

SEARCH AND SEIZURE OF COMPUTERS

Sri. U. Rama Mohan,
Computer Crime Analysis Expert
APFSL, Hyderabad

Introduction

In less than one generation, the Information technology revolution has introduced the computer into virtually every critical dimension of our daily lives and the economy. History is filled with competition between those who commit crime and those who try to prevent crime. This competition is a never-ending test of who can best create a new solution. There is no other form of crime that cuts so broadly across the types of criminals and the severity of their offences. Even though there has been substantial publicity in recent years about computer systems risks and attacks, it turns out that most system penetrations go unreported. Today, the spread of computer crime has touched nearly every form of occupation. It is estimated that within the next decade nearly all crimes will involve the computer in some way or other. Thus it has become inevitable for the law enforcement agencies to answer this most urgent need of the hour, tackling of Computer Crime. As an endeavour to meet the need, various states of India have started Cyber crime police stations and APFSL has taken a lead in setting up the first of its kind, Computer Crime Analysis Laboratory in a state FSL.

As per section of IT Act, 2000 only police officers and above the rank of Deputy Supdt. Of Police can investigate offences under the IT Act, 2000. However

electronic evidence may be relevant in ordinary IPC crimes also. Most of the I/O's are asking several questions about search and seizure of the computers, the following article will throw some light and answer few basic questions of I/O's on the various practices to be followed and the precautions to be taken while conducting search and seizure of electronic evidence.

Preparation for the Seizure

As with any search and seizure operation good preparation is the key to success. Obtain as much information as possible about the type of computer system, the location of the equipment within the building, the layout of the building, the number of people present etc. If possible find out the number of computers that may need to be examined and the size of the hard disks

To seize or not to seize

There are basically two ways of dealing with computers when on a search operation

- i) *Seize the computer and its associated hardware and forward it to APFSL where the contents can be examined*
- ii) *Complete the imaging on site without taking possession of the computer itself*

The ideal situation is to take the computer if the system belongs to an accused. However, it may not be possible to do this when the computer does not belong to the accused, or it might be vital to the owners business for it to remain on site.

How to handle a 'live' computer

In order to seize a computer it must first be switched off. The general rule is that if a computer is turned on at the scene then switch it off using the mains switch or removing power cable from CPU. Do not allow the owner to touch it since you do not know if they have set certain keystrokes to perform non-standard operations of a destructive nature.

There are situations where it is impossible to just switch the machine off due to damage that will be caused to the hard disk contents. This is rarely a problem with standalone machines or small networks (up to five workstations).

What to seize and where to look

First identify the computer and its peripheral hardware -keyboard, monitor, printer and so on

The general rule is to take possession of all the attached hardware

Sometimes it so happens that an item is needed at a later date for some previously unidentified reason. For example, it may need to have the printer examined to establish if it produced a particular document. Items such as modems and network adapters will be needed if the system proves to be non-standard and must be rebuilt at a later

date in the laboratory. While keyboards and monitors are fairly standard, there are some differences, so to be on the safe side take them

Always look carefully for floppy disks and portable storage media

They may be anywhere on the site and have proven vital in a number of cases. Cautious suspects will often store information on floppy disks that they will not keep on the hard disk. If you find floppy disks always pack them according to their location at the scene. For example, put the disk that was near the monitor in a separate bag to the ones found in the desk drawer. Clearly mark the location of the disks on each packet.

Floppy disks, zip disks, optical cartridges and sometimes even CD's may also contain backup files which can be restored at a later date in the laboratory. These can be most useful for establishing significant event time sequences

Talk to the owner or operator of the machine

While all this is going on it is a good to talk to the owner or operator of the machine and ask if there are any password protection devices or access control systems that need to know about. If there are any, make a note of them together with the name of the person you discussed with. In practice it is rare to find desktop machines protected with passwords but quite common on portable and notebook computers. The presence of a password can itself indicate that there is something suspicious and 'worth hiding' on a machine.

Under any circumstances do not attempt to examine the contents of a machine directly!

Photographing and recording equipment layout

In case of seizing more than one computer system, make sure which peripherals belong to which processing box. This can be done by labelling each cable as it is disconnected and removed.

Use digital camera to record the layout and the actions being taken. The images can be cheaply and easily stored.

Bagging, tagging and removing equipment

Once disconnected, equipment should be placed in high density polythene bags or anti magnetic and anti static current baggages. Each parcel should be sealed and labeled with details such as. description of contents and location. Disk drives are fairly robust but transport and handling the system box should be gentle.

All equipment should be handled carefully

Storage of seized equipment

A record should be maintained of all actions and movements involving the item together with details of any seals. Seized equipment should be stored in a clean, dry and secure location. Stored equipment should be kept away from

excessive heat or cold (i.e. radiators or air conditioning vents), any magnetic fields (i.e. functioning electrical equipment or loudspeakers) and it should not be allowed to get dusty or dirty.

Dealing with UNIX/Linux Operating systems

When dealing with UNIX/ Linux systems it is not advisable to unplug the power cable directly. When the computer is switched ON it is better to follow the regular procedure of shutting down by using SHUTDOWN command, as the files which are currently running and not saved cannot be retrieved if the system is shutdown by unplugging the power cable. Deleted files cannot be retrieved in UNIX as in Windows operating system.

Dealing with large networks

Obtain specialist help

In case of seizing a large network, it is essential to obtain specialist help from someone familiar with a similar system. The way in which the system is configured may be crucial to successful examination at a later date. It may also not be necessary to seize all parts of the system and technical assistance may identify only those parts that are required. It is preferred that a person from Cyber crime police station of C.I.D or a scientist from A.P.F.S.L, should be requested for the help.



"If you are not criticized, you may not be doing much."

- Donald H. Rumsfeld (1932-)