

# Forensic Computing

## *Developing a Conceptual Approach for an Emerging Academic Discipline*

Vlasti Broucek, Paul Turner

*School of Information Systems, University of Tasmania, GPO Box 252-87 Hobart, Tasmania, Australia, E-mail: Vlasti.Broucek@utas.edu.au, Paul.Turner@utas.edu.au*

‘The process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable’. (McKemmish, 1999)

‘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’. (Farmer & Venema, 1999)

**Key words:** Forensic Computing, Digital Evidence, Legal admissibility, Computer Security

**Abstract:** Forensic computing (FC) is an emerging academic discipline that is difficult to define. This paper attempts to define taxonomy and interrelationships between specific academic and scientific disciplines involved. First, it provides a review of recent forensic computing literature and presents a taxonomy of the emerging field based on the contributions of authors from a number of disciplines including computer security, computer law and information systems management. Second, this paper conducts a preliminary exploration of the interrelationships between a number of specific issues that converge on some of the central themes of forensic computing as identified by McKemmish (1999): identification, preservation, analysis and presentation of computer evidence. Four specific issues are examined: the sophistication of technical security measures versus the need for evidence acquisition, a key distinction between computer security and forensic computing, the management strategies and

issues involved in FC and last but not least the political dimensions of forensic computing.

## **1. BACKGROUND**

‘The growth of the Internet and on-line technologies is having a significant impact on governments and communities - transforming the way they do business, provide information and services, network and interact... The information economy provides new opportunities to strengthen systems for communication, interaction and information exchange...’ National Office for the Information Economy (<http://www.noie.gov.au>).

Digitalisation creates risks and challenges for legal, technical and social structures. The technical capability to store, manipulate, and transmit all types of data at high speeds across global digital networks has become common place in academic, business and social environments. Alongside the exciting opportunities of the ‘information age’, there is a growing awareness of the serious risks and challenges posed by these digital developments.

A fundamental cause of many of these risks is the large numbers of ways that individuals and/or groups can utilise these technologies to engage in inappropriate, criminal, or other illegal behaviour. While it can be assumed that much of this behaviour continues to go on undetected, when it is identified the need for evidence and proof becomes of paramount importance. However, aside from the technical difficulties of detecting, identifying and recording such behaviour, other additional considerations arise over certain types of evidence acquisition (‘forensic’) behaviour and the legal admissibility of the digital evidence that they generate.

At a practical level, the last ten years have seen large numbers of publications by computer security specialists, legal professionals and information managers on technical, legal and organisational issues arising from illegal or inappropriate behaviours in digital environments.

In this context, numerous researchers from a variety of disciplines have explored different aspects of these risks and solutions. However to date, exploration of the interrelationships between these issues has been hampered by a general lack of awareness of the range of issues and the lack of a conceptual framework within which to position these different research approaches. From an academic perspective the lack of a coherent conceptual framework has contributed to a fragmented approach and inhibited the

development of the specialised skill sets required to advance the theory and practice of forensic computing.

The next section provides a preliminary attempt to identify the range of legal, technical, management and policy approaches that contribute to the emerging discipline of forensic computing research.

## **2. PART ONE: DEVELOPING A TAXONOMY OF FORENSIC COMPUTING**

The lack of an overarching conceptual framework for forensic computing is both confusing and frustrating for researchers who wish to explore the inter-disciplinary dimensions of issues concerned with the identification, collection and analysis of computer evidence. As a preliminary starting point it is useful to first consider the range of topics and viewpoints that intersect in the research space central to the emerging discipline of FC. It is anticipated that this initial taxonomy will evolve and change rapidly as the volume of research and issue areas expands in FC. The taxonomy is presented in a structured form of known facts as presented in the literature. We hope that this approach will be able to be further refined by future developments in this field. Four major disciplines form this preliminary taxonomy of forensic computing - computer science, law, information systems and social sciences.

### **2.1 Computer Science**

FC is thought to be primarily about computing and computing technologies. However, in the networked environment, it is evident that a holistic approach covering all aspects of digital communication is important (Patel & Ciardhuáin, 2000). Mobile phones, PDAs and other electronic devices can store vital information; hence these devices also have to be a subject for forensic computing. Three major parts of computer science can be identified as important in the development of FC.

#### **2.1.1 Operating Systems and Application Software**

Operating systems and their sub-systems maintain valuable log files suitable for forensic investigation. These files are usually 'time-stamped'; however, their time resolution is relatively low. Some privileged commands (like UNIX's *su*) maintain their own log files.

Expert knowledge of operating system's abilities is also important in discovering tampered/changed/new files in the system. For example MACtimes (abbreviation derived from UNIX *mtime*, *atime* and *ctime* attributes of files) can be very useful. However, detailed knowledge of the rules for changing these time-stamps is necessary, as there are huge differences between different operating systems (eg UNIX derivatives and Microsoft Windows NT) (Farmer, 2000).

Farmer and Venema (2000) argue that system administrators/forensic computing experts have a distinctive advantage over offenders<sup>1</sup> because of their detailed knowledge of the system and its logging facilities, for example:

- Suspicion of intrusion should arise whenever WWW servers on well-known sites are, 'according' to log files, idle for several hours.
- Combinations of different log files can provide a better picture and more accuracy in relation to system activity.
- Destruction of information can be more complicated than may initially be acknowledged. This is discussed further by Farmer and Venema (Farmer, 2001; Venema, 2000a).
- 90% of files on servers are not touched (their MACtimes are not changed) for more than year. This period may be even longer for Microsoft based systems (Farmer & Venema, 2000).

### 2.1.2 Systems Programming and Programming Languages

Programming and debugging skills together with detailed knowledge of systems programming are necessary to discover and/or analyse modified or new processes/programms running on systems. In the first instance, the forensic expert will utilise built in commands and shell scripting. Built in commands such as *grep* and *strings* can be very useful if mastered by administrators and investigators. This is further discussed by Venema (2000c).

It is argued that languages with bounds checking, pointer validation, memory management are needed for more secure applications, for example, ADA and Java (Sibert, 1996). Unfortunately, particularly Java developments have not to date lived up to expectations and many problems with implementation continue to mean that often it is not very secure.

<sup>1</sup> The authors would contest this viewpoint. From personal experience in network administration it is clear that top hackers often have much better skills than administrators. Indeed, many security holes are discovered and reported to software companies by 'friendly hackers'.

### 2.1.3 Computer security

Forensic computing is often wrongly considered as being simply another term for computer security. The second part of this paper presents arguments to counter this view. However, computer security remains one of the most important parts of FC.

It is critical to be prepared for system intrusion (Venema, 2000a). Network administrators and forensic computing experts should study and closely follow advice issued by organisations like AUSCERT, CERT, FIRST, SANS.

Advanced logging systems should be implemented. For example, TCP Wrappers available from <ftp://ftp.porcupine.org/pub/security/index.htm> by Dan Farmer and Wietse Venema are widely used. These systems provide much more comprehensive logging and security than standard auditing tools.

Many recent cases of computer vandalism arose due to a lack of, or the poor quality of virus protection (Lemos, 2000) and virus protection plays an important role in computer security and indirectly in forensic computing.

Boulanger (1998) identifies five distinct categories of tools and techniques successfully used by both hackers and the professional security community:

- Scanners - network auditing tools – SATAN (Farmer & Venema, 1995), ISS and host based static auditing tools COPS (Farmer & Spafford, 1990)
- Remote exploits: leading to development of firewalls
- Local exploits: 3 times the number of new local versus remote exploits reported
- Monitoring tools – sniffers and snoopers
- Stealth and backdoor tools

## 2.2 Law

Another core dimension of FC as an academic discipline is research into legal issues related to inappropriate, criminal, or other illegal behaviour using information technology tools. The key issues relate to the admissibility of computer evidence, evidence acquisition behaviours and privacy/data protection.

### 2.2.1 Computer Law

There are a host of legal questions concerned with FC. These were articulately presented at a special expert working group meeting in Tokyo in October 1998 organised by United Nations (Graycar, 2000).

Sommer (1998a, 1998b) explores computer law and computer security from several viewpoints and in his work highlights:

- Current systems are rarely designed to collect and protect the integrity of the type of data required for, and admissible in legal proceedings.
- Multiple and independent streams of evidence are required for legal proceedings.
- Legal ‘proof’ does not correlate directly with scientific ‘proof’.

Different approaches are employed in common law and civil law jurisdictions. This fact raises many issues about supra-national and international legal codes, eg European Union, OECD.

The computer industry often regards computer crimes as technical problems with technical solutions. However, legal solutions and knowledge are also vital. Often the technical investigation of illegal behaviour will produce ‘proof’ and evidence that may be inadmissible or flawed in terms of legal proceedings.

At present, there is a strong trend towards greater international co-operation on encryption controls and specialised FC training. Also many efforts with privacy, eg European Union, data protection directive and *Draft Convention on Cyber-crime* (European Committee on Crime Problems & Committee of Experts on Crime in Cyber-Space, 2000).

Finally, Masters (2000) highlights the following in the specific area of computer crime:

- Issues are complex, difficult and involve multiple jurisdictions.
- Legal frameworks continue to lag behind technological developments, eg definitions of computer crime within the Australian legislation are already outdated
- The general lack of case law is impeding the development of solutions.

### 2.2.2 Criminal, Civil and Soft Law

To date there has been a strong focus on criminal law, its investigation and prosecution. However, areas that require further examination include the measures and approaches that can be employed in civil cases and additionally what soft law ‘codes of practice’ and business procedures can be deployed to reduce risk. Another key aspect is *enforcement* of any new laws that are introduced.

Other dimensions include unusual legal defences for particular behaviours, eg case where a teenage hacker obtained ‘not guilty’ verdict based on a defence that such behaviour was ‘computer addiction’ (*Bedworth Case - UK*, 1993; Kelman, 1999).

## 2.3 Information Systems

Information systems contribute to the taxonomy of forensic computing in two distinctive areas of systems management/policies and user education.

### 2.3.1 Systems Management and Policies

Systems monitoring, remote control, e-mail and Internet access policies are central to FC. But there are clearly legal and social issues with the development of such policies, most obviously privacy and surveillance concerns.

Other management issues relate to reactions to computer attacks. Only management can decide how to behave in the case of cyber attacks. Two dominant strategies tend to be deployed - allowing monitoring and/or investigations on-line or 'pulling the plug'<sup>2</sup>. There is already a wide-ranging discussion on these different strategies:

- A number of successful cases have been based on the former approach (Cheswick, 1998; Christy, 1998; Stoll, 1988, 1989); Mitnick admits that this approach led to his arrest (Poulsen, 2000).
- 'pulling the plug' can be deployed for a number of reasons, but primarily it is deployed to protect company interests and/or intellectual property, eg recent Microsoft case (*Microsoft Responds to Security Issue*, 2000)

### 2.3.2 User Education

The authors' personal experience highlights that user education can significantly decrease risk of inappropriate, criminal, or other illegal behaviour. Users have to be educated about protection against computer viruses and inappropriate use of Information Technology, eg vindictive e-mail (Verreck, 2000). Recently, the majority of inappropriate, criminal, or other illegal behaviour related to Information Technology has been generated not by external attackers but by employees (insiders).

## 2.4 Social Science

A key topic on the socio-political agenda at national and international levels is privacy versus encryption control and involves debates about Key Escrow (the old clipper debate) (Denning, 1997; Denning & Branstad, 1996; Reno, 1996) versus PGP (Zimmerman, 1996, 2001).

<sup>2</sup> 'pulling plug' - preventing any access to compromised/attacked system to prevent further spread of attack/compromise

Activism, hacktivism and cyber-terrorism in the public sphere have continued to attract the attention of politicians, the media and the general public (Denning, 1999) and also impact on FC.

Additionally there are debates on the potentially negative social and psychological effects of computing on particular sectors of society, eg youth. The tendency to create social isolation and changed perception of reality (right and wrong) in the Internet space and the implications of inappropriate behaviour arising from the creation of the 'computer game mentality'.

