Edith Cowan University
Research Online

Australian Digital Forensics Conference | Conferences, Symposia and Campus Events

3-12-2008

Digital forensics and the legal system: A dilemma of our times

James Tetteh Ami-Narh
Edith Cowan University

Patricia A.H. Williams
Edith Cowan University

Follow this and additional works at: https://ro.ecu.edu.au/adf

 Part of the Computer Sciences Commons

Recommended Citation

Ami-Narh, J. T., & Williams, P. A. (2008). Digital forensics and the legal system: A dilemma of our times.
DOI: https://doi.org/10.4225/75/57b268ce40cb6

DOI: 10.4225/75/57b268ce40cb6
6th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2008.
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/adf/41

Digital forensics and the legal system: A dilemma of our times

James Tetteh Ami-Narh
Edith Cowan University
taminarh@student.ecu.edu.au

Patricia A H Williams
Edith Cowan University,
trish.williams@ecu.edu.au

Abstract

Computers have become an important part of our lives and are becoming fundamental to activities in the home and workplace. Individuals use computer technology to send emails, access banking information, pay taxes, purchase products, surf the internet and so on. Business also use computers and the Internet to perform accounting tasks, manage customer information, store trade secrets, and develop new products and services. State, Federal and Local government agencies use the computer and Internet to create and access information. Similarly, digital systems have become the mainstay of criminal activity. Legal proceedings have always been influenced by tradition and court decisions. These legal traditions and decisions have necessitated the development of complex sets of rules that are used to assess forensic evidence in legal matters. Information and communication technology has impacted enterprise investigation and associated legal matters by requiring electronic evidence to be considered. However, not all evidence presented by digital forensic investigators in legal proceedings has been admissible. The digital forensics investigator must adopt procedures that adhere to the standards of admissibility for evidence in a court of law; proper content inspection of a computer system, proper analysis documentation and professional court representation to ensure a successful outcome. This paper presents an overview of issues in the discipline of digital forensics and explores some areas in the legal system where digital forensics evidence is most likely to be questioned. These include case jurisdiction, search and seizure, spoliation of evidence and issues of "good faith", evidence preservation, investigation and analysis.

Keywords

Digital forensics, legal issues, evidence, forensic process.

INTRODUCTION

The impact of information technology on the world provides limitless benefits for individuals, business, commerce and industry. Unfortunately, as technology develops so does the vulnerability of systems to failure, to unauthorised access and to attack. In the past few years law enforcement agencies have seen an increase in computer related crime including fraud, hacking, equipment misuse, cyber stalking, embezzlement, forgery, harassment, discrimination, sabotage, copyright infringement, security violations, illegal spreading of pornographic materials, theft and virus attacks. The 2005 FBI computer crime survey revealed that 75.1% of the 1762 organisations incurred a financial loss because of computer security incidents. Indeed, the total estimated loses of 313 respondents of the CSI/FBI 2006 survey amounted to $52,494,290 (Gordon et al., 2006). Computer and law enforcement professions have been challenged by the dynamic and evolving nature of computer crime to develop expertise to combat these crimes through the use the collection and analysis digital evidence (Vacca, 2005, p.4).

This paper presents an overview of legal issues in computer forensics. Further, it explores areas within the legal system where digital forensic evidence is most likely to be questioned, which includes case jurisdiction, search and seizure, evidence preservation, investigation and questions relating to analysis.

ISSUES IN EVIDENCE

Biros and Weiser (2006) define digital forensics as "scientific knowledge and methods applied to the identification, collection, preservation, examination, and analysis of information stored or transmitted in binary form in a manner acceptable for application in legal matters". Digital forensic investigation requires defined procedures that comply with industry practice, organisational practice and appropriate laws, whether as part of a criminal investigation or as part of a more general security incident response. The technique and tools used by forensic investigators may vary, however the process generally includes planning, acquisition, preservation,

analysis and reporting as shown in Table 1. Presenting digital evidence is a unique legal challenge facing computer forensic professionals (Kenneally, 2002). Evidence in legal cases is admitted or not admitted based on the relative weight of its probative and prejudicial value (Johnson, 2005, p.150). Given that the legal system is based on precedents, forensic investigators must introduce cohesion and consistency in the expanding field of extracting and examining evidence.

