noticed for example in the U.S. Department of Justice digital evidence guide[39] which states: *"Acquire the subject evidence to the examiner's storage device using the appropriate software and hardware tools"*. 'Acquire the evidence' is still seen by the vast majority of investigators and law enforcement as making a physical copy of computer storage, typically performing a disk-to-disk copy. This approach is becoming increasingly difficult to implement and impractical, because we are facing the following technological challenges:

- By 2007 single hard disk drives reached the capacity of 1TB (terabyte) in standard PC form, and 20GB in microdrive form. The drives use perpendicular magnetic recording technology which promises even higher capacities.[40] Large capacity drives create practical issues: copying data is slow, and searching acquired data takes even more time. To visualize the problem: a single 1TB disk can digitally store all world literature produced in one year.[41]
- Data file systems used in computers allow for data to be hidden from a normal user, and made visible only if special tools are used.[42]
- Many properties and mechanisms of computer operating systems are not documented, or poorly documented by their developers, and some properties can be used to hide data.[43]
- On-line storage (also known as Internet storage or virtual hard drive) became more popular and accessible.[44] Some Internet service providers offer free storage space,

---

37 *X-Ways Software for Forensics, Data Recovery and IT Security* X-Ways Software Technology AG <http://www.winhex.com/> at 1 March 2005.

38 *University of Western Sydney Computer Forensics, Software* University of Western Sydney, Australia <http://www.scm.uws.edu.au/compsci/computerforensics/Software/index.php> at 20 January 2007.

39 Hart, above n 33.

40 Hitachi Global Storage Technologies was formed in 2003 as a result of the strategic combination of IBM and Hitachi's storage technology businesses. The company became a storage market leader with combined 80 years of hard disk drive expertise. See: *Hitachi Global Storage Technologies* <http://www.hitachigst.com/portal/site/en/menuitem.368c8bfe833dee8056fb11f0aac4f0a0/> at 1 February 2007.

41 JISC, 'The Data Deluge: Preparing for the explosion in data' (2004) <http://www.jisc.ac.uk/> at 18 January 2007.

42 Ewa Huebner, Derek Bem and Cheong Kai Wee, 'Data hiding in the NTFS file system' (Spring 2002) Volume 3(Issue 4) *Digital Investigation.*

43 Derek Bem and Ewa Huebner, 'Alternate Data Streams in Forensic Investigations of File Systems Backups' (Paper presented at the ATINER, Athens, Greece, 2006).

44 *Internet Virtual Storage* <http://www.cryer.co.uk/resources/virtualstorage.htm> at 3 January 2007.

data encryption, and client details confidentiality. Data of interest to a forensic investigator may not necessarily reside in the physical box in front of them.

- Storage virtualisation technologies allow for data to be kept on storage devices which are physically at other locations, possibly in other legal jurisdictions and countries, and can be used and accessed as if they were local.[45]

- It became easy to establish and maintain a Web site which is physically located beyond local legal jurisdiction,[46] and securing the cooperation of other countries legal systems can be slow, costly, and difficult. In lower profile cases it may simply be too impractical to obtain the data. Even the Web hosting sites located in countries with well developed electronic crime laws often create complex rules preventing the release of any client details to investigators unless a valid subpoena is presented and subpoena compliance costs are paid.[47]

- Data encryption algorithms became so good that breaking a password using a brute force attack method (trying all possible values of encryption key till the right key is found) to access protected data is practically impossible. As an example, one older source estimated that it would take 270 days to break 56-bit RC5 encryption using 4000 teams operating 10,000's machines.[48] While such estimates are continuously changing as more powerful computers became available, standards for encryption keys are also changing. Longer encryptions keys are even more difficult to break. To illustrate: assuming so called AES-128 encryption (Advanced Encryption Standard with 128-bit long key) and an attacker with a system that tries one billion keys per second, a totally unrealistic time of 10 000 000 000 000 000 000 000 years would be required to check all possible key combinations.[49] Various strong encrypting tools, which not so long ago had only limited distribution, are now available freely to anyone.[50]

