CPRC

CANADIAN POLICE RESEARCH CENTRE

CCRP

CENTRE CANADIEN DE RECHERCHES POLICIÈRES

# TM-11-98
# ADVANCED INTERNET INVESTIGATIONS COURSE EVALUATION REPORT

By: Sergeant Keith Daniels
Criminal Investigative Services
Ottawa-Carleton Regional Police Services

**TECHNICAL MEMORANDUM**

Submitted by
Canadian Police Research Centre

**June, 1998**

NOTE: Further information about this report can be obtained by calling the CPRC information number (613) 998-6343

## EXECUTIVE SUMMARY

The Canadian Police Research Centre's efforts to research and identify high quality training for Canadian high technology and computer investigators have resulted in a joint research effort with the Computer Crime and Intellectual Property Section (CC&IP) of the United States Department of Justice.

The CC&IP Section of the United States Department of Justice is coordinating the National Cybercrime Training Partnership (NCTP), which is composed of subject matter experts in high technology and computer crime investigations from approximately 50 North American law enforcement agencies. The NCTP has researched law enforcement training requirements and has had six investigator courses created to meet those requirements.

The Ottawa-Carleton Regional Police Service (OCRPS) with support from the Canadian Police College, the Economic Crime Branch of the Royal Canadian Mounted Police and the Canadian Research Centre has had the NCTP's recently developed Advanced Internet Investigations Course evaluated for Canadian requirements. This was done by sending Sergeant Keith Daniels, an experienced OCRPS computer crime investigator, to evaluate a pilot course in Sacramento, California in June 1998. Sergeant Daniels' evaluation of that course is the subject of this CPRC Technical Report.



## RÉSUMÉ

Afin de mettre au point une formation de qualité à l'intention des enquêteurs canadiens en matière de haute technologie et d'informatique, le Centre canadien de recherches policières (CCRP) a entrepris un projet de recherche mixte avec la section des délits informatiques et de la propriété intellectuelle (SDIPI) du ministère de la Justice des États-Unis.

La SDIPI coordonne le National Cybercrime Training Partnership (NCTP) (partenariat national de formation en cybercrimes), qui regroupe des experts dans le domaine des enquêtes relatives à la technologie de pointe et aux délits informatiques provenant d'environ cinquante organismes d'application de la loi nord-américains. Le NCTP a étudié les exigences de formation des organismes d'application de la loi et a conçu six cours d'enquêteurs en conséquence.

Le Service de police régional d'Ottawa-Carleton (SPROC), en collaboration avec le Collège canadien de police, la Sous-direction de la police économique de la Gendarmerie royale du Canada et le Centre canadien de recherches policières, s'est chargé d'évaluer en fonction des exigences canadiennes le Cours supérieur sur les enquêtes reliées à l'Internet, récemment élaboré par le NCTP. Pour ce faire, le sergent Keith Daniels, un enquêteur chevronné en délits informatiques du SPROC, s'est rendu à Sacramento, en Californie, en juin dernier afin d'évaluer un cours pilote. Cette évaluation du sergent Daniels fait l'objet du présent rapport technique du CCRP.


# Evaluation Report
# Advanced Internet Investigations
# Course June 15 - 26, 1998

Course Developed and Delivered by;

**SEARCH**
**The National Consortium for Justice Information and Statistics**
**7311 Greenhaven Drive, Suite 145**
**Sacramento, California 958831**

(916) 392-2550
fred.cotton@search.org

Evaluation prepared by;

**Sgt. Keith Daniels**
**Sexual Assault & Child Abuse Section**
**Criminal Investigative Services**
**Ottawa-Carleton Regional Police Services**
**474 Elgin Street**
**Ottawa, Ontario**
**K2P 2J6**

(613) 236-1222 extension 5461

# EXECUTIVE OVERVIEW

**The Advanced Internet Investigations Course** is funded by the U.S. Department of Justice. The **SEARCH GROUP** ( The National Consortium for Justice Information and Statistics) has been given a grant to create and instruct courses in all aspects of "High Tech" computer investigations. While the SEARCH group is based in Sacramento, they do numerous remote presentations and instruction.

The course in question is ten days in duration and consists of nine hours per day with a total of eighty hours of instruction. It is fairly well balanced between lectures and hands on computer lab time.

A UNIX version known as LINUX Red-Hat was the Lions' share of the course. In fact a full five days were dedicated to it. Two world renowned experts provided a base knowledge of LINUX and the hacking concepts that goes hand in hand with this type of system. Each student was required to install the Red-Hat version and then download programs using this operating system. The second phase showed how computer systems are compromised and exploited, how to recognize these compromises and then install an intrusion detection device. It is important to note that this was by no means a block in teaching UNIX to a proficient level. The purpose was to encourage the student to install this system on their own computer and become familiar with its uses from there.

With respect to the legal portion of the course it should be noted that there were approximately two days set aside for this. This would of course have to be modified to Canadian content. While I feel that it might be difficult to find a single person that has as much in depth court experience as the District attorneys that we heard from, there would be sufficient knowledge from a core group. This portion should in my view act as a gelling point for Canadian wide uniformity from search warrant, to arrest, to the evidence capturing and its presentation.

There is little doubt that a course such as this would be of great benefit to law enforcement agencies in Canada. As of this time officers using the Internet for investigative purposes have by and large learned their skills by themselves. It should also be noted that the number of crimes being committed on the Internet multiplies on a daily basis. It is now possible to purchase almost every kind of identification from blank drivers' licences for all states and provinces to blanks for money reproduction. Blank money masks are purchasable and when reproduced on a high quality printer are almost undetectable. Even the old pigeon drop scam and others like it are cropping up regularly people are, and will continue to be bilked out of millions of dollars. Organized crime is playing a large part in Internet crime.

While at this time Internet investigators are small in number, five years from now most general investigators will have to be fully functional in using the Internet as an investigative tool. It is important to note that California is presently in the process of legislating that all first line officers and investigators complete a high technology crimes and computer seizure training course by the year 2000.

With respect to the prerequisite for this course, I feel that a basic knowledge of LINUX commands was somewhat understated in the SEARCH course prerequisite. Most of the students in my class were finding this difficult. It is however mandatory that investigators have a knowledge of this operating system. Without doubt a good working knowledge of the Internet is recommended. While there was a block that gave a review of the students knowledge, this should not be considered as a learning exercise.

For an investigator to begin or continue with this type of investigation, it is important to note that the most up to date equipment should be used. While we will never keep up with the criminal element with respect to technology, it is important to have the best equipment available. A separate telephone line that is not billed directly to the police agency prevents hackers from accessing pertinent information. At least two undercover accounts with an Internet provider (paid by cash with a fictitious name and address). This would be required for each investigator in the unit. Each investigator would require a laptop preferably with a cellular phone modem. It can be of great assistance to go on-line with the suspect just prior to the raid.

In conclusion, it is the opinion of the writer that this course would be of great benefit to Canadian Law Enforcement. It would seem however that it would be to our advantage to have the core instructors from the SEARCH group provide a portion of this education.

**Sgt. Keith I Daniels**
**Ottawa Carleton Regional Police Service**
**474 Elgin Street**
**Ottawa, Ontario**

**(613) 236-1222 extension 5416**

# TECHNICAL EVALUATION

It should be noted from the outset that while the course outline was clear, this is only the second course of its kind in the United States. The outline appeared only as a guide to the instructors and was not necessarily taught in the order in which it was portrayed. In fact some of the items were not covered and others that were not mentioned were.

# MONDAY, JUNE 15, 1998

## 0800 TO 0900 HOURS.

**Fred Cotton**. Staff instructor. Initial introduction of the faculty and students. Basic information as to the geographical area of SEARCH and its functions.

## 0900 TO 1200 HOURS.

**Glenn Lewis**. Staff instructor. Provides a review of the Internet and some of the techniques used in the investigative field. While this was not provided as an instructional process, it was to review some of the aspects of the Internet that may be used by the investigators. Some of the topics covered were basic Internet services.
For example:

- **Telnet**. A method of dialing into another computer.
- **Internet Relay Chat (IRC).** Probably the most frequently used method of meeting and communicating with other persons in real time. It should be noted that there are at times over 10,000 chat groups covering all topics imaginable. This area is used by paedophiles, fraud artists and hackers regularly. There was not a lot of time spent during the course on this subject. I feel that this is an integral part of the investigative field and at least one whole day should be spent on this with the investigators actually going on-line in an undercover capacity while being supervised.
- **FTP**. File Transfer Protocol is used to transfer files from one computer to another.
- **Winzip.** A method used to compress files for quicker transfer and storage.

- **Cookies.** A small program that is often placed on a computer by the site visited to provide information about the user and possibly his computer. When the site is visited again, the cookie will alert the site accordingly. This is typically used when a user downloads a program on a trial basis with the cookie alerting the company that your free review of the program is complete. It will then disallow the user from accessing the program again until payment is received.

- **Browser functions**. Both Netscape and Microsoft Explorer have similar functions in allowing the user to, among other things, view sites on the Internet. It is important to note that they keep a log of sites visited and in fact it leaves a footprint. It should be noted that at this time that hackers will not communicate with a person using explorer, they do not feel that it is adequate.

## MONDAY, JUNE 15 TO THURSDAY, JUNE 18, 1998

### JUNE 15 - 1300 TO JUNE 17 - 1300 HOURS.

**UNIX/LINUX - Red Hat Version.** Instructor **Ross Mayfield** is a faculty/ guest instructor for the SEARCH group and is in fact on their board of members constructing the courses. He is a Professor with Pepperdine University in California and is a volunteer officer with the Los Angeles police department. He has been used by numerous world wide companies to review their computer systems. There probably is not a computer system that he cannot exploit. This portion of the course is referred to as UNIX boot camp. The students were required to:

Install a UNIX/ LINUX flavour known as RED HAT. This was done with Mayfield actually giving the keystroke commands and explaining their features as he did so. As mentioned in the executive summary it is important to note at this time that an appendix to this report will give the requirements for a lab that would be adequate to support this type of course.

Upon the completion of the installation and several students having to reinstall, we were provided with tools that allow the user to access LINUX. We then used it for general Internet uses such as, e-mail, downloading and transferring files, performing investigative

searches such as Whois and trace-route. The students performed all of these functions as well as using the LINUX graphic interface X-Windows and a word processing package known as PICO which is relatively small and similar to wordpad in Windows

This block of the course was provided in an effort to clear the path for a subsequent instructor **Andrew Gross** in the second week. It was made clear that UNIX is a system that will enable the investigator to use it as an investigative tool. It is important to become familiar with the O/S that is most widely used by hackers to exploit other computers. As the millennium approaches it would appear that UNIX will be a required operating system for investigators and Windows NT being the mainstay for computer usage in everyday life with Microsoft moving to this from Windows 98.

This instructor is without doubt the integral part of the course with respect to UNIX. I doubt that a Canadian instructor exists with the same level of expertise and policing knowledge. I do however feel that either his portion of the course has to be longer or the initial knowledge of the student would have to be higher with respect to UNIX. The latter could be difficult to find in the investigative field at this time. Equally important to note is that this was not designed to teach all about UNIX but to give a taste for it and hopefully the student will continue his or her quest to become fluent in the UNIX/LINUX operating system. There is little question that UNIX/LINUX is the backbone of this course.

## THURSDAY, JUNE 18, 1998

### 1300 TO 1400 HOURS.

**Overview of Internet Service Providers** - Guest instructor **George Hall**, gave a detailed overview of an Internet service provider and what can be expected of them during an investigation. While this was both informative and well presented, a Local provider could present this block adequately. It is an essential part of the course. While many people have used the Internet, it is useful to understand how the information is captured and presented to the user. The Internet provider is an excellent resource to the investigator. Being well versed in their operations assists the investigator in knowing how to approach them and what to ask for.

### 1400 TO 1700 HOURS.

**Corporate Security Investigations**. This block was presented by guest lecturer **Tim O'Neal.** Mr. O'Neal is a retired police officer who had an in depth background in the computer field that was mostly self taught. He left the policing field to work for Hewlett Packard in the Corporate computer security field. He gave an overview of several cases that he has worked on in conjunction with police investigators and provided insight into what is required from both sides if an investigation is to be conducted.
This block could be taught by a local expert in this field.

## FRIDAY, JUNE 19, 1998

### 0900 TO 1200 HOURS.

**Overview of Windows NT.** This block was presented by **Mr Mark Menz,** a SEARCH staff member who is the Systems specialist. During a class project in which there were two groups attempting to locate information on a suspect, he hacked into the systems using various systems to observe where we were going and slowing us down in the process. As previously mentioned, this will become the main operating system of the computer population by the year 2000. An insight into the security holes and administration of such a system was imperative.

This instructor invented a piece of hardware and software, known as SNAPPY in which clips can be captured from a video camera and presented on the computer. He is an integral part of the instruction team.

### 1300 TO 1700 HOURS.

**Law and its Application to the Internet**. Instructed by **Mr Don Ingram** a California State District Attorney. Covered subjects as:

- Economic espionage.
- State Law.
- PC502 (Computer crime law).
- pc 499 (Trade secret theft).
- Evidence code.
- Harassing telephone calls.
- Trap and trace orders.
- Search warrants for Internet accounts
- inter-agency cooperation.
- Enforcement agencies.

This block as taught would have no influence on the legal perspective as it would apply to Canadian evidence. This 4-hour block would be an important time to have our Assistant Crown Attorney give such an overview, with consistency in search warrants playing a large part., i.e., the ongoing saga of 487 vs. 487.01 warrants.

## MONDAY, JUNE 22, 1998

### 0800 TO 1700 HOURS.

**Case Preparation and Presentation - Communication Strategies** was to have been taught by guest lecturer **Cal Dalrymple** of the F.B.I. Unfortunately Mr. Dalrymple did not make it due to other commitments. This valuable block was given by Mr. **Mike Menz** (twin brother of Mark Menz). I do feel that in this new world of computer crime and its presentation to the courts, this is a cutting edge presentation and would be invaluable. Mr. Mike Menz is a member of the High Tech Task Force of Sacramento a multi agency squad. This presentation covered very important topics such as:

- Documentation of evidence and system diagraming. Both Judges and Juries tend to be uneducated in the field of computer crime an as such need to be provided with graphical explanations.
- Organization of reports.
- Plain English investigative reports.
- Technical reports. What did you find and how was it found.
- Items overlooked in searches such as computer watches, V-brom chips (bios

password chips).
- Driver licences and blank money available from the Internet. Menz related that he in fact printed five $50 U.S. bills that worked in machines in Reno Nevada on a test basis. These bills were printed with the aid of a Hewlett Packard 720 printer.
- Several 2600 magazines that provide hackers with up to date methods and a second magazine used by hackers known as Black Listed 411.
  Several sites in which the topic of discussion was the exploitation of computers.

This block also contained a discussion on the execution of search warrants. While the U.S. executes their search warrants in a different manner, there is no doubt that we should be taking more care. Menz mentions that guns are located in the majority of searches and in one case a bomb was found by Menz inside the computer. Expert examination of the bomb revealed that it would have killed anyone within fourteen feet. It is not unusual for the initial entry to be made by the SWAT team and a bomb dog then doing a scan of the property.

They always video tape the interior of the property where a computer search is conducted. This gives an excellent overview for the court of the scene. A review of the video can on occasion reveal something that was missed or has been reconfigured wrongly.

**NOTE:** This would require the use of a 487.01 warrant in Canada as well as the traditional 487 warrant.

Other search related topics covered included:
- knowledge of the suspect including photographs as some of the officers on the search may not know the suspect.
- Map of the location.
- Personnel required for the search. Some computer searches are long and require many officers. It is easier to release officers from a scene than it is to get them there.
- Equipment required to conduct the search.
- If an NT system is suspected obtain the proper assistance. More and more of these machines will be seized.
- Preparation of forms for the seizure and takedown.
- List of all personnel and their pager and phone numbers given to all participants.
- Have a central lead investigator that all questions are directed to.
- Emergency information and numbers if out of town officers are involved.
- Availability of translators.
- Always Fingerprint the inside of the CPU.

One of the techniques used by Menz to ascertain information about the computer and the occupants is to employ a lottery commission scam asking five specific questions and offering 10 free tickets for a lottery.

On a personal note, I have been able to obtain more information by posing as an Internet service provider and offering 10 free hours from my service if the person assists me by completing the telephone questionnaire. This can provide valuable evidence for the search warrant and subsequent court proceedings where identification of the person using the computer is in question

Menz covers the requirement of officers conducting the computer takedown having a forensic tool kit. He recommends one sold by a company called ICAST at 916-773-2199. He indicates that it sells for $30. (We did not see such a kit and therefore we were unable to evaluate it).

Regular items for the search are similar to those used in any search:

-marking pens
-masking tape
-ties
-bags
-boxes
-tools
-stick-on coloured dots

This block was extremely valuable. The same evidentiary problems exist regardless of location. The better a computer case is presented to the courts the greater the chance that it will be understood by the trier of fact. The equipment, preparation and officers' safety are equally important. We do tend to be less cautious with computer searches however, thus, far we have not met with any real level of resistence.

**NOTE:** What was not covered in the course was the actual deployment and briefing. This is one of the most important parts of any raid. The success or failure of the search can rest on this.

# TUESDAY, JUNE 23 TO THURSDAY, JUNE 25, 1998

## JUNE 23 - 0800 TO JUNE 25 - 1200 HOURS.

**UNIX/LINUX continued.** Instructed by **Andrew Gross.** Andrew is a young man who has a PH.D. with the University of Southern California. He is touted by members of the SEARCH group and Ross Mayfield as one of the top three computer experts in the world specializing in and the tracing of UNIX hackers. He has been involved in several National and International cases. Without doubt he is brilliant at what he does. Several of the students and myself found him to be lacking in presentation skills which detracted from the topics covered during the two and one half days of this presentation. For the most part the students felt that this block was above them and would have liked to have been much more UNIX conversant to have understood and participated in it.

He covered topics such as:

- SYN Flooding in which an attacker initiates large numbers of connections from random addresses to tie up operating system resources. Considerable information on hacking is found in alt.2600 news groups.
- E-mail spam, while not an intrusion method it ties up resources, mail is usually to a third party and generates many complaints for the party in that the message was sent to. Hackers like to hack into a site and send spammed mail from there.
- Trojan horses.
- Tools.
- SATAN and ISS scan systems for a known set of bugs and will give a list of possible entry points.
- COPS and TIGER scan the local system for malfunctions and known vulnerable versions of system programs. Also, gives a list of possible vulnerabilities.
- ROOTKIT. A very popular set of tools, a set of back doors, a sniffer and system programs to hide the intruders tracks.

A considerable length of time was spent on actually reviewing case files of hackers logging into a site and attempting to log in as the root. This would then have provided them with the ultimate power of the system and allowed them to conduct whatever business they wished either within that system or moving to another site from there while actually

looking as if they were from that site. Hackers tend to use this system to set up their WAREZ sites from which they publish access numbers (cracks) for software piracy. Sites such as these are often running for a considerable length of time prior to either being taken down by the system administrator or police intervention. Of course in the majority of cases it is not cost effective for the company and is embarrassing to say the least to announce that your system has been compromised. Accordingly, complaints are not always made to police.

His presentation of **How to Approach a Compromised Site** was most interesting and covered the following topics:

- Is the intruder still active?
- How can one tell without tipping off the intruder?
- Does one monitor the intruder or shut them down?
- What is important to protect? Data, integrity or availability.
- What data exists on the host or in the enclave that would help the analysis of the intrusion?
- Is one getting all of the data? E.g., does it log what everyone thinks it is logging?

GROSS spent some time covering network intrusion as it is going to play a large part in the Internet investigators' toolkit.

## THURSDAY, JUNE 25, 1998

### 1300 TO 1700 HOURS.

**NETWORK INTRUSION (NID).** Instructed by **Glen Lewis** and **Fred Cotton.** This block provided the installation of the Network Intrusion Device (NID) which is a United States program and was provided to the students from within that country. Unfortunately it is not legal to bring it into Canada at this time and is not in the possession of the writer. Once installed into LINUX and configured to the network that is being compromised, it allows for the interception of all packets sent and received in real time. This can be monitored live or logged for future reference. In a class project we installed the system and divided into groups of three. We then set up a Windows 95 machine as the sender of a message to a UNIX machine with the NID installed between. As the message was sent, it was instantly received by both machines.

This type of system should ideally be placed at the point where the company goes out to

the Internet. Less ideal, would be on the network segment with the compromised machine. This is less ideal as one cannot see organization wide activity.

NID is a program put out by Lawrence Livermore National Laboratory. Further information is available on the Internet at http://ciac.llnl.gov/cstc

NID is a collection of tools that help detect, analyze and gather evidence of specific behavior. It is a good trap tool that is passive and does not put any packets out. It cannot be detected on the network. It has the capability of e-mailing the investigator when the system is compromised. It also allows remote access.

This was a most interesting presentation and shows the effectiveness of a system such as NID. I am unaware of any similar programs that are Canadian, undoubtedly there may be. If this were the case and such a program was located, it is suggested that this company could instruct the class accordingly. Lawrence Livermore National Laboratory does put on an in depth course on their software. I feel that more than a half day could be spent on this subject. In the event that NID was chosen and is available in Canada, **Lewis and Cotton** have sufficient knowledge of this system to provide a good overview.

## FRIDAY, JUNE 26, 1998

### 0800 TO 1200 HOURS.

**Law and its Application to the Internet** instructed by **Fred Smith** a district attorney that has spent a great deal of time prosecuting computer related cases. His presentation was well prepared and he made good use of Powerpoint for his presentation. It was light and informative with his showing a great deal of his preference for art and described the evolution of the Internet with it. Again this could and should be presented by a Canadian Legal representative. It should be noted that a good deal of this morning was intended to stimulate discussion on this subject.

One important point covered by him was that of a company called LEXIS/NEXIS, who for a fee, will provide an incredible amount of information about a possible suspect. This company and another that we heard of earlier in the course called AUTOTRACK provided an astonishing amount of information when we used it in a test mode. One of the students names was entered and for a fee of one dollar per minute a detailed search is conducted. Typically it takes about 10 minutes to complete. When done, it provides

information about the person, his family, residences, phone numbers, social insurance numbers, phone numbers of next door neighbours, previous addresses, outstanding debts and work information. This information is kept up to date and is only approximately three weeks to a month behind. This is an excellent investigative tool. In fact another name was entered who was a suspect in one of the students cases. He was trying to locate the wife who had moved away from the State and who was believed to be harbouring the suspect. Information from this search led to the arrest before the course was completed.

## 1300 TO 1700 HOURS.

**Course Review.** Head instructor **Fred Cotton** and his **assistants Glen Lewis and Mark Menz** provided a review of the two weeks, a debriefing and class evaluation. Each student was provided with a compact disk that had been recorded by the SEARCH group. This student c/d provides a large amount of information with respect to the course material. Numerous programs that are considered freeware are also on the disk. It will however take a long time to categorize for it to be useful. This was done to streamline the process of using handouts. The class as a whole was adamant that a handout book would be of great use both during the class and after as a reference manual. SEARCH will be reverting to this in subsequent classes.

Students were given copies of both NIP and PGP. These programs were not included in the writers c/d for customs purposes.

## CONFIGURATION OF THE CLASSROOM AND THE LABORATORY

The class was made up of 18 students. They were linked to 20 computers all linked to a network with Windows 95 installed. Each machine was linked to a T1 line which provides the maximum speed of access to the Internet. Each machine is built and configured with exactly the same hardware. This is done exclusively to speed up the loading of LINUX and is critically important. While expensive to create, any other setup would slow down the LINUX installation and become confusing. LINUX requires the information of the hardware.

# CONCLUSION

As previously stated, the course itself is two weeks in duration and includes eighty hours of instruction and lab time. It could not have been done in any less time.

With respect to the faculty, **Cotton, Lewis, Menz and Mayfield,** it is important to note that they have been hand chosen for their areas of expertise and presented themselves and their subjects clearly, concisely and professionally. Their balance of lab time versus lecture time kept the flow working well. If a course such as this was to be offered in Canada, we would be remiss if we did not access their expertise.

It should be noted that at one point in the course Mr. Menz was discussing IRC (Internet relay chat) and possible hacks to it. Many of the students had never seen the IRC in operation and Mr. Menz was unsure of the nuances of it. The writer spent approximately thirty minutes with the students actually accessing a chat room and locating paedophiles. At least two cases were generated that could lead to charges. I would recommend that a block be devoted to this area.

A surprising and most accurate point was made by **Fred Smith,** when he related to a proposed law amendment under Assembly bill #2351 dated April 2, 1998. This bill indicates under section 13515.55 that. “Every city police officer or deputy sheriff at a supervisory level and below who is assigned field or investigative duties shall complete a high technology crimes and computer seizure training course certified by the Commission on Police Officer Standards and Training by January 1 2000".

This bill shows how serious the problem is and how California intends to bring all front line officers up to a standard of knowledge where they are comfortable with computer crime and seizure. At present, we tend to utilize a small corp of computer savvy detectives to complete the computer recovery. Time is fast approaching where this will not be possible due to time constraints. Field officers will be required to power down computers and seize them in a manner that critical information will not be lost.

As Internet crime is Worldwide and border less, problems that take normally five years or longer to arrive in Canada from the United States are here now and must be addressed accordingly. As law enforcement agencies we need to be as pro-active as possible. Training in the area is most important.