Table 1: Forensic investigation processes (Hershensohn, 2005; Ryder, 2002; Yeager 2006)

Process	***Description***
Identification	Incident is recognised as needing investigation. Triggered by the detection of irregularities in a system, information about a crime and so on.
Search and seizure	Obtain search warrant, prepare tools and techniques. Adopt strategy that maximises the collection of untainted evidence and minimises impact on victim.
Preservation	Involves taking steps to stop or prevent any activity that can damage digital information being collected. Consists of operations such as stopping ongoing deletion processes, preventing people from using computers during collection, using the safest way to collect information.
Examination	Systematic search of evidence about the incident being investigated. Examination of computer media, such as floppy disks, hard disk drives, backup tapes, CD-ROM's and any other media used to store data. Data objects may include timestamps, log files, data files containing specific phrases etc.
Analysis	Evidence analysis is required to identify the perpetrator of crime, claim damages and defend copyrights. Involves determining significance, reconstructing data fragments of data and drawing some conclusions based on the evidence collected. May require the use of tools, and test may also be done more than once to support the crime theory. Technical knowledge required to do undertake an effective analysis process.
Reporting	Translating, summarising and providing some conclusions on the analysis of the evidence. Presentation should be in a layperson's language.

JURISDICTION OF CASE

Portability and connectivity of computer systems lead to questions about jurisdiction (Allen, 2005). The legal system in one jurisdiction differs from another in the location of data and information (Wilson, 2008). Digital forensic evidence must meet the formal evidentiary requirements of the courts if it is to be admissible in a court of law in a particular jurisdiction. An act that may constitute a computer crime that is actionable in one country may be acceptable in another (Mohay et al., p.17). For instance in a landmark case, an Australian businessman was awarded the right to sue for defamation in Australia by the Australian High Court over an article published in the United States and posted on the Internet (OUT-LAW.COM News, 2002). The appeal court case Braintech v. Kostiuk is about the jurisdictional right of the Supreme Court of Canada to adjudicate a case involving an alleged wrongful doing by a resident of British Columbia through the use of the internet. The Court held that merely presenting information via the Internet which is accessible to users in foreign jurisdictions does not provide sufficient grounds to allow a court in another country to assert jurisdiction. Therefore, the Texas Court had no right to assert its jurisdiction over a British Columbian resident (Zorzi, 2000).

SEARCH AND SEIZURE OF DIGITAL EVIDENCE

Digital evidence seizure is closely linked to the issue of privacy. Article 12 of the UN Declaration of Human Rights endorses the right of privacy of everyone (CRL, 2006). Therefore, people have the right to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. In the court case of United States v. Triumph Capital Group, the government sought and obtained a search warrant to search and seize a laptop computer in a public corporation case to avoid an infringement of privacy and spoliation of evidence (Kroll Ontrack Inc, 2004). This seizure is often a target for protestation in court.

Search warrant
Search and seizure of digital evidence is the first process that is most commonly disputed in court cases. During this initial process of forensic investigation, the use of an improper methodology or unlawful search and seizure can negatively affect the admissibility of the evidence (Rizvi & Misra, 2005). The forensic investigator must therefore ensure that the privacy of a culprit is not infringed in any search. The legal procedure for searching and seizing computers with a warrant largely mirrors the legal framework for other forensic investigations. Notwithstanding the similarities of the framework, digital forensic searches may adopt a non-traditional method which differs from other searches (USDoJ, 2002). In the case *State v. Cook*, the defendant contented that the search warrant used by the police search and seizure of personal property was stale and therefore sought to suppress the use of the evidence. The suppression of motion was overruled by the trial court stating that the warrant for the search and seizure was still valid (Wolff, 2002).

Limits of the warrant
The forensic investigator must not only identify and articulate a probable cause necessary to obtain a search warrant but also recognize the limits of warrants for the search and seizure. In a criminal case of child pornography, Yahoo! technicians retrieved all information from the defendants e-mail account after obtaining a search warrant. A lower court ruled that the seizure of the e-mails by Yahoo! was unlawful because of the absence of police presence during the search of the defendant's e-mail account. However a higher court reversed the lower court's decision. The higher court ruled that the search of the defendant's e-mails without a police officer present was reasonable under the US Fourth Amendment and therefore the defendant's privacy rights were not violated (Kroll Ontrack Inc, 2004).

A further example is Wisconsin v. Schroeder where more than one warrant had to be sought during the forensic investigation process. A search warrant for evidence of online harassment was issued and given to the detective to search and seize the defendant's computer and related items. During the initial search the computer lab examiner found some pornographic images of children. The search process was halted and a second warrant sought to provide authority to search for evidence of child pornographic pictures (Patzakis & Limongelli, 2003). Also in People v. Carratu, the defendant filed a motion to suppress the discovered evidence seized, claiming that the search warrants and supporting affidavits only limited to textual evidence relating to his illegal cable box operation and thus the forensic examiner violated the defendant's Fourth Amendment rights upon inspection of non-textual files with folder names clearly relating to other illegal activity. The court held that the search of the other files violated the Fourth Amendment because the warrant authorized only search for evidence pertaining to the device, and therefore did not authorize a search of image files containing evidence of other criminal activity (Kroll Ontrack Inc, 2004).