## 2.5 Non-Specific

The work of some authors does not fit neatly into the taxonomy, but is still a part of the emerging area of FC. The topics covered here are:

- The need for comprehensive documentation (Anderson, 1998)
- The need for specialised training in FC and what that training might cover (Reno, 1996)
- The need for evidential authentication (Bates, 2001)

## 3. PART TWO: FORENSIC COMPUTING ISSUES: EXPLORING SOME INTERRELATIONSHIPS.

The preliminary taxonomy above covers a broad range of issues and approaches impinging on the emerging discipline of forensic computing. It highlights that any coherent research framework must acknowledge differences in the focus of the approaches: individual, organisational, national, and supra-national; differences in the scale of systems: personal computer and other individual devices; intranet; extranet, VPN and the Internet; and differences in the participants and audiences engaged in these topics. It also highlights that a number of specific issues involve series of perspectives, levels of abstraction and interrelationships.

The second part of this paper conducts a preliminary exploration of the interrelationships between a number of specific issues central to ongoing FC research.

The sophistication of technical security measures versus the need for evidence acquisition (McKemmish, 1999; Sommer, 1998b). This relates to the fact that most systems currently used for computer security are not designed with the need to track, trace and generate legally admissible evidence.

An aspect of this issue can be illustrated in relation to the hacker attack on the Rome Air Development Center, Griffiss Air Force Base, New York, March 28, 1994 ('Rome Labs'). This case is interesting, not least because while the crime was conducted in USA, proceedings against one of the hackers were initiated in the UK.

Following Christy (1998), the Rome Labs incident was fully investigated by the Air Force Office of Special Investigation (OSI) but left numerous questions unanswered. In this regard, Sommer (1998b) illustrated how the intrusion detection systems (IDS) used in the Rome Labs could also be utilised as forensic tools. Sommer analyses the investigation conducted by OSI both as an academic and as a professional FC expert<sup>3</sup>. Following a detailed analysis he concludes that

'Almost every individual stream of digital evidence could be challenged.'  
(Sommer, 1998b)

Ultimately, this evidence was never tested in court because the defendant engaged in a plea-bargaining deal and pleaded guilty. However, Sommer's analysis is very useful in pointing out that '*Current intrusion systems are not designed to collect and protect the integrity of the type of information required to conduct law enforcement investigations*'. This analysis also details a range of issues involved in using log files to derive evidence, particularly that they can be compromised prior and during collection of the evidence as well as during post-collection analysis.

Increasingly there is an acknowledgement that computer security systems can easily be tainted and their evidence contaminated. There are many known hacks to fix *wtmpx*, *utmpx* and other log files often used as a source of information on system events (Farmer & Venema, 1993). In a series of recent articles Farmer and Venema (Farmer, 2000, 2001; Farmer & Venema, 2000; Venema, 2000a, 2000c) have dealt directly with these issues from a technical perspective. In a personal communication to the authors, Venema indicated that FC is still very immature and at the beginning of a steep learning curve (Venema, 2000b). However beyond these technical approaches and given the Rome Labs example there is a need for more consideration of the legal implications of manipulating log and audit files in terms of legal admissibility.

From a more legalistic perspective McKemmish (1999) has tried to formalise key elements of FC and has tried to establish what he calls *Primary Activities of Forensic Computing* and *Rules of Forensic Computing*. The four rules he establishes are – minimal handling of the original, account

<sup>3</sup> Sommer was hired by defence lawyers in the UK involved in the Rome Labs case to test the quality of the OSI prosecution teams computer 'forensic' evidence.

for any change, comply with the rules of evidence and do not exceed your knowledge.

The distinction between computer security and forensic computing (Patel & Ciardhuáin, 2000). For example, ‘child pornography on the world-wide web’. Here criminal activity requiring forensic analysis is conducted without any breach of computer security systems.

The difference between IT security and FC is clarified in Patel and Ciardhuáin (2000) using the well-known issue of the use of the Internet for distributing child pornography. While this activity is clearly illegal in a majority of legal jurisdictions and is a matter for forensic computing investigations, it is rare for these cases to involve computer security measures being broken. Paedophiles do not need to break into WWW servers to access data and can use completely legal ways of accessing the data. Hence, computer security cannot usually be used to prevent this type of repugnant behaviour.

