Forensic Resources For Network Professionals

Stephen J. Specker, Northern Michigan University, USA
Kenneth R. Janson, Northern Michigan University, USA

ABSTRACT

Network professionals face an environment characterized by constantly increasing technological complexity and the daunting challenges posed by ill-intentioned intruders. Securing the systems that they are entrusted to manage is a task of primary importance. Effective network security includes protocols to detect, to investigate, and to preclude the recurrence of any breach in the installed security systems. This study investigates principal forensic techniques that are available to the network professional and provides an efficient access path to practical solutions to the post-breach segment of security system design.

Keywords: forensics, network professionals, network curriculum

INTRODUCTION

Since the earliest development of electronic data processing systems, organizations that have adopted those systems to boost business process efficiency have faced many challenges. Concerns about physical security prompted the development of facilities protocols that accorded the Corporate Data Center fortress-like status. Machine integrity was monitored with internal mechanisms, such as parity checks, while the possibility of careless input errors prompted the design and implementation of tools, such as validity and limit tests, check sums and hash totals. Worries about possible collusion by employees led to carefully structured job descriptions and the segregation of data center duties. As processing systems have evolved to include distributed networks with world-wide connectivity through the ubiquitous Internet, the challenges facing those who would assure system security have increased exponentially. Network professionals must assure that the systems in their care are reasonably protected from threats to their integrity and that attempted attacks on those systems are recognized and addressed.

Enormous process efficiencies for business systems are made possible by routing elements of those systems over public channels – namely the Internet. Connectivity with widely dispersed business units, but more importantly, potential connectivity with new customers and business partners, generally trumps the heightened security concerns that accompany an entity's decision to place portions of its business systems on the Net. For the network professional, the enriched data transport environment comes with constantly expanding security concerns. The malevolent intentions of those who would access a firm's systems for other than their intended purposes are aided by the shear scope of the Internet. Further, those intentions are abetted by jurisdictional issues that remove borders for those who would commit crime but raise barriers to thwart those who would react. Network professionals must include in their repertoire tools to protect their systems from malicious intrusions and detection skills to assure that both attempted and successful attacks are recognized and effectively investigated. When a crime has been committed, forensic science is applied to systematically investigate and document evidence that can support the identification, apprehension and prosecution of perpetrators and, of possibly more importance, the identification and repair of system vulnerabilities that had made the security breach possible in the first place.

Quite understandably, the very same extensive scope and reach of the Internet that both enables the broad power and efficiencies of net-based business systems while exposing those systems to the criminally inclined, also qualifies the Internet as a rich source of forensic information to thwart those same criminals. In the analysis that follows, we explore the forensic resources available to network professionals through the Internet.

METHODOLOGY

A Google.com search on the term network forensics returns approximately 2.9 million citations (August 2009). Related queries produce similarly extensive suggested resource lists. Clearly, there is an overwhelming abundance of material that addresses, to a greater or lesser degree, the forensic knowledge-base needs of networking professionals. An exhaustive review of these sites would, in a static environment, be a nearly impossible endeavor. Moreover, in the dynamic environment that more properly characterizes this quickly evolving field, the task of reviewer quickly becomes a Sisyphean challenge. Our goal, however, has been to illustrate and categorize the resource base available to network professionals facing forensic issues. Our methodology addresses that objective.

We examined approximately 1000 prioritized citations (113 pages with an average of about 9 citations per page) from a network forensics search query on google.com and selected 38 sites for extensive review. Our selection criteria included apparent relevance to the resource needs of one or more of four groups of professionals who labor in the networking field. Networking educators, criminal justice educators, law enforcement professionals and real-world network administrators all require effective knowledge-base strategies for maintaining effectiveness in the forensic science arena. For each reviewed site, we provide a synopsis and then score the site for relevance to each of the professional groups. Our relevance scale ranges from 1 which is of limited relevance to 5 which is highly relevant. Codes are NE = Networking Education, CJE = Criminal Justice Education, LE = Law Enforcement Personnel and RWA = Real World Network Administrators.