PRESERVATION
Evidence preservation is another important aspect of forensic investigation. The dynamic nature of electronically stored information and the routine operation of computers technology can modify or delete information. Therefore, it is critical to address evidence preservation early in an investigation (Alan & McCort, 2007). The forensic investigator preserves forensic evidence to ensure that that evidence is not destroyed or damaged.

Digital evidence can be very fragile, and inherently has several challenges unlike evidence encountered during traditional investigations (Kornblum, 2002):

- Memory resident programs can be lost when the system is shutdown
- Digital evidence can be manipulated during the collection, analysis and presentation of the evidence.
- Digital evidence can be altered without traces
- Digital evidence stored computer systems can be accessed several times
- It is sometimes difficult to attribute a computer activity to an individual, because the digital evidence is circumstantial

The evidence should be protected from virus infection, mechanical and electromechanical influences. The forensic investigator must be able to demonstrate that the evidence was not altered in any way before or during its collection or subsequently. In Weiller v. New York Life Ins. Co., the defendant in a class action lawsuit in New York was ordered to preserve documents. The defendant also asserted that preservation of the computer information would cost a considerable amount of money. However, the New York court determined that the federal preservation orders were not sufficient protection for the plaintiff (Kroll Ontrack Inc, 2006).

Similarly, in a multi-district litigation by Vioxx Products Liability Litigation, the court ordered all parties to preserve evidence relevant to the litigation including hardcopy and softcopy information (Westlaw, 2006). In another civil case, Kucala Enterprises, Ltd. v. Auto Wax Co., Inc., the district court dismissed the plaintiff's

case because the plaintiff did not preserve evidence but rather destroyed evidence using Evidence Eliminator. The plaintiff was also ordered to pay the defendant's attorney fees and cost incurred with regard to the sanction (Patzakis, 2008).

SPOLIATION OF EVIDENCE

Individuals and organisations commonly destroy documents during the ordinary course of business activities (Walker & McCurdy, 2002). However, the obligation to preserve electronic data and documents requires good faith and reasonable efforts to retain information which can be relevant pending dispute or perceived litigation. Where relevant information is destroyed, the court may impose sanctions from monetary penalties to default judgement (Rothstein, Hedges & Wiggins, 2007).

One example of this is in the case of Associates International, Inc. v. American Fundware, Inc. The plaintiff complained the defendant deliberately destroyed its computer code after legal action was severed to the defendant. The court held that since the defendant was aware of the dispute it had the obligation to preserve the computer codes. Default judgement was granted in favour of the plaintiff (Walker & McCurdy, 2002). In another example, Mosaid Tech. Inc. v. Samsung Electronics Co., the defendant was sanctioned by the court because it failed to preserve discoverable evidence that was potential for the dispute (Venzie, 2007). Similarly, in the Applied Telematics, Inc. v. Sprint Communication dispute, the defendant failed to preserve the backup tapes of a computer system. The plaintiff argued that the defendant knew the about the potential importance of the information for the lawsuit. The court found out that the defendant did not deliberately destroy the evidence, and court therefore awarded plaintiff monetary sanctions for the destruction of evidence (Schauwecker, 2006).

EXAMINATION

The investigation stage of the forensic process requires a significant amount of planning and consideration to carefully preserve the original. The forensic investigator must ensure evidential integrity of the investigation by imaging an exact copy of all media (servers, floppy disks, hard disk drives, backup tapes, CD-ROM's etc.) using appropriate and usually proprietary imaging software. The collection of electronic data can be a complex task in a digital forensic investigation exercise due to the wide variety of electronic storage locations and the vast amount of data available. Mirror image can preserve the evidentiary value of the information recovered (Benson, 2004).

In the case Gates Rubber Co. v. Bando Chemical Industry, the court awarded sanctions when electronic evidence was destroyed by the defendant's employees. The defendant's expert was criticized by the court for not making an image copy of the drive at issue for production (Kroll Ontrack Inc, 2006). Also in State v. Cook, the defendant appealed against the court ruling for the receipt and possession of child pornography. The defendant claimed that part of the evidence admitted by the court were not were mirror image generated from his hard drive. The court discussed the mirror imaging process, the authenticity of the data taken from the image, and the likelihood for tampering; the appellate court upheld the decision of the trial court. The evidence was properly admitted (Kroll Ontrack Inc, 2006).

