14th BILETA Conference: "CYBERSPACE 1999: Crime, Criminal Justice and the Internet".

Monday, March 29th & Tuesday, March 30th, 1999.
College of Ripon & York St. John, York, England.

Basic Considerations in Investigating Computer Crime, Executing Computer Search Warrants and Seizing High Technology Equipment

By Sergeant John J. McLean

Inevitably and often without notice or adequate preparation, police investigators find themselves confronted with the challenges of high technology. When in the course of a basic criminal investigation an investigator comes across computer equipment (hardware & software) that may contain important evidence, the question that often surfaces is, what should the investigator do? This question can not be answered with a simple response such as "shut it down and take it". Instead, investigators need to know what valid options there are and become properly trained in computer search & seizure and computer-related evidentiary issues.

High technology evidence presents unique and challenging situations for the investigator. In addition to ensuring that the necessary forensic examination and essential preservation of computer evidence is done, the investigator needs specialized training and tools with which to work with. The use of advanced search programs, access to sophisticated computer equipment, a working knowledge of evidence recovery methods, and a keen understanding of the types of associated computer evidence are all key factors that help investigators find evidence in computers.

Search Warrant Considerations

When investigators learn that a computer system is involved in some measurable way with the offense, they need to elaborate on "how" the computer was used. For example, if the police have learned from knowledgeable and reliable sources that a particular person uses a computer data base and spreadsheet program to account for illicit drug sales, then investigators need to include this information in their affidavits. Furthermore, investigators should carefully decide on how much of this information should be included in the affidavit without compromising source identity. Obviously, if we are protecting a confidential informant who may be one of only a few persons having access to this particular computer data, we may prematurely reveal our source.

In many cases, sophisticated drug dealers, money launders, organized crime accountants and others, have effectively used coded/encrypted shipment, financial and customer data files in the furtherance of their criminal activities. In the situation mentioned above, the computer now becomes an instrumentality of the offense besides being evidence of a crime and a storage device or container of evidence. Of course, our immediate right for seizure is further justified, so long as we have articulated it in the affidavit as particular items to be seized.

If, on the other hand, during a lawful search, without any prior knowledge of computers being used, we discover a computer system at the scene, can we look in its files? The answer to this is, yes! Using the example above, we can justify the computer data search so long as we had asked for

judicial permission to search for records associated with illegal sales, distribution, design, manufacturing, production, cultivation, importing, and illicit use of controlled drugs. Investigators should include in their affidavits some commonly accepted language that generally describes computer evidence such as, "Any and all records pertaining to (specify), found in either electronic or written form, located in devices capable of data storage and retrieval." This should effectively cover network, desktop, laptop and pocket computers, data watches, memory telephones and most other electronic data storage systems, where evidence could be found.

Investigators are allowed to reasonably search in any place where these items (data records) could be located. Investigators should justify their search into these devices based upon some specific training, knowledge and/or experience they obtained, suggesting that the described records can in fact be stored on computer systems.

In the writing of the affidavit, investigators should to be aware of the correct computer terminology when describing the places to be searched and items to be seized. Examples of specific computer language can often be found in previous search warrants, and selected training materials. Investigators should avoid adopting so called "boiler plate" search warrants. In order to help satisfy the particularity requirement, investigators need to describe the particular computer system sought. When investigators do not know the exact description of the computer, but suspect or know of its use, then using general descriptions and definitions of a computer system might be adequate.

Computer Evidence

Depending on the particular crime being investigated and its relationship with various computer applications, there can be a number of specific files to look for. For instance, in child pornography cases, investigators should look for not only the graphic images, but also the associated communication and transfer programs that might have been used to capture, download, modify, view and produce the image. Programs and files such as e-mail attachments, original compressed files, news & file retrieval agents, browser programs, dial-up information, file captures, session logs and many others can have a wealth of valuable information. Associated computer evidence found in various computer files can and often will reveal the time, date, manner, location, email address, history logs, web site, file transfer location, IP Internet address and other useful information. Any computer crime investigator, worthy of his name, knows the value of such information.

