

COMPUTER RELATED CRIMES

- by **RAMNISH**, Dy.S.P./CCIC/CBI

As digital technology has advanced over the past 50-odd years with a force unprecedented in history, governments, businesses and people around the world have been affected immeasurably. The already enormous and exponentially growing capacities for electronic storage, transmission and rapid manipulation of data changed the modern landscape virtually overnight, making the world of today's children unrecognizable in many ways to those of earlier generations. Perhaps with some of the bias that is part of our generation, the changes have included substantial benefits. However, such fundamental restructuring in society also results in certain disadvantages, at all levels. Our vulnerability increases with the perceived value of and reliance on this technology. Increased opportunities for the industrious to be more productive also allow the less-upright new avenues for mischief.

At the same time, the Internet has expanded the reach of society's predators - scam artists, child exploiters, stalkers, and thieves. Criminal denizens of the Internet can be harder to track, and evidence of their crimes more difficult to collect, preserve, and present. New tools and new techniques must be applied, and expertise acquired to address novel legal questions. The sheer volume of crime on the Internet is daunting, and a recent FBI/CSI survey reports that over 90% of

responding businesses suffered digital security breaches in the last 12 months of survey.

In this article, the author will attempt to introduce you to the emerging world of the computer crimes and initial steps an investigator can take to detect the same. While writing this article, it is presumed that the reader showing interest in this article is having basic knowledge of computers and Internet.

Definition of Computer Crime

Although there is no recognised definition of the computer crimes, but the writer feels that it can be defined as:

A criminal act in which a computer is essential to the perpetration of the crime

A criminal act where a computer, non-essential to perpetration of the crime, acts as a store of information, concerning the crime.

These crimes are committed by the cyber criminal under the cover of anonymity provided by the Internet and are very difficult to investigate. The victim sometime is not aware of the crime committed against him/her. While investigating such crimes, quick reaction to the reporting of such crime is essential. since, in case of infrastructural hacking,

it may affect public life and property. This is why top priority is given by the developed world which has a highly computerised public infrastructure - to prevent and detect hacking.

ROLE OF COMPUTERS IN A CRIME

In the context of Cyber crime, the computer is nothing but a "tool" or "implement" used in perpetrating crimes like extortion, money laundering, cheating, stalking etc. Within this paradigm the following broad "roles" of a computer emerge:

1. Computer as "object":

The Computer is an object or target when someone accesses a computer system without permission for the purpose of stealing or destroying data/information, intellectual property, cyber-trespass, etc. For this the offender accesses the operating program of the target system by masquerading as the system's manager, thus giving the intruder access to virtually every file in the compromised system.

2. Computer as "Subject":

When the computer becomes the physical site of a crime, or is the source of or reason for unique forms of assets losts, then the computer is called "Subject" of crime. The launching of viruses, worms, Trojan horses, etc. fall in this category.

3. Computer as "Instrument":

When a computer system is used as an

instrument or tool to gain access to other computer systems and to manipulate such system to produce the desired results then such system is called "instrument" to crime.

4. Computer as "Incidental":

The computer is not essential for the crime to occur, but the computerisation helps the crime to occur faster. Cyber laundering, unauthorised banking transactions, conspiring with the use of e-mail, crime records of a gang or individual, etc. The role of computer here is "incidental".

Crimes on the Internet can be broadly classified into:

- (1) Crimes on the Internet itself - i.e. using the infrastructure available.
- (2) Web based crimes
 - a) Web sites related crime
 - b) E-mail crimes
 - c) Internet Relay Chat crimes
 - d) Usenet related crimes

INTERNET CRIMES

Possible criminal uses of the infrastructure of the Internet are:

★ Hacking:- Unauthorised access to a computer system. This can be done for:-

- ◆ Defacing web site
- ◆ Theft of information
- ◆ Theft of Passwords

- ◆ Theft of credit card numbers
- ◆ Launch of malicious programmes (Programs made for doing such acts which may cause harm to computer, data stored therein, source code of computer or may make computer to do such acts which may harm other computer systems)
- ◆ Denial of Service attacks
- ◆ Distributed denial of service attacks;- In a typical connection, the user sends a message asking the server to authenticate it. The server returns the authentication approval to the user. The user acknowledges this approval and then is allowed onto the server.