Whilst it is possible to fabricate electronic evidence, forensic processes can reveal intentional misrepresentation. In a property dispute, Premier Homes and Land Corp. v. Cheswell, Inc., the plaintiff claim that the defendant was not complying with the terms of a lease. To support its claim the plaintiff offered an email sent from a stockholder of the defendant from plaintiff's president. The defendant alleged the email was fabricated and filed a motion for the preservation and production certain electronic evidence. The court allowed the motion, stating that it was necessary to determine the origin of the disputed e-mail, ordered the defendant's experts to create mirror images of the plaintiff's computer hard drives, backup tapes, and other data storage devices. The plaintiff later admitted that he had fabricated the e-mail by pasting most of a heading from an earlier, legitimate message and altering the subject matter line. The court granted defendant's motion was granted and was awarded attorney and expert fees due to plaintiff's fabrication of email used as evidence (Kroll Ontrack Inc, 2006).

In another case, Commonwealth v. Ellis, the defendants filed a motion to suppress the computerized data obtained pursuant to the search warrants, claiming that the evidence was improperly seized and searched by a computer expert. The motion was denied. To broaden the case, the defendants alleged an infringement of his privacy due to the fact that the forensic expert used a file-by-file search instead of a keyword. The court noted that the expert began the computer investigation with a keyword search but could not properly execute the search because of the file system and structure. The court stated the fraud investigator's method of searching the data file-by-file instead of by a keyword search was logical under the circumstances. Based on the expert's representation, the court denied the defendant's motion, with a few exceptions, determining that the computer search was constitutional and reasonable (Kroll Ontrack Inc, 2006).

A final example of this issue is in the criminal case of United States v. Jackson, where the defendant filed a motion to exclude evidence of chat room conversations with the argument that portions of the transcript were omitted. The under cover police used a cut-and paste approach to capture the evidence. A computer forensics expert confirmed that the cut-and-paste method used by the police officer created several errors and that several portions of the defendant's conversations were omitted. The court decided that the cut-and-paste document was not authentic under the Federal Rules of Evidence and therefore not admissible evidence for trial (Dean, 2007).

EVIDENCE ANALYSIS

The admissibility of findings in a court of law are determined by the rules of evidence, which demand that the accuracy of the methods used to collect the evidence is known and that the evidence is not tampered with in the process of its analysis. (Huebner & Hensksen, 2008). Digital forensics involves essentially taking an autopsy of the forensic evidence using specialized software and techniques to analyse exactly what actions were executed on the computer and what data was stored (Thomas, 2004). Improper analysis of evidence can adversely affect its admissibility in court. The forensic investigator should be able to defend forensic finds in court.

Galaxy Computer Servs., Inc. v. Baker, is an example of a court case where experience of computer forensic expert was challenged. In this legal contention, the defendant argued that the testimony of the computer forensic expert of the plaintiff should be excluded because he was unqualified and had used incorrect procedures. The court rejected the defendant's motion stating that the computer forensic expert good educational background, skill, knowledge and experience (FindLaw, 2005). In Peach v. Bird, the defendant was first acquitted from the charge of possessing child pornography. The analysis of evidence taken from the defendant's computer could not link the defendant to the child pornographic websites. The plaintiff appealed and based on the use Encase evidence analysis and the testimony of an expert the appellant court overturn the dismissal and ordered a case retrial (Patzakis & Limongelli, 2003).

V Cable Inc. v. Budnick is also another example where the police seized computers from a defendant and asked an independent software company to analyse the evidence. The defendant argued that the evidence had been corrupted and therefore inadmissible. However, the court decided that the analysed evidence was trustworthy and admissible (Howell & Cogar, 2003).

CONFRONTING THE DILEMMA

The cases discussed highlight the dilemma that the forensic investigator faces in undertaking computer forensic investigation. Digital evidence has shifted paradigms in collecting, preserving, analysing and presenting forensic evidence. The forensic investigator must ensure that all the processes and procedures in conducting forensic investigation are within the required legal framework. A proposed representation of this is given in Figure 1. The computer forensic investigator has to conform with the rules and regulations of legal systems if the evidence uncovered is to be acceptable to the courts. Forensic investigators must have sound knowledge of legal issues involved in computer forensics investigations. These include the privacy protection rights of employees and other individuals; knowledge about what constitutes a legal search of a stand-alone computer as opposed to a network; laws about obtaining evidence and securing it so that the chain of custody is not compromised; and electronic communications that can be legally intercepted or examined (Wegman, 2004).

