THE NEED FOR AND CONTENTS OF A COURSE IN FORENSIC INFORMATION SYSTEMS & COMPUTER SCIENCE AT THE UNIVERSITY OF CAPE TOWN

A. STANDER, B. CANNY & A. WITTE
Dept Information Systems
University of Cape Town
astander@commerce.uct.ac.za

Abstract. This paper aims to investigate the need for and contents of a course in forensic Information Systems and Computer Science at UCT. In order to do this, the reader is introduced to computer crime and shown how the forensic process of identifying, preserving, recovering, analyzing, and documenting computer data supposedly used in crimes committed using computers is helping in investigating and solving these types of crime. An actual forensic approach known as the End-to-End Digital Investigation is also discussed.

1. Introduction

Modern computer technology, especially the internet, has led to, and enabled computer and computer related crime to become an issue in today's society. This is clearly illustrated in the 2005 Computer Crime and Security Survey which documents approximately one hundred and thirty million dollars worth of losses accruing to computer crimes (Gordon, Loeb, Lucyshyn, & Richardson, 2005).

The pertinent legal issues pertaining to the admissibility of computer evidence that result from a forensic investigation are reviewed. It shows the broad requirements needed for this evidence to hold up in a South African court of law. Examples of how computer crime is affecting South Africa are provided in the aim of assessing the need for computer forensics in South Africa.

Research into degrees offered by higher education institutes regarding computer forensics is investigated with the intention of further emphasising the potential need for some form of formal education with regards to computer forensics.

2. Computer Crime

2.1 COMPUTER CRIME DEFINED

In order for the reader to understand the difference between conventional crime and computer crime, the term "computer crime" must first be defined.

Computer crime encompasses such a wide spectrum of possible crimes that a single, clear, definition would fail to cover all the aspects relating to computer crime (Wallace, Lusthaus & Kim, 2005). For this reason computer crime has been broadly defined as the contravention of any criminal law that required the knowledge or use of computer or computed aided technology in its perpetration, investigation, or prosecution (Goodman, 2001). Nceba (1999) adds to this definition with the view that computer equipment may also be the actual target of the offence not merely a tool aiding the crime.

2.2 TYPES OF COMPUTER CRIME

The term computer crime referees to broad spectrum of possible offences. It is widely accepted that almost any traditional crime can be adapted and perpetrated as a computer crime (Herselman & Warren, 2004). There are however new types of crimes which have evolved that rely specifically on computer technology. Hacking or, spying, forms the majority of these new cyber crimes, whilst other crimes such as denial of service attacks and viruses also play a major role (Wallace et al., 2005).

2.2.1 Viruses

A computer virus is defined as a self executing, self replicating program written to change the way a computer functions without the knowledge or permission of the user. These relatively small programs continue to top the lists as the cause of the greatest financial losses (Gordon, Loeb, Lucyshyn & Richardson, 2005). Coulthard & Vuori (2002) attribute the virus problem to the fact that the distribution of virus code continues to become more and more easy, thanks to the use of the internet and e-mail in everyday life.

2.2.2 Intellectual property crime

Intellectual Property Rights refer to the rights granted to creators and owners of works that are result from some form of human intellectual creativity (Madhavan, 2006) and is categorized into four categories namely: patents, trademarks, trade secrets, and copyright (Piquero, 2005; Madhavan, 2006).The growth of technology within the realm of intellectual property crime "has far outstripped the growth of the law in copyright issues" (Bencivenga, 1997).

2.2.3 Denial of service attacks

A denial of service attack (DoS) occurs when a party or parties from single or multiple locations use the internet or associated network to bombard a host computer with a constant flow of requests in an attempt to block legitimate traffic from being serviced (Hussain, Heidemann & Papadopoulos, 2003). Herselman & Warren (2004) add that denial of service attacks may also take place when a host computer is sent information it does not expect or is not equipped to receive.

2.2.4 Identity theft

Identity theft occurs when a person knowingly, and without permission, uses another persons identifying information to commit and/or aid in committing some form of unlawful conduct (Federal Trade Commission, 2004). McCoy (2005), breaks identity theft into three main categories, these being:Financial credit identity theft, Medical identity theft and Character identity theft.

