Proceedings of the 8th Colloquium for
Information Systems Security Education
West Point, NY June 2004

Electronic Forensics Education Needs of Law Enforcement

Helen Armstrong and Phillip Russo

Abstract – *This paper discusses the trends in crime to utilize computer systems and the Internet and the resultant need for law enforcement to be knowledgeable about computer systems. Law enforcement's education needs in electronic forensics is discussed, followed by the description of a masters program designed to give specific skills in the area of computer forensics and the associated technologies to meet those needs.*

Index terms: computer forensics, electronic evidence, computer security education, law enforcement

I. Introduction

Electronic evidence from computer systems has become an important source of evidence in the investigation and prosecution of traditional crimes. Perpetrators involved in homicide, child pornography, drug trafficking, terrorism, fraud and money laundering are increasingly using computers to store information relating to their crimes as well as utilizing Internet facilities to communicate. In a recent case in Australia a woman was convicted of murdering her husband even though no body was found. Amongst other evidence on her home computer police found downloaded web pages on how to hire a hit-man and how to dispose of a body. Other recent cases in the US and Canada used electronic evidence to substantiate allegations of sexual harassment, prove theft of trade secrets by an employee or others, validate copyright infringement or verify the improper use of licensed software, obtain data of fraudulent or criminal activity, substantiate wrongful termination of employment, provide evidence of insider trading, establish relationships between murder victims and the accused, and provide evidence of death threats sent by email [1].

Although computer literacy is generally increasing the majority of the public do not understand the architecture of a computer or how it stores and retrieves data. Many have no idea what information is stored on their own computer or other servers when they access an Internet site. Many perpetrators attempt to delete potentially incriminating evidence without realizing what records are stored on their own as well as other computer systems.

Although police officers are well versed in crime investigation techniques, their general level of knowledge in computer security is currently inadequate to handle potential electronic evidence collection and ensure its protection to aid prosecution in a court of law. In a recent case a police officer attending the scene of a crime was requested to seize the suspect's home computer for further investigation. The officer brought in the keyboard and screen, believing that to be the complete system. The officer was shown a number of processing unit cases and sent back to retrieve the missing items. The processor and disk drives were eventually found taped inside a cardboard box. Many police officers have not seen the components of a computer and would not recognize them at the scene of a crime.

A common story appears to emerge from many law enforcement services. Officers with a good knowledge of computers or specialist skills in electronic evidence rarely attend the initial investigation at the scene of a crime. In many cases detectives with the required skills are not involved until well into the investigative process. This means that vital electronic evidence may be either overlooked or unwittingly contaminated.

There is an undeniable need for law enforcement officers to have skills and knowledge in the proper handling computers at the initial crime scene attendance in addition to the protection of potential electronic evidence on computers and other electronic devices related to the crime. Specialists in the field need to be flexible and continually learning [2]. There is also the risk that findings and opinions may be dismissed by a court where a computer forensic expert cannot prove sufficient knowledge, education, skill and experience [3]. Qualifications in the specific area of electronic evidence and digital forensics are an advantage for those who need to appear in court as an expert witness in the area.

Dr Helen Armstrong, School of Information Systems,Curtin University, Western Australia.
Phillip Russo, Western Australia Police Service, Computer Crime Investigation, Commercial Crime Division, Western Australia

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

II. Skills and Knowledge Required by Law Enforcement Officers

The computer security and electronic forensics skills and knowledge requirements of law enforcement officers cover a broad spectrum and includes the following:

1. Handling of computers at the scene of a crime and the initial investigation of crimes where computer systems or other electronic devices may contain evidence. This includes the identification and preservation of electronic evidence, requiring basic knowledge and skills in computer architecture and operating systems, network connectivity, Internet functions and potential sources of evidence within computer and networked systems in addition to the seizure and protection of physical equipment and potential electronic evidence.
2. Producing verifiable images of electronic media and data for subsequent investigation. A detailed knowledge of computer and network hardware, wireless technologies, software, encryption, computer media forensics, and operating systems is required.
3. Retrieving evidence from computer systems and other electronic devices for prosecution of crimes. This requires detailed knowledge of computer hardware, wireless technologies, computer media forensics, network architectures, the Internet, VPNs, operating systems, application and other systems software, databases and encryption hardware and software.
4. Analysis and reporting of electronic evidence. This includes knowledge of operating systems and software tools for computer forensics, standards, methodologies and approaches to gathering evidence and building cases, lateral thinking and problem solving techniques.
5. Presentation of evidence and cross-examination in a court of law. Knowledge of criminal and civil law, past case history, operating systems and software tools for computer forensics, means of authenticating evidence, methodologies, standards, defensive strategies, and admissibility of evidence in court.
6. Computer security measures to protect the integrity, confidentiality and availability of their own computer systems and networks.

In identifying different levels of skills required, law enforcement officers have been categorized into three levels: new recruits and police officers 'on the beat', detectives and investigators, and computer crime specialists.