Information technology and the boundless environment of the Internet enable cyber-crime activities to span from personal desktops to fibre networks that circle the globe (Radcliff, 2008). Criminals in one country can perpetrate a crime against another person in another country using network servers located in a third country (Kessler, 2005). Digital forensic investigators need to know the legal issues that cross conventional geographic jurisdictions and that are fundamental to pursue digital evidence and wrongdoers.

The courts will uphold the fundamental rights of people against unreasonable search and seizure (Kenneally, 2002). The forensic investigator must ensure that authority for search and seizure of forensic evidence has obtained prior to the investigation. A search warrant must be clear about the searching of network and file servers, and backup media. Also, it must be clearly stated if hardware, software, and peripherals of crime scene can be removed to another location to conduct the search (Whitehead, 2005). In addition, any search warrant obtained should specifically identify the places to be searched coherently as possible, and also limitations imposed within the search warrant on what could and could not be searched (Baggilli, n.d.).

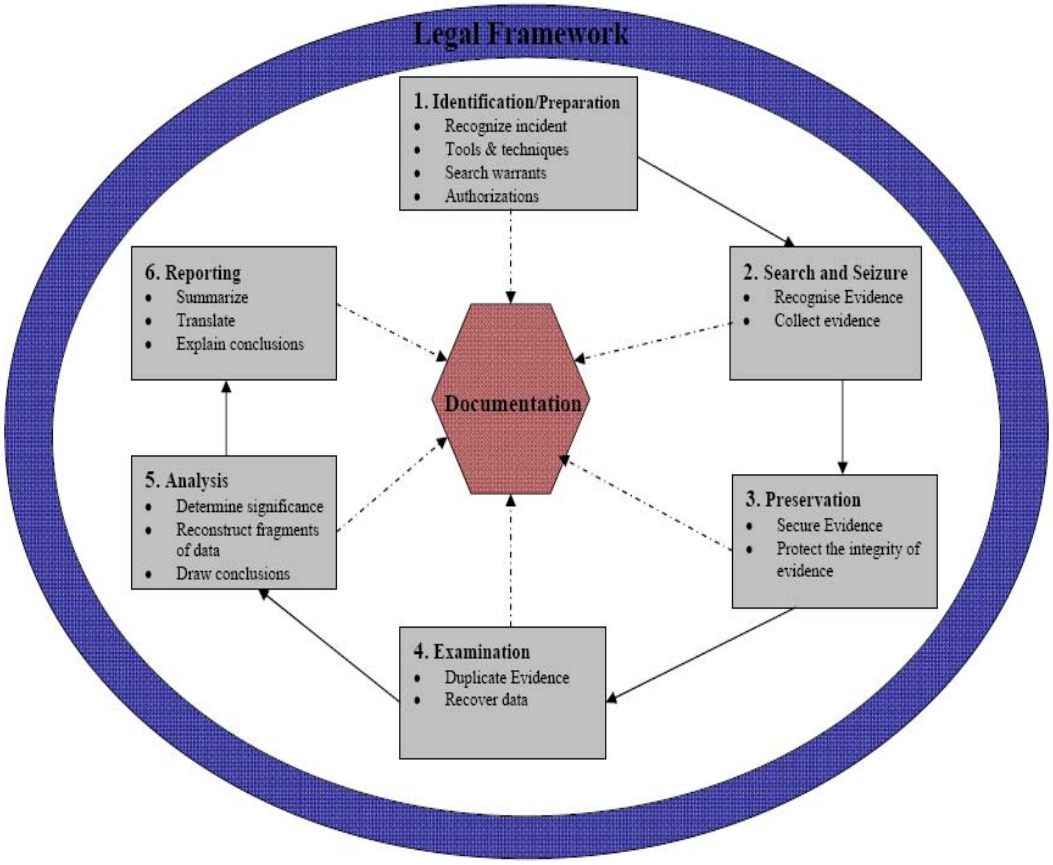

Figure 1: A process Model for seizure and handling of forensic evidence

In order to avoid pitfalls of spoliation of evidence, the forensic investigator should: ensure protection of evidence during investigation, prevent any introduction of computer virus, and properly manage relevant evidence and a continuing chain of custody (Leeds & Marra, 2000).