In a denial of service attack, the user sends several authentication requests to the server, filling it up. All requests have false return addresses, so the server can't find the user when it tries to send the authentication approval. The server waits, sometimes more than a minute, before closing the connection. When it does close the connection, the attacker sends a new batch of forged requests, and the process begins again—tying up the service indefinitely.

★ Spoofing:- A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of

techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.

- ★ Espionage
- ★ Spamming

SECTIONS OF LAW:-

Relevant sections of IPC and section 43, 65, 66 & 70 of IT Act, 2000.

QUESTIONS TO ASK THE VICTIM:-

- When was attack detected?
- What abnormal act of the system led to suspicion by the victim?
- Were access log in records maintained?
- Was the system protected with Firewall. if yes, what type of firewall was installed?
- Which operating system is being used on the victim computer system?

Investigation:-

- In a 'simple' case of hacking it would be possible to trace out the IP address by the 'who is' query.
- The IP address may be found in the "Page Source" head - (Netscape) and "source" head in Internet Explorer?
- However in complex hacking cases the IP address may be misleading- because it may be just 'one' of the victims being used. The "tracer route" software will help here.

- This is the stage when 'normal' investigation will take over - like who is the possible suspect
 - Disgruntled employees?
 - Business rivals?
 - Enmity?
 - Mischief?
- The nature of the "stamp" the hacker leaves on the hacked page might also give a clue to the 'rid' of hackers involved. This hacker stamp may be found in the form of the url of the picture imbedded in the defaced page. The type of the program used for intrusion etc.
- ◆ In case of surveillance tactics to be used by the IO, proof of every intrusion or attempted intrusion.
- ◆ Log-in details of the suspected hacker from the ISP concerned for the relevant time, and before and after for analysis of any trend, pattern etc.
- ◆ Once the suspect is traced down, on and during search and seizure of the suspects' premises, possible finger prints of the suspect on the mouse, screen, monitor body, CPU body, subject to human handling can be lifted after they are found by using normal finger print detecting techniques as evidence to prove the possession of the attacking machine along with necessary accessories by the suspect.

Evidence to be collected

- ◆ The record of the "firewall" if the firewall is installed showing date & time of attempted intrusion.
- ◆ If firewalls are not installed, the statement and printout of the corrupted" pages on the websites/files, if the person who first noticed it.
- ◆ If it is a network, the logs of the system administrator will help prove that the particular hacker was "logged" on to the net at that particular time.
- ◆ Photographs of the location of the machine, along with photograph of modem and connections to power supply etc. to prove the machine on which hacking/intrusion/virus was first noticed, (in the presence of independent, technical witnesses).
- ◆ Copy of the hard disc of the affected machine with the help of experts.

World Wide Web Crimes

This actually means any crime taking place from a particular web site/sites affecting the innocent victims accessing the site. The cases in this category are much easier to investigate, especially because you start off on a focused note.

Possible Criminal Uses

- Cheating & Frauds
- Advance Fee Scheme
- Insurance Frauds
- Impersonation Frauds
- Letter of credit Frauds
- Nigerian Letter Frauds
- Ponzi Schemes

- Pyramid Schemes
- Theft
- Gambling
- Distribution of Pornography
- Sale of pirated softwares
- Credit Card number theft, etc

Sections of law applicable

Relevant sections of the IPC and Sec. 67 of IT Act 2000 in case of Child Pornography/Pornography.

QUESTIONS TO ASK THE VICTIMS

Apart from asking the usual questions relevant to any specific crime, the additional questions in a web site crime to be asked are:-

- a) What was the URL or IP address of the suspect site?
- b) When was this site visited by the victim?
- c) Does the victim have a hard copy of the screen of the suspected site?
- d) Was the web site saved on the hard disk of the computer or in any other media?
- e) From where the suspected site was visited i.e. home, business, cyber cafe, etc.?
- f) Was any online payment made with the credit card?
- g) Was the site having any contact e-mail address, if yes, was it noted?

INVESTIGATION:

- Confirm identity of suspect by running the "whois" query".
- The "whois" details" generated may be genuine or that of a "compromised" machine.
- Server service provider for that particular suspect website may be asked for the details of the ownership of that site and also the log-in details of that site.
- After identifying the suspect, his premises may be searched for collecting vital evidence.
- The suspect can be interrogated for ascertaining the administrative password of the site for obtaining the files of that particular site.
- If the case relates to financial cheating, the suspects financial transactions can be examined.
- All other relevant information may be collected from the computer of the suspect, his server and other records etc.
- All other relevant investigation techniques applicable to the specific crime.

Evidence to be collected:-

As specified in "Internet Crimes" and on the lines specified above.

E-MAIL CRIMES

The speed of communication has reduced the world to "seconds" in time zone. The

same has also provided criminals a very effective instrument for planning and executing the offences.

POSSIBLE CRIMINAL USE:-

- * Threats
- * Extortion
- * Stalking
- * E-mail bombing
- * Defamations
- * Frauds
- * Launching of malicious programmes.

SECTIONS OF LAW APPLICABLE:-

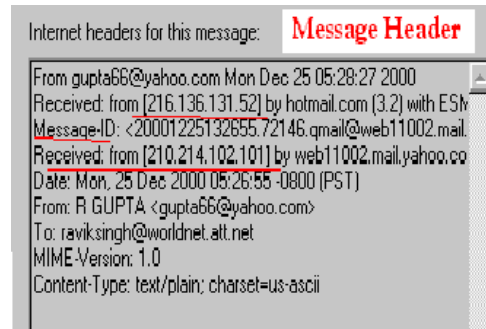
Relevant sections of IPC and other relevant Acts and section 43, 65, 66 & 70 of Information Technology Act, 2000.

QUESTIONS TO ASK THE VICTIM:-

In case of a crime reported by a victim involving E-mail, the following additional questions are required to be asked:-

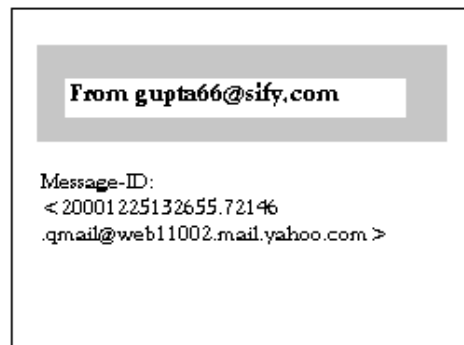
- ◆ What is the name of the Internet Service provider of the victim?
- ◆ Does the victim have a printed copy of the E-mail? if yes, collect the same.
- ◆ Had the victim printed the E-mail header?
- ◆ Did the victim save the e-mail on his/her computer?
- ◆ Is the e-mail still in the mailbox of the mail server of the victim?
- ◆ What was the subject of the mail

- ◆ What was the screen name and e-mail of the offender?



INVESTIGATION:-

- Get the "message header". Some of the mail sites provides "header" in the mail it self. If the same is not provided, the message header can be obtained by downloading the E-mail with the help of "Outlook express" and by viewing the sub head "details" in properties of that particular e-mail



- The header will give the IP address. Run "whois" to ascertain the details of

the Service provider, whose Mail service were used by the suspect.

- If by analysing circumstances, it is felt that the "whois" result is genuine, the location of suspect can be traced with the help of ISP.
- In case of a forged/bogus or disguised/ number- letter mixup e-mail identities, the ISP can help in identifying the suspect with the help of the E-mail header by analysing its contents and "message ID".(see boxes for forged/ bogus, disguised senders details)
- The ISP will be able to help in locating a suspect, because when a person dials up to connect with an ISP, he/she is logged on to one of the Servers of the ISP. This server assigns (depending on the port of entry) a specific IP address to the user. This IP address temporarily becomes the IP address of the user for that specific session.
- All relevant material from the sender's and receiver's machines and from the ISPs.

CAUTION:-

Sometimes even the e-mail headers don't provide us with sufficient or correct information as some of the sites provide for remailing and anonymous remailing facilities. When a mail is sent by using remailing facility, the remailer removes the original header and sends the mail with its own identity. In case of

anonymous remailers, no mail header is received. Such cases will have to be investigated by normal deductive investigation.

EVIDENCE TO BE COLLECTED:-

As specified in "Internet Crimes" and on the lines specified above.

To learn more about E-mail headers refer to **www.stopspam.org/headers/headers.html**.

USENET NEWSGROUPS CRIMES

Usenet is a popular mean of sharing and distributing information on the web with respect to specific topics or subjects. It provides access to various types of discussions. Some sites provide access to hundreds or thousands of usenet groups whereas others provide fewer sites. Usenet is made up of the people and systems who agree to exchange articles. In the usenet, the messages are not exchanged between individuals like in case of E-mails but are transmitted from computer to computer. Usenet is similar to a bulletin board system (BBS), except that most BBS have one manager and one computer supporting BBS. In Usenet, there is no single system, person or computer as administrator of the usenet, but is supported by all the users. Each computer system, which is a part of a Usenet runs softwares to receive, manage and forward the messages/ articles. The box on the side displays a list of Usenet Newsgroups related to hackers.