Scope of the Investigation Search

The process of taking down a computer system depends in large upon the scope of the search, according to the system's configuration (LAN, WAN networks, mainframes, servers, PC's, etc.). If the subject of the warrant is operating on a network, then keep in mind that the ability to store evidence throughout that network is possible. When conducting controlled searches, investigators should also look at network drives, the network & local backup copies, including mirrored/redundant logical drives, the local disk drives and various removable storage drives, disks and tapes. Investigators should also know that many businesses store their backup information off-site, often with contracted third party vendors.

Identifying & Seizing Software/Hardware

Prior to the execution of the search warrant, the investigator should get as much information on the type of computer system they are searching for and possibly seizing. Police need to know that computer systems can comprise a number of hardware components and software. Today's computer system can obviously have a printer, mouse, monitor, modem, keyboard, central processing unit, main circuit board, expansion board, hard, floppy, tape, removable, CD-ROM/DVD and optical drives, memory modules, computer chips and so much more. Police need to be able to recognize computer equipment when they come across it and seize these items if they are within the scope of

the search and listed as items to be seized.

Network Computers

When investigators are executing a warrant on a network system, the use of a computer network expert is the recommended method, so long as the police direct and control the search. Investigators employing civilian experts or officers from other jurisdictions in executing search warrants should get judicial permission in their affidavits prior to the search. The procedure for executing local or wide area network search warrants is an exacting and detailed process, often specific to the individual computer network. Investigators should also seek the assistance from trusted, non-targeted, inside personnel. They can provide an enormous amount of detail about the computer system's configuration and structure. Remember to be careful in not making your cooperatives "agents of the government" avoiding illegal searches and interceptions. Except in rare cases, investigators will not seize an entire network of computers. Instead, a controlled forensic search and retrieval of the evidence might be done on-site.

Seizing Smaller, Whole Computer Systems

When investigators are dealing with smaller networks, desktops PC and workstations an attempt to justify the taking of the whole system should be based on the following criteria. When an entire organization is pervasively involved in an ongoing criminal scheme, with little legitimate business, (in non-essential services) and evidence of the crime is clearly present throughout the network, an entire system seizure might be proper.

In small desktop situations, investigators should seize the whole system, after requesting to do so in the affidavit. Investigators seizing whole systems should justified it by wording their affidavits in such a way so as to refer to the computer as a "system", dependant on set configurations to preserve "best evidence" in a state of original configuration. This can and often does include peripherals, components, manuals, and software.

In addition to the above, investigators should make every effort to lessen the inconvenience of an on-site search. Some estimates of manual data search and analyses are 1 megabyte for every 1hour of investigation work. Based on this equation, a 1-Gigabyte hard drive can take up to 1000 hours to fully examine. This equation assumes that each piece of data is decrypted, decoded, compiled, read, interpreted and printed out.

Condition of Evidence

Computer files can be found on many other storage mediums in all sorts of deceptively modified, hidden, compressed, encrypted and semi-erased conditions. Therefor, investigators need to be technically prepared to deal with evidence found in these conditions and should mention these conditional factors in their affidavits in order to legally expand the their scope.

Onsite Interviews

Investigators need to seek critical information from persons present or having direct knowledge of the computer system. The most important information that investigators need is information about passwords/security devices on the system. If there is no actual custody or interrogation of the suspect asking for this information without the standard Miranda warnings is permissible, however giving the warnings is the preferred method. Sometimes by asking other persons present, the investigator can obtain the same information. Also, ask if there are onsite/offsite backups, privilege levels and access controls present in the computer system. Of course, investigators should also ask about the evidence they seek to find in the computer, relating to their case. If a person states that the evidence you seek to find is located in the computer system, a cursory examination is not necessary. However,

don't restrict your search to the areas that the suspect directs you to look. Be prepared for evidence in multiple locations.