Forensic investigator can ensure preservation of evidence in accordance to legal requirements by taking the following actions (Thomas, 2004; Hershensohn, 2005):

- Avoid magnetic sources, humidity, excessive heat, or extreme cold, shock , etc
- Evidence removed should be documented and sealed
- Document the entire evidence transportation process
- Handle evidence and electronic equipment properly to avoid damages
- Maintain a chain-of-custody.

After documentation and custody procedures, the forensic investigator must use tools and techniques acceptable to the legal system to examine and analyse the evidence. In addition to having good communication and presentation skills, the forensic investigator should be able to defend the tools and methods used in the forensic process in court.

CONCLUSION

The widespread use of computers and the Internet in homes, businesses, and government facilities has revolutionized access and storage of information. The digital revolution has created the need for new laws, computer forensic investigators, forensic methods, forensic tools and techniques. Computer forensic investigation has become a dominant resource for attorneys and prosecutors in both criminal and civil proceedings. The computer forensic investigator faces the dilemma of conducting forensic investigation and presenting forensic evidence that would be admissible in court. The forensic investigator is expected to be competent in the use of a variety of forensic tools and ensure that every forensic investigation process is

conducted within the acceptable legal framework of the court system. The model proposed gives a representation of the forensic processes which should be adhered to. Further development of this model could be undertaken to highlight particular areas of concern for the presentation of evidence in court. The areas identified as the most likely to be questioned in a legal case were case jurisdiction, search and seizure, spoliation of evidence, preservation of evidence, examination and analysis of evidence. In addition, common pitfalls and suggested rectifications for errors in the process could be investigated. There is a growing body of precedents in which objection to digital evidence has been challenged and this confirms the importance of forensic procedures and adherence to them. Models such as that initiated in this paper should be the cornerstone for development of an area which will no doubt become more important in the future.

REFERENCES

2005 FBI Computer Crime Survey. Retrieved September 5, 2008, from http://www.digitalriver.com/v2.0-img/operations/naievigi/site/media/pdf/FBIccs2005.pdf.

Alan, S. M., & McCort, M. (2007). *Maximize the effectiveness of your computer forensic expert and electronic data evidence*. Retrieved October 24, 2008, from http://technology.findlaw.com/articles/01195/010900.html.

Allen, W. (2005). Computer forensics. *Security & Privacy, IEEE, 3*(4), 59-62.

Angela Brungs, & Rodger Jamieson. (2005, Spring). Identification of legal issues for computer forensics. *Information Systems Management*. Retrieved from 26, 2008

Baggili, I. (n.d). *Search and Seizure from a Digital Perspective: A reflection on Kerr's Harvard Law.* Retrieved November 17, 2008, from http://www.forensicfocus.com/search-and-seizure-digital-perspective.

Berghel, H. (2007). Credit card forensics. *Commun. ACM, 50*(12), 11-14.

Carroll, M. D. (2006). Information security: examining and managing the insider threat. In Proceedings of the *3rd Annual Conference on Information Security Curriculum Development* (pp. 156-158). Kennesaw, Georgia: ACM.

Casey, E., & Stellatos, G. J. (2008). The impact of full disk encryption on digital forensics. *SIGOPS Oper. Syst. Rev., 42*(3), 93-98.

CCLSR. (2004). *Corporate law judgments.* Retrieved October 22, 2008, from http://cclsr.law.unimelb.edu.au/judgments/states/federal/2004/may/2004fca562.htm.

Dean, B. (2007). *Knoxville's EDiscovery newsletter*. Retrieved September 13, 2008, from http://www.forensicdiscoveries.com/previousnewsletters/September_EDiscovery_Newsletter.pdf.

Dixon, P. (2005). An overview of computer forensics. *Potentials, IEEE, 24*(5), 7-10.

Eggendorfer, T. (2008). Methods to identify spammers. In Proceedings of the *1st International Conference on Forensic Applications and Techniques in Telecommunications, Information, and Multimedia Workshop* (pp. 1-7). Adelaide, Australia: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

FindLaw. (2005). *Defense expert's notes, Depo Bar Trial Testimony in Merger Dispute*. Retrieved October 24, 2008, from http://news.findlaw.com/andrews/m/ese/20050622/20050622galaxy.html.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006) *CSI/FBI Computer Crime and Security Survey*. Retrieved September 5, 2008, from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.

Group, T. C. D. E. S. F. W. (2006). Standardizing digital evidence storage. *Commun. ACM, 49*(2), 67-68.

Guha, S., Tang, K., & Francis, P. (2008). NOYB: privacy in online social networks. In Proceedings of the *First Workshop on Online Social Networks* (pp. 49-54). Seattle, WA, USA: ACM.

