CERIAS Tech Report 2003-30

# THE FUTURE OF COMPUTER FORENSICS: A NEEDS ANALYSIS SURVEY

Marcus K. Rogers & Kathryn Seigfried

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907

# The Future of Computer Forensics: A Needs Analysis Survey

Marcus K. Rogers & Kate Seigfried
Center for Education and Research in Information Assurance and Security,
Purdue University

*Keywords*

Digital forensics, computer forensics, cyber crime, computer crime

## *Abstract*

The current study was a pilot study and attempted to add to the growing body of knowledge regarding inherent issues in computer forensics. The study consisted of an Internet based survey that asked respondents to identify the top five issues in computer forensics. 60 respondents answered the survey using a free form text field. The results indicated that education/training and certification were the most reported issue (18%) and lack of funding was the least reported (4%). These findings are consistent with a similar law enforcement community study (Stambaugh et al., 2001). The findings emphasize the fragmented nature of the computer forensics discipline. Currently there is a lack of a national framework for curricula and training development, and no gold standard for professional certification. The findings further support the criticism that there is a disproportional focus on the applied aspects of computer forensics, at the expense of the development of fundamental theories. Further implications of the findings are discussed as well as suggestions for future research in the area.

## *Introduction*

In today's increasingly complex world, we find ourselves at a rather unique societal and cultural cross road. At no other time in history has society been so dependent on technology and its various offshoots and incarnations (United Nations, 1999). The influence of technology is pervasive in our private and professional lives. The use of such conveniences as e-mail and chat groups has changed the fundamental ways in which we interact as a society (Rogers, 2003a; NRC, 2002). This fundamental change is also apparent in business and the economy. With the rapid growth of e-commerce both business to business, and business consumer, the national economy is now directly impacted by the information infrastructure (NIPC, 2003). The US Census Bureau estimated that for the year 2001, e-business retail sales were $34 Billion (US Census Bureau, 2002).[1]

The same information infrastructure that is driving our economy is being utilized to support our critical infrastructures. The information infrastructure has become the foundation for our communications, banking, health care, transportation, etc. (NIPC, 2003). We are, in essence, placing all of our eggs into the proverbial basket of the

[1] Most recent statistics available.

information infrastructure (Molander, Riddile, & Wilson, 2000). This convergence toward a single point of access and conversely failure has been capitalized on by the criminal and extremists elements in our society (NIPC, 2003). The risk of terrorist organizations turning their attention to technology and cyberspace is very real (Rogers, 2003c). The appeal of the Internet as a "business enabler" for these organizations is fairly obvious (e.g., marketing, recruiting, fund raising, communication etc.). However, the attention can also be focused on using the technology to gather information on potential targets/victims (i.e., intelligence gathering) or targeting the technology and the underlying infrastructure itself (e.g., power grids, financial networks) (Rogers, 2003c).

The recent CSI/FBI Computer Crime Survey estimated that the cost to US businesses in 2003 was approximately $200 Million (Richardson, 2003). The same survey indicated that approximately 85% of the respondents suffered known computer security breaches. Other studies indicate that the rate of "attacks" against the infrastructure is steadily increasing. Carnegie Mellon's CERT Coordination Center handled 82, 904 incidents in 2002 as compared with 52,658 incidents in 2001 (CERT/CC, 2003). The total number of incidents handled by CERT/CC since 1989 is a staggering 225,049 (CERT/CC, 2003). The trends represented by the data are obvious; attacks are increasing and the loss to businesses and consumers are substantial.