Another example, from the author’s personal experience, illustrates this difference. A student at the University was personally attacked by e-mail following an innocent chat on ICQ. The student began to receive life-threatening e-mails. Initially with only verbal threats, but later on with attached pictures and movies. At no time were any security measures breached. In this particular case the ‘forensic’ investigation was very easy because the offending e-mails were sent from a ‘hotmail’ account with the sender making no attempt to disguise his/her identity. Using simple UNIX commands (*nslookup*, *traceroute* and looking into several log/auditing files) the offender was traced back to his/her dial-up point. The following table illustrates key distinctions between computer security and forensic computing.

Table 1. Key distinctions between Computer Security and FC

Security	Forensic Computing
Protects the system against attack	Does not protect the system against attack
Usually in real time	Post mortem
Conducted by computer specialists	Can be conducted by computer specialists, but often this is not the case
Restricted environment for presentation of developments, issues	Evidence is nearly always presented to non-IT/IS personnel
Can be bypassed by trusted individuals/users	Integrity of the evidence is most important

The management strategies and issues involved in allowing on-going security breaches for evidence acquisition and tracking versus ‘pulling the plug’. A number of corporate examples are discussed to illustrate these issues.

From the perspective of allowing ongoing security breaches for evidence acquisition it is clear that the Rome Labs case (Christy, 1998), the Mitnick case (Shimomura, 1995), the development and use of 'Honey pots' (Even, 2000) and the tracking of computer espionage (Stoll, 1988, 1989) provide strong arguments against 'pulling the plug'. These cases illustrate the advantages for forensic investigations of tracking and tracing hackers during ongoing security breaches. On the flipside of this, the recent Microsoft case (Bace, 2000; Leyden, 2000; Maher, 2001; *Microsoft Responds to Security Issue*, 2000; Mitnick, 2000; Poulsen, 2000; Rohde, 2000; Sliwa, 2000; Verton, 2000; Weiss & Rosencrance, 2000) highlights how sensitive this issue can be, particularly for information and communication based industries. Here business reputation as well as specific commercial data are at risk.

The political dimensions of forensic computing in an era of free access to public encryption (PGP and Key Escrow debates).

The use of encryption by individuals as well as by public and private sector organisations has become increasingly common. For policy-makers access to encryption creates issues in relation to law enforcement, privacy and surveillance powers. Clearly for criminals, hackers and other individuals engaging in illegal or inappropriate behaviour, encryption provides protection. As the Aldrich Ames Spy case illustrated (Reno, 1996) encrypted data files obtained as part of an investigation are basically useless as evidence.

Internationally a systematic response to cyber crime is still in its early stages of formulation but moves are beginning to be made. For example, the *Draft Convention on Cyber-crime* (European Committee on Crime Problems & Committee of Experts on Crime in Cyber-Space, 2000). This has subsequently attracted the attention of libertarian groups, Internet service providers (ISPs) and user communities because of the potential threat to freedom of information and privacy.

#### 4. CONCLUSION

This paper has explored some of the key issues in forensic computing and from an academic perspective has initiated the development of a more coherent conceptual framework within which to consider developments in FC. Although the paper is clearly exploratory it is anticipated that it will make a valuable contribution to the emergence of forensic computing as an academic discipline.