Forensic Image Backup

Computer crime investigators recognize the vulnerability of electronic data and strongly suggest that forensically acceptable image duplication software be used in investigations. After the investigator makes a duplicate image of the seized media (hard drive, floppy, removable drives, etc.) and restores this backup onto another system, the original evidence should be secured away. The restored backup image (exact copy of the original) now becomes the location to search for electronic evidence. Remember a proper forensic image will copy each sector of the original media, including unused areas, data that is hidden, partially erased and encrypted, allowing the investigator to attempt restoration of data.

Searching & Retrieving Evidence

A number of forensic tools exist that enable investigators to streamline and control their search for evidence in storage devices. A detailed list of computer forensic software is available by request. For instance, there are a number of specialized search programs that allow investigators to structure customize searches for important evidence. Investigators need to know that encrypted data and various compressed data formats will not allow these types of searches until the data is uncompressed or decrypted.

After evidence is located it needs to be understood and correlated to the case being investigation. Computer investigators utilize specialized viewer and conversion programs that can accommodate many file formats for quick viewing and printing of evidence.

Investigative Barriers

As mentioned earlier, investigators often encounter data in modified, protected, corrupted partially erased, compressed and hidden forms. Investigators need to become aware of these conditions and the methods employed to defeat them. These file conditions can frustrate and impede investigations. Except for high level encryption, with adequate training, and sophisticated tools, investigators can overcome most of these encountered conditions.

Case Expansion

Investigators need to be prepared for case expansion after seizing computer systems relating to their cases. In hacker type cases, it's not uncommon to find evidence of credit card fraud, copyright violations, telephone fraud as well as malicious destruction of computers. In some cases involving child pornography, the uncovering of local rape victims and child prostitution rings might be encountered. In online fraud cases, it's often discovered that the offenders move from location to location and from one computer based fraudulent scheme to another.

Processing & Preparing Evidence for Prosecution

The evidence presented in trial should be the original and best evidence. For cases, where there is a huge volume of records and documents, a stipulation accepting imaged records and displayed images from the mirrored forensic hard disk image should be agreed to. This can make the data search and presentation of evidence much easy in a court setting than traditional methods. For instance, prosecutors can utilize such equipment as video/LCD projectors, multiple set monitors, high quality color printers and sophisticated image and data base software for case presentations.

Investigators should reproduce the evidence in the format and condition as close as possible to the

state of originality. For instance, in cases involving child pornography, if the imagery was printed out and disseminated, then duplicate the printouts with the same printer. Police can enhance graphic images for the purposes of investigation, but caution should be taken on making any substantive modifications to the original evidence. Investigators need to properly document all modifications to evidence.

Computer Search Warrant/Seizure Guidelines

The following guidelines are not meant to be a rigid and set procedure. Rather, they are intended to generally guide the investigator. Each computer investigation should be based on the uniqueness of the particular computer system and the case being investigated.

GATHER INTELLIGENCE INFORMATION ABOUT THE CRIME MAKING NEXUS TO THE COMPUTER

OBTAIN SUBPOENAS/COURT ORDERS AND OTHER COMPULSORY PROCESSES ABOUT THE SUSPECT

DOCUMENT UNDERCOVER OPERATIONS/CAPTURE LOGS & SESSIONS AND FILE TRANSFERS

BE CAREFULL WITH "ENTRAPMENT" AND "AGENCY" ISSUES

SEEK LEGAL ADVISE & REVIEW FROM YOUR PROSECUTORS BEFORE SECURING A COMPUTER SEARCH WARRANT

DESCRIBE COMPUTER SYSTEM (GENERICALLY OR IN DETAIL IF KNOWN)

DESCRIBE THE SPECIFIC FILES/PROGRAMS CONTAINING EVIDENCE (GENERICALLY OR IN DETAIL IF KNOWN)