Computer crime is a lucrative criminal activity that continues to grow in its prevalence and frequency (Casey, 2000; CERT/CC, 2003; Richardson, 2003; Kruse & Heiser, 2002). This increase in criminal activity places a strain on law enforcement and government. The shift from document-based evidence to digital/electronic-based evidence has necessitated a rapid reformulation of standards and procedures (Casey, 2002). Today, traditional criminal investigations need to be supported with digital evidence collection tools and techniques. This need has led to the development of digital forensic science and specifically computer forensics (Shinder, 2002; Whitcomb, 2002). The area of computer forensics is at a cross roads in its journey to become a recognized scientific discipline (Rogers, 2003a; Whitcomb, 2002). To date, computer forensics has been primarily driven by vendors and applied technologies with very little consideration being given to establishing a sound theoretical foundation (Reith et al., 2002; Carrier & Spafford, 2003). While this may have been sufficient in the past, it will certainly not be so for the future. The national and international judiciary has already begun to question the "scientific" validity of many of the ad hoc procedures and methodologies and is demanding proof of some sort of theoretical foundation and scientific rigor (Sommer, 1997; Smith & Bace, 2003). The US Supreme Court in the *Daubert V Merrell* decision provided specific criteria for the lower courts to rule on the admissibility of scientific evidence:

- Whether the theory or technique has been reliably tested;
- Whether the theory or technique has been subject to peer review and publication;
- What is the known or potential rate of error of the method used; and
- Whether the theory or method has been generally accepted by the scientific community.

These criteria place the onus back onto the discipline to develop itself into a more mature field of scientific investigation (IOCE, 2003; NTI, 2003; SWGDE, 2002). Unfortunately, there is little evidence to indicate that there is any unified strategy being developed to address these criteria.

Other significant issues and challenges have been identified at the federal level. Eric Holder, *Deputy Attorney General of the United States Subcommittee on Crime of the House Committee on the Judiciary and the Subcommittee on Criminal Oversight of the Senate Committee on the Judiciary,* testified before the senate that cyber crime today and in the foreseeable future, presents three broad categories of challenges (Marcella & Greenfield, 2002):

- Technical challenges that hinder law enforcement's ability to find and prosecute criminals operating online;
- Legal challenges resulting from laws and legal tools needed to investigate cyber crime lagging behind technological, structural, social changes; and
- Resource challenges to ensure we have satisfied critical investigative and prosecutorial needs at all levels of government.

While several authors and researchers have commented and editorialized on the weaknesses inherent in computer forensics, there have been very few actual studies conducted (Stambaugh et al., 2001). The National Institute of Justice (NIJ) in 1999 conducted a study designed to identify the issues that the law enforcement community was experiencing in relation to computer crime. The study concluded that in general:

- There is near-term window of opportunity for law enforcement to gain a foothold in containing electronic crimes.
- Most State and local law enforcement agencies report that they lack adequate training, equipment and staff to meet their present and future needs to combat electronic crime.
- Greater awareness of electronic crime should be promoted for all stakeholders, including prosecutors, judges, academia, industry, and the general public.

The study also identified ten critical issues. These issues were: public awareness, data reporting, uniform training and certification, management assistance for onsite electronic crime task forces, updated laws, cooperation with the high-tech industry, special research and publications, management awareness and support, investigative and forensic tools, and structuring a computer crime unit (Stambaugh et al., 2001).

Apart from the NIJ study, there has been no other subsequent published empirical research that addressed the issues and needs related to computer forensics in either the public or private sectors.

### *Current Study*

The current study was designed as a pilot study. Its purpose was to provide a more up to date prospective on what computer forensics researchers and practitioners felt were the top five issues facing the discipline. The findings from the study will be used to determine strategies and methods for addressing these issues, and to focus research and funding efforts.

## Method

### *Participants*

The respondents in the study were researchers, students, academics, and private/ public sector practitioners in the area of computer forensics (N = 60). As the study solicited anonymous responses to the survey question, no respondent demographics were available. Participation in the study was completely voluntary and no incentives were provided.

### *Procedure*

A single question, free form answer, survey was posted on the forensics research webpage belonging to the Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University. The survey was identified as being informal and simply an attempt to begin collecting meaningful data for the computer forensics community. The survey consisted of a single question that asked the respondents to list what they considered to be the top five issues related to computer forensics. Once the respondents filled out the drop down box, the response was anonymously e-mailed to a generic e-mail account belonging to the principal researcher. The duration of the study was approximately one month.

The existence of the web survey was made known via postings to the various news list-servers dedicated to computer forensics (e.g., computer forensic tool testing, computer forensic investigator, forensics, Internet crime, and Linux forensics).