POSSIBLE CRIMINAL USES:-

- ❖ Distribution/sale of pornography material
- ❖ Sale of stolen property
- ❖ Distribution/sale of pirated softwares
- ❖ Distribution of Hacking softwares
- ❖ Discussion on methods of hacking
- ❖ Sale of Stolen Credit card numbers
- ❖ Sale of stolen data
- ❖ Consumer scams
- ❖ Chain letter scams
- ❖ Ponzi schemes, etc.

QUESTIONS TO ASK THE VICTIM:-

- Who is complainant's Internet Service provider?
- Name of the Newsgroup?
- Title of the posting?
- When was the same accessed by the complainant?
- From where was the it accessed by the complainant?
- Does the complainant have a printed copy of the posting? if yes, take a copy
- Did the complainant download the posting? if yes, take a copy on a removable media.

INVESTIGATION:-

- ◆ Zero down on the administrator of the newsgroup using the IP address and other facilities on-line.
- ◆ Log-in records of the particular newsgroups to be obtained from the ISP to show the victim's logging on at the particular time.
- ◆ Details of the posting and possible origin of these postings through the IP address.
- ◆ Details of the transactions/agreement entered into through the newsgroup.
- ◆ Other investigation on normal lines.

EVIDENCE:-

- ◆ To prove that this was a newsgroup - registration details.
- ◆ To prove the complainant's membership with the newsgroup.
- ◆ To prove the offenders membership with the newsgroup.
- ◆ Other evidence as specified in "Internet Crimes" and on the lines above.

To learn more about "usenet & newsgroups" refer to
www.dejanews.com
www.reference.com
www.sunsite.unc.edu/usenet-i/
www.internetdatabase.com/maillist.htm
www.catalog.com/vivian/interest-group-search.html

INTERNET RELAY CHATS CRIMES

One of the most popular parts of the Internet is Internet Relay Chat (IRC). These IRC servers have various channels which are commonly called Chat Rooms. In these chat rooms people from anywhere the world can come together and chat with each other.

In the Chat rooms, different windows like dialogue box, images and provide informations about users, other channels, etc. Some chat channels also provide user profiles and some also provide IP address of the User.

POSSIBLE CRIMINAL USES:-

- ◆ Cyber Stalking
- ◆ Fraudsters use chat rooms for developing relations with unsuspecting victims
- ◆ Criminals use it for meeting coconspirators.
- ◆ Hackers use it for discussing their exploits or sharing the techniques.
- ◆ Paedophiles use chat rooms to allure small children.

SECTIONS OF LAW APPLICABLE:-

Relevant sections of IPC and other laws with sections 65, 67 & 70 of IT Act 2000 in cases related to hacking, pornography/ child pornography.

QUESTIONS TO THE VICTIM:-

- Name of Internet Service Provider of the Victim/complainant
- Name of the Chat Server
- Name of Chat Room
- Nick name/ Screen name of the offender
- Had the complainant noted the profile of the suspect user
- Was the copy of Chat dialogue printed or downloaded by the complainant, if so obtain a copy.

INVESTIGATION:-

- ◆ Obtain Log-in records from the chat server for that particular session in the chat room.
- ◆ Obtain chat details, if available from the server.
- ◆ Identify the suspect with the help of his/her ISP.
- ◆ Identify other users of the chat room in that particular session and examine them, if possible.
- ◆ Other relevant investigation.

EVIDENCE TO BE COLLECTED:-

As specified in "Internet Crimes" and on the lines specified above.

In the end, I will like to submit that however easy it may seem, the

investigation of the computer related crimes is not easy. As this technology has made the whole world a tangled web full of poisonous spiders, the evidence for making out a fool proof case is not easy to be collected. The crime which might have been committed by a criminal with

victims in his own city may have the crucial links spread all over the world. Even the highly advanced and technology supported police forces of the world can claim to a success rate of hardly 10 percent.



The problem of power is how to achieve its responsible use rather than its irresponsible and indulgent use-of how to get men of power to live for the public rather than off the public.

- John F. Kennedy (1915-1962)