FORENSIC RESOURCES

1. http://portal.acm.org/citation.cfm?id=317089&dl=ACM&coll=portal&CFID=11111111&CFTOKEN=2222222 This site discusses a portal solution to problems that arise when sensitive information must be kept in log files on an untrusted machine. In the event that an attacker takes over or gains access to one of these machines, the portal would act to guarantee that little or no useful information is gleaned from the log files and limit the attacker's ability to corrupt the log files. Portal describes an inexpensive method for making log entries impossible for an attacker to read, and also impossible to modify or destroy.
   Relevance: NE 2, CJE 2, LE 4, RWA 4.
2. http://search.techrepublic.com.com/search/computer+crime.html Tech Republic maintains a web site of resources related to computer crime. The content is especially strong in the area of evidence and evidence preservation. For instance, they have a valuable step-by-step protocol for a security incident. They believe consumers aren't capable of taking the steps necessary to prevent computer compromise. The site gives excellent examples of how to defend against attack.
   Relevance: NE 2, CJE 2, LE 4, RWA 4.
3. http://portal.acm.org/citation.cfm?id=317089&dl=ACM&coll=portal&CFID=11111111&CFTOKEN=2222222 This Portal site is dedicated to specific tasks for advanced security issues. Tasks include: Authentication metric analysis and design, secure audit logs to support computer forensics and Flexible control of downloaded executable content. This site covers highly complex concepts and techniques beyond the scope of networking or CJ students. The site also has excellent real world applications for recovery in the event an attacker captures control of a machine.
   Relevance: NE 1, CJE 1, LE 3, RWA 3.
4. http://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf An Examination of Digital Forensic Models - This paper explores the use of scientifically proven methods of digital evidence preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of evidence collected from digital sources for the purpose of reconstructing events suspected of being criminal. The site is very useful on a theoretical level but also has other hands-on applications and tools for conducting forensic investigations.
   Relevance: NE 2, CJE 2, LE 3, RWA 1.

5. http://www2.tech.purdue.edu/cpt/courses/TECH581A/Rogers.pdf The future of computer forensics: a needs analysis survey. This study was an attempt to add to the growing body of knowledge regarding computer forensics and attempted to identify the top five issues in the field. In an academic setting the paper would be excellent reading for the class and would provide endless opportunities for analysis and discussion. This site could be useful in a budget process to identify security issues and documenting needs for funding.
   Relevance: NE 5, CJE 3, LE 1, RWA 2
6. http://www.giac.org/practical/gsec/Dorothy_Lunn_GSEC.pdf Computer Forensics – An Overview. This paper would be an excellent resource for the classroom because it addresses forensics from an introductory point of view. It starts with a simple definition of what computer forensics is and then covers the history of forensics and how the legal environment has adapted to this relatively new source of evidence. Also covered are the effects of computer crime on national security laws such as The Economic Espionage Act of 1996 which deals with trade secret theft and The Electronic Communications Privacy Act of 1986 which deals with interception of electronic communications.
   Relevance: NE 5, CJE 3, LE 2, RWA 2
7. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1019405 A recursive session token protocol for use in computer forensics and TCP traceback. This paper introduces a new set of rules (protocols) designed to assist in forensic investigations of malicious or illegal network activity. The paper covers a step by step approach that might be used by an attacker to hide their identity from network administrators and steps that can be taken to defeat the approach. The paper also links to several other possibly useful sites. Overall, this site would have very limited worth to all but advanced individuals in the forensics field.
   Relevance: NE 1, CJE 2, LE 5, RWA 5
8. http://portal.acm.org/citation.cfm?id=1047403 Computer forensics programs in higher education: a preliminary study. This site presents a paper which looks at degree programs in computer forensics in North America. Topics covered in the paper included degree requirements for certificate, associate, bachelors, and master's programs. It also covers factors that should be considered when attempting to start a new program such as curriculum design, faculty, students and budgets.
   Relevance: NE 4, CJE 1, LE 1, RWA 1
9. http://www.sei.cmu.edu/pub/documents/05.reports/pdf/05hb003.pdf First Responders Guide to Computer Forensics: Advanced Topics. This handbook presents techniques for the advanced forensic user to collect data and evidence from electronic files. It is designed for highly experienced security and network professionals that have an advanced understanding of forensic issues. The overall goal was to help train network professionals who are able to understand the advanced issues of computer forensics with the target audience being network administrators and law enforcement.
   Relevance: NE 1, CJE 5, LE 5, RWA 4
10. http://portal.acm.org/citation.cfm?id=1047894 Computer forensics: a critical need in computer science programs. This paper looks at the increasing number of computer security incidents in the world today and the reason for this increase. It also investigates network professionals' inability to respond to the crisis because of the lack of training. The paper goes on to define the field of forensics and its development over the years. Law enforcement topics such as child-related sex crimes and the digital evidence of such crimes are discussed. This paper also states that university computer science programs are perfectly suited to respond to this crisis. With minor changes, computer science programs can address the growing demand for forensics professionals.
    Relevance: NE 3, CJE 3, LE 3, RWA 2
11. http://www.forensiccomputerservice.com/?gclid=COq4yY-KsZYCFSMgDQodeE9oLQ Welcome to Forensic Computer Service. This is a great commercial site that provides expert analysis and witness services on data collected from personal computers, PDA's, cell phones and any other hardware devices in corporate, criminal, civil, and private concerns. Their forensic experts are experienced professionals who have testified many times in federal and state courts in both civil and criminal cases ranging from murder and possession of contraband to theft of corporate information and domestic issues such as divorce and child custody. This site also maintains an employment link for qualified professionals to apply.
    Relevance: NE 1, CJE 5, LE 5, RWA 5