## Results

### *Descriptive Analysis*

The data were examined using descriptive statistic analysis. The data were initially grouped into ten high order categories. These categories were: tools, theory, education/certification/standards, data acquisition, encryption, evidence correlation, technologies, legal justice system, funding, and other. Each respondent's answers were placed into one of the ten categories. If two or more of a respondent's answers were of the same category, they were combined and scored as a single item in that category (e.g., DES, AES, RSA, Encryption - scored as encryption). A frequency analysis indicated that the category of education was the most frequently reported category (18%), and once the category "other" was factored out, funding was the least reported (4%) (see Table 1). Chart 1 illustrates the relative frequencies of each of the reported categories.

*<Insert Table 1 about here>*
*<Insert Chart 1 about here>*

## Discussion

The finding that education, training and certification were the most reported issue is consistent with the findings form the previous law enforcement study conducted by Stambaugh et al., (2001). Both the law enforcement community and the private sector/academia are concerned with the lack of a standardized, or even a consensus approach to training computer forensics practitioners. The concern extends to academia and the sudden proliferation in course offerings in computer forensics. Unfortunately the quality of many of these academic courses is suspect, and do not appear to be based on any common body of knowledge in the domain (Rogers, 2003b).

The community as a whole is also concerned that currently there is no national “gold standard” for professional certification in computer forensics (Rogers, 2003b). To date, many of the certifications are tied to specific vendor products, or to a particular operating system. These proprietary certifications only increase the level of fragmentation within the industry and perpetuate the misguided belief that there is no generic conceptual approach to computer forensics (i.e., every case is so unique that standards are meaningless). Other areas of forensic science have clearly shown that this is not true, and that a common conceptual approach is not only possible but is imperative in order to be considered a scientific discipline by the courts (Saferstein, 2001).

The finding that lack of funding was the least reported issue is indicative of the general tendency of those persons in the field to focus on the applied aspects of computer forensics. The development and use of tools has historically been the focus of most of the efforts in computer forensics (Whitcomb, 2002). What have largely been ignored are the theoretical underpinnings for these applied tools and ad hoc methods. The lack of fundamental theories has resulted in some indefensible attacks against the reliability and validity of the tools and techniques (e.g., known error rates) (Carrier & Spafford, 2003).

The findings appear to indicate that there is a consensus regarding significant gaps or needs in the computer forensics discipline. What is less obvious is a consensus approach to addressing the identified issues and needs. The computer forensics discipline is somewhat unique as it serves several different communities (i.e., military, law enforcement, private sector, public sector and academia) (DFRWS, 2001). These communities or constituents have historically operated in silos with little or no sharing of information or ideas (Carrier & Spafford, 2003; Rogers, 2003b; Whitcomb, 2002). In order for computer forensics to successfully meet the challenges of maturing as a true scientific discipline, this silo mentality needs to be abandoned and replaced with a mindset of cooperation and openness.

Another key factor in the maturation process will be the availability of funds for research, training, and education. A truly national framework for academic curricula needs to be developed and appropriately funded. This framework must include input from the private sector, public sector, law enforcement, and the research community. It would act as the conceptual model for the development of a nationally unified approach for undergraduate and graduate courses and programs in computer forensics. Once a national approach is developed, the focus must shift to an international approach in order to properly reflect the reality of a truly global criminal community.

Computer forensics is a vital component of the war on terrorism, and homeland security, and is not just limited to white collar crime, child pornography, and malicious code investigations. Traditional funding agencies need to step up to the mark and emphasize the importance of computer forensics by making the appropriate funds available.

Although the findings of the current study are of interest, caution must be taken when making any sweeping generalizations. The fact that the N size was only 60, while sufficient for statistical analysis, reduces the confidence in generalizing the results to the larger computer forensics population. Future research should sample a larger number of respondents, collect detailed demographics information and look at not only identifying issues, but also obtain feedback on methods for addressing these issues.

# References

Carrier, B., & Spafford, E. (2003). *Getting physical with the digital forensics investigation*. International Journal of Digital Evidence, Winter 2003.

Casey, E. (2000). *Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet*. Boston: Academic Press.