- Small, easy to hide (or destroy) storage devices became common and inexpensive. By the end of 2006 USB flash drives reached capacities of up to 64GB.[51] There are free solutions available which allow users to *"carry your favorite computer programs along with all of your bookmarks, settings, email and more with you"* and *"use them on any Windows computer. All without leaving any personal data*

---

45 Tom Clark, *Storage Virtualisation technologies for Simplifyng Data Storage and Management* (1 ed, 2005).

46 Joshua Gordon, 'Illegal Internet Networks in the Developing World' (2004) <http://cyber.law.harvard.edu/home/research_publication_series> at 6 December 2005.

47 See, eg, USA based company, *Domains by Proxy 's Privacy Policy* <http://www.domainsbyproxy.com/popup/subpoenapolicies.aspx> at 12 December 2006.

48 Jason Siegfried et al, 'Examining the Encryption Threat' (2004) Volume 2(Issue 3) *International Journal of Digital Evidence.*

49 This example illustrates that an approach where all possible key combinations are tried leads to time required to break the encryption which is approximately in the same range as the estimated life of the Universe. See: Svante Seleborg, 'About AES – Advanced Encryption Standard' (2004) at 2 November 2006.

50 See, eg, robust and free encryption software, *True Crypt - Free Open-Source On-The-Fly Disk Encryption Software* TrueCrypt Foundation <http://www.truecrypt.org/> at 10 March 2006

51 One of many manufacturers of large capacity USB flash key memory: *Kanguru Flash Drive Max* <http://www.kanguru.com/flashdrive_max.html> at 20 November 2006.

behind". The hardware required is a USB flash key with capacity of 256MB or more.[52]

The main conceptual problem in computer forensics is the need to understand that data we intend to capture is not static, but dynamic. While making a static copy of a hard disk may produce some useful results, it may as well be that all crucial data was lost when the computer was powered off. An investigator should be aware that data has a certain span of life, and it naturally disappears (sometimes irrecoverably) in a certain order dictated by the architecture of computer systems and the technology used to build them. Data life span can be only nanoseconds if it resides in computer registers or caches, a bit longer when it resides in the main memory or on the network, and relatively longer (seconds to years) when it resides on hard disks. Finally, it is assumed that data stored on backup media has a life span of many years.[53] This is often referred to as the Order of Volatility.[54]

In particular, computer memory can potentially reveal more than just information regarding the current state of the computer system. When pages of memory are used by a process and the process terminates, these pages are marked as free, but the data is not overwritten immediately, often not until the pages need to be reused by the system. There are no specialised software tools or techniques that have been developed which can be used to assist in collecting and analysing the data contained in these pages in such a way that it is admissible in a court of law. The data in these pages is invisible to standard software tools used in the analysis of physical memory images, because logically this data no longer exists.[55] Similarly data streaming over network connections, unless continuously monitored, is irretrievably lost.

7. Lack of Standards

As information security magazine Security Wire Digest noticed in 2003:[56]

> *"In order for computer forensics to be a legitimate scientific discipline, it must meet the same standards as other forensic sciences. These include formal testable theories, peer reviewed methodologies and tools, and replicable empirical research. Sadly, these standards are not being met."*

There have been many attempts to formulate a set of standards, but none of these sets is developed and updated as often as the discipline requires, and none is commonly accepted. Some are listed below:

---

52 *PortableApps.com* <http://portableapps.com/> at 20 March 2006.

53 Farmer, above n 16.

54 Ibid.

55 See research paper, Jason Michael Solomon, *Computer Forensics: The Persistence of Data in Physical Memory* University of Western Sydney, 2006).

56 Marc Rogers, 'Security Perspectives Computer Forensics: Science or Fad?' (2003) Vol. 5, No. 65 *Security Wire Digest.*

- The International Organization for Standardization (ISO) set "ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management".[57] While compliance with ISO 17799 is sometimes quoted in relation to computer evidence it should be remembered that this standard deals mainly with computer security.
- The National Institute of Standards and Technology (NIST) produced the *"Guide to Integrating Forensic Techniques into Incident Response"*[58] which provides a good basis for describing the computer forensics process. The guide correctly noticed that acquiring data involves collecting volatile data and duplicating non-volatile data (many other guides ignore the volatile data aspect of the collection process). The NIST also offers a series of reports on disk imaging.[59]
- The International Organization on Computer Evidence (IOCE)[60] does not offer any relevant publications on the matter.