12. http://www.tlsi.net/articles/SCMagazine0802.pdf Computer Forensics Detecting the Imprint. This article stresses the importance of forensic monitoring tools which can act as an early warning system to alert management to the possibility of threats on their computer systems. The article discusses prevention, planning and deployment of security protocols for businesses of all sizes to use to identify security issues which should be investigated more thoroughly. Their focus is on obtaining and analyzing information in combination with policy to protect, detect and respond to any threat. The article covers many examples of hacking incidents and discusses the massive amounts of undetected intrusions believed to be happening today.
    Relevance: NE 4, CJE 2, LE 1, RWA 3
13. http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/8882/28060/01254321.pdf?arnumber=1254321 Automated analysis for digital forensic science: semantic integrity checking. This site points out that computer forensic people have to determine the causes and effects of computer security violations by performing the extremely tedious task of finding and preserving useful clues hiding from detection in massive amounts of data. This company offers products that would automate this tedious process by developing software that can analyze data to find attackers attempting to hide their presence. Once a threat is identified attention can then be applied to the areas of concern.
    Relevance: NE 1, CJE 1, LE 1, RWA 4
14. http://www.giustizia.it/cassazione/convegni/dic2000/sommer_6.pdf Digital Footprints: Assessing Computer Evidence. This article describes some of the more common forms of computer evidence and the new techniques for collecting, preserving and analyzing it. The article also explains some of the problems and issues related to collecting data and assessing it. This article is written from an introductory point of view in an easy to understand format. Some of the topics covered include networks of all sizes and the Internet and its contribution to computer crime. Several techniques for addressing forensic problems are discussed.
    Relevance: NE 5, CJE 4, LE 1, RWA 3
15. http://www.security6.net/courses_en.pdf Protect yourself - learn hacking. This paper promotes learning the technique used by hackers when they are trying to break into your network. The paper says that by learning the same techniques used by hackers and applying them in a structured way, it is possible to close down security holes in your own network. The paper provides a link to a company web site that will train (for pay) network professionals in a variety of 2 day workshops. Areas covered in the workshops include wired and wireless security as well as many other topics with the target group being anyone working with networking.
    Relevance: NE 3, CJE 3, LE 1, RWA 4
16. http://www.acpr.gov.au/pdf/Presentations/inpalmsforensicchs2.pdf The Nature of the E-crime Problem. This book starts with a discussion covering the phenomenal growth in the numbers of people with the technical expertise to launch a cyber-attack. For instance, they believe that just a few years ago that only several thousand people in the US had that capability. They then say that today, it is estimated that 17 million people in the US have the ability to launch such attacks. The book continues by discussing the newer types of attacks being committed including denial of service attacks, viruses, unauthorized entry, information tampering, cyber stalking, spamming, page-jacking, dumping or phone-napping, and computer damage. Also, crime can now routinely have an international dimension because we are globally connected.
    Relevance: NE 5, CJE 5, LE 1, RWA 1
17. http://books.google.com/books?id=hMIxjthVsmsC&lr=&source=gbs_summary_s&cad=0 The Effective Incident Response Team. This book stresses that having a plan in place before an intruder, worm, virus, or automated attack happens on your corporate computer system can greatly reduce the costs of the attack to your organization. Also covered is a step by step approach to forming a computer incident response team which they believe is not a trivial task. Many of the major pitfalls of both internal and external solutions to these problems are discussed. The book then continues with a discussion of how the response process must evolve as technology changes and the types of vulnerabilities seen change.
    Relevance: NE 3, CJE 3, LE 1, RWA 5