## 5. REFERENCES

- Anderson, M. R. (1998). *Computer Evidence Processing: Good Documentation Is Essential*, [www]. New Technologies, Inc. Available: <http://www.forensics-intl.com/art10.html> [2000, 20 December 2000].
- Bace, B. (2000). *Understanding Microsoft's October 26th Incident*, [www]. TripWire. Available: <http://www.tripwire.com/press/beckybaceWP.cfml> [2000, 12 December 2000].
- Bates, J. (2001). *DIVA Computer Evidence (Digital Integrity Verification and Authentication)*, [www]. International Journal of Forensic Computing. Available: <http://www.forensic-computing.com/archives/diva.html> [2001, 26 March 2001].
- Bedworth Case - UK*. (1993). [www]. Available: [http://www.eff.org/pub/Net\\_culture/Hackers/uk\\_court\\_acquits\\_teenage\\_hacker.article](http://www.eff.org/pub/Net_culture/Hackers/uk_court_acquits_teenage_hacker.article) [2001, 26 March 2001].
- Boulanger, A. (1998). Catapult and grappling hooks: The tools and techniques of information warfare. *Systems Journal*, 37(1).
- Cheswick, W. (1998). An Evening with Berferd. In D. E. Denning & P. J. Denning (Eds.), *Internet Besieged: Countering Cyberspace Scofflaws* (pp. 103-116): ACM Press.
- Christy, J. (1998). Rome Laboratory Attacks: Prepared Testimony of Jim Christy, Air Force Investigator, before the Senate Governmental Affairs Committee, Permanent Investigation Subcommittee, May 22, 1996. In D. E. Denning & P. J. Denning (Eds.), *Internet Besieged: Countering Cyberspace Scofflaws* (pp. 57-65): ACM Press.
- Denning, D. E. (1997, 26 February 1997). *Description of Key Escrow System*, [www]. Available: <http://www.cosc.georgetown.edu/~denning/crypto/Appendix.html> [2001, 16 March 2001].
- Denning, D. E. (1999). *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, [www]. Available: <http://www.nautilus.org/info-policy/workshop/papers/denning.html> [2001, 13 January 2001].
- Denning, D. E., & Branstad, D. K. (1996). A Taxonomy for Key Escrow Encryption Systems. *Communications of the ACM*, 39(3).
- European Committee on Crime Problems, & Committee of Experts on Crime in Cyber-Space. (2000, 22 December 2000). *Draft Convention on Cyber-crime (Draft N° 25 Rev. 5)*, [www]. Council of Europe. Available: <http://conventions.coe.int/treaty/EN/projets/cybercrime25.htm> [2001, 26 March 2001].
- Even, L. R. (2000). *What is a Honeypot?*, [www]. SANS Institute. Available: <http://www.sans.org/newlook/resources/IDFAQ/honeypot3.htm> [2001, 20 March 2003].
- Farmer, D. (2000). What are MACtimes? Powerful tools for digital databases. *Dr Dobb's Journal*, 29(10).
- Farmer, D. (2001). Bring Out Your Dead. The Ins and Outs of Data Recovery. *Dr Dobb's Journal*, 30(1).
- Farmer, D., & Spafford, E. H. (1990). *The COPS Security Checker System*. Paper presented at the Summer USENIX Conference, Anaheim, CA.
- Farmer, D., & Venema, W. (1993). *Improving the Security of Your Site by Breaking Into it*, [WWW]. Available: <http://www.fish.com/security/admin-guide-to-cracking.html> [2001, 12 January 2001].
- Farmer, D., & Venema, W. (1995). SATAN - Security Analysis Tool for Auditing Networks.
- Farmer, D., & Venema, W. (1999). *Internet Security Auditing Class Handouts*, [www]. Available: <http://www.porcupine.org/auditing/> [2001, 10 January 2001].
- Farmer, D., & Venema, W. (2000). Forensic Computer Analysis: an Introduction. Reconstructing Past Events. *Dr Dobb's Journal*, 29(9), 70-75.