Casey, E. (2002). *Handbook of Computer Crime Investigation*. Boston: Academic Press. CERT/ CC. (2003). Cert statistics. Retrieved June 1, 2003, from http://www.cert.org/stats/.

Digital Forensic Research Workshop. (2001). *A road map for digital forensic research.* Report from the first Digital Forensic Research Workshop, August 2001, Utica, New York.

International Organization on Computer Evidence. (2003). *Digital evidence, standards and principles*. Retrieved May 22, 2003, from http://www.fbi.gov.

Kovacich, G. L., and W. C. Boni, (2000*). High-Technology Crime Investigator's Handbook*. New York: Butterworth Heinemann.

Kruse, W & Heiser, J. (2002). *Computer Forensics: Incident Response Essentials*. New York: Addison Wesley.

Marcella, A. J., and R. S. Greenfield, (2002). *Cyber Forensics*. New York: Auerbach Publications.

Molander, Riddile, and Wilson. (2000). *Strategic information warfare: A new face of war*. Santa Monica: RAND.

National Institute of Justice. (2000). *State and local law enforcement needs to combat electronic crime*. US Department of Justice Research Briefs.

National Infrastructure Protection Center. (2003). *NIPC white paper: risk management: an essential guide to protecting critical assets*. Retrieved June 1, 2003, from http://www.nipc.gov/publications/nipcpub/newnipcpub.htm.

National Institute of Justice. (2000). *State and local law enforcement needs to combat electronic crime*. US Department of Justice Research Briefs.

National Research Council. (2002). *Making the nation safer: The role of science and technology in Countering Terrorism*. Washington: National Academy of Sciences.

New Technologies Inc. (2003). Junk science legal challenge explained. Retrieved June 4, 2003, from http://www.forensics-intl.com/def14.html.

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence, Spring 2002, 1.*

Richardson, R. (2003). *CSI/FBI 2003 computer crime survey*. Retrieved June 5, 2003, from http://www.gocsi.com.

Rogers, M. (2003a). The role of criminal profiling in computer forensic investigations. *Computers and Security, issue 4.*

Rogers, M. (2003b). Computer forensics: Science or fad. *Security Wire Digest, Vol 5. No. 55*, July 24.

Rogers, M. (2003c). The psychology of cyber-terrorism. In Silke & Merari (Eds.). Terrorists, Victims and Society: Psychological. Perspectives on Terrorism and Its Consequences (pp. 75-92). London: Wiley and Sons.

Saferstein, R. (2001). *Criminalistics: An introduction to forensic science.* New York: Prentice Hall.

Scientific Working Group on Digital Evidence. (2002). *SWGDE draft best practices*. Retrieved June 5, 2003, from ttp://ncfs.ucf.edu/digital_evd.html.

Shinder, B. (2002). *Scene of the cybercrime: Computer forensics handbook*. Rockland, MA: Syngress Press.

Smith, F., & Bace, R. (2003). *A guide to forensic testimony: The art and practice of presenting testimony as an expert technical witness.* Boston, MA: Addison Wesley.

Sommer, P. (1997). *Computers forensics, and introduction.* Retrieved, June 3, 2003, from http://www.virtualcity.co.uk/vcaforens.htm.

Stambaugh, H., Beaupre, D., Icove, D., Cassaday, W., & Williams, W. (2001). *State and local law enforcement needs to combat electronic crime.* National Institute of Justice Research in Brief.

United Nations. (1999). International review of criminal policy: United nations manual on the prevention and control of computer-related crime. Retrieved May 15, 2003, from http://ifs.univie.ac.at/~pr2gg1.