18. http://scholar.google.com/url?sa=U&q=http://cs.ua.edu/691Dixon/Forensics/ForensicsIntro.doc Forensic Analysis in the Digital World. This paper discusses how world cultures are becoming more dependent on digital systems and networks and that this dependency is becoming commonplace in many people's lives. Also discussed is how the availability of digital technology has led to misuse by anti-social or criminal individuals as well as ordinary people. They continue by addressing the growing need for a scientifically based approach to conducting forensic investigations in a digital world and then adapting it to benefit law enforcement. They say you must start by educating consumers that the new technology can be used for unauthorized and possibly unlawful purposes.
    Relevance: NE 1, CJE 1, LE 3, RWA 1
19. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.48.2513 Software forensics: Extending authorship analysis techniques to computer programs. Based on the number of occurrences and severity of computer based attacks such as viruses, worms, logic bombs, and Trojan horses all types of computer crime have become of increasing concern for corporations. In an attempt to better deal with these problems, this site provides links to many of the most common threats encountered over the Internet at both an introductory level and at an advanced level. They even provide links to the programs (the Internet worm program) that have caused havoc for so many systems around the world
    Relevance: NE 5, CJE 5, LE 3, RWA 3
20. http://www.google.com/search?hl=en&lr=&q=%22De+Vel%22+%22mail+Authorship+Attribution%22 This site addresses forensic investigations dealing specifically with email issues in the corporate setting. The first link describes an investigation into email content mining for the purpose of identifying an author of a document. This site provides links to supporting information on similar topics as well as links to several non-related topics.
    Relevance: NE 4, CJE 4, LE 3, RWA 2
21. http://www.cosgroveconsult.com/documents/computer_magazine_article.pdf Encase: A Case Study in Computer-Forensic Technology. This site links to an article that discusses the benefits of a forensic tool called Encase. The article says that if you talk to police departments in the US with computer forensics units, they'll tell you that the tool they use most often is Encase. About 2,000 law-enforcement agencies around the world use it. Encase is a 1-Mbyte program written in C++ that combines 15 forensic utility programs used in the past to conduct forensic investigations. This tool starts by making a read only image of the suspect's hard drives to prevent an investigator from altering the original drive and thereby invalidating the evidence.
    Relevance: NE 4, CJE 5, LE 5, RWA 4
22. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=713392 Future technologies from trends in computer forensic science. This paper discusses why computer forensic development was necessary and then examines the evolution of forensic technologies along with expected future development. Topics discussed include techniques for recovering information from storage media after attempts to destroy files or to inflict physical damage to a computer. Included is a discussion on the specialized tools and techniques required to recover information from physically damaged disks. The paper also covers the legal issues involved for forensic investigators when preparing evidence for court presentations.
    Relevance: NE 3, CJE 3, LE 3, RWA 2
23. http://www.l0t3k.org/security/docs/forensic/ Computer Forensics: The Complete Documentation. This site starts by asking two simple questions: What exactly do forensic analysts do? and, How can this type of work help law enforcement or corporate security managers? They continue with a discussion of why security managers must have proper authorization before conducting an analysis on a computer. The site provides forty or more links to many of the topics that would be needed in any classroom setting. Links to topics include firewalls, hacking, gathering information, Linux systems, passwords and many more. This site could be very useful in many different situations.
    Relevance: NE 5, CJE 5, LE 3, RWA 4