- Graycar, A. (2000, 19 February 2000). *Nine Types of Cyber Crime*, [www]. Available: <http://www.aic.gov.au/conferences/other/cybercrime.html> [2001, 26 March 2001].
- Kelman, A. (1999). *Computer Crime in the 1990s, A Barrister's View*, [www]. Available: <http://www.csrc.lse.ac.uk/ComputerCrime1990s.htm> [2000, 1 December 2000].
- Lemos, R. (2000). *Top 10 security stories of 2000* (24 December 2000), [www]. ZDNet News. Available: <http://www.zdnet.com/zdnn/stories/news/0,4586,2668051,00.html> [2001, 22 January 2001].
- Leyden, J. (2000). *Microsoft hacked in Balkans. U.S. Companies' overseas web sites are dropping like flies*, [www]. SecurityFocus.com. Available: <http://www.securityfocus.com/news/125> [2000, 17 December 2000].
- Maher, W. (2001, January 2001). Learning from the Microsoft Crack. *Australian Personal Computer*, 22, 114-115.
- Masters, D. (2000). Cyber Crime and Punishment. *e-Access*, 46-52.
- McKemmish, R. (1999). What is Forensic Computing. *Trends and Issues in Crime and Criminal Justice*(118).
- Microsoft Responds to Security Issue*. (Press release)(2000). Redmond: Microsoft.
- Mitnick, K. (2000). *Microsoft hack wasn't espionage*, [www]. SecurityFocus.com. Available: <http://www.securityfocus.com/commentary/112> [2000, 7 November 2000].
- Patel, A., & Ciardhuáin, S. Ó. (2000, November 2000). The Impact of Forensic Computing on Telecommunications. *IEEE Communications Magazine*, 64-67.
- Poulsen, K. (2000). *When Microsoft Kicked a hacker off its network, the FBI may have lost its chance for a bust*, [www]. SecurityFocus.com. Available: <http://www.securityfocus.com/news/109> [2000, 1 November 2000].
- Reno, J. (1996). Law Enforcement in Cyberspace Address. In D. E. Denning & P. J. Denning (Eds.), *Internet Besieged: Countering Cyberspace Scofflaws* (pp. 439-447): ACM Press.
- Rohde, L. (2000). *Bulletin: Microsoft stung by hack attack*, [www]. ComputerWorld. Available: [http://www.computerworld.com/cwi/story/0,1199,NAV47\\_STO52929,00.html](http://www.computerworld.com/cwi/story/0,1199,NAV47_STO52929,00.html) [2001, 26 January 2001].
- Shimomura, T. (1995). *Takedown: the Mitnick Case*, [www]. Available: <http://www.takedown.com/>.
- Sibert, O. W. (1996). *Malicious Data and Computer Security*, [www]. Available: <http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper048/MALDATA.PDF> [2001, 26 March 2001].
- Sliwa, C. (2000). *Users show some sympathy to Microsoft over security breach*, [www]. ComputerWorld. Available: [http://www.computerworld.com/cwi/story/0,1199,NAV47\\_STO53471,00.html](http://www.computerworld.com/cwi/story/0,1199,NAV47_STO53471,00.html) [2000, 07 November 2000].
- Sommer, P. (1998a). Digital Footprints: Assessing Computer Evidence. *Criminal Law Review Special Edition*, 61-78.
- Sommer, P. (1998b). *Intrusion Detection Systems as Evidence*. Louvain-la-Neuve, Belgium.
- Stoll, C. (1988). Stalking the Wily Hacker. *Communications of the ACM*, 31(5), 484-497.
- Stoll, C. (1989). *The Cuckoo's Egg*: Doubleday.
- Venema, W. (2000a). File Recovery Techniques. Files Wanted, Dead or Alive. *Dr Dobb's Journal*, 29(12).
- Venema, W. (2000b). *Forensic Computing*, [Personal e-mail] [2000, 12 December 2000].
- Venema, W. (2000c). Strangers in the Night. Finding the Purpose of an Unknown Program. *Dr Dobb's Journal*, 29(11).

- Verreck, P. (2000). *Case Study - Vindictive e-mail*, [www]. International Journal of Forensic Computing. Available: <http://www.forensic-computing.com/archives/vind.html> [2000, 25 November 2000].
- Verton, D. (2000). *Think tank warns that Microsoft hack could pose national security risk*, [www]. ComputerWorld. Available: [http://www.computerworld.com/cwi/story/0,1199,NAV47\\_STO55656,00.html](http://www.computerworld.com/cwi/story/0,1199,NAV47_STO55656,00.html) [2001, 5 January 2001].
- Weiss, T. R., & Rosencrance, L. (2000). *Update: Microsoft stung by hack attack*, [www]. ComputerWorld. Available: [http://www.computerworld.com/cwi/story/0,1199,NAV47\\_STO52949,00.html](http://www.computerworld.com/cwi/story/0,1199,NAV47_STO52949,00.html) [2000, 28 October 2000].
- Zimmerman, P. (1996). *Testimony of Philip R. Zimmerman to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation.*, [www]. Available: <http://web.mit.edu/prz/testimony.shtml> [2001, 20 March 2001].
- Zimmerman, P. (2001). *A note to PGP users*, [www]. Available: [http://web.mit.edu/prz/PRZ\\_leaves\\_NAI.txt](http://web.mit.edu/prz/PRZ_leaves_NAI.txt) [2001, 22 February 2001].