JIST 5(3) 2008

Journal of Information Science and Technology

www.jist.info

Computer Forensics - Past, Present and Future

Derek Bem, Francine Feld, Ewa Huebner, Oscar Bem

University of Western Sydney, Australia

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 objectives 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 would be helpful 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*

Introduction

This paper is about the discipline of computer forensics - its past, its present, and our view of its future. We argue that the challenges facing the discipline today call for new directions and approaches. If computer forensics is to develop into a mature discipline, the work in the areas of definition of terms, standardisation and certification needs to continue. The challenges facing the discipline require a rethinking of its objectives in recognition both of its strengths and of its limitations. Computer forensics needs to move beyond its pre-occupation with purely mechanistic approaches of copying and pre-

serving data: it must embrace technologies and methods that will enable the inclusion of transient data and live systems analysis. This new direction might require a corresponding change in expectations: if we are to develop ways of collecting and analysing volatile information, it may be necessary to ease the requirements for absolute accuracy and certainty of findings.

We aim primarily to appeal to legal professionals, both because there is a lack of literature explaining computer forensics in non-technical terms, and because our vision of the future will involve an interdisciplinary collaboration. The paper is also relevant to computer forensic examiners, law enforcement personnel, business professionals, system administrators and managers, and anyone involved in computer security, as the need for organizations to plan for and protect against technologically-assisted crime is becoming critical (e.g. Edwards, 2006).

The paper begins with a brief overview of the emergence of computer crime and the development of computer forensics as a discipline over the 30 years of its existence. We then discuss some of the challenges the discipline now faces, before making suggestions for its future direction.

Our methodology is in the nature of a meta-analysis of the literature, using some case law and statute law from various jurisdictions (mainly the United States and Australia) as examples. We have not conducted an exhaustive analysis of the issues and law in any one or a number of jurisdictions. However, we believe that the future directions we propose are relevant universally. The nature of computer crime and to some extent the legal responses to it are likely to be similar around the world.

The Emergence of Computer Forensics

Computers first appeared in the mid 1940s, and rapid development of this technology was soon followed by various computer offences. Computer crime is broadly understood as criminal acts in which a computer is the object of the offence or the tool for its commission (AHTCC, 2005). In the mid-1960s Donn Parker, of SRI International, began research of computer crime and unethical computerized activities. He noticed that: *"when people entered the computer center they left their ethics at the door"* (Bynum, 2001). Parker's work continued for the next two decades and is regarded as a milestone in the history of computer ethics.

The first prosecuted case of computer crime was recorded in Texas, USA in 1966 (Dierks, 1993) and resulted in a five-year sentence. In the 1970s and 1980s personal computers became common, both at home and in the workplace; subsequently law enforcement agencies noticed the emergence of a new class of crime: computer crime (Overill, 1998).

[1] Cases and statute law are cited according to the conventions of the particular jurisdiction. When quoting, the original spelling is retained, while Australian spelling is used in the remaining parts of the paper.

Like all crime, this new class required reliable evidence for successful prosecutions. So emerged the discipline of computer forensics, which aims to solve, document and enable prosecution of computer crime. By the 1990s, law enforcement agencies in every technologically advanced country were aware of computer crime, and had a system in place for its investigation and prosecution. Many scientific research centres were also formed, and the software industry started to offer various specialized tools to help in investigating computer crime (Noblett et al, 2000).

With rapid technological progress, computer crime has flourished. However, it is interesting to note that many offences then and now are unreported and subsequently never prosecuted. USA annual Computer Crime and Security Surveys conducted by the CSI/FBI (Gordon et al, 2006) show that from 1999 to 2006, 30% to 45% of respondents did not report computer intrusion, mainly for fear of negative publicity. Australian surveys show much higher figures: in the 2006 AusCERT survey (AusCERT, 2006) 69% of respondents chose not to report attacks to any external party. A reason for not reporting, given in 55% of cases, was that they "didn't think law enforcement was capable" (AusCERT, 2006, p 35). These statistics suggest that the incidence of computer crime is much higher than it might seem, and that confidence in law enforcement capability might result in a higher reporting rate. It is not clear why there is a lack of confidence in law enforcement capability, but it is conceivable that the maturing of computer forensics might increase law enforcement capability and ultimately lead to an improvement in reporting behaviour.