24. http://www.netsourceasia.net/resources/atstake_opensource_forensics.pdf The debate between open source and closed source software in forensics. This paper chronicles the debate between open and closed source software use in forensics investigations. Topics include security, reliability and support issues. Each side presents arguments that resonate well with their users, but the paper states that there seems to be no clear winner in the debate. This paper addresses the tools used to analyze digital data and find evidence that someone did or did not commit a crime. The paper examines the legal requirements of digital forensic tools and addresses how these tools satisfy the requirements.
    Relevance: NE 3, CJE 5, LE 3, RWA 2
25. http://portal.acm.org/citation.cfm?id=947180#abstract This abstract says that in recent years digital technology has experienced dramatic growth which in many cases has provided users with the ability to commit crimes and conceal their activities. This has raised the need to develop the field of digital forensics which covers the preservation, identification, extraction and documentation of digital evidence. The paper also presents the procedures and rationale used in the development of forensic courses at both the undergraduate and the graduate levels.
    Relevance: NE 1, CJE 1, LE 1, RWA 1
26. http://iospress.metapress.com/index/Q0L134L2PD6XVKHC.pdf Providing process origin information to aid in computer forensic investigations. This article suggests that the number of computer attacks has been growing dramatically not just because the Internet has grown but because attackers have little or no disincentive to conducting attacks because they can easily avoid detection by creating a chain of connections through a series of hosts. They contend that this method is effective because most current audit systems just do not monitor for the problem. To solve the problem, the paper introduces an inexpensive method that allows both on-line and forensic matching of incoming and outgoing network traffic. Results are presented to show the method to be effective.
    Relevance: NE 2, CJE 1, LE 1, RWA 5
27. http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/100_Article.pdf COMPUTER FORENSICS FOR COMPUTER BASED ASSESSMENT. This article addresses the issue of conducting a computer based investigation at an educational institution and lists several problems that could arise. The article states that almost no academic institution has a computer forensic department that can conduct or assist with a computer forensic investigation. The purpose of this project was to apply computer forensic principles to identify and prosecute any party who violates the rules of the institution. Another aim of the paper was to provide an overview of previous works.
    Relevance: NE 1, CJE 1, LE 1, RWA 1
28. http://www.ddj.com/documents/s=881/ddj0009f/ Forensic Computer Analysis: An Introduction. This paper states that if you want to solve a computer crime effectively you need to look at the system as a detective, not as a user. As a user, you're often trying to fix problems of your own making. However, solving a computer crime is more like trying to solve a more traditional crime. For example, you generally don't have a lot of time to solve the crime and evidence seems to vanish over time. The paper gives several examples of the problems involved in both pre and post planning for an attack.
    Relevance: NE 3, CJE 3, LE 2, RWA 3
29. http://www.moreilly.com/CISSP/DomA-3-Importance%20of%20a%20Standard%20Methodology%20in%20Computer%20Forensics.pdf
    Importance of a Standard Methodology in Computer Forensic. Many cases are lost or don't even make it to court because of compromised evidence. So evidence must be handled very carefully to avoid any problem that would cause it to be dismissed from court. You must be very careful to ensure that evidence is not destroyed or altered because the slightest change could cost you the case. With that in mind, the article proposed a standard set of procedures to follow when collecting and presenting evidence obtained with forensic techniques.
    Relevance: NE 4, CJE 4, LE 2, RWA 3

30. http://www.giac.org/practical/GSEC/Jonathan_Isner_GSEC.pd This site states that currently most law enforcement agencies and corporations don't have enough trained investigators to handle the amount of active investigations. According to the Federal Bureau of Investigation in the year 2000 there were 2,032 cases opened involving computer committed crimes. Of those cases, only 921 were brought to some kind of closure and of those only 54 convictions were handed down in court. This information shows that corporations that rely on a strong web presence to conduct business transactions over the Internet are especially in need of the services of trained computer forensic experts.
    Relevance: NE 2, CJE 2, LE 2, RWA 2
31. http://cais.isworld.org/articles/12-27/article.pdf SARBANES-OXLEY ACT. This article shows some of the recent laws passed that require the retention of electronic data. One of those is the Sarbanes-Oxley Act that was signed into law in 2002 and represents an aggressive effort by the U.S. Congress to address data retention and preservation. This law mandates the retention of electronic documents and also that companies produce their electronic records and other documents when summoned by legal authorities. It also imposes strict criminal penalties for altering or destroying records. Corporations must have trained personnel capable of implementing the necessary procedures to avoid compliance issues.
    Relevance: NE 4, CJE 3, LE 1, RWA 3
32. http://www.springerlink.com/content/r82m17v470581t34/ This article states that in today's world cyber crime is constantly increasing and information is becoming the most sought after commodity. With this in mind, an effective and efficient information security system is deemed essential. They discuss how improved technology and a pro-active attitude toward computer investigations is now a mandatory component of the corporation. Most companies should now require their information system departments to not only secure the network but to routinely conduct digital forensics readiness exercises to ensure the ability to respond in any situation.
    Relevance: NE 1, CJE 1, LE 1, RWA 3
33. http://md.hudora.de/publications/2005-dornseif-teaching-it-security.pdf This paper states that at the university degree level, it is a general rule of good academic practices to teach long-term methodological knowledge instead of short-term system knowledge. In the area of data security, this rule has resulted in university programs which tend towards theoretical topics. This can leave university graduates with an incomplete idea of the security threats they will face in their professional career. Moreover, a typical computer science graduate, even if they have specialized in data security, usually has very little practical experience with the way real systems react when under attack. They argue that practical experiences with real security failures should be a central part of university degree level education.
    Relevance: NE 4, CJE 4, LE 1, RWA 2
34. http://portal.acm.org/citation.cfm?id=949953.949956 This paper was divided to two parts. Part one identified common security and privacy problems with email and web browsers and highlighted the major problems for organizations that result from their employees online activities. This part also tried to raise awareness of the security weaknesses among users and to encourage administrators to enhance their security procedures. Part two makes recommendations for improved user education as a component of information systems security management practices. These recommendations were generated from a forensic computing perspective. From this perspective these policies and practices should improve security of organizations.
    Relevance: NE 2, CJE 2, LE 1, RWA 4
35. http://www.trainingcamp.com/usa/info/Overview.aspx This is a commercial site that offers training camp style classes with the end result being certification testing for the participants. They state that their *training camp* approach will enable the attendee's employer to show a return on their investment in short order. The camps offer highly personalized sessions and claim to be the most efficient training available in the industry. The schools are available in most major cities around the world.
    Relevance: NE 1, CJE 1, LE 2, RWA 5