2.2.5 Hacking

Hacking refers to the unauthorized use of computer and network resources (Palmer, 2001). This definition alone does not however fully define hacking as being a crime. It is noted that in order for hacking to be considered a crime the unauthorised use of these computers and associated network resources must be done with the intent to commit a serious offence (Krone, 2005). Furthermore, any changes made to data with the intent to inconvenience or harm the hacked party would also constitute as being offensive and thus would be considered unlawful (Krone, 2005).

Another role for hackers is that of the Ethical Hacker. This type of hacker provides system and or network security testing services to business owners. These ethical hackers are employed to test systems by using the same conventional hacking tools and methodologies used by malicious hackers, but with the goal of discovering weaknesses within a given system or network (My Choice, 2004).

2.2.6 Cyber Bullying

Cyber bullying is “the use of modern communication technologies to embarrass, humiliate, threaten, or intimidate an individual in the attempt to gain power and control over them” (Stutzky, No Date).

3. Computer Forensics

The need for computer forensics has arisen from the startling increase in the number of computer crimes that are committed annually (Balon, Stovall, & Scaria, No Date). After a computer system has been breached and the crime has taken place, there is a need for a computer forensics investigation to follow. The field of computer forensics has begun to play a role in the solving of computer crimes as it provides a mechanism by which incriminating evidence can be collected in such a way that it can be used in the court of law. Computer forensics is often confused with computer security and for

this reason the definition of computer forensics will be provided (Dathan et al, 2005; Paroff & Wall, 2005).

3.1 COMPUTER FORENSICS DEFINED

The term forensics means to apply a discipline, any discipline, to the law (Anderson et al, 2003). More specifically forensic science is any science used for the purposes of the law, and therefore provides impartial scientific evidence for use in the courts of law, and in criminal as well as civil investigations and trials. A well-known subfield of forensic science is that of criminal forensics, which makes use of techniques such as matching fingerprints, ballistic testing, and DNA matching to help identify and prosecute criminals (Dathan et al, 2005).

The discipline of computer forensics is by this definition also a subfield of forensic science as it deals with identifying, preserving, recovering, analyzing, and documenting computer data supposedly used in crimes committed using computers. This data is stored in the form of magnetically encoded information.

The computer forensics field is a relatively new one, compared to the other subfields, as the term was only coined in 1991 at the first training session held by the International Association of Computer Specialists. The field centres on the fact that criminals using computers may leave some evidence of their activities on their computers. Confiscating and analyzing such digital evidence has become an important aspect of the prosecution of computer criminals (Anderson et al, 2003; Dathan et al, 2005; Dhillon, 2006; Paroff & Wall, 2005).

An important distinction needs to be clarified at this point and that is the one between internet and computer forensics. The answer to which lies in the source of the inspiration of these two areas. Computer forensics was championed early on by law enforcement as it fits well within the overall investigative methodology. On the contrary however, internet forensics evolved as a response to the hacker community. Internet forensics specialists, in fact, have fundamentally the same skill sets as their adversaries. For the purposes of this paper, the main focus will be placed on computer forensics as it the basis of the topic (Dathan et al, 2005).

The more general application of computer forensics is information forensics or inforensics which, much like criminal forensics, is the application of forensic techniques to investigate crimes, and involves either directly or indirectly, information, computer technology and information storage media. Inforensics is made up of activities quite different from those of traditional forensics because there is no unified body of theory. Also both the evidence itself and the tests applied to it are artefacts developed in a commercial market-place and not in traditional research laboratories. The aim of information forensics is to assign responsibility for an event by bringing together separate streams of evidence, each furnishing a part of the scenario to create a complete and accurate account of the crime. Its raw material is not a natural or

manufactured product, nor is its tools and discovery techniques. In other words it is the computer data stream itself that forms the evidence, rather than any conclusions about what a test result means (Anderson et al, 2003).

The definition of computer forensics does not deal with the key aspects and issues of the actual investigation process. These issues being: who does the forensic investigation, the typical approach used to carry out such an investigation, and how it actually helps to solve a computer crime.

3.2 FORENSIC COMPUTER SCIENTISTS

Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel. A key skill in forensic computer science is thus the challenge that lies in informing the court: not only knowing how the event might have happened, but also assembling event traces into acceptable legal evidence in a form that tells a complete and convincing story, without distorting any of it (Anderson et al, 2003; Paroff & Wall, 2005).

3.3 APPROACH TO FORENSIC INVESTIGATION

The Centre for Digital Forensic Studies proposes an investigation process called the End-to-End Digital Investigation (EEDI) process. The process contains a collection of generalized steps that a forensic computer scientist, investigating a computer crime, must perform in order to preserve, collect, examine and analyze digital evidence.

3.4 THE EEDI PROCESS

The basic End-to-End Digital Investigation process consists of: (1) Collecting evidence, (2) Analysis of individual events, (3) Preliminary correlation, (4) Event normalizing, (5) Event deconfliction, (6) Second level correlation (7) Timeline analysis, (8) Chain of evidence construction, (9) Corroboration (Stephenson, 2003). The process will briefly be elaborated on in the following paragraphs.

3.4.1 Collecting Evidence

Unlike traditional evidence used in criminal cases to convict criminal, evidence in computer crime cases has no such physical manifestation such as paper records, blood spatters, footprints, or wounds. The evidence is of a completely electronic nature and thus requires a completely different set of tools and expertise to analyse (Dathan et al, 2005)

The first step in the EEDI process is that of collecting evidence which, in a computer security incident, is very time sensitive. The biggest challenge in collecting evidence is that an event by itself may no be particularly noteworthy, but if taken in the context of other events, it may prove to be extremely important. This would mean that all relevant events whether they appear to have been tied to an incident or not, need to be

considered which could become a tedious process. This is where forensic investigation tools come into play in order to take an impartial look at the data thereby ensuring that the investigator does not draw early or inaccurate conclusions (Schwartz, 2004).

Critical sources of evidence in this are: images of effected computers, logs of intermediate devices, especially those on the Internet, logs of effected computers, and data from intrusion detection systems (Stephenson, 2003).

This process of evidence collection is closely followed by the analysis of individual events which may very well be duplicates reported in different sources and have value both as they appear and "normalized" (Stephenson, 2003).

3.4.2 Event Normalization and Deconfliction

Normalization is the combining of evidentiary data, of the same type, from different sources into a single, integrated terminology that can be used effectively in the correlation process (Stephenson, 2003).

The process of deconfliction follows on from the normalization process to combine multiple reportings of the same evidentiary event, into a single, reported, normalized evidentiary event. This step is needed because sometimes events are reported multiple times from the same source (Stephenson, 2003).

Before and after the steps of normalization and deconfliction, the so called correlation steps take place. The main purpose of the correlation steps are to understand, in broad terms, what happened in the crime, which is achieved by examining the individual events to see how they may correlate into a chain of evidence (Stephenson, 2003).

3.4.3 Corroboration

A timeline analysis follows, which is where normalized and deconflicted events are used to build a timeline (Stephenson, 2003). The process is an iterative one and should be updated constantly as the investigation continues to develop new evidence. This step is followed by a construction of a chain of evidence (Beebe & Clark, 2004)

The final step in the process is the corroboration stage. In this stage the computer forensic scientist attempts to corroborate each piece of evidence and each event in the chain. For this the non-correlated event data is used, as well as any other evidence developed digitally. The best evidence being that which has been developed digitally and been corroborated. The final evidence chain should detail the incident in question as best as possible, with the intension of then using this in a criminal trial (Stephenson, 2003).

4. Legal aspects of a forensic investigation

4.1 COMPUTER CRIME LEGISLATION

Little to no legislation has been passed relating to this field (Hershensohn, 2005). The only computer related Act that exists in South African law is the Electronic Communications and Transactions Act of 2002 (Sharrock, 2004). The legislation contained within this Act does not relate specifically to computer crimes, but rather to online contracting. Online contracting deals with contracts made via e-mail and other types of electronic communications (Franco, 2006). The second area of law that would contain regulations on computer related crime is in case law. Case Law is law passed by judges in applying the law to the facts of the case before them (Franco, 2006). This area of the law also contains very little in the way of computer crime regulations because there are only a handful of computer crime related cases that make it past the Magistrates Court which, in terms of the South African court structure, means that little of it becomes case law. (Franco, 2006; Sharrock, 2004).