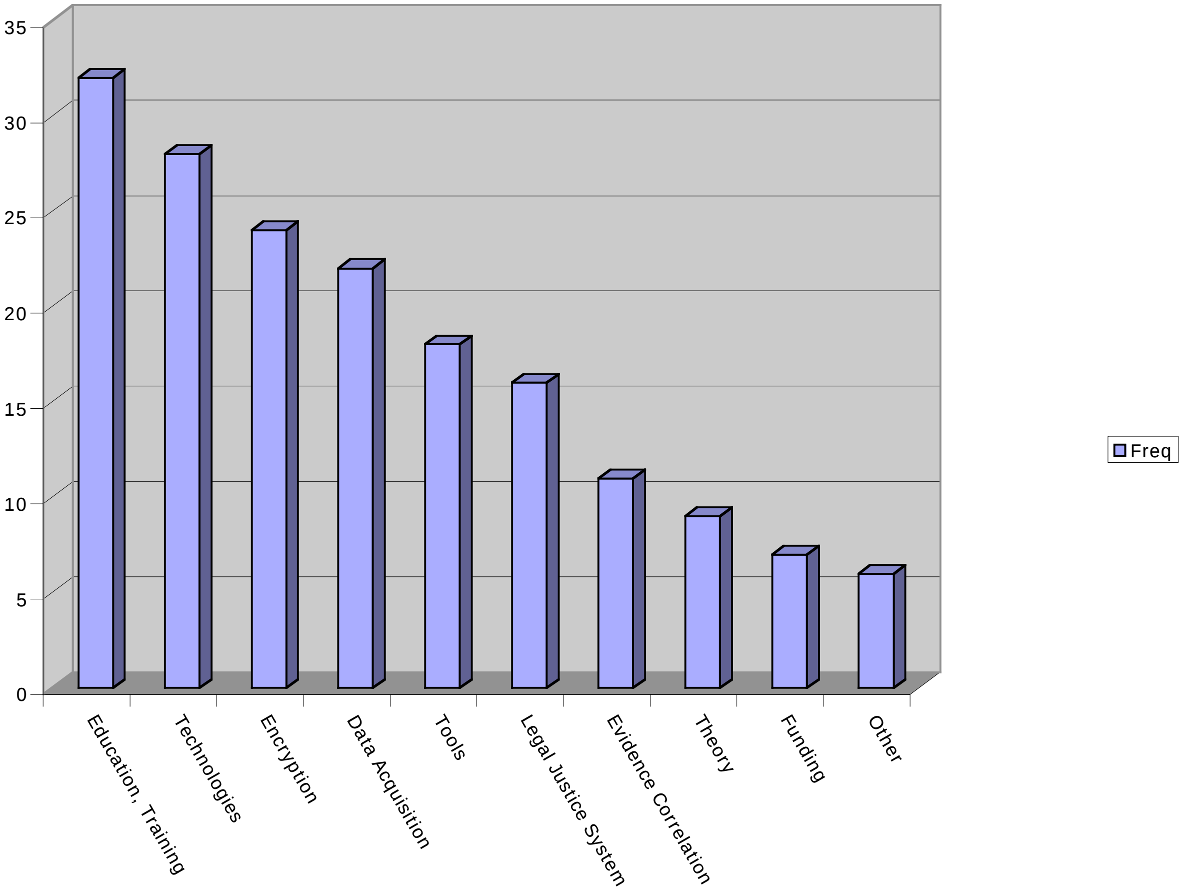
US Bureau of Census. (2002). 2001 e-commerce multi-sector report: Retrieved June 1, 2003, from http://www.census.gov/eos/www/ebusiness614.htm.

Whitcomb, C. (2002). A historical perspective of digital evidence: A forensic scientist's view. *International Journal of Digital Evidence, Spring 2002, 1.*

*Table 1*
*Frequency Analysis of Reported Issues*

| | Frequency | Percentage |
|---|---|---|
| Education/Training/Certification | 32 | 18 |
| Technology | 28 | 16 |
| Encryption | 24 | 14 |
| Data Acquisition | 22 | 13 |
| Tools | 18 | 10 |
| Legal Justice System | 16 | 9 |
| Evidence Correlation | 11 | 6 |
| Theory/Research | 9 | 5 |
| Funding | 7 | 4 |
| Other | 6 | 3 |
| *Total* | *173* | *100* |

*Chart 1*
*Reported Issues Category Frequency*


Education, Training
Technologies
Encryption
Data Acquisition
Tools
Legal Justice System
Evidence Correlation
Theory
Funding
Other
Freq