36. http://www.pacis-net.org/file/2002/085.PDF This paper states that computer forensics is a relatively new field and is still undergoing a process of evolution and definition. Because of this the authors suggest that administrators must create a better way of collecting evidence to enhance forensic investigations methods. This new methodology would enable the establishment of chain of evidence procedures that would be more useful across the entire corporate intranet. Administrators should be considering critical factors that determine the quality of evidence and also planning for any existing limitations. This article discusses the two phases of forensic investigation; the first phase is the exploratory phase, which is an attempt by the investigator to identify if there is problem. If a problem is detected then phase two, the evidence phase would start.
    Relevance: NE 3, CJE 3, LE 1, RWA 4
37. http://portal.acm.org/citation.cfm?id=771860 This paper states that the increasing awareness of security vulnerabilities of computer systems has led to the introduction of several university programs in computer security. Southern Oregon University has recently started a new undergraduate track in computer security and information assurance. In this paper they describe the development of lab exercises designed for this curriculum. The process was designed to mirror an actual enterprise and allows machines to be attacked. Their next step was to design assignments that modeled real-world situations.
    Relevance: NE 5, CJE 5, LE 1, RWA 1
38. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=883490 This paper states that the increasing use of telecommunications in commerce has led to increasing opportunities for computer crime. This increase has created an urgent new demand for forensic computing experts with the knowledge and ability to conduct criminal and civil investigations. The article summarizes the state of forensic computing and its likely future development. The paper then discussed how these changes will impact the telecommunications industry and identifies several research and development issues.
    Relevance: NE 4, CJE 4, LE 1, RWA 2

CONCLUSION

The ubiquitous Internet is both blessing and curse for network professionals. By spreading the reach of the business systems in their care to every corner of the world, the Internet boosts process efficiencies and allows interaction with myriad new and potential customers and partners. On the other hand, that same broad reach exposes the systems to malicious attack. Network professionals must rely on a dynamic set of tools and resources to effectively counter the constantly evolving threats that their systems face. In this paper, we have reviewed a representative sample of the resources available to educators, law enforcement personnel and systems administrators who must effectively address these forensic science needs.

AUTHOR INFORMATION

Stephen Specker is Instructor of Computer Information Systems at the Walker L. Cisler College of Business at Northern Michigan University. He teaches primarily in the areas of computer networking and information systems. His research interests include network design and network forensics. He earned his MBA degree from Northern Michigan University. Contact: sspecker@nmu.edu

Kenneth Janson is Professor of Accountancy at the Walker L. Cisler College of Business at Northern Michigan University. He teaches primarily in the areas of accounting and auditing. His research interests include banking, capital markets and audit practice. He earned his PhD degree from the University of Wisconsin-Madison and is a Certified Public Accountant. Contact: kjanson@nmu.edu