Probably the most consistently updated series of publications are offered by the NIJ (National Institute of Justice), the research, development, and evaluation agency of the U.S. Department of Justice.[61] The guides cover all aspects of computer forensics, and include a cautionary statement defining their scope and role like the one below:[62]

> *"The recommendations presented in this guide are not mandates or policy directives and may not represent the only correct course of action. The guide is intended to be a resource for those who investigate crimes related to the Internet and other computer networks. It does not discuss all of the issues that may arise in these investigations and does not attempt to cover traditional investigative procedures."*

Despite this caution, compliance with the NIJ guides is probably as close to following a standard as is currently possible, while proper, formal standards are missing.

In summary, there are many 'best practice' guides or recommendations from many sources, but no single and widely accepted international standard. It is probably unrealistic to expect that such an internationally accepted and up to date standard will be created in the near future, or indeed ever.

---

57 *ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management* (2005) International Organization for Standardization <http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html> at 12 January 2007

58 Karen Kent et al, 'Guide to Integrating Forensic Techniques Into Incident Response' (2006), National Institute of Standards and Technology (NIST) <http://csrc.nist.gov/publications/nistpubs/>.

59 *NIST National Institute of Standards and Technology, Computer Security Resource Centre (CSRC)* <http://csrc.nist.gov/> at 12 January 2006.

60 *International Organization on Computer Evidence (IOCE)* <http://www.ioce.org/> at 12 January 2007.

61 *National Institute of Justice* <http://www.ojp.usdoj.gov/nij/> at 20 January 2007.

62 David W. Hagy, 'Investigations Involving the Internet and Computer Networks' (January 2007), U.S. Department of Justice Office of Justice Programs, Technical Working Group for Electronic Crime Scene Investigation <http://www.ojp.usdoj.gov/nij/pubs-sum/210798.htm> at 20 January 2006.

8. Failure of The Current Approach

Sooner or later anyone working with computer forensic evidence notices that it would help tremendously "if only":[63]

- *"... all investigators used the same approach, from sys admins and IT security specialists right through to police;*
- *... we could be sure that the same approach would be followed by investigators in other jurisdictions;*
- *... the companies running e-services had systems running which could prove what was going on (pre-investigation)"*.

And sooner or later a project is founded to make these wishes a reality. One such attempt is analysed here in more detail to demonstrate what problems are faced by the computer forensics discipline.

The CTOSE (Cyber Tools On-Line Search for Evidence) project was founded by three Universities, two R&D organizations and two commercial companies, supported by the European Commission's IST program.[64] The aim was *"to develop a methodology, architecture, a process model, and a common set of tools and procedures for an electronic investigation"*. Three pilot scenarios were developed to demonstrate the need for new methodology. The project closed in September 2003, and it did not deliver any significant results. It closed with a promise of future development:

> *"The project partners, along with SIG members, are now setting up an electronic evidence research network, provisionally called ENDEM, which will bring together researchers interested in further work on the challenges posed by electronic evidence"*

The ENDEM research network never eventuated, and the CTOSE project folded without providing any significant input to the field. This story illustrates the typical life span of computer forensic research projects which often start enthusiastically, but due to unforeseen complexities of the field and its multi-disciplinary characteristics do not produce the expected results and are eventually abandoned.

Cases like this show that computer forensics is still in the very early days of development, suffering from a lack of clear direction and appropriate development support.