Herath, A., Herath, S., Samarasinghe, P., & Herath, J. (2005). Computer forensics, information security and law: a case study. In *Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop* (pp. 135-141).

Hershensohn, J. (2005). *I.T. Forensics: the collection and presentation of digital evidence.* Retrieved October 20, 2008, from http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/076_Article.pdf.

Howell, R. T., & Cogar, R. N. (2003). *Record retention and destruction: current best practices*. Retrieved October 25, 2008, from http://www.abanet.org/buslaw/newsletter/0021/materials/recordretention.pdf.

Huebner, E., & Henskens, F. (2008). The role of operating systems in computer forensics. *SIGOPS Oper. Syst. Rev., 42*(3), 1-3.

Kenneally, E. (2002). *Computer forensics - beyond the buzzword*. Retrieved November 14, 2008, from http://www.usenix.org/publications/login/2002-08/pdfs/kenneally.pdf.

Kerr, O. S. (2005). *Search warrants in an era of digital evidence*. Retrieved September 8, 2008, from http://www.olemiss.edu/depts/ncjrl/pdf/02-KERR.pdf.

Kessler, G. C. (2005). *The role of computer forensics in law enforcement*. Retrieved November 12, 2008, from http://www.garykessler.net/library/role_of_computer_forensics.html.

Kornblum, J. (2002). *Preservation of Fragile Digital Evidence by First Responders.* Retrieved October 23, 2008, from http://helix.e-fense.com/Docs/Jesse_Kornblum.pdf.

Kroll Ontrack Inc. (2004). *Cyber Crime & Computer Forensics News.* Retrieved September 3, 2008, from http://www.krollontrack.com/newsletters/Cybercrime/oct04.html.

Kroll Ontrack Inc. (2006). *Cyber Crime & Computer Forensics News*. Retrieved September 3, 2008, from http://www.krollontrack.com/newsletters/cybercrime/dec07.html.

Leeds, G. S., & Marra, P. A. (2000). *Discovering and preserving electronic evidence: How to avoid spoliation pitfalls in the computer age.* Retrieved November 16, 2008, from http://www.spsk.com/Articles/artdscov.cfm.

Lingxi Peng, Zhengde Li, Jinquan Zeng, Jian Zhang, Caiming Liu, & ChunLin Liang. (2007). A Computer Forensics Model Based On Danger Theory. *In Intelligent Information Technology Application, Workshop* (pp. 87-90).

McDonald, J. T., Kim, Y. C., & Yasinsac, A. (2008). Software issues in digital forensics. *SIGOPS Oper. Syst. Rev., 42*(3), 29-40.

Michael E Busing, Joshua D Null, & Karen A Forcht. (2005, Winter). Computer forensics: the modern crime fighting tool. *The Journal of Computer Information Systems*. Retrieved from September 23, 2008.

OUT-LAW.COM News. (2002). Australia rules on where to sue for internet defamation. Retrieved September 5, 2008, from http://www.out-law.com/page-3184

Patzakis, J. (2008). *Kucala Enterprises, Ltd. v. Auto Wax Co., Inc.* Retrieved October 25, 2008, from http://www.forensicexams.org/index.php?option=com_content&task=view&id=1079&Itemid=176.

Patzakis, J., & Limongelli, V. (2003). *Evidentiary authentication within the Encase.* Retrieved October 24, 2008, from http://www1.stpt.usf.edu/gkearns/Articles_Fraud/EEEauthentication.pdf.

Peisert, S., Bishop, M., & Marzullo, K. (2008). Computer forensics. *SIGOPS Oper. Syst. Rev., 42*(3), 112-122.

Radcliff, D. (2008). *Computer forensics faces private eye competition - projects security.* Retrieved November 17, 2008, from http://www.baselinemag.com/c/a/Projects-Security/Computer-Forensics-Faces-Private-Eye-Competition/.

Reith, M., Carr, C., & Gunsch, G. (2002). *An examination of digital forensic models*. Retrieved October 26, 2008, from https://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf.

Robbins, J. (2008). *An explanation of computer forensics* . Retrieved October 24, 2008, from http://computerforensics.net/forensics.htm.

Robert J Benson. (2004, November). The Increasing Significance of Computer Forensics in Litigation. *Intellectual Property & Technology Law Journal*. Retrieved from October 26, 2008

Rothstein, B. J., Hedges, R. J., & Wiggins, E. C. (2007). *eldscpkt.pdf (application/pdf Object).* Retrieved October 26, 2008, from http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf.