A further challenge presents itself in the fact that, until recently, few lawyers or law enforcement officers had qualifications in information technology (Dathan et al, 2005)

Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device (Lázaro, 2004) and is often time-sensitive, fragile and can be easily altered, damaged, or destroyed. In a trial, the electronic evidence like any other evidence used in Court must be admissible, authentic, accurate, complete and convincing to judges (Lázaro, 2004).

4.2 ADMISSIBILITY OF COMPUTER EVIDENCE

“Legal rules which determine whether potential evidence can be considered by a court” (Sommer 2002, pp. 10) is the definition that will be adopted to define the idea of “admissibility” of the electronic evidence. The issue of whether or not evidence resulting from computer forensic investigation will hold up in court and be accepted as evidence in a case is two-fold. The judges must determine if the evidence was legally obtained and secondly that the integrity of the original data was maintained (McMillian, 2000; Schwartz, 2004; Sommer, 2002).

The first issue is if the investigator had a legal right to seize and investigate the suspects’ computer (McMillian, 2000). This requires the investigator to obtain appropriate approval and any necessary documentation such as a search warrant or a subpoena prior to conducting any investigation (McMillian, 2000).

The second aspect of whether or not evidence will hold up in court is in the evidence gathering techniques. The correct investigation software is crucial if a company ever want to use evidence in court (Schwartz 2004). Broucek & Turner (2001) point out that many of the current systems are rarely designed to collect and protect the integrity

of the type of data required for legal proceedings in such a way as to remain admissible in court. Investigation software should help security investigators examine local or remote disks, using everything from keyword searches to restoring deleted files, without altering data or metadata (Schwartz, 2004).

4.3 THE JUDGMENT

In order to pass judgment in a particular case, the judges require concrete proof that the criminal in question carried out certain actions that meet the definition of the crime in question (Sommer, 2002). In civil cases this is done on a basis of balance of probabilities, but in a criminal case the judgment must be made beyond any reasonable doubt. Therefore the evidence presented must be of such a nature that it all leads a judge to precisely the same conclusion and leaves no room for doubt (Sharrock, 2004). A computer forensics investigation that is correctly carried out will therefore aid the judgment process by providing evidence of the crime that is in an acceptable form in court.

5. The Need for Courses in Computer Forensics

Computer crime is resulting in large financial losses in South Africa. Unfortunately information pertaining to computer crime in South Africa is scarce as costs may be more difficult to define as well as the fact that businesses are reluctant to divulge information relating to this topic (Africa @ Work, 2006).

The fact that computer crime is such a new topic in South Africa has meant that a large portion of computer crimes in South Africa have not been prosecutable accruing to a lack of applicable controlling legislation and forensic knowledge. This in turn means that South African businesses are being adversely affected by these types of crimes (Herselman & Warren, 2004).

Studies on the needs for a course in computer forensics have shown that the need for trained computer forensic experts is expected to grow in the future. These studies further confirm that crimes using computers are increasing, and the associated financial losses are great. The studies have further revealed that experts in this field are highly desirable in business. (Dathan et al, 2005; Troell, Pan, & Stackpole, 2003)

A forensics course is needed to provide students with the ability to identify and employ tools used for tracking intruders, gathering, preserving and analyzing evidence. The ability to apply the procedures used to gather and preserve this evidence to ensure admissibility in court has proven to be invaluable and somewhat of a rare skill (Troell et al, 2003). This fact is confirmed by McMillian (2000) in pointing out that since 1992, the number of computer crime cases that are sent to federal prosecutors in the US has tripled, while the number of cases that are actually prosecuted has remained the same. These cases that went unprotected were dismissed due to lack of evidence (McMillian, 2000).

5.1 FORENSIC COURSES

Institutions have begun to offer courses and degrees in an effort to educate individuals to become skilled professionals in the computer forensics field (University of Glamorgan, 2006).

Universities such as De Montfort University, The University of Rhode Island, Kingston University and The University of Glamorgan all offer some form of undergraduate degree in Forensic computing, whilst others such as Staffordshire University, Dublin City University, John Jay College of Criminal Justice and The University of Bradford now even offer masters programs in computer forensics (E-Evidence Information Centre, 2005).

All the above mentioned institutions seem to focus on specific core competencies within the various degrees offered. These competencies include: Computer law, the internet and internet protocols, computer system & network security, network architecture & hardware, operating systems, mathematics & stats, *programming languages as well as f*orensic tools & procedures. De Montfort University also teaches computer related Ethics.

An interesting observation is that South African universities currently do not offer any degrees or courses dedicated to computer forensics. This therefore means that further research into the need for and contents of a course in forensic IS/Computer Science at UCT is required.

6. Summary

In reviewing the available literature pertaining to computer crime, it was found that various types of computer crimes are affecting the business world today. Viruses and hacking appear to the largest contributors to financial losses (Gordon et al, 2005)

The dramatic increases in the number of computer crimes being committed annually lead to the need for some form of structured investigation. This scenario led to the formation of a field in computer forensics. This process has begun to play a significant role in the solving of these computer crimes. (Dathan et al, 2005; Paroff & Wall, 2005)

Research showed that the EEDI process appeares to be the standard method in the formulation of a chain of evidence acceptable in the South African court of law. This requires that all related data integrity remain intact (Stephenson, 2003). A lack of South African legislation as well as the lack of admissible electronic evidence regarding computer crimes was found to be a major issue in resolving computer crime cases (Hershensohn, 2005).

Similar international studies highlight the need for formal training in the computer forensics field (Troell et al, 2003). Although computer crime is affecting South Africa, no South African higher education institute offer any form of computer forensics degree or even diploma. This situation clearly lends itself to further research with the aim of ascertaining the need for and contents of a course in forensic IS/computer science in South Africa

References

Africa @ Work: Examining the real cost of virtual crime. (2006). [Online]. Available: http://www.polity.org.za/pol/opinion/africa/?show=69510 [2006, April 15].

Anderson, A., Collie, B., De Vel, O., McKemmish, R. & Mohay, G. (2003). Computer and Intrusion Forensics, Artech House, London.

Beebe, N.L. & Clark, G.J. (2004). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. [Online]. Available: http://scholar.google.com/scholar?num=100&hl=en&lr=&q=cache:f0i64Re1eSgJ:www.dfrws.org/bios/day1/Beebe_Obj_Framework_for_DI.pdf+%22timeline+analysis%22+%22Computer+forensics%22 [2006, April 19].

Bencivenga, C. (1997). Protecting copyrights. The New York Law Journal. [Online]. Available: http://www.ljx.com/internet/1016cpdig.html [2006, April 16].

Broucek , V. & Turner, P. (2001). Forensic Computing Developing a Conceptual Approach in the Era of Information Warfare. [Online]. Available: http://scholar.google.com/scholar?num=100&hl=en&lr=&q=cache:ZxrFGGUU9GgJ:www.infosys.utas.edu.au/publications/research/2000-2001/research_papers/14.Broucek-turner.pdf+approach+computer+forensic+investigation [2006, April 11]

Coulthard, A. & Vuori, T. (2002). Computer Viruses: a quantitative analysis. Logistics information management, vol. 15, no. 5/6, pp 400-409.

Dathan, B., Fitzgerald, S., Gottschalk, L., Liu, J. & Stein, M. (2005). 'Computer forensics programs in higher education: a preliminary study', Technical Symposium on Computer Science Education, [Electronic], vol. 37, no. 1, pp 147 – 151, Available: The ACM Digital Library.

Dhillon, G. (2006). Principles of information system security, Hoboken, New Jersey; Wiley.

E-Evidence Information Centre: The Electronic Evidence Information Center. (2005). [Online]. Available: http://www.e-evidence.info/education.html [2006, April 6]

Federal Trade Commission. (2004). [Online]. Available: http://www.ftc.gov/opa/2004/10/facataidtheft.htm [2006, April 9].

Franco, J. (2006). Business Law 1. Cape Town: University of Cape Town. [Course notes].

Goodman, M. (2001). Making Computer Crime Count. United States Department of Justice Federal Bureau of Investigation Washington, The FBI Law Enforcement Bulletin.

Gordon, L., Loeb, M., Lucyshyn, W. & Richardson, R. (2005). Computer Crime and Security Survey. Computer Security Institute.

Herselman, M. & Warren, M. (2004). Issues in Informing Science and Information Technology: Cyber Crime Influencing Businesses in South Africa, Informing Science, pp 253-266.

Hershensohn, J. (2005). Computer crime blog. [Online]. Available: http://www.hershensohn.com/tiki-index.php [2006, April 18].

Hussain, A., Heidemann, J. & Papadopoulos, C. (2003). A Framework for Classifying Denial of Service Attacks. [Online]. Available: https://users.cs.jmu.edu/aboutams/Public/IP TraceBack/Classifying DoS Attacks.pdf [2006, April 11].

Krone, T. (2005). Hacking Motives. High Tech Crime Brief, Canberra; Australian Institute Of Criminology, Australian Government.

Lázaro, P.G.C. (2004). Forensic Computing from a Computer Security perspective. [Online]._Available:_http://scholar.google.com/scholar?num=100&hl=en&lr=&q=cache:m8PcKzirR_EJ:www.ep.liu.se/exjobb/isy/2004/3588/exjobb.pdf+Computer+Crime+%22legal+right+to+seize%22 [2006, April 19].

Madhavan, M. (2006). Intellectual Property Rights: An Overview. [Online]. Available: http://www.jisclegal.ac.uk/ipr/IntellectualProperty.htm [2006, April 11].

McMillian, J. (2000). Importance of a Standard Methodology in Computer Forensics. [Online]. Available: http://www.moreilly.com/CISSP/DomA-3-Importance%20of%20a%20Standard%20Methodology%20in%20Computer%20Forensics.pdf [2006, April 19].

My Choice: Certified Ethical Hacker. (2004). [Online]. Available: http://www.mychoice.co.za/ehacking.php [2006, April 6].

Nceba, G. (1999). Computer crime: Challenges of new technology. Nedbank ISS Crime Index, vol. 3, no 3. [Online]. Available: http://www.iss.co.za/Pubs/CRIMEINDEX/99VOL3NO4/Computer.html [2006, April 16].

Paroff, J. & Wall, C. (2005). 'Cracking the Computer Forensics Mystery', The Computer & Internet Lawyer, [Electronic], vol. 22, no. 4, pp.1-6, Available: EBSCOhost Business Source Premier.

Piquero, N. (2005). Causes And Prevention Of Intellectual Property Crime. Trends in Organized Crime, vol 8, no 4, pp 40-61. [Online]. Available: http://search.epnet.com/login.aspx?direct=true&db=aph&an=18333916 [2006, April 11].

Schwartz, M. (2004). Best Practices: Collecting Computer Forensic. [Online]. Available: http://esj.com/security/article.aspx?EditorialsID=826 [2006, April 19].

Sharrock, R. (2002). Business Transactions Law, Republic of South Africa; Juta.

Sommer, P. (2002). Digital Evidence: Emerging Problems in Forensic Computing, International Journal of Digital Evidence, vol. 1, no. 1, pp 1 – 75.

Stephenson, P. (2003). A comprehensive approach to digital incident investigation. [Online]._Available:_http://people.emich.edu/pstephen/my_papers/Comprehensive-Approach-to-Digital-Investigation.pdf [2006, April 18].

Stutzky, G. (No Date). Cyber Bullying Information, School of Social Work, Michigan State University

Troell, L., Pan, Y. & Stackpole, B. (2003). 'Forensic Course Development', Conference On Information Technology Education, [Electronic], pp 265 - 269, Available: The ACM Digital Library.

University of Glamorgan. (No Date). Courses BSc Computer Forensics. [Online]. Available: http://www.glam.ac.uk/coursedetails/685/51 [2006, April 18].

Wallace, R., Lusthaus, A. & Kim, J. (2005). Computer Crimes, American Criminal Law Review, vol. 42. [Online]. Available: http://www.questia.com/PM.qst?a=o&se=gglsc&d=5009916521 [2006, April 8].