9. New Directions For Computer Forensics

As computer technology develops it facilitates processing larger and larger volumes of data, which is not only transient but also not limited to any specific location. In this sense

---

63 Neil Mitchison, 'The challenge of electronic evidence – the European response' (2003) at 12 September 2005.

64 *CTOSE Cyber Tools On-Line Search for Evidence* <http://www.ctose.org/info/index.html> at 12 October 2006.

evidence collected from computer systems is not like other physical evidence, and it cannot be subjected to the same rules. If the demands of physical evidence are placed on computer evidence, much of the data which can be collected will not be admissible as evidence in court, and many computer crimes will escape prosecution. In a sense even in simple cases it is misleading to treat the hard disk storing data as synonymous with that data.

Computer forensics is already moving beyond the analysis of hard disk images. Memory forensics and live system investigation methodology are developing both in terms of research and specific forensic software tools. Collecting memory images, the system footprint and unallocated pages invariably changes the data being collected. So far no universal method has been discovered to avoid this, and perhaps such a method will never be devised. Similarly, live investigation by its very nature modifies the data stored in memory, hard disks and other storage devices. It has to be accepted that this is inevitable, and evidence collected in this manner has to become acceptable to the courts of law.

Further, computer systems are increasingly complex, and analysing their parts, like the disk or memory image, may not readily reveal all available information. A new approach to computer forensics investigation is to attempt to recreate the computer system and its immediate environment by reproducing the collected images in a controlled way on similar or simulated hardware, and observe its behaviour. This has the potential to provide a valuable insight into the dynamic relationship of the investigated system with the outside computer networks and systems, as well as the specific setups and functions of the system itself.

The important difference of the proposed approach is that it removes the expectation of certainty that somehow the investigator will be able to obtain the original evidence, and create a perfect copy not only of the hard disk, but also the full environment being investigated. The evidence obtained this way is not a physical object, like a hard disk, but resembles more a visit to the crime scene. The advantage is that this process can be repeated any number of times without any further damage to the evidence already collected.

The reconstruction of the computer system from known parts may appear not to add anything new to the investigation. This is only superficially true. As stated already a computer system is complex, and analysis of its parts may demand too much time and expert knowledge to be of practical use. This may be compared to attempting to determine the colour of a cat by examining its DNA. Although this is in theory possible, it demands sophisticated tools and knowledge. If we can see the cat, its colour can be determined instantly.

We propose to expand the Computer Forensics definition to include collection of hardware and software details of the investigated computer system with the aim to recreate the environment being investigated as closely as possible. It has to be accepted that it is not possible to copy the investigated computing environment completely, or to recreate it later in a completely faithful way. It is also not possible to measure precisely how much of the environment was recreated.

There are already software tools available which allow for the creation of virtual systems following required specifications.[65] These tools can be further developed to create

---

[65] See, eg, *Live View* <http://liveview.sourceforge.net/> at 24 March 2006.

dedicated forensic software to make the reconstruction process more suitable for a forensic investigation. We do not envisage that this will replace the currently used analysis of hard disk images. Rather it should proceed in parallel once the forensically sound disk images are available. In practice the recreation of the system may provide valuable clues for the conventional investigation. This way even if the evidence provided by reconstruction is not admissible in court, it may significantly speed up obtaining results by conventional methods.

While following legal requirements is necessary to ensure the validity of findings, the computer forensics process may also be used in certain situations where it is known that legal prosecution is unlikely. For example the same process may be used to determine the reason of a security breach which was caused by a bug in software when criminal intentions are not present.

10. Conclusion

U.S. Attorney General Janet Reno said in 1995: *"As technology advances, computer crime has grown. We have to ensure that the law keeps up with changing times."*[66] Twelve years later the gap between computer crime and the means to respond to computer crime still exists. We believe that to avoid a crisis it should be acknowledged that it is not possible to formalize, describe and predict every situation, and that a purely mechanistic approach of 'copy all without disturbing the original, analyse the copy, present unquestionable findings' may never be possible in computer forensics. Thus we are proposing a new direction for the development of computer forensics with the aim of providing a better understanding of the strengths and limitations of this discipline.

---

66 'Administration, Congress Introduce New Computer Crime Legislation' (1995) <http://www.usdoj.gov/opa/pr/Pre_96/June95/370.txt.html> at 12 December 2005.