INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | March 2024
ISSN: 2582-6433

EXAMINING CYBER CRIME INVESTIGATION AND METHOD OF PREVENTING E CRIME.

AUTHORED BY - GARGI SHUKLA
ICFAI UNIVERSITY DEHRADUN
Pursuing master in cyber law
Email I'd- gargishuklamrt55@gmail.com

ABSTRACT

The digital revolution has already changed how people live, work, and communicate. And it's only just getting started. But the same technologies that have the potential to help billions of people live happier, healthier, and more productive lives are also creating new challenges for citizens and governments around the world. From election meddling to data breaches and cyberattacks, recent events have shown that technology is changing how we think about privacy, national security, and maybe even democracy itself.

Using the computers for our day-to-day transactions is quite common now a days. For example, we pay our life insurance premium, electricity bills, reserve flight or train or bus tickets, order book or any other product online using personal computer, smart phones, public browsing etc.

METHODOLOGY OF RESEARCH STUDY -This is a doctrinal research on cyber crime .

KEYWORDS -

INTRODUCTION TO Cybercrime Investigation

The advancement of technology has made man dependent on internet for all his needs. Internet has given man access to everything while sitting at one place. Social networking, online shopping, online studying, online jobs, every possible things that Man can think of can be done through the medium of internet.

Using the computers for our day-to-day transactions is quite common now a days. For example, we pay our life insurance premium, electricity bills, reserve flight or train or bus tickets, order book or any other product online using personal computer, smart phones, public browsing centers etc.

The number of users doing online transactions are growing rapidly ever since, because of the convenience it gives to the user to transact business without being physically present in the area

ISSN: 2582-6433

where the transaction happens. Criminals committing cybercrime are also growing day-by-day with the increased number of users doing online transactions.

Ever since the creation of the Internet, people have been finding ways to conduct illegal activities using it as a tool. Online exploitation and abuse of girls and boys; the black cyber markets for the purchase and sale of illicit drugs and firearms; ransomware attacks and human traffickers making use of social networks to attract victims. The unprecedented scope of cybercrime - crossing borders in our homes, schools, businesses, hospitals and other vital service providers - only amplifies the threats.

Investigation of a Cybercrime is process consisting of investigating, analyzing, and recovering forensic data for digital evidence of a crime. It involves the use of specialized tools and techniques to investigate various types of cyber crimes, such as hacking, phishing, malware, data breaches, and identity theft. Cyber Crime Investigation is a multifaceted field within the investigative community. Cyber crimes range from simple password stealing and phishing schemes to more complex and heinous acts such as child exploitation, human trafficking, and ransomware attacks. Investigative tactics vary based on the nature of the cybercrime. The unstoppable growth of cyber-crime means organizations of all sizes need to rethink their approach to the security. Everyone knows that security is important. We all rely on the Internet, IT and other connected systems, all of which without the appropriate protection could be at risk from cyber-crime.

Examples of evidence in a cyber crime investigation include a computer, cell phone, automobile navigation system, video game console, or other networked device found at the scene of a crime. This evidence helps cyber crime investigators determine the perpetrators of a cyber crime and their intent.

The investigation process is conducted by cyber crime investigators, who are responsible for conducting thorough and accurate investigations, preserving evidence, and collaborating with law enforcement agencies to bring cybercriminals to justice. Cybercrime investigation is essential for businesses and individuals to protect against the growing threat of cybercrime, and to ensure that justice is served for victims of cybercrime.

For conducting cyber-crime investigation, certain special skills and scientific tools are required without which the investigation is not possible. Investigating a crime scene is not an easy job. It requires years of study to learn how to deal with hard cases, and most importantly, get those cases resolved.

In a cyber crime investigation, unlike an “ordinary” criminal matter, the first step in preparing to testify is to evaluate the prosecutor’s level of technical expertise. This is essential because a cyber crime prosecution, like all other criminal cases, is a team effort between the investigator and the

ISSN: 2582-6433

prosecutor. If the prosecutor doesn't understand how and where the investigator found the evidence or the prosecutor does not understand the significance of the evidence, the prosecutor will not be able to effectively elicit testimony from the investigator. If your testimony is not presented effectively, the finder of fact will be confused, and the defense attorney will be able to exploit that confusion to create doubt in the jury's mind—this is to be avoided.

Definition - Cybercrime investigation is the process of analyzing, investigating, and recovering critical forensic digital data/evidence from the networks or systems associated in the cyber attack which could be the Internet/www or a local network in order to identify the executor of the cyber/ digital crime and their main motive behind the attack.

Cybercrime investigators should be experts in computer science, understanding not only computer software, file systems and operating systems, but also the working of networks/software and hardware in a computer system. They should have enough knowledge to determine how the inter-linking connection between all these components occur, in order to get a full description of what has happened, why it was happened, when it was happened, who has performed the cybercrime or cyber attack, and how can be victims will protect themselves or there near ones in the future against these types of cyber attacks.

Understanding Your Role as a Cyber Crime Investigator

With great power comes great responsibility.

—Uncle Ben to Peter Parker in Spider-Man

Post-mortem versus Live Forensics

Post-mortem and live forensics are both great evidence gathering techniques. However, in cases where you can only conduct a post-mortem forensics, the need to look at other systems within the environment is strengthened. This expansion of your scope to include other systems on the network will give you a better understanding of how the target system acted within its native environment.

Technology has evolved in such a way that conducting live investigations is really the only option you have under certain circumstances. In the days of old, computer networks were simple. In today's world, the evolution of the enterprise network work makes it difficult for system administrators, IT security personal, and the like to be at more than one location. Managing IT resources at a single site can be a daunting task.