- Level 1 officers require the skills and knowledge to handle computers at the scene of a crime and the initial investigation as detailed in 1 above. Computer security measures to protect their own systems is also required at this level.
- Level 2 officers require skills in handling not only computers and electronic evidence at the initial investigation but also the analysis and reporting of electronic evidence and the presentation of that evidence in court, as detailed in 1, 4, 5 and 6 above.
- Level 3 officers need to be highly skilled in all six areas, with particular emphasis on generating verifiable images and retrieving evidence from computers and other electronic devices.

A similar three-level categorization is proposed for law enforcement by Nelson, Phillips, Enfinger & Steuart comprising:

- 'Level 1 – acquiring and seizing digital evidence, normally performed by a street police officer.
- Level 2 – managing high-tech investigations, teaching the investigator what to ask for, understanding computer terminology and what can and cannot be retrieved from digital evidence. The assigned detective usually handles the case.
- Level 3 – specialist training retrieving digital evidence, normally performed by a data recovery or computer forensics expert, network forensics, or Internet fraud investigation.' [4]

This grouping, however, is too general for our purpose as it omits to define specific skills and expertise, and does not include presentation of evidence in a court of law.

III. Proposed Computer Forensics Education Programs

A suite of education programs designed jointly by academics and law enforcement officers will address the skills and knowledge identified in the six areas above. The idea is to incorporate computer security and electronic forensics skills in current education programs provided by law enforcement in addition to offering new academic programs at graduate level at Curtin University.

The training in procedures for recognizing and protecting electronic evidence at the scene of a crime (1 above) are skills and knowledge applicable mainly to law enforcement officers and system administrators within business organizations. In fact, this knowledge is considered essential for all police officers and will be integrated into the initial training program for recruits in 2004 within the Police Academy of Western Australia. New recruits will also be introduced to basic skills relating to presenting evidence in court and securing their

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

own computer systems. This will result in officers receiving a good grounding as part of their diploma in policing (in Australia this is the Diploma of Public Safety (Policing)).

Education in the remaining areas will be included in academic programs offered at several levels by the university. The graduate programs include a graduate certificate, graduate diploma and professional masters in computer forensic technologies.

Figure 1 presents an overview of the suite of programs to be offered in computer forensic technologies at both the Police Academy and Curtin University. The modules in the university-run programs cover the disciplines of information systems, computer science and computer engineering and will be taught by academics together with law enforcement officers.

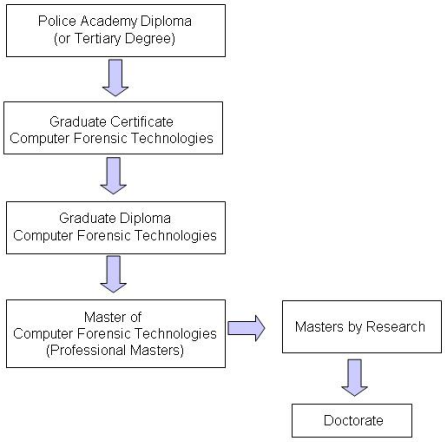

Figure 1: Articulation of education programs in computer security and forensics

Details of the programs to be offered are:

A. Diploma of Public Safety (Policing)

This current diploma will be adjusted to incorporate knowledge and skills in computer hardware and software, handling computers and potential evidence at the scene of a crime, and basic computer security measures. The new modules will be taught at the police academy by police officers from the computer crime unit together with academics.

B. Graduate Certificate in Computer Forensics Technologies

This program forms the first stage of the professional masters program and consists of four modules. The areas studied cover Internet fundamentals, technological infrastructure, network infrastructure (the first Cisco certification module), and computer programming. Each module contributes 25 credits to a program total of 100 credits. Studying full-time students may complete the certificate in one semester.

C. Graduate Diploma in Computer Forensics Technologies

This program forms the second stage of the professional masters program and consists of an additional four modules covering advanced network infrastructure (the second Cisco certification module), computer hardware forensics, network security and advanced problem solving. Students completing the two Cisco modules are eligible to sit the Cisco CCNA certification examination. Each of the eight modules contributes 25 credits to a program total of 200 credits. In a full-time study mode, the graduate diploma may be completed in two semesters.

D. Master of Computer Forensics Technologies

This program is a professional masters degree designed for specialists who are working in the fields of computer forensics, electronic forensics, or computer crime investigation and prosecution. The program would also be appropriate for auditors of computer systems and networks. It comprises the eight modules in the graduate diploma plus a further four modules covering computer forensics, wireless technologies, criminal law and business intelligence and cyberwarfare. Each of the twelve modules contributes 25 credits to a program total of 300 credits. In a full-time study mode, the professional masters may be completed in three semesters.

As this program does not contain a significant research component it is not designed as an entry point to doctoral studies. Students wishing to progress to doctoral studies are required to complete additional units in forensics and research methods together with a major research project.

IV. PROGRAM STRUCTURES

The modules comprising each of the university programs are listed in Table 1.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

This suite of educational programs is designed to provide several levels of skills and knowledge in electronic forensics. Students completing the Masters should graduate with a combination of technical, practical and generic skills, the aim being to produce a problem-solver as well as an electronic forensic specialist. The programs also provide credibility to those law enforcement officers presenting evidence and being cross-examined in a court of law.

Modules	**Credits**
Graduate Certificate in Computer Forensic Technologies	
Internet Fundamentals	25
Technological Infrastructure	25
Network Infrastructure 1 (1st Cisco network administrator module)	25
Computer Programming	25
Total Credits (Graduate Certificate)	**100**
Graduate Diploma in Computer Forensic Technologies	
Computer Hardware Forensics	25
Network Infrastructure 2 (2nd Cisco network administration module)	25
Enterprise Network Security	25
Advanced Problem Solving	25
Total Credits (Graduate Diploma)	**200**
Master of Computer Forensic Technologies (Professional Masters)	
8 Graduate Diploma modules plus	200
Computer Forensics	25
Wireless Technologies	25
Criminal Law	25
Business Intelligence & Cyberwarfare	25
Total Credits (Professional Masters)	**300**
Optional Units for Bridging to Doctoral studies	
Network Programming (Cisco certification)	25
Web Services	25
Enterprise Network Management	25
Data Mining & Advanced Database Management	25
Managing IS Projects and Risks	25
Forensic Sexology	25
Research Methods	25

Table 1: Modules in the university graduate programs

One of the distinguishing features of the program is the inclusion of the module on advanced problem solving. This module presents problem solving methodologies and extensive practical work in lateral thinking and creativity. It is scheduled mid-way into the Masters program, when students have gained some background knowledge and skills in infrastructure and networks. This module encourages participants to let go of preconceived ideas and approaches and build a bigger and more informative picture of the problem situation.

Each of the modules has the content, teaching methods and assessment linked to well-defined objectives and student learning outcomes. All modules are reviewed regularly and required changes incorporated prior to the next teaching semester. All the teaching materials for the modules are offered electronically via the web, and all students are issued with Internet and email accounts.

The problems associated with an emerging discipline such as computer forensics support the establishment of an international standard for accreditation or expertise. Britz highlights the risk of self-proclaimed 'experts' hindering prosecutorial efforts by utilizing unrecognized methodologies and suggests an accreditation process would bring 'professionalism to computer investigations, extend awareness among the community, and decrease the likelihood of successful evidentiary challenges' [5]. Standards and regulations in the area of computer forensics will form an integral part of the Masters program and updating of these will be performed in the regular reviews of the course objectives and contents.

V. TEACHING MODES

Modules run in one of three modes, regular weekly classes, intensive classes over 4-5 days, or ten half-day sessions during summer school. The mode alternates each time the module is offered. This provides a more flexible program for not only students whose jobs require frequent travel, but also allows students to fast-track through the Masters program. From an administrative viewpoint, this flexibility in teaching mode also minimizes timetable clashes.

Although the program is not specifically designed for distance learning, students located in remote areas are able to undertake the degree provided they have Internet access to obtain to the teaching materials and can attend the intensive classes. This allows police officers servicing remote locations to undertake further studies previously not possible.

Although the university programs in particular have been designed to meet law enforcement's needs, these programs will also be appropriate for high-tech crime investigators, IT auditors, legal IT specialists, independent computer forensics experts, IT security consultants and system and network administrators. Education and awareness programs are essential for an effective strategy to fight cybercrime, including education

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

for all those involved in preventing, detecting, reporting and prosecuting crime [6].

The structure of the programs and the module contents will be reviewed by a panel of industry experts prior to final approval by the university. The new modules will be incorporated into the police academy studies for presentation in the second half of 2004, and the university programs are planning a first intake in the Masters program at the beginning of 2005.

VI. Conclusion

The increasing use of computer systems in the perpetration of crimes has raised the need for all law enforcement officers to be knowledgeable about computer architecture and operations. A study of the skills and knowledge in electronic forensics and computer security has been undertaken for law enforcement officers identifying education needs at several levels. A suite of education programs has been designed jointly by law enforcement and academia to meet these needs. The introductory program will be taught at the police academy and the graduate programs at university.

The programs are designed to provide graduates with a balance of technical, specialist and generic skills and knowledge, with an emphasis on problem solving. The university programs will also provide an opportunity for lawyers, auditors, independent investigators, and computer forensic practitioners to specialize in electronic forensics.

VII. References

[1] Gahtan Alan M, 1999, *Electronic Evidence*, Carswell Thompson Professional Publishing, Canada

[2] Kruse Warren G. & Heiser Jay G., 2002, *Computer Forensics: Incident Response Essentials*, Addison-Wesley, Boston

[3] Slade Robert, 2004, *Software Forensics: Collecting evidence from the scene of a digital crime*, McGraw-Hill

[4] Nelson Bill, Phillips Amelia, Enfinger Frank & Steuart Chris, 2004, *Guide to Computer Forensics and Investigations*, Thomson Course Technology

[5] Britz Marjie, 2004, *Computer Forensics and Cyber Crime*, Pearson Prentice Hall

[6] Littlejohn Shinder Debra, and Tittel Ed, 2002, *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE