Walking the Beat on the Path to Technology - Developing Computer Savvy Police

Helen Armstrong[1] and Phillip Russo[2]

[1] School of Information Systems, Curtin University, Western Australia
[2] Computer Crime Unit, Western Australian Police Service, Western Australia
Helen.Armstrong@cbs.curtin.edu.au; phill.russo@ciasolutions.com.au

Abstract

This paper focuses on a joint project to develop specialized training for law enforcement in the search and seizure of electronic evidence. The paper describes the training program developed jointly by law enforcement and academic staff and presented to law enforcement officers in the state of Western Australia, and reports informally on the success of the program.

Keywords: electronic evidence, e-crime, law enforcement, computer forensics, seizure of electronic evidence, Operation Auxin.

Introduction

The ICT industry continues to equip criminals with the tools and facilities to effectively carry out crime at low cost. Increasingly powerful electronic equipment, software and global communications not only presents the opportunity for business organizations and governments to function more efficiently but also provides a sophisticated environment and readily available set of tools to carry out crime. Criminal exploitation of new technologies has brought about three main results: new forms of crime, more traditional forms of crime are committed in new ways that increase benefits or reduce risks to offender, and the more general use of the technologies by offenders, to organise, to communicate, and to shield their activities from surveillance (Roast, Lavender & Wisniewski, 2001).

More specifically, Eurim (2003) reports that the advancing technology has resulted in several major effects on crime –

1. Crimes are more efficient using computers and the Internet allowing access to larger numbers of potential victims at lower cost and risk to the perpetrator. Some examples include auction fraud, identity cloning, mis-selling and paedophilia,
2. Conventional criminal activities can be managed through the use of electronic services. Examples include the use of email, mobiles, search engines, funds transfer in support of blackmail, fraud, extortion, drug or people trafficking, and
3. Crimes can now be carried out against computer systems.

In addition, the Internet is attractive to criminals because it provides opportunities for stealth and anonymity, the opportunity to automate and organise multiple crimes, automated tools for reconnaissance, and tools and routines to not only escape but also to cover one's tracks (Eurim, 2003).

Electronic evidence from computer systems has thus 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 (Armstrong & Russo, 2004). The Internet also provides the facilities for people with criminal intent, particularly paedophiles, to associate and exchange intelligence with reduced risk to their personal identification (Armstrong & Forde, 2002).

There are indications that criminal groups learn from each other and provide community support for their members. In some cases the collaboration and backing is quite sophisticated. For example, an information warfare division to support organised crime was recently created in Holland. In an effort to hinder a police investigation of drug organisations, criminals from this information warfare division were reported to have burglarised the homes of attorneys and police officers, tapped phone lines of high police officials, decrypted analogue communications used by Dutch government agencies, and eavesdropped on pager networks, storing the intercepted communications on a database (Denning 1999). By analysing the data collected, these criminals were able to determine which law enforcement and justice units were collaborating on the investigation.

Law enforcement officers need specialist skills to deal with the increasing number of crimes involving electronic evidence. The aim of this paper is to discuss a training program on the seizure and protection of electronic evidence developed jointly by law enforcement and academic staff and presented to law enforcement officers in the field prior to a national police operation against paedophilia.

E-Crime Education Needs

Law enforcement officers are trained in search and seizure at the Police Academy prior to graduation and generally become adept at seizing evidence in traditional crimes. Crimes involving computers have raised the need for law enforcement officers to know more about computers and networks and be able to seize and appropriately handle electronic evidence.

Unfortunately, the majority of police officers are not highly trained in computing and those with a good knowledge of computers or specialist skills in electronic evidence rarely attend the initial investigation at the scene of a crime (Armstrong & Russo, 2004). This means that vital electronic evidence on computer systems and electronic devices may be either overlooked or unwittingly contaminated. The majority of police specialists in computer forensics have to rely on the police officer in the field to seize and protect the evidence. A mistake at the scene could cause loss of credibility to the computer forensics investigating officer in the subsequent legal hearing if another expert witness can demonstrate that proper or appropriate courses of action were mismanaged (Armstrong, C., 2003).

According to Broersma (2004) the criminal justice system (in the UK in particular) is ill-equipped to handle computer related crime, specifically the investigation of crimes requiring technical skills, sifting through huge amounts of evidence and the lack of new forensic standards. In addition a recent joint report by Eurim and the UK Institute for Public Policy Research (IPPR) highlights the need for greater training for police in e-crime and computer forensics:

> *"New skills are required at all levels within the police and supporting services to enable investigators and forensics experts to trace and analyse*

criminal activities that involve computers and networks and to gather intelligence from them. New skills are required at all levels within the police and supporting services to enable investigators and forensics experts to trace and analyse criminal activities that involve computers and networks and to gather intelligence from them. New and different techniques are needed to ensure the provenance of evidence in digital form" (Eurim, 2004)].

Britz (2004) highlights the lack of resources awarded to law enforcement in the fight against computer-related crime. "Digital evidence requires additional personnel, skills, hardware and housing. "Many agencies have poorly trained computer investigators who are functioning in several capacities at once … Law enforcement has been seriously under-funded since its inception. This trend has been exacerbated with the advent of high-technology crime" (Britz, 2004:8-9). Britz goes on to suggest that emerging technologies require perpetual training as the propensity for computer criminology has exponentially increased. Australia is no different to other western societies with limited availability of education and training in e-security (Warren, 2003).

In the experience of the authors police officers attending the scene of crimes seize a variety of questionable equipment and peripherals, often leaving the most important items behind. One case the officer brought in only the screen, requesting the computer forensic investigator "get data from this – I saw it on the screen so it must be in there somewhere". In another case a detective left a white I-Mac behind (similar to that in Figure 1) because he thought it was only a screen, and did not realise it also contained the hard-drive containing the electronic evidence he was looking for.

Figure 1: I-Mac screen and processor

Many police officers have limited exposure to computer systems and very few have seen the physical components of a computer. It is difficult for officers to thus recognize artifacts containing potential evidence at the scene of a crime. In a further example a detective mistook the karate image on a suspect's Windows XP logon screen to be a picture of the offender as the suspect's name and the words Computer administrator were adjacent to the image.

Tom
Computer administrator

Figure 2: Windows XP User Account image kick.bmp

The variety of electronic storage devices grows daily. The array of electronic storage and communications devices is extensive and continually changing. In addition, with the miniaturisation of computer components, a suspect's system can be easily concealed. Home made computer systems are often housed in non-traditional cases, such as cardboard boxes, small suitcases, toys and other household items.

Figure 3 illustrates mini-itx.com systems concealed in a miniature jute box, a toy train, a toy animal and a robot (see http://www.mini-itx.com for additional miniature systems). If officers are not familiar with traditional presentation of computer systems there is little likelihood they would recognise concealed devices and systems such as those illustrated in Figure 3. This supports the view that 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" [Kruse & Heiser, 2002].

In response to a Training Needs Analysis conducted via the Child Abuse Unit within the Western Australian Police Service, a specialised training program in the seizure and protection of electronic evidence was designed and developed to specifically meet the need of law enforcement officers in the field.

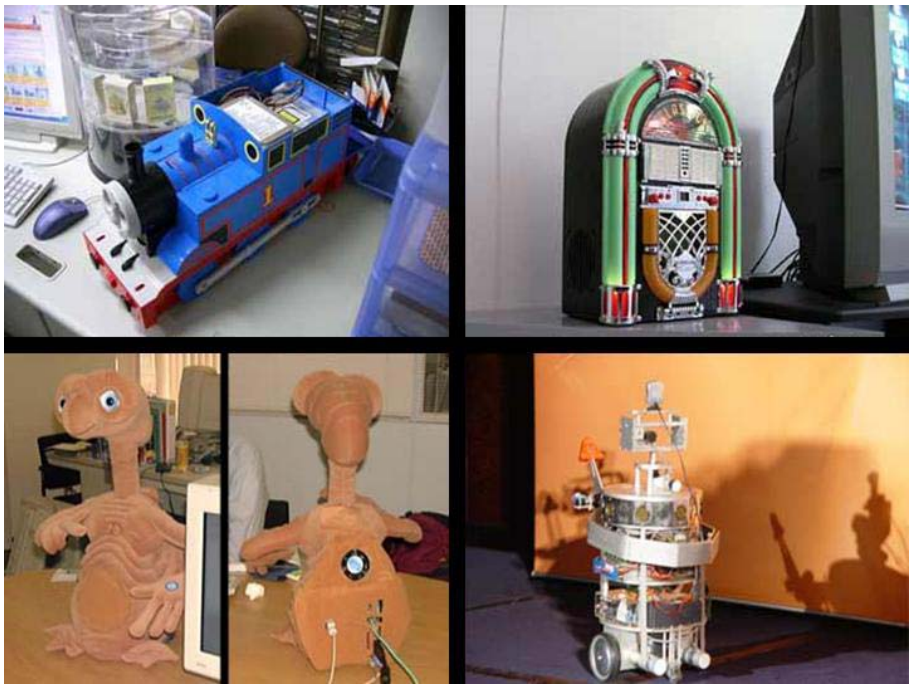

Figure 3: Non-traditional housing for computer systems (source: http://www.mini-itx.com)

The Training Program and Police Operations

The electronic evidence training program was developed and presented to law enforcement officers in the field in Western Australia just prior to a major police operation, Operation Auxin. Operation Auxin is a national operation undertaken jointly with the FBI, Australian Federal Police and Australian State Police to succinctly arrest offenders involved in paedophilia and prosecute them Australia-wide. Operation Auxin is a sister operation to Operation Falcon in the USA and Operation Ore in the UK. Due to the ongoing and sensitive nature of this operation, only publicly available information on Operation Auxin is presented in this paper.

On 30 September, 2004, the Sydney Morning Herald newspaper reported the following details. Last January Operation Falcon in the USA identified five international child pornography web sites and a credit card company that processed payments for clients of those web sites. The investigations led to hundreds of arrests in the USA, UK and Australia. There were initially 191 arrests Australia-wide with police seizing more than 380 computers containing more than two million pornographic images involving children. Some of the images dated back three decades with the number of illegal images ranging from a few pictures to a library of 250,000 images. In Western Australia more than half of the two million images seized nation-wide were found and more than 80 computers were seized (SMH, 2004).

E-Crime Training Program

The training material in the seizure of electronic evidence was designed specifically for detectives, investigating officers and police officers in the field and consisted of

- seminar notes
- photographs of equipment and devices
- details of procedures
- procedure summary sheets giving instructions
- checklists for investigators
- examples of devices, equipment, cables and plugs.

The seminars consisted of eight modules structured as follows:

Sessions 1 and 2

- The role of the WA Police Computer Crime Investigation unit.
- Computer and electronic hardware devices that may contain evidence including towers, desktops servers, concealed systems, notebooks and laptops, wireless devices, USB watches and keys, cameras, NAS and external storage devices.
- Network servers and cables.
- Mobile phones, PDAs, iPods.
- Internet kiosks.
- All kinds of cables, plugs and ports including P/S2, USB, Video, LPT, Serial, Firewire, AT, RJ-11, RJ-45, and the like.

Sessions 3 and 4

- Types of information as digital evidence, the nature and importance of digital evidence.
- Where to find evidence.
- Fragility of digital evidence.

- Evidence destruction utilities – e.g. cyber scrub, evidence eliminator, windows washer, PGP.
- Acquiring passwords.
- Hiding places for devices, information and passwords.
- Encryption and biometrics.
- Email interception.
- Relevant laws.

Sessions 5 to 8

- Power supplies and UPS.
- What to seize and what to leave behind.
- Actions for seizing a computer and protecting the power supply.
- Actions for capturing details of the crime scene.
- Different Operating Systems and shut down procedures for each.
- Legal aspects of search and seizure.
- Importance of linking a person to the devices and equipment seized.
- Bagging and tagging articles seized.
- Risks to storage and transport of electronic equipment.
- Treat all components as FRAGILE cargo when transporting.
- Protecting seized equipment from magnets, excessive heat, moisture, speakers and radios, etc. (particularly police radio transmitters in the vehicle boot or rear seat).
- Ensure 'start up' of the seized computer does not occur prior to forensic computing examination.
- Complying with agency property management and exhibit guidelines.
- Storing computers and electronic devices (PDAs, iPods, etc).
- Ongoing power supply for memory retention devices identified and maintained (PDAs, phones).
- Effect of electromagnetic and electrostatic discharge, assessment and response procedures.
- Return of equipment on completion of forensic analysis.

Delivery of the Training Program

The Western Australian Police Service is responsible for a large physical area. Australia is a continent with a total land area of 7,617,930 square kilometres. It is slightly smaller than the USA with 9,158,960 square kilometres and just less than half the land mass of Russia at 16,995,800 square kilometres (http://www.photius.com/wfb1999/rankings/total_land_area_0.html). Western Australia is 2,529,875 square kilometres, approximately one third of the land mass of Australia. It is more than 2,400 kilometres from the most southern to the most northern points of Western Australian and the UK, at 241,590 square kilometres, is one tenth of the size of Western Australia. Although the population of Western Australia is small compared to the UK (approx. 2 million versus 59 million), the vast distance between major towns makes the delivery of training difficult for police officers in the field.

The training program was presented to law enforcement officers at multiple metropolitan and six country locations - Karratha, Geraldton, Kalgoorlie, Bunbury,

Busselton (just south of Bunbury) and Albany (see Figure 4). Law enforcement officers in other areas traveled to the closest training location.

Figure 4: Police Regions of Western Australia.

The duration of the program was one full day in each location. Due to the covert nature of the operation the training was presented only by staff of the Computer Crime Investigation unit, who travelled more than 7,000 kilometres over a three week period, with more than 200 detectives and uniformed officers from the Western Australian state police attending.

Results

The size of this operation was far greater than any previously experienced by the WA Police Computer Crime Investigation unit. Officers who had previously preferred to keep away from technology-related warrants located, recognised and seized a wide variety of potential evidence sources. Apart from the computers seized, officers attending the scenes also seized PDAs, mobile phones, consoles, USB drives, flash cards, memory sticks, digital cameras, plus a variety of storage media and other items. Although some of the items were not those requested, the officers illustrated they were thinking

beyond the previous limited boundaries and were attempting to seize any potential evidence. Officers were issued with procedure sheets which aided them in visually identifying equipment and also provided a checklist for investigators. In addition to the equipment and devices seized, officers also recovered passwords, ISP details and biographical dictionaries.

Due to the large number of computer systems and devices seized, efficient handling systems were established within the Computer Crime Investigation unit to ensure effective processing of the evidence, disk wiping and prompt return of the equipment.

As this was a covert operation no formal papers or statistics were recorded, however verbal feedback from the officers in the field was positive. Their comments included:

- "I now know how to seize a computer properly"
- "I wish I had done this course before I did that last warrant"
- "It's easier than I thought"
- "Great course. I wish I had time now to go back over previous warrants"
- "Now I know not to start up computers and have a quick look around".

Where the crime scene involved networks, the officers readily recognised the configurations and immediately contacted the Computer Crime Investigation unit for instructions. Officers were able to confidently seize items without fear of contaminating evidence and there were no reported cases of officers starting up or looking into computers in a non-forensic environment. As a result no evidence or potential evidence was compromised.

Overall the training program provided not only the core knowledge the officers required but also installed confidence in their seizures not previously experienced.

Conclusion

One of the main contributors to the success of the training project was that it closely preceded a specific police operation which required the skills and knowledge contained in the program. Detectives and uniformed police faced their 'practical examination' when they were forced to apply the knowledge in situ within a few weeks of the training. Had the period between the training and practical application been longer the success rate may not have been quite so high. In addition, the constantly changing nature of equipment and media containing potential electronic evidence makes the need for frequent updated training essential.

Information and documentation on the seizure of electronic evidence has been disseminated across a large physical area. There will be a ripple effect and this will assist with future computer crime related operations. The good feedback from the officers in the field indicates a definite need for the skills and knowledge presented in the training program. Computer crime is not currently included in initial training at the police academy, however the current content could be easily adapted and implemented into police recruit training.

Disclaimer: The views of the authors are not necessarily those of the Western Australian Police Service.

References

Armstrong, Colin J., 2003, Mastering Computer Forensics, in Security Education and Critical Infrastructures, Irvine, Cynthia and Armstrong, Helen, (Ed's), Kluwer Academic Publishers, Boston, pp 151-158

Armstrong, Helen & Forde, Patrick, 2003, Cyber criminals and their use of the Internet, Journal of Information Management & Computer Security, October, Vol. 11, No. 5.

Armstrong, Helen & Russo, Phillip, 2004, Electronic Forensic Education Needs of Law Enforcement, Proceedings of CISSE8, West Point Military Academy, West Point, NY

Britz, Marjie T., 2004, Computer Forensics and Cyber Crime, Pearson Prentice Hall, New Jersey

Broersma, Matthew, 2004, UK Internet Crime Efforts are Criminal says Study, Computerworld, Sunday, 23 May, 2004, Available WWW:
http://www.computerworld.co.nz/news.nsf/UNID/BB017D2244CD06D3CC256E9A0073384A

Denning, Dorothy, 1999, Information Warfare and Security, Addison-Wesley, Reading Massachusetts

EURIM 2003, E-Crime Study, Partnership Policing for the Information Society, Working Paper 4: Roles and Procedures for Investigation, Available WWW: http://www.eurim.org/consult/e-crime/dec03/ECS_WP4_web_031209.htm

EURIM, 2004, *Supplying the Skills for Justice*, available WWW: (http://www.eurim.org/consult/e-crime/may_04/ECS_DP3_Skills_040505_web.htm).

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

Roast, S., Lavender, P. & Wisniewski, T., 2001, Global Impacts, Future Challenges and Current Issues in training within the Police Computer Crime Unit, Proceedings of the Second World Conference on Information Security Education, July, Western Australia, pp 7-23

SMH, 2004, Operation Auxin explained, Sydney Morning Herald, September 30, available http://www.smh.com.au/media/2004/09/30/1096527872004.html

Warren, M., 2003, Australia's Agenda for E-security Education and Research, in Security Education and Critical Infrastructures, Irvine, Cynthia and Armstrong, Helen, (Ed's), Kluwer Academic Publishers, Boston, pp 109-114