Live investigations allow investigators to capture volatile information that would not normally be present in a post-mortem investigation. This information can consist of running processes,

ISSN: 2582-6433

event logs, network information, registered drivers, and registered services. Why is this important to us, you ask? Let's take a look at the case of running services and how this could be extremely important us.

Running services tell us the types of services that may be running on a computer. These services run at a much higher priority than processes, and many users are unaware that these services actually exist. Given their high priority and lack of attention by the typical end user, they are a common target for hackers. By conducting a live investigation, we are able to see the state of these services, which could prove crucial to our investigation. For example, a hacker could turn off the service for McShield, which is a McAfee Antivirus service, and then later come back and infest the machine with malicious software.

In a postmortem investigation, physical memory (RAM) is potentially the most important piece of evidence that is lost. However, this crucial piece of evidence is easily captured using live forensic and investigative tools, allowing the entire contents of RAM to be captured locally and even remotely.

Conducting cyber investigations

We often fear most what we don't understand. That could be said about computers and the investigation of computer crimes. Many investigators cringe at the mention of a computer and seek to offload any computer-related crime to the "computer crime guy" in their office. Although computers have been around for a few decades, they've finally reached levels where it is feasible to expect that everyone has access to a computer. The computer is no longer a "nice to have," it is a "must have. "Those who don't own their own computers can walk into a public library or cyber cafe to gain access to a computer. Similarly, access to the Internet is becoming ubiquitous through connections provided by libraries, coffee shops, computer stores, and even fast food restaurants. This explosion of computer technology and acceptance has opened up a whole new world of opportunity to the criminal element that constantly looks for new ways to exploit people through time proven scams and tactics. As computers become more deeply integrated within society, it is likely that a computer or similar type device will play a role in criminal activity. A basic understanding of computers is all that investigators will need to learn that computer crime is just plain old crime packaged up in a shiny new wrapper.

Demystifying Computer/Cyber Crime

Computers start to play a role in crime in situations where the capabilities of the computer allow a person to commit that crime or store information related to the crime. An e-mail phishing scam

ISSN: 2582-6433

is a common example where the bad guy generates a fictitious e-mail for the sole purpose of enticing people to a spoofed site where they are conned into entering sensitive personal information. That sensitive information is then available to the bad guy in order to perpetrate an Identity Theft. In another example, a suspect might use the computer to scan and generate fake bank checks, or create fake identification. In both of these cases the crime required the inherent capabilities of the computer for its commission.

The mere presence of a computer does not make a crime a computer crime. We must be careful not to hastily label a crime a "computer crime" just because a computer was involved. What if the new laptop I purchased was stolen from my vehicle while I was in the convenience store getting milk? This would not be a computer crime just because a computer was involved, but a theft. How about an office fight where an employee strikes another with the keyboard of their computer— should we call out the Forensic team? Absolutely not (well, maybe, if the assault resulted in a homicide). The computer in and of itself is not important, it is just merely an object like many others in our lives.

Since computers are so pervasive, it is an absolute necessity that investigators learn how to investigate crimes that involve a computer. The basic design of computers—including vast amounts of storage and meticulous file times tamping—can make them a wealth of evidence as traces of the crime can often be retrieved by an experienced investigator. This does not mean that every investigator needs to become an expert in computer technology, but there are basic concepts and methods that must be learned in order to develop old school leads. The key is to gain at least some basic computer knowledge and skills to put you ahead of the average computer user; skills that allow you to apply traditional policing skills and procedures to the case.

The crimes that are being committed haven't changed, just the manner in which they're being committed. Think about it. Back before the Internet, the telephone, the telegraph, and the Pony Express, if a person wanted to threaten to kill someone, it was likely they would have to physically place themselves in proximity to the person and speak that threat. As services and technologies developed, new ways emerged through which a person could commit that same threatening act. They could send a letter, a telegram, or even better, make a phone call. Now we can send an e-mail or instant message[1] (IM). Same crime; same underlying elements and facts to be proven. The only change is the manner of delivery. The key to a successful investigation of a computer

[1] IM stands for instant message. Instant messaging is another way for people to communicate with each other by computer in real time. A chat session is established between two or more computers using compatible applications through which written messages and files can be transmitted back and forth. The unique challenge of instant messages is that their content is not often recorded by service providers or the applications facilitating the chat. Once the IM session closes, the contents tend to be lost. This is not always the case as users can turn on chat logging, but by default most chat applications do not record sessions.

ISSN: 2582-6433

crime is the development and follow-up of case leads. Although many leads will dead end, it is the one that continues to develop into further leads that can end up solving your case. Many believe that investigations involving computers are above their capabilities, but that is often not the case. By learning and adapting some basic computer knowledge and skills, today's investigator can react to new technologies and still develop workable old school leads.

Throughout this chapter, critical skills will be discussed that prepare an investigator to deal with computer crime investigations. By developing a basic understanding of key concepts and learning to apply basic computer skills, an investigator can learn how to proceed with computer crime cases much in the same way as traditional cases. Issues such as IP Addresses, Networks, Wireless Devices, and Interpersonal Communication will be discussed with the sole purpose of providing the investigator with a basic understanding of each topic area and the skills that can be employed to yield workable physical leads. Many of these skills will build the foundation of computer crime investigations not only today, but well into the future as these technologies expand and become more complex.

Understanding IP Addresses

All law enforcement investigators need to understand the basics of IP addressing in order to trace users of the Internet to a physical location. Just as a phone number that shows up on a caller id box from a threatening phone call can provide investigators with a specific starting location for their investigations, an IP address can provide that same type of lead. By understanding what IP addresses are, how they're assigned, and who has control over them, an investigator can develop workable case leads. IP addresses provide a connection point through which communication can occur between two computers. Without getting into too much detail about them, it is important that you understand how to identify an IP address when you see one. These addresses are made up of four 8-bit numbers divided by a ".", much like this one: 155.212.56.73. Currently the Internet operates under the IPv4 (Internet Protocol Version 4) standard. In IPv4 there are approximately 4 billion IP addresses available for use over the Internet. That number will be expanding in the near future to about 16 billion times

that number when transition is made to IPv6.