For early investigators involved in computer crimes it became obvious that if findings were to be useful as court evidence they had to comply with the same rules as 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" (Saferstein, 2001). It also became clear that when investigating computer crime the same basic rules applied as in any other crime scene investigation. The investigation process includes phases of physical scene preservation, survey, search and reconstruction using collected evidence, all of which must follow a rigid set of rules and be formally documented (Bassett et al, 2006). This process is detailed in many books, manuals and guides, e.g. Fisher (Fisher, 2003).

First Period Leads to First Definitions

It soon became apparent that computer crime has features justifying a separate field of knowledge or discipline. This field is commonly known as 'computer forensics'. Other names are also used, e.g. 'forensic computing' (McKemmish, 1999), or 'digital forensics' (DFRWS, 2005). The broader term 'digital forensics' refers to digital evidence, understood to be "any information of probative value that is either stored or transmitted in a digital form"

(Whitcombe, 2002). Thus it refers not only to computers, but also to digital audio and video, digital fax machines, and similar. One would expect to see even broader terms like 'electronic forensics' or 'e-forensics' covering all electronic digital and analogue media, but those are rarely used. It appears that by 2008 the term 'computer forensics' is used in a broader sense in relation to all digital devices.

In 1999, Farmer and Venema (Farmer & Venema, 2005) 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 suggested a series of stages an investigator should follow:

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

Another more computer specific definition was offered in 1999 by the Australian Institute of Criminology (McKemmish, 1999):

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

The same guide defines four key elements of this process:

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

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

- Minimal handling of the original.
- Accounting for any change.
- Compliance with the rules of evidence.
- Not exceeding your knowledge.

Subsequently various researchers offered more detailed descriptions of the computer forensics process. For example Mandia, Prosie, and Pepe (Mandia et al, 2003) describe seven components of incident response:

1. Pre-incident preparation.
2. Detection of incident.
3. Initial response.
4. Formulate response strategy.
5. Investigate the incident: data collection followed by analysis.
6. Reporting.
7. Resolution (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. 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 unique to a computing environment. If one were to remove computer specific terms, the definitions would remain valid.
4. Some definitions miss the 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 point that "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.

Computer Forensics as a Separate Science Discipline

The first 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 (1996 in Australia), and the first specialized software tools were developed in the mid-1980s (Whitcombe, 2002). Yet today (early 2008) there is still no agreement on matters of definition and classification. Agreement on terms, standards, and the boundaries of the body of knowledge, as suggested in the previous section, will go a long way to developing computer forensics into a mature scientific discipline.

Like other forensic sciences (e.g. forensic ballistics, pathology, or psychiatry), computer forensics is a distinct body of knowledge requiring approaches and tools specific to its objectives, and specialised education and training of its experts. While the distinctive position of computer forensics might be generally accepted, the formal recognition of computer forensics as a field of forensic science has not yet eventuated. For example, at the time of

writing, there are three forensics institutes in Australia: National Institute of Forensic Science, Senior Managers of Australian and New Zealand Forensic Laboratories and the Australian And New Zealand Forensic Science Society. While these organisations are aware of computer forensics, none of them formally recognises it as a distinct discipline. This can have consequences for the recognition of computer experts as court witnesses.

In Australian courts, the suitability of an expert witness is governed by a combination of rules at the Commonwealth and State levels. The Evidence Act 1999 is the body of rules governing the admissibility of evidence in federal cases and some state courts. Section 79 of that Act allows for the admissibility of expert evidence by a person who "has specialised knowledge based on the person's training, study or experience".

The rule incorporates at least two requirements for admissibility of evidence: (1) that there exists a body of specialised knowledge that is acceptable to the courts; and (2) that the witness has this specialised knowledge. As to (1), the question is whether the particular body of knowledge is sufficiently reliable to form the subject matter about which expert evidence can be given. In common law cases the question is similar: does the evidence derive from a "field of expertise" that is acceptable to the courts? In determining this issue in particular cases, Australian courts have been influenced by case law in the United States. For some time, courts followed the reasoning in Frye v United States (Frye v United States, 1923), which stipulated that a body of knowledge would be acceptable to the courts if it had reached the stage where it was "generally accepted" in the relevant scientific community.

The Frye test was replaced in the United States in 1993 with the Daubert test (Daubert v Merrill, 1993). The Daubert test represents a move away from the scientific community, to the courts themselves as the arbiters of the reliability of scientific evidence. The U.S. Supreme Court suggested five criteria for determining whether science was reliable and, therefore, admissible (Daubert, 1993, p 594):

(1) Is the evidence based on a testable theory or technique?

(2) In the case of a particular technique, does it have a known or potential error rate?

(3) Does the technique have and maintain standards controlling its operation?

(4) Is the underlying science generally accepted within the relevant scientific community?

(5) Has the theory or technique been subjected to peer review?

The fifth criterion makes it clear that courts will seek the views of the relevant scientific community, if necessary, in determining the reliability of the particular body of knowledge.

In Australia, there is no general agreement about which test applies (Frye or Daubert), if either. The law requires that expert evidence meet a

standard of evidentiary reliability, i.e. the specialised knowledge be "sufficiently organised or recognised to be accepted as a reliable body of knowledge or experience" (HG v The Queen, 1999).

The second requirement in Australian law is that the witness has the required specialised knowledge by demonstrating appropriate qualifications and experience. In computer forensics, there is still no formal expert accreditation available. Some private institutions offer computer forensics training (Volante, 2005), and many offer vendor specific software training. While such training is useful it can not be seen as leading to a recognized certification. A similar situation is prevalent in other technologically advanced countries (Ball, 2004), (Armstrong, 2002).

While computer forensic evidence is already being accepted in courts, the discipline will gain much from further specialisation and accreditation. Even though the courts may recognise the general area of computer forensics, the tools, methods and findings in any particular case remain under court scrutiny. Computer forensic experts may be able to give evidence about some matters, but not others, if the court thinks that a particular subject area, method, or findings are insufficiently reliable. The lack of accreditation standards may not have caused great concern during the discipline's infancy. However, as recognised by Meyers and Rogers (Meyers & Rogers, 2004), the scrutiny of expert witnesses and the contesting of their qualifications in court is likely to become more common, making the certification of experts according to recognised standards critical.

Lack of Standards within the Discipline

Another concern is standardisation within the discipline itself. As information security magazine Security Wire Digest noticed (Rogers, 2003):

"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."

Meyers and Rogers outline the areas where standardisation is becoming critical: certification of experts (as discussed above); search and seizure of evidence; and analysis and preservation (Meyers & Rogers, 2004).

There have been many attempts to formulate a set of standards in computer forensics, but none of these sets is updated as often as the discipline requires, and none is commonly accepted, for example:

- The International Organization for Standardization (ISO) set "ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management" (ISO/IEC, 2005). While compliance with ISO 17799 is sometimes quoted in relation to computer evidence, this standard deals mainly with computer security.

- The National Institute of Standards and Technology (NIST) "Guide to Integrating Forensic Techniques into Incident Response" (Kent et al, 2006) 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).

Probably the most consistently updated series of publications are offered by the National Institute of Justice (NIJ), the research, development, and evaluation agency of the U.S. Department of Justice (NIJ, 2007). The guides cover all aspects of computer forensics, and include a cautionary statement defining their scope and role like the one below (Hagy, 2007):

"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.

In summary, there are many 'best practice' guides or recommendations from many sources, and there is interesting exploratory research being done. For example, Carney and Rogers present a statistical approach for computer forensics event reconstruction as a first step towards a standardised method (Carney & Rogers, 2004). As the authors point out, studies in other forensic sciences have yielded standardised processes for determining the sequence of events, for example, to determine how long a body will take to decompose under certain conditions. A standardised process for determining the sequence and timing of digital events within a measurable accuracy rate "would take computer forensics one step closer to being an established forensic science" (Carney & Rogers, 2004, p 7).

Standards across disciplines

Sooner or later anyone working with computer forensic evidence notices that it would help tremendously "if only" (Mitchison, 2003):

- ... 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)".

In other words, standardisation is required not only within the discipline, but also amongst all professionals that interact in the investigation and prosecution of computer crime: lawyers, IT professionals, enforcement officers and businesses.

One attempt to develop common standards for investigation is analysed here in more detail to demonstrate problems 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 (CTOSE, 2006). The aim was "to develop a methodology, architecture, a process model, and a common set of tools and procedures for an electronic investigation". The project closed in September 2003 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 illustrates the typical life span of computer forensic research projects which often start enthusiastically, but due to complexities of the field and its multi-disciplinary nature 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.

Emerging problems

A major new challenge for the future of computer forensics is to modernise its methods and processes to maximise the yielding of valuable evidence. It is necessary to cover some of the discipline's history to understand its current approach and the future directions that need to be taken.

The first period in computer forensics history is characterized by dealing with relatively small capacity storage devices ("A Brief History of the Hard Disk Drive", 2005). This allowed for the complete hard disk to be copied and analysed exhaustively in search for evidence. Since then 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 households as well as most workplaces use it extensively.

Many books dealing with digital evidence were written during the last decade, and computer forensics methodology was well developed to handle simple, typical cases. A good example is a series of publications from the U.S. Department of Justice, the National Institute of Justice (NIJ, 2007). The

NIJ publications are probably the most complete set forming a small library which covers all main areas of interest to digital forensics personnel. Some areas covered are:

- "A Guide for First Responders" (Ashcroft, 2001)
- "Forensic Examination of Digital Evidence: A Guide for Law Enforcement" (Hart, 2004)
- "Investigations Involving the Internet and Computer Networks" (Hagy, 2007)
- "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors" (Hagy, 2007)

The NIJ also tests and publishes the test results of various tools, e.g. disk imaging tools and write blockers (devices that prevent writing to storage media).

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 utilities which they considered appropriate. One of the most useful tools was a hex editor, which allowed for examination of the underlying structure of computer media. Some software developers noticed the potential of the emerging field and developed their products in this direction. Since the 1990s many companies developed software tools aimed at the forensic market, and there are also many free and open source tools.

The current philosophy faces a problem which was noticed in the U.S. Department of Justice digital evidence guide (Hart, 2004) stating: *"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, because of the following technological challenges:

- By 2007 single hard disk drives reached the capacity of 1TB (terabyte) in standard PC form. Large capacity drives create practical issues: copying data is slow, and so is searching for evidence. To visualize the problem: a single 1TB disk can digitally store all world literature produced in one year (JISC, 2004).
- File systems used in computers allow for data to be hidden from a normal user, and made visible only if special tools are used (Huebner et al, 2006).
- Many properties and mechanisms of computer operating systems are not documented, or poorly documented, and some can be used to hide data (Bem & Huebner, 2006).

- On-line storage (Internet storage or virtual hard drive) became easily accessible ("Internet Virtual Storage", 2007). Some Internet service providers offer free storage space, data encryption, and client details confidentiality.
- Storage virtualisation technologies allow for data to be kept on storage devices which are physically at other locations, in other legal jurisdictions and countries, and can be accessed as if they were local (Clark, 2005).
- It is easy to maintain a Web site located beyond the local legal jurisdiction (Gordon, 2004), and securing the cooperation of other countries' legal systems can be slow, costly, and difficult. Even the Web hosting sites 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 ("Domains by Proxy's Privacy Policy", 2006).
- Various strong data encrypting tools, which not so long ago had only limited distribution, are now available freely to anyone (TrueCrypt, 2007). As an example, one source estimated that it would take 270 days to break 56-bit RC5 encryption using 4000 teams operating 10,000's machines (Siegfried et al, 2004). Longer encryptions keys are more difficult to break, e.g. 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 time of 10 000 000 000 000 000 000 000 years would be required to check all possible combinations (Seleborg, 2004).
- Small, easy to hide (or destroy) storage devices have become common and inexpensive. By the end of 2006 USB flash drives reached capacities of up to 64GB (Kanguru, 2007). 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 without leaving any personal data behind"* (PortableApps, 2006).

The main conceptual problem in computer forensics is the need to understand that data we intend to capture is dynamic. While making a static copy of a hard disk may produce 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 in a certain order dictated by the architecture of computer systems and the technology used to build them, e.g. data life span in the main memory or on the network may only be nanoseconds. This is often referred to as the Order of Volatility (Farmer & Venema, 2005).

New Directions in 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 evidence collected from computer systems is not like other physical evidence, and it may not be subjected to the same rules. 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. For example, the Cyber Forensic Field Triage Process Model (Rogers et al, 2006) is a model for onsite identification, analysis and interpretation of digital evidence without acquiring a complete forensic image. The model is designed to be useful in situations where investigations of the whole system need to be made onsite in a short space of time.

Collecting memory images 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 courts of law.

Courts scrutinise evidence carefully to ensure that convictions are based only on the most reliable of evidence. However, that does not mean that all evidence must be 100% certain. Evidence gains its strength, in many cases, from aggregation. This is particularly so for circumstantial evidence: a combination of evidence that would not stand up to scrutiny alone might be very compelling when taken together (Shepherd v The Queen, 1990).

Courts readily accept evidence of less than 100% accuracy. Consider fingerprint evidence which is well recognised by courts despite a momentary attack on its credentials under the *Daubert* test in the case of *U.S. v. Llera Plaza (U.S. v Llera Plaza, 2002).* A fingerprint comparison is an expert opinion based on points of identity between the two prints. Fingerprint analysis, like all types of "pattern matching" evidence (including ballistics) is not an exact science. DNA evidence, also widely accepted, is expressed in terms of statistical probability - again, not 100% certainty. The important thing is that the expert be able to explain to the court the potential effect of any lack of certainty, that is, whether or not the uncertainty is fatal to the integrity of the data as a whole.

We might draw an analogy to the field of computer forensics. If investigators are able to take an image from memory indicating the presence of a pornographic image, the fact that the investigation technique had modified the data in memory in the process may not matter. It will only matter to a court if the modification could possibly have constructed a pornographic im-

age (or fragment of one) where there was none originally. The probability of such a spontaneous event is so minimal that the courts could nevertheless find the data to be reliable.

Computer systems are increasingly complex, and analysing their parts, like the disk or memory image, may not readily reveal all available information. This calls for a new approach (again, one that removes the expectation of certainty) i.e. to attempt to recreate the computer system and its immediate environment by reproducing the collected images in a controlled way, 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, as well as the specific setups and functions of the system itself. 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.

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 computing environment completely, nor to recreate it later in a completely faithful way.

There are already software tools available which allow for the creation of virtual systems following required specifications (Live View, 2007). These tools can be further developed to create dedicated forensic software making the reconstruction process more suitable for a forensic investigation. This should proceed in parallel with the analysis of hard disk images. The reconstruction 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.

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."* (U.S. Department of Justice, 1995).

Thirteen years later, the gap between computer crime and the means to respond to it still exists. The continuing lack of agreement on definitions, standardised processes, and accreditation standards are preventing the growth of computer forensics into a mature scientific discipline. This has consequences for the discipline's credibility in the eyes of the law and, hence, the successful prosecution of cases. The pre-occupation with the mechanistic approach of 'copy all without disturbing the original, analyse the copy, present unquestionable findings' is problematic - it carries with it the risk that valuable evidence will be lost by failing to investigate alternatives such as reconstruction

of the investigated environment, memory forensics and analysis of live systems.

We must work across disciplines to ensure standards are developed for all participants in the system. We must recognise that, while it is necessary to develop and maintain exacting standards to ensure accuracy of data where possible, we should also acknowledge that less-than-100% accurate data can still yield results that are invaluable both to the investigation and to the prosecution of computer crime.

References

AHTCC. (2005). Concepts and terms. High Tech Crime Brief Retrieved 12 August 2006 from www.aic.gov.au/publications/htcb/htcb001.pdf

Armstrong, I. (2002) Computer Forensics Detecting the Imprint. SC Magazine.

Ashcroft, J. (2001) Electronic Crime Scene Investigation: A Guide for First Responders. from http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm

AusCERT. (2006) 2006 Australian Computer Crime and Security Survey: AusCERT.

Ball, C. (2004) Finding the Right Computer Forensic Expert. Retrieved 23 October 2005 from www.craigball.com

Bassett, R., Bass, L., & O'Brien, P. (2006) Computer Forensics: An Essential Ingredient for Cyber Security. Journal of Information Science and Technology, JIST 3(1)

Bem, D., & Huebner, E. (2006) Alternate Data Streams in Forensic Investigations of File Systems Backups. Current Computing Developments in E-Commerce, Security, HCI, DB, Collaborative and Cooperative Systems, pp 449-460, Athens

A Brief History of the Hard Disk Drive. (2005) Retrieved 28 November 2005 from http://www.pcguide.com/ref/hdd/hist-c.html

Bynum, T. (2001) Computer Ethics: Basic Concepts and Historical Overview. Stanford Encyclopedia of Philosophy. Retrieved 12 January 2007 from http://plato.stanford.edu/archives/win2001/entries/ethics-computer/

Carney, M., & Rogers, M., (2004) The Trojan Made Me Do it: A First Step in Statistical Based Computer Forensics Event Reconstruction International Journal of Digital Evidence, 2(4)

Clark, T. (2005) Storage Virtualisation technologies for Simplifyng Data Storage and Management (1 ed.). Upper Saddle River, NJ: Pearson Education.

CTOSE Cyber Tools On-Line Search for Evidence. (2006) Retrieved 12 October 2006 from http://www.ctose.org/info/index.html

Daubert v. Merrell Dow Pharmaceuticals Inc (92-102), 509 U.S. 579 (1993) Legal Information Institute (LII). Retrieved 15 January 2007 from http://straylight.law.cornell.edu/supct/html/92-102.ZS.html

Daubert: The Most Influential Supreme Court Ruling You've Never Heard Of. (2003) Tellus Institute.

Dierks, M. P. (1993) Computer Network Abuse. Harvard Journal of Law & Technology, 6(2)

Digital Forensic Research Workshop (DFRWS). Retrieved 22 April 2005, from http://www.dfrws.org/

Domains by Proxy 's Privacy Policy. (2006). Retrieved 12 December 2006 from http://www.domainsbyproxy.com/popup/subpoenapolicies.aspx

Edwards, C. (2006) Computer forensics: are you clued-up? Information Professional 3(2), pp 32-35.

Farmer, D., & Venema, W. (1999). Murder on the Internet Express. Retrieved 15 June 2006 from http://www.porcupine.org/forensics/

Farmer, D., & Venema, W. (2005) Forensic Discovery (1st ed.). Upper Saddle River, NJ: Addison-Wesley.

Fisher, B. A. J. (2003) Techniques of Crime Scene Investigation (7 ed.): CRC Press.

Frye v United States (Frye v United States 293 F 1012 (1923)

Gordon, J. (2004) Illegal Internet Networks in the Developing World. Retrieved 6 December 2005 from http://cyber.law.harvard.edu/home/research_publication_series

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006) 2006 CSI/FBI Computer Crime and Security Survey.

HG v The Queen (1999) 197 CLR 414.

Hagy, D. W. (2007) Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. Retrived 15 December 2007 from http://www.ojp.usdoj.gov/nij/pubs-sum/211314.htm

Hagy, D. W. (2007) Investigations Involving the Internet and Computer Networks. Retrieved 20 January 2006 from http://www.ojp.usdoj.gov/nij/pubs-sum/210798.htm

Hart, S. V. (2004) Forensic Examination of Digital Evidence: A Guide for Law Enforcement. Retrieved 20 November 2005 from http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm

Huebner, E., Bem, D., & Wee, C. K. (2006) Data hiding in the NTFS file system. Digital Investigation,3 (4).

Internet Virtual Storage. (2007) Retrieved 20 November 2006 from http://www.cryer.co.uk/resources/virtualstorage.htm

ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management. Retrieved 12 January 2007 from http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html

JISC (2004) The Data Deluge: Preparing for the explosion in data. Retrieved 18 January 2007 from http://www.jisc.ac.uk/

Kanguru Solutions. (2007) Retrieved 22 February 2007from http://www.kanguru.com/

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006) Guide to Integrating Forensic Techniques Into Incident Response. Retrieved 16 June 2007 from http://csrc.nist.gov/publications/nistpubs/

CERT, Software Engineering Institute. (2007) Live View. Retrieved 12 February 2007 from http://liveview.sourceforge.net/

Mandia, K., Prosie, C., & Pepe, M. (2003). Incident Response & Computer Forensics, Second Edition (2nd ed.). Emeryville, CA: McGraw-Hill/Osborne.

McKemmish, R. (1999) What is Forensic Computing? : Australian Institute of Criminology.

Meyers, M., & Rogers, M. (2004) Computer Forensics: The Need for Standardization and Certification International, Journal of Digital Evidence, 3(2)

Mitchison, N. (2003). The challenge of electronic evidence - the European response. Retrieved 12 September 2005 http://www.gi-ev.de/fachbereiche/sicherheit/fg/sidar/imf2003/imf2003-keynote-neil-mitchison.pdf

National Institute of Justice. (2007) Retrieved 20 January 2007 from http://www.ojp.usdoj.gov/nij/

Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and Examining Computer Forensic Evidence. Forensic Science Communications, 2(4)

Overill, R. E. (1998) Computer crime - an historical survey. Retrieved 20 December 2006 from http://www.kcl.ac.uk/orgs/icsa/Old/crime.html

PortableApps. (2006) Retrieved 23 August 2006 from http://portableapps.com/

Rogers, M. (2003). Security Perspectives Computer Forensics: Science or Fad? Security Wire Digest, 5(65)

Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006) Computer Forensics Field Triage Process Model, Conference on Digital Forensics, Security and Law, from http://www.digitalforensics-conference.org/CFFTPM/CDFSL-proceedings2006-CFFTPM.pdf.

Saferstein, R. (2001) Forensic Science Handbook (Vol. 1): Prentice Hall.

Seleborg, S. (2004) About AES - Advanced Encryption Standard. Retrieved 2 November 2007 from http://www.axantum.com/AxCrypt/etc/About-AES.pdf

Shepherd v The Queen (1990) 170 CLR 573

Siegfried, J., Siedsma, C., Countryman, B.-J., & Hosmer, C. D. (2004). Examining the Encryption Threat. International Journal of Digital Evidence, 2(3).

TrueCrypt. (2007) True Crypt - Free Open-Source On-The-Fly Disk Encryption Software. Retrieved 15 January 2007 from http://www.truecrypt.org/

United States v Liera Plaza, (2002) 188 F.Supp.3d 549 (E.D.Pa., 2002)

U.S. Department of Justice, Administration, Congress Introduce New Computer Crime Legislation (1995). Retrieved 12 December 2005 from http://www.usdoj.gov/opa/pr/Pre_96/June95/370.txt.html

Volante (2005) Retrieved April 2005 from http://www.volante.com.au/

Whitcombe, C. M. (2002). An Historical Perspective of Digital Evidence: A Forensic Scientist's View. International Journal of Digital Evidence, 1(1).

Author Biographies

Derek Bem is a lecturer in the School of Computing and Mathematics, University of Western Sydney, and a member of the Computer and Network Forensics Research group. He has over 30 years of experience in ICT industry, academia, and as a court examiner and expert witness in computer forensics. His research interests focus on the role of virtual environments in computer forensics and live forensic investigations. He published in major computer journals and international conferences.

Francine Feld is a lecturer in the School of Law, University of Western Sydney, and a member of the Computer and Network Forensics Research group. She teaches and researches in the areas of cirminal law, procedure adn evidence.

Ewa Huebner, Fellow of the Australian Computer Society, is the leader of the Computer and Network Forensics Research group in the School of Computing and Mathematics, University of Western Sydney. Her main research field is operating systems and computer forensics, specifically memory forensics. She published her work in major international journals and conferences. She was the guest editor for the special issue on computer forensics of the ACM Operating Systems Review 42(3) April 2008.

Oscar Bem is a fourth year student of law and business at the School of Law, University of Western Sydney.