USE WORKABLE LANGUAGE AND UNDERSTANDABLE COMPUTER TERMINOLOGY

DEVELOP SEARCH WARRANT EXECUTION PLANS FOR TAKING DOWN COMPUTERS

CONSIDER THE TIME OF EXECUTION, BEFORE COMPUTERS ARE IN USE. ALTERNATIVELY, ONE CAN EXECUTE DURING ACTUAL USE & ONLINE TIMES (MORE RISKY)

SECURE/FREEZE COMPUTER SYSTEM DURING PROTECTIVE SWEEP

DON'T LET THE TARGET/SUSPECTS/WORKERS USE THE COMPUTER SYSTEM ANY FURTHER (THEY CAN ADVISE YOU, BUT BE CAUTIOUS WITH THEIR INSTRUCTIONS)

DON'T PULL POWER PLUGS, OR FLIP SWITCHES (YET)

TAKE VIDEO/PHOTO OF COMPUTER SCREEN DISPLAYS (IF OF EVIDENTIARY VALUE)

WITH A COMPUTER FORENSIC PERSON PRESENT - ATTEMPT TO CAPTURE UNSAVED MEMORY DATA AND MEMORY/PRINTER BUFFERS AS DUMPS TO SOME EXTERNAL MEDIA (I.E. 3.5 FLOPPY)

WITHOUT A COMPUTER FORENSIC PERSON PRESENT - PULL THE MODEM/DATA COMMUNICATION NETWORK CABLES FIRST (NETWORKS HAVE SHUTDOWN COMMANDS USUALLY RESERVED AT THE CONSOLE/ADMINISTRATOR/SUPERUSER LEVEL). LARGER NETWORKS WILL BE PROBLEMATIC/SEEK ADVICE

•. WITH A COMPUTER FORENSIC PERSON PRESENT - DO A NORMAL NETWORK/PC SHUTDOWN

•. PULL POWER CORD FROM COMPUTER - IF COMPUTER IS ALREADY TURNED OFF

•. INSERT, BUT DON'T RUN, A WRITE PROTECTED/SEIZURE DISK IN THE FLOPPY DISK DRIVES OR ANY OTHER BOOTABLE DISK DRIVES (CD-ROM/DVD/REMOVABLE DRIVES)

•. WITH A COMPUTER FORENSIC PERSON PRESENT - IF COMPUTER IS ON, DETERMINE IF THE ENTIRE DRIVE IS ENCRYPTED (LOOKING FOR SPECIAL ENCRYPTED FILES AND UNIQUE PARTICIANS/PROGRAM SIGNATURES).

•. IF THE SYSTEM IS RUNNING & THE HARD DRIVE IS ENCRYPTED, FIRST, COMMENCE AN ON-SITE FILE-BY-FILE BACKUP THEN AN IMAGE COPY BEFORE SHUTTING DOWN THE SYSTEM (ONCE SYSTEM IS SHUT DOWN THE ENCRYPTED DRIVE MIGHT BE IMPOSSIBLE TO ACCESS)

•. IF COMPUTER IS ON CHECK FOR BIOS-CMOS LEVEL PASSWORDS, WINDOWS USER PASSWORDS, SCREEN SAVER PASSWORDS AND OTHER PROGRAM PASSWORDS. ADJUST & CHANGE THESE SETTINGS TO A POLICE PASSWORD IF POSSIBLE (DOCUMENT CHANGE)

•. IF COMPUTER IS ON, NO ENCRYPTED HARD DRIVE, DO NORMAL PC SHUT DOWN COMMANDS (LIST IS AVAILABLE FOR UNIX/LINUX/WINDOWS/SUN OS AND OTHERS)

•. PULL POWER CORD FROM COMPUTER AFTER NORMAL SYSTEM SHUT DOWN

•. SKETCH, PHOTOGRAPH AND IF POSSIBLE, VIDEO TAPE THE COMPUTER DESKTOP AREA AND REAR OF COMPUTER SYSTEM

•. DUAL LABEL ALL WIRED CONNECTIONS TO THE COMPUTER SYSTEM FOR EASY RESTORATION

•. LOCATE HANDWRITTEN NOTES AND POSSIBLE PASSWORDS NEAR THE COMPUTER

•. GATHER & SAFELY PACK (BUBBLE WRAP) ALL RELATED COMPUTER COMPONENTS, ALL COMPUTER STORAGE DEVICES (FLOPPY/HARD/CD/DVD/REMOVABLE MEDIAS, ETC.)

•. TAKE COMPUTER MANUALS, PRINTOUTS AND TECHNICAL NOTES

•. TRANSPORT COMPUTER EVIDENCE WITH EXTREME CAUTION AVIODING RADIO TRANSMITTERS, STRONG MAGNETIC FIELDS AND POWERFUL GENERATORS

•. SAFELY STORE AT ROOM TEMPERATURES COMPUTER MEDIA, DO NOT ALLOW PROLONGED EXPOSURE TO HEAT OR MOISTURE

•. UNLESS DONE ON-SITE, COMMENCE MAKING TWO FORENSIC IMAGE COPIES OF THE SEIZED MEDIA WITHIN A REASONABLE AMOUNT OF TIME (ASK FOR PERMISSION TO DO THIS IN YOUR SEARCH WARRANT)

Forensic & Utility Software/Hardware

Investigators conducting computer forensic examinations need some of the best utility and specialized software programs available. Forensic software programs are needed for:

Safe Seizure/Write Protection/Evidence Processing/Hardware & Software Referencing

Making Image Copies of the Seized Media

Analyzing Seized Media and Computer Systems

Password Breaking (decryption software)

Customized Data Searching

Multiple File Viewing and File & Language Conversions

Investigators also need to have fast, reliable and powerful forensic computers to conduct examinations with the restored media images. Usually this involves having an expandable full-tower computer unit, Pentium II based, with an large amount of memory (128 MB) having multiple swappable hard disks for storage. Moreover, investigators need to obtain various external/removable drives/read & write CD-Drives and perhaps most importantly a high quality, color printer.

Training & Technical Assistance

Investigators should seek out specialized training in the areas of:

Computer Crime Investigations

Computer Forensics/Computer Evidence

Computer Undercover & Specialized Operations

Some organizations and associations that provide training and assistance to law enforcement are:

HTCIA (High Technology Crime Investigation Association) http://www.htcia-ne.org

HTCU (Massachusetts Attorney General's Office, High Tech Crime Unit) 617-727-2200

NWCCA (National White Collar Crime Association) http://www.iir.com/nwccc/nwccc.htm

SEARCH (Nat. Consortium for Justice Information/Statistics) http://www.search.org/

NTI (New Technologies Incorporated) http://www.secure-data.com

IACIS (International Association of Computer Investigative Specialists) http://cops.org/

FLETC (Federal Law Enforcement Training Center) http://www.treas.gov/fletc/mission.htm

MCJTC (Massachusetts Criminal Justice Training Council) http://www.mcjtc.org/

Other Federal Agencies (FBI-DOJ-OJJDP) http://www.FBI.gov/

This article is not intended to be a comprehensive manual on computer search warrants, computer investigations and computer evidence. Investigators should always seek specialized training and legal advice especially when they are confronted with complicated and technically challenging investigations.

Medford Police Sergeant J.J. McLean is currently supervising the Attorney General's High Tech Crime Unit and has actively investigated numerous computer crime cases. He is an instructor for the MCJTC, DOJ-OJJDP and Northeastern University. He is the President of the High Technology Crime Investigation Association, New England Chapter. He has both BS & MS degrees from Northeastern University's, University College and the College of Criminal Justice.