Ryder, K. (2002). *Computer Forensics - We've Had an Incident, Who Do We Get to Investigate*?. Retrieved October 20, 2008, from http://www.sans.org/reading_room/whitepapers/incident/652.php.

Schauwecker, P. (2006*). Electronic Discovery and the Environmental Litigator*. Retrieved October 26, 2008, from http://www.bdlaw.com/assets/attachments/154.pdf.

Scott, C. (2003). *Computer Sleuth: Beating down the evidence trail with computer forensics*. Retrieved November 14, 2008, from http://www.thefreelibrary.com/Computer+Sleuth%3a+Beating+down+the+evidence+trail+with+computer...-a099012632.

Srinivasan, S. (2006). Security and Privacy in the Computer Forensics Context. *In Communication Technology, 2006. ICCT '06. International Conference* on (pp. 1-3).

Stahlberg, P., Miklau, G., & Levine, B. N. (2007). Threats to privacy in the forensic analysis of database systems. In Proceedings of the *2007 ACM SIGMOD International Conference on Management of Data* (pp. 91-102). Beijing, China: ACM.

Takahashi, I. (2004). Legal system and computer forensics business. *In Applications and the Internet Workshops, 2004. SAINT 2004 Workshops. 2004 International Symposium* on (pp. 74-77).

Thomas, D. S. (2004). *Legal methods of using computer forensics techniques for computer crime analysis and investigation*. Retrieved September 15, 2008, from http://www.iacis.org/iis/2004_iis/PDFfiles/ThomasForcht.pdf.

Turnbull, B. (2008). The adaptability of electronic evidence acquisition guides for new technologies. In Proceedings of the *1st International Conference on Forensic Applications and Techniques in Telecommunications, Information, and Multimedia Workshop* (pp. 1-6). Adelaide, Australia: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Venzie, J. C. (2007). *The new era of e-discovery*. Retrieved October 26, 2008, from http://www.cfma-portland.org/portals/0/images/publications/db%20articles/the%20new%20era%20of%20e-discovery.pdf.

Walker, C. (2006). *Computer forensics: bringing the evidence to court*. Retrieved August 23, 2008, from http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf.

Walker, C. A., & McCurdy, M. R. (2002). *The dangers of destroying documents in the normal course of business.* Retrieved October 26, 2008, from http://www.fwlaw.com/documents.html.

Wegman, J. (2004). *Computer forensics: admissibility of evidence in criminal cases*. Retrieved November 12, 2008, from http://www.cbe.uidaho.edu/wegman/Computer%20Forensics%20AA%202004.htm.

WestLaw. (2006). *American Law Reports*. Retrieved September 15, 2008, from http://www.charleshogshead.com/INNSOFCOURT/PROGRAM_MATERIALS/ElectronicDiscovery/ALR_6th_2006_6.pdf.

Whitehead, A. (2005). *Computer forensic: seizing the evidence*. Retrieved November 12, 2008, from http://free-backup.info/computer-forensic-siezing-the-evidence.html.

Wilson, N. (2008). Forensics in cyber-space: the legal challenges. In Proceedings of the *1st International Conference on Forensic Applications and Techniques in Telecommunications, Information, and Multimedia Workshop* (pp. 1-6). Adelaide, Australia: ICST

Wolff, P., & Grady, J. (2002). *State v. Cook, 149 Ohio App.3d 422, 2002-Ohio-4812*. Retrieved October 23, 2008, from http://bulk.resource.org/courts.gov/states/Ohio.Ct.App.02/2002-ohio-4812.pdf.

Xie, M., Yin, H., & Wang, H. (2006). An effective defense against email spam laundering. In Proceedings of the *13th ACM Conference on Computer and Communications Security* (pp. 179-190). Alexandria, Virginia, USA: ACM.

Yasinsac, A., Erbacher, R., Marks, D., Pollitt, M., & Sommer, P. (2003). Computer forensics education. *Security & Privacy, IEEE, 1*(4), 15-23.

Yeager, R. (2006). Criminal computer forensics management. In Proceedings of the *3rd Annual Conference on Information Security Curriculum Development* (pp. 168-174). Kennesaw, Georgia: ACM.

Zorzi, D. (2000, March). *DZ Law -- Internet Law Review*. Retrieved October 22, 2008, from http://www.delzottozorzi.com/internetlawreview3/jurisdictionissue.html .

COPYRIGHT

[James T Ami-Narh & Patricia A H Williams] ©2008. The author/s assign Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. The authors also grant a non-exclusive license to ECU to publish this document in full in the Conference Proceedings. Any other usage is prohibited without the express permission of the authors.