During the birth and initial development of today's Internet, IP addresses primarily were assigned to computers in order for them to pass network traffic over the Internet. Computers were physically very large, extremely expensive, and pretty much limited to the organizations that controlled the primary networks that were part of the primordial Internet. During this time, an IP address most likely could be traced back to a specific computer. There are a limited number of

ISSN: 2582-6433

large organizations that own and control most of the IP Addresses available with IPv4.Therefore, if an investigator has been able to ascertain the IP address of an illegal communication, they will also be able to determine which organization owns the network space within which that address is contained. That information in and of itself will often not be enough since many of these organizations sublease blocks of the IP Addresses they own to smaller companies, such as Internet Service Providers (ISP). It will be the investigative follow-up with the ISP that is likely to provide the best results. Using an analogy, we can think about IP addresses much like phone numbers, where the major corporations are states and ISPs are towns or calling districts. If an investigator was following up on a case involving a phone number, the area code would narrow the search down only to a particular state, and the remaining numbers would identify a particular account.

Digital forensics and analyzing data

Digital forensics is probably the most intricate part of the cyber crime investigation process. It is often where the strongest evidence will come from. Digital forensics is the scientific acquisition, analysis, and preservation of data contained in electronic media whose information can be used as evidence in a court of law. practice of Digital Forensics can be a career all in itself, and often is. Other times it is a subset of skills for a more general security practitioner. Although the corporate digital forensic practitioner is not a law enforcement officer, it is a wise practice to follow the same procedures as law enforcement does when performing digital forensics. Even in a corporate environment, the work one performs can quickly make it to a courtroom. Regardless if the case is civil or criminal the evidence will still be presented the same.

The Evolution of Computer Forensics

Traditional digital forensics started with the seizure of a computer or some media. The drives and media were duplicated in a forensically sound manner bit by bit. Way back—if there is such a thing in computer technology—the forensic duplication would be combed through using a hex or disk editor application. Later the forensic applications and suites evolved and automated some of the processes or streamlined them.The forensic practitioner would undelete files, search for temporary files, recover e-mail, and perform other functions to try and find the evidence contained on the media. Today there are more user-friendly programs that present data in a GUI, and automate much of the extremely technical work that used to require in- depth knowledge and expertise with a hex editor. There is also a wealth of hardware to make the practice even more conducive, but the reality is the processes thus far have not changed that much. From the time of

ISSN: 2582-6433

those first primordial seizures to today, a set of Best Practices has emerged; the attempt is to provide a foundation for the work per- formed under the heading Digital Forensics:

- ■ *Do not alter the original media in any way.*
- ■ *Always work on a duplicate copy, not the original.*
- ■ *The examination media must be sterile as to ensure that no residual data will interfere with the investigation data.*
- ■ *The investigator must remain impartial and report the facts.*

Unlike other forensic sciences, digital forensics subject matter continues to evolve, as do the techniques. Human fingerprints may be changing and evolve over time, but it won't be noticeable to the fingerprint specialists in their lifetime. The trace chemicals in a piece of hair may change, but the hair itself is going to stay pretty much the same. The techniques may evolve, but the subject matter does not noticeably. Digital evidence on the other hand continues to change as the technology does. Operating systems and file systems will progress and change. Realistically, operating systems change nearly every five years. Storage arrays continue to grow larger and larger as the technology improves, magnetic data density increases, and the price points come down. Flash media drives continue to grow larger in capacity and smaller in form factor. The volume of devices with potential storage for evidence has grown exponentially and will continue to. Gaming systems, digital audio player, media systems, Digital Video Recorders—the list continues to grow. The boom in the digital camera market created a tremendous volume of devices and analysis need that traditionally were in the realm of photographic examiners, not the computer geek. As the assortment of potential evidence sources continues to grow, the methodologies need to expand greatly. For example, a cellular phone normally needs to stay powered on to retain all the data. If the device stays on it may connect to a wireless network. To ensure the device is isolated from the network the investigator will need to use a Faraday device[2]—but in reality by removing the device from the network we actually change the data on the device. The device will make a note to itself of the details of going off the network.

Phases of Digital Forensics

Traditional digital forensics can be broken down into four phases. Some of the work performed may overlap into the different phases, but they are very different:

[2] A Faraday device or Faraday cage is a device constructed to block radio signals from entering or exiting the protected area, creating an electromagnetic shield. It consists of a metal conductor or a mesh that prohibits the entry or escape of electromagnetic signals.

ISSN: 2582-6433

i. ■ **Collection**
ii. ■ **Examination**
iii. ■ **Analysis**
iv. ■ **Reporting**

Collection is the preservation of evidence for analysis. Current best practices state that digital evidence needs to be an exact copy—normally a bit stream copy or bit-for-bit duplication—of the original media. The bit stream copy is then run through a cryptographic hashing algorithm to assure it is an unaltered copy. In modern digital forensics often this is done by physically removing the hard drive from the device, connecting it to a write blocking unit, and using a piece of forensic software that makes forensic duplicates.

Examination is the methodical combing of the data to find the evidence. This includes work such as document and e-mail extraction, searching for suspicious binaries, and data carving.
Analysis is the process of using the evidence recovered to work to solving the crime. The analysis is the pulling together of all the bits and pieces and deciphering them into a story of what happened.
Report is the phase where all the other phases are documented and explained. The report should contain the documentation of the hardware, the tools used, the techniques used, and the findings. All the individual phases have their own issues and challenges.

Collection

Traditional digital forensics best practices are to make a full bit stream copy of the physical volume. This normally entails physically removing the hard drives from the suspect system, and attaching the drive to another system for forensics duplication. A forensic image is a bit-by-bit copy of the original media. It copies all the data on a storage device, including unused portions, the deleted files, and anything else that may have been on the device. The suspect hard drive should be protected from alteration (remember the procedure?) by a hardware solution, a software solution, or both. The hardware solution is normally either a write-blocker or a hardware imaging device. A write-blocker blocks the write commands from the examination system that some operating systems would normally perform. Software solutions entail mounting the suspect drive or device as read-only by the operating system. The data must be unaltered and the chain of custody must be maintained. Where practical, all the work should be performed on a copy; the originals need to be preserved and archived. To be able to ensure the data is unaltered, the original

ISSN: 2582-6433

drive and the imaged drive are hashed and the hashes[3] are compared to ensure that an exact bit-by-bit copy has been acquired.

Digital evidence needs to be:

- ■ Admissible It must conform to certain legal rules before it can be put before a court.
- ■ Authentic The data must be proven to relate to the incident. This is where additional documentation is important.
- ■ Complete It must be impartial and tell the entire account.
- ■ Reliable There can be nothing relative to the collection and handling of the evidence that could create any doubt. Chain of Custody procedures become crucial.
- ■ Believable The reports and documentation must present everything so it is believable and understandable by a judge or jury.

Any digital evidence collected must meet these requirements. The challenge that is surfacing is the admissibility. There are the traditional rules and best practices that concentrate on data from static or powered down systems.

As we will see next, there are issues where this approach is either difficult, impossible, or may leave large amounts of data behind. Challenges to collecting the data for analysis can be getting the files off the systems, and once they are off the system. Does the system have some way of connecting external storage or is there even physical access to do so? If there is no physical access, how long will it take to move the data off the system to work with it? An option may be to work with the data on the system, but is there enough storage on it to be able to duplicate and analyze it? If the system was compromised, can the use of the utilities and binaries on it be trusted? Most likely not. The next option is to move the data off via the network connection.

Examination

Examination consists of the methodical sifting and combing of the data. It may consist of examining dates, metadata, images, document content, or anything else. Many forensic practitioners use the same step-by-step process for their examination; key word search, obtain web histories, search unallocated space, search file slack.

Forensic Tools

[3] Hashes use cryptographic algorithms to create a message digest of the data and represent it as a relatively small piece of data. The hash can be used to compare a hash of the original data to the forensic copy. When the hashes match, it is accepted as proof that the data is an exact copy.

ISSN: 2582-6433

There are many tools that can assist with forensic examination. The tool selection can be based on personal preference, or the strengths of the individual application, or sometimes budget. There are forensic packages that can cost thousands of dollars or be freeware. Regardless of the tools chosen, it is a best practice, when possible, to use multiple tools. The primary reason is to not miss a piece of evidence due to an issue inherent to the tool—when the multiple tools agree on a finding it helps remove any doubts surrounding the reliability of the tool.

Utility of Hash Sets

Hash sets are precompiled lists or databases of known file hashes. For instance all the files associated with an application install or a series of illegal images are hashed with a cryptographic algorithm and the resulting hashes are put into an indexed collection. During an examination, the hashes of the application set are compared to all the hashes of the files found on the system. A matching hash mathematically nearly guarantees the file is a file associated with the application regardless of its name. Hashes traditionally have been used to find known suspicious files such as malware, cracker tools, or illegal images.

Just as hash sets can be used to look for known bad things, through the same process they can be used to locate known good or benign files. By using hash sets to locate the files that are not related to the investigation or are unchanged operating system files, for example, they can filter out the noise. Dependant on the triage of a case, a hash set of known operating system files can quickly filter out a quantity of files that in all likelihood do not need to be examined. For instance an incident where there is not believed to be a compromise of the system would not initially need to search or examine all the driver files. The use of hashes to filter out known files known to be unaltered from the hardware vendor can greatly reduce the volume of information to be examined and in turn the time to examine a system. The files left behind are either altered or files in user space that will probably be where the real evidence or information lies.

The creation of personal hash sets as part of the preparation task can be a time saver later. Creating hash sets of all of an organization's gold or standard images of workstations and servers used for new installs necessitates only altered or added files to be analyzed. The files of internal applications can also be hashed and sets created to also help filter out files that would not be included in more main- stream hash sets.

Difficulties Associated with Examining a System with Full Disk Encryption

An increasingly common issue is full disk encryption. This will change how hard drives are

ISSN: 2582-6433

acquired. As the issues of lost and stolen laptops continue to impact organizations, many IT departments are turning to full- or partial-disk encryption to protect data. For the forensic practitioner, this usually means the data of interest will be in the encrypted portions of the drive. If all the data of interest is encrypted, traditional forensic practices will be useless. The choices are to perform a live image of the system with the encrypted storage mounted, if possible, or unencrypt the drive after acquisition. As are many other issues in contemporary digital forensics, this is another area where the best practices and procedures are trailing the technology. Which solution you use should be evaluated and your own procedures created. In a crunch, the live system image will almost always be faster.

Trusted Platform Module (TPM)

The Trusted Platform Module is another emerging technology that will enhance existing encryption schemes. The TPM is a chipset being installed in newer machines that stores keys, passwords, and certificates. The chipset pro- vides for hardware-based encryption functionality that may prove to be a challenge.

Analysis

Every cyber crime incident will involve at least some analysis of data retrieved from systems. Some will consist of only a few small files from a system or two, or may range to terabytes from many machines.The core of an investigation could consist of a single piece of media or it may consist of thousands of hard drives. The trick lies in the analysis that will put all the pieces together. The analysis of an entire cyber crime event can be far more complex than the analysis of any of the systems themselves; the sum of the parts is truly greater than the whole. It can be likened to a symphony. Any single instrument may be difficult to play, but to bring all the pieces together is far more complex. The cyber crime investigator needs to build a toolbox of utilities to analyze the data from a myriad of systems and be able to correlate the data into a complete, coherent picture.

The analysis of the digital forensic process is the phase where we look deeper into the data. The analysis is the sum of all the data applied toward the resolution of the incident.

An example of an analysis follows.

An intellectual property theft case didn't yield much until the data from a bunch of systems were pulled together. The file server audit logs were reviewed and the user list it provided was used to query the proxy server logs. When the log files for those uses were reviewed a short list was

ISSN: 2582-6433

created by focusing on webmail and forum traffic. The short list was used to triage and prioritize the exams of the user workstations. The exams of the workstations quickly revealed the individual when the webmail messages were pulled from the internet cache, and recreated.

During the analysis phase it is imperative to tie in any other investigation intelligence that has been gathered. It is in this phase that the data from multiple systems or sources is pulled together to create as complete a picture and event reconstruction as possible. There is a difference in evidence for court and evidence to find the next piece for the investigation. A piece of evidence discovered may not be strong enough to stand on its own, but may be the item that provides the next lead. Another factor that is a challenge is that analysis of large amounts of data takes time. In the heat of an incident or a large high profile investigation it is
often difficult to manage the expectation of management. It can take huge amounts of time to import logs into various applications. It can take hours to move and copy data between storage systems.

Reporting

At the end of examinations and analysis comes perhaps the most tedious but arguably the most important phase. The report is compilation of all the documentation, evidence from the examinations, and the analysis. The report needs to contain the documentation of all the systems analyzed, the tools used, and the discoveries made. The report needs to have the dates and times of the analysis, and detailed results. It should be complete and clear so the results and content are understood perhaps years down the road. The report may be the most important phase of digital forensics. If the report is incomplete, or does not accurately document the tools, process, and methodology, all the work may be for nothing. Reporting will vary depending on the needs of your organization, but in most cases the minimum must include the documentation of the devices that were examined, the tools used, and the factual findings. Even if a procedure was used and yielded nothing of value it should be documented not only for completeness, but to demonstrate that the examination covered all the bases. Perhaps the greatest challenge after all the other hurdles of acquisition, examination, and analysis is how to present it all in a manner that cannot be questioned. There is a very real risk that some newer forensic techniques have not yet been challenged in a court room.

Phases of Digital Forensics

- *Data storage diversity requires many tools and procedures.*
- *The increased data storage requires large target storage devices.*

ISSN: 2582-6433

- *The time requirement for collection will continue to increase.*
- *More data collected equates to more data to sift through.*
- *The increased use of techniques to reduce the data of interest should be employed.*
- *The increase in the data available can simplify the final analysis, or it can just create a bigger haystack to hide the needle in.*
- *The analysis of the entire incident is far more complex than the examination of any single system.*
- *Reporting is possibly more important than ever as the techniques and procedures must be more finely documented because of potential impacts on volatile data.*
- *A poor report can make the best cyber crime investigation appear a disaster.*

Investigation Steps:

1. Crime Assessment - Developing and defining the background of the cyberattack with the known facts that will help the investigators or investigating company a commencing point to establish what they are facing, and how much information they have when handling the initial cybercrime report of that particular cyberattack.

- Ask fundamental questions: "Who, what, where, why, how, and when?"
- Gather surface-level information to prioritize resources.
- Determine the tools needed for evidence discovery.

2. Evidence Collection Procedure - This is One of the most important step any cybercrime investigator must do is collect as much information/facts as possible about the cyberattack.
Was it an automated/AI attack, or a planned human targeted attack? Was there any loopholes/open opportunity for this attack to happen? What is the scope and implications? Can this attack be executed by anyone, or by particular people with specific skills? Who are the potential suspects? What digital crimes were committed? Where can the evidence be found? What are the potential evidences? Do we have access to such evidence sources?
These and other questions are valuable considerations during the information collection process.
Surveillance involves not only security cameras, videos and photos, but also electronic devices surveillance that details what's being used and when, how it's being used, and all the potential digital behavior involved.

ISSN: 2582-6433

One of the most common ways to collect data from cybercriminals is to configure a honeypot that will act as a victim while collecting evidence that can be later be used against attacks.

- Follow established procedures by investigating supervisors or department officers.
- Ensure evidence is collected in the correct order to maintain the chain of custody.
- Avoid legal challenges by handling evidence appropriately.
- Obtain necessary warrants or court orders for device inspection.

3. Evidence Assessment

- Examine various devices to identify their relevance to the case.
- Determine the type of evidence that can help solve the crime.
- Follow established procedures for evidence collection and cataloging

4. Crime Methodology and Evidence Identification

- Decide what actions would be required to commit the crime or leave evidence.
- Tailor the investigation based on the nature of the crime.
- Acquire the necessary warrants or court orders for device inspection.

5. Evidence Examination - Once the Investigator have collected enough data and facts about the cyberattack, it's time to examine the digital systems that were affected, or those supposed to be involved in the execution of the attack. This process involves analyzing network connection raw data, hard drives, file systems, caching devices, RAM memory and other potential evidences. Once the forensic work starts, the involved investigator will follow up on all the involved trails looking for fingerprints in system files, network and service logs, emails, web-browsing history, etc.

- Analyze collected evidence using custom search profiles.
- Use search profiles developed during the assessment stage.
- Collaborate with the prosecution team to build the case in court
- Subpoena additional evidence if required.

6. Reporting Phase

ISSN: 2582-6433

- Compile complex information and analysis for the prosecution.
- Work with experienced forensic scientists to translate findings into a format comprehensible to prosecutors.
- Utilize ADF Tools reporting feature to present evidence validity in an easily understandable format.

Cyber Crime Investigation Techniques

While techniques may vary depending on the type of cybercrime being investigated, as well as who is running the investigation, Activities that a computer crime investigator performs include recovering file systems of hacked computers, acquiring data that can be used as evidence to prosecute crimes, writing reports for use in legal proceedings, and testifying in court hearings.

Cyber crime investigation techniques include:

Performing background checks -Establishing the when, where, and who of a crime sets the stage for an investigation. This technique uses public and private records and databases to find out the backgrounds of individuals potentially involved in a crime.

Gathering information- One of the most important things any cybersecurity researcher must do is grab as much information as possible about the incident.

Was it an automated attack, or a human-based targeted crime? Was there any open opportunity for this attack to happen? What is the scope and impact? Can this attack be performed by anyone, or by certain people with specific skills? Who are the potential suspects? What digital crimes were committed? Where can the evidence be found? Do we have access to such evidence sources? This technique is one of the most critical in cyber crime investigations. Here, investigators ask questions such as: What evidence can be found? What level of access to sources do we have to gather the evidence? The answers to these and other questions provide the foundation for a successful investigation.

Running digital forensics - Cyber crime investigators use their digital and technology skills to conduct forensics, which involves the use of technology and scientific methods to collect, preserve, and analyze evidence throughout an investigation. Forensic data can be used to support evidence or confirm a suspect's involvement in a crime.

Once researchers have collected enough data about the cybercrime, it's time to examine the digital systems that were affected, or those supposed to be involved in the origin of the attack. This

ISSN: 2582-6433

process involves analyzing network connection raw data, hard drives, file systems, caching devices, RAM memory and more. Once the forensic work starts, the involved researcher will follow up on all the involved trails looking for fingerprints in system files, network and service logs, emails, web-browsing history, etc.

Tracking the authors of a cyber crime- With information about a crime in hand, cyber crime investigators work with internet service providers and telecommunications and network companies to see which websites and protocols were used in the crime. This technique is also useful for monitoring future activities through digital surveillance. Investigators must seek permission to conduct these types of activities through court orders.

Cybercrime Investigation Tools

Cybercrime investigation requires the use of specialized tools and software to collect, preserve, and analyse digital evidence. These tools can be used to identify suspects, track their activities, and gather evidence to build a case against them.

Here are some of the most common cybercrime investigation tools used by investigators:

Digital Forensics Software: It is used to recover deleted files, analyze metadata, and examine network traffic logs. Popular digital forensics software includes tools like EnCase, FTK, and Autopsy. Digital forensics helps investigators piece together evidence and determine the timeline of events in a crime. It is mainly made up of network forensics and memory/disk analysis. By analyzing information found on disks and through networks, investigators can learn about other potential conspirators in the crime. This could help them track down these individuals and stop them before another crime is committed.

Network Analysis Tools -They are used to monitor network traffic, identify suspicious activity, and track the flow of data. Network analysis tools include tools like Wireshark, tcpdump, and Netscout.

Malware Analysis Tools- They are used to analyze and reverse engineer malware to understand its behavior and identify its source. Malware analysis tools include IDA Pro, OllyDbg, and Binary Ninja.

Password Recovery Tools- They are used to recover passwords from encrypted files, databases,

ISSN: 2582-6433

or other sources of digital evidence. Password recovery tools include tools like Cain and Abel, John the Ripper, and Hashcat.

Social Media Analysis Tools - They are used to track suspects' activities and gather evidence from social media platforms. Social media analysis tools include tools like Hootsuite, Followerwonk, and Mention.

Above are the few examples of the many cybercrime investigation tools available to investigators. It's important for investigators to have a deep understanding of these tools, as well as knowledge of the latest trends and techniques in cybercrime investigation. By using these tools effectively, investigators can help to identify and prosecute cyber criminals and protect individuals and organizations from the growing threat of cybercrime.

Cybercrime investigators must be experts in computer science, understanding not only software, file systems and operating systems, but also how networks and hardware work. They must be knowledgeable enough to determine how the interactions between these components occur, to get a full picture of what happened, why it happened, when it happened, who performed the cybercrime itself, and how victims can protect themselves in the future against these types of cyber threats.

Crime Scene Investigation: Search and Seizure

The sequences of steps for digital crime scene investigations are:

Identifying and securing the crime scene- Obtain IP Address, Locating the IP address of the suspect, and Gaining access to the IP address, through the Internet service provider by way of either a warrant, subpoena, or court order;

On identifying the internet Service Provider (ISP) (i.e. the IP Network provider), contact the provider's management, (In some countries, this is done through the Police); to request to be able to gain access to the call detail records (CDRs), through the allotted IP address used by the suspect(s) - The Internet Service Provider (ISP) may cooperate fully, or you may need to obtain a subpoena, warrant, or court order, for this purpose.

(NOTE that ISPs have records of everything a subscriber does on the Internet!

- *Forensic duplication*
- *Conducting interviews*
- *Labeling and documenting of the evidence*
- *Packaging and transportation of the evidence*

ISSN: 2582-6433

- *Panchanama (Seizure Memo) and Seizure Proceedings T - The legal provisions empowering the IOs to conduct search and seizure are provided under Section 165 Cr PC and Section 80 of the ITAA 2008*
- *Make sure one of the technical people from the responder side along with two independent witnesses is part of the search and seizure proceedings, to identify the equipment correctly and to guide the IO and witnesses*
- *Please refer to the notes made during the pre-investigation assessment for cross verifying and correctly documenting the technical information regarding equipment, networks, and other communication equipment at the scene of crime*
- *Time Zone/System Time play a very critical role in the entire investigation. Please make sure this information is noted carefully in the panchanama, from the systems that are in Switched on condition*
- *Please don't switch ON any device*
- *Make sure a serial number is allotted for each device, and the same should be duly noted not only in the panchanama but also in the Chain of Custody and Digital Evidence Collection forms*
- *Make sure each device is photographed before starting the investigation process at their original place along with respective reference like cubicle number or name room surroundings, etc*
- *Make sure to photograph the Hard Disk Drive or any other internal part along with the system, once removed from the system*
- *If possible, please paste the serial number along with PF number/Crime number/section of law*
- *Capture the information about the system and data you are searching and seizing in the panchanama*
- *Brief the witnesses regarding the tools used to perform search and seizure of the digital evidence*
- *Make sure that the panchas have some knowledge and ability to identify various digital devices*
- *Document the Chain of Custody and Digital Evidence Collection forms explained below, apart from your regular panchanama as a Best practice, for digital evidences*
- *Please make sure all the details mentioned in the forms are completely filled*

Chain of custody

Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence. These would be people who have seized the equipment, people who are in charge of transferring the evidence from the crime scene to the forensic labs, people in charge of analyzing the evidence, and so on.Once the evidence is collected and every time the evidence is

ISSN: 2582-6433

transferred, it should be documented and no one else other than the person entrusted with the exhibit shall have access to the evidence.

Procedure related to Investigation in INDIA

Generally the provisions of the Criminal Procedure Code (hereinafter referred to as the CrPC) prescribe the procedure for investigation and trial of the offences. Section 4 of the CrPC lays down the following and reads as follows:-

4. Trial of offences under the Indian Penal Code and other laws.

1. All offences under the Indian Penal Code (45 of 1860) shall be investigated, inquired into, tried, and otherwise dealt with according to the provisions hereinafter contained.
2. All offences under any other law shall be investigated, inquired into, tried, and otherwise dealt with according to the same provisions, but subject to any enactment for the time being in force regulating the manner or place of investigating, inquiring into, trying or otherwise dealing with such offences.

Section 4(1) of the CrPC provides that offences under the IPC are to be investigated, inquired into and tried in accordance with the provisions of the CrPC. According to the provisions of Section 4(2) of the CrPC, offences under any other law, which includes the offences under the Information Technology Act, 2000 (hereinafter referred to as the IT Act), shall also be investigated, inquired into and tried or otherwise dealt with according to the CrPC, subject to any special provision applicable under the special law. Thus the provisions of the CrPC govern the investigation, trial etc of offences under the IT Act with a few exceptions provided under the Act. The exceptions have been contained under Section 78 and Section 80 of the IT Act. These Sections read with Section 81 of the IT Act prevail over the provisions of the CrPC.

Section 78 of the IT Act reads as follows :-

78. Power to investigate offences.–Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of [Inspector] shall investigate any offence under this Act.

According to the provisions of this Section, the offences under the IT Act can be investigated only by a police officer not below the rank of an Inspector.

Section 80

80. Power of police officer and other officers to enter, search, etc.–

ISSN: 2582-6433

1.Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of a Inspector, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

Explanation.–For the purposes of this sub-section, the expression ―public place‖ includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

2.Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

3.The provisions of the Code of Criminal Procedure, 1973 (2 of 1974) shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

According to this section, any police officer, not below the rank of an inspector, may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act. Under the IPC, only preparation to commit dacoity and preparation to wage war against the Government are offences. In the cases of offences under the IT Act, the search and arrest is applicable even in cases where the offence under the Act is about to be committed. However, it is important to note here that the Section is applicable only to "public places" and not to private places. Apart from these two exceptions given under Section 78 and Section 80, investigation, trial etc. for an offence punishable under the IT Act is to be conducted according to the CrPC. These two exceptions are however, supplementary to the provisions of the CrPC, and both the Acts are applicable unless the provisions of the CrPC are inconsistent with the provisions of the IT Act, in which case the procedure shall be governed by Section 78 and Section 80.

The police station under whose jurisdiction, the offence has been committed has the jurisdiction to investigate into the offence. Therefore, normally, the information (FIR) regarding a cognizable

ISSN: 2582-6433

offence is lodged in the police station within whose jurisdiction, the offence was committed. However, according to the Hon'ble Supreme Court in State of Andhra Pradesh v. Punati Ramulu if for some reason, the information of the cognizable offence is given to another police station, then the police should record it (known as "Zero FIR") and forward it to the police station within whose jurisdiction, the offence or part of it appears to have been committed. This is more important in cases of offences related to cyber crimes especially Bank Frauds and identity theft, where time is of great importance and essence.

The Indian legal system has structured many procedures, rules, regulations which are enacted it in a statute. The technological advancements and developments have inverted in the digital India for its progression. Cyber-crimes usually transgress geographical hurdles. Cybercrime is a fast-growing meadow of crimes. The Cyber criminals are exploiting the speed barriers and anonymity of the internet for the commission of different types of criminal activities. No border, virtual or physical, can cause serious harm and rise real threat to worldwide victims other than Cybercrimes. In order to deal with the issue of Cyber-crimes, the Criminal Investigation Department (CID's) of various cities established, Cyber Crime Cells (CCC) in various parts of the country. The IT Act, 2000 made it clear.[4]

The investigators must be experts in computing, understanding not only software, file systems and operating systems, but also how networks and hardware work. They need to be knowledgeable enough to work out how the interactions between these components occur, to urge a full picture of what happened, why it happened, when it happened, who performed the cybercrime itself, and the way victims can protect themselves within the future against these sorts of cyber threats.

Section 78 of the Act power to investigate offences by police officer which states that ―Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of [Inspector] shall investigate any offence under this Act. Section 80 of the same act sates that the police officer which was mentioned under section 78 or any other officers in which the state and central government has authorized power to search at any public place, seize, inquire and even can also arrest the suspected person who commits the offence.

NATIONAL CYBER SECURITY COORDINATION CENTRE (NCSC) is an agency under cybercrime in which it coordinates with different agencies at national level for to secure the cyber

[4] See International journal of legal developments and allied issues Volume 7 Issue 2 – ISSN 2454-1273 March 2021 https://thelawbrigade.com/

ISSN: 2582-6433

related matters.

To fight against the cybercrime the CBI has established the special units:

- Cybercrime Research and Development Unit
- Cybercrime Investigation Cell
- Cyber Forensic Laboratory
- Network Monitoring Centre

Which Police Station shall have jurisdiction to investigate a case related to cyber crime?

Jurisdiction of Police station in registering FIR related to cybercrime:

1. The concerned police station will have the jurisdiction to register an FIR under section 156 (1) read with section 177 of the Code of Procedure and conduct the investigation of the victim's account from which the money is withdrawn illegally.

2. In cases of economic offenses where it is not certain in which area the crime has been committed or if the crime has been committed under more than one locality or is of a consistent tendency (continuous offenses) Section 178 read with section 156 (1) Code of Criminal Procedure, can be registered in any related police station and investigation can be conducted.

Example - Money is withdrawn from the account of a person who is located in Ranchi by a criminal sitting in Jamtara and it is transferred to more than one account. There will be jurisdiction in all the places from where money has been transferred.

3. In cases where the offense has been committed in the jurisdiction of one police station and its effect will be in the jurisdiction of any other police station then the offence can be registered in either of the two police stations under the provisions of Section 156 (1) of Code of Criminal Procedure.

Example- In offences related to social media, if the objectionable post has been made the jurisdiction of a police station, and it is uploaded on the social media through the Internet, and it is seen in other jurisdictions.

4. In case the offence is a result of a criminal conspiracy. Here, where the crime has been committed or where criminal conspiracy has been done, both places can be investigated by registering the case under the provisions of Section 180 read with Section 156(1) Code of Criminal Procedure.

Example - In cases where the illegal withdrawal of funds through cyber crime has been done on more than one victim, and that amount has been transferred to a bank account of some other jurisdiction and the beneficiary is found accomplice under S. 120 IPC, then in this case the offence can be registered either in the jurisdiction of the bank account of the victim or the

ISSN: 2582-6433

beneficiary and the investigation and the trial can be conducted

5. In cases where economic communication or social media communication is done through telecommunication like internet, mobile etc., the place where the communication was made, or where it was received, the jurisdiction of the concerned police station, will be Section 182 read with Section 156(1) under the Code of Criminal Procedure.

Example: If the OTP of an account holder is obtained by criminals sitting in the jurisdiction of any other police station through mobile or telecom and internet, then both the police stations will have jurisdiction.

The Level of Expertise Necessary to Testify as a Cyber Crime Investigator

Cyber crime investigators are primarily percipient witnesses[5]. This means that although the analysis of a computer might have involved complex technical issues, the basic purpose for which the investigator's testimony is offered is to describe what the investigator saw and did, rather than to offer complex technical information about computers or forensic software. Although cyber crime investigators frequently use high-tech tools like forensic software to find evidence, ultimately their testimony is not different in kind from that of a police officer who used a complex pair of binoculars to find evidence. A police officer using such binoculars to witness a drug transaction would not be expected to be an expert in binoculars and optics in order to testify at trial concerning what he saw. Similarly, a cyber crime investigator who used a complex computer program to discover child pornography on a suspect's computer would not have to be an expert computer programmer to describe what the investigator discovered through the use of the program. Although cyber crime investigators must be generally familiar with computers and the forensic software that they used to perform their investigation, there is no need in order for a cyber crime investigator to testify to be a computer expert with qualifications such as an advanced degree in computer science.

Expert Witness's Expertise

[5] An expert witness is a witness who possesses specialized knowledge that an ordinary juror would not likely possess. A percipient witness is a witness who testifies about what he "perceived" (e.g., what he saw, did, or heard).

ISSN: 2582-6433

Sometimes cyber crime investigators are qualified by courts to testify as expert under sec 45 of Indian evidence act and sec 39(1) of bhartiya sakshya adhiniyam because of specialized knowledge that they possess.

Cyber crime prevention

For many of us, using a computer for the first time was an amazing experience. We couldn't believe what we saw or what was happening inside "that machine. "Today, wristwatches, sun glasses, an ordinary looking pen, cell phones, and, of course, personal digital assistants (PDAs) can do more than my Apple II computer system. We have seen remarkable technologies come to fruition and achieve a life of their own. Who would have thought that a tiny device called an iPod would change society? Or that we would witness what seems like our total assimilation with the BORG, given the digital devices now attached to our ears, mouths, and waistbands… Forget the nerd pocket holders—we go straight for the insertion point and attach devices wherever we can! Again, who would have imagined such changes? Certainly not me.

The point is, with all the remarkable and amazing technological introductions over the past 30 years, both with personal computer systems and today with handheld devices, we are still vulnerable to the frailties of human behavior. We may have the best technology devices ever introduced, and yet succumb to our "creature of habits" lifestyle, allowing portions of our lives to be exposed, manipulated, and/or destroyed. By that, I am suggesting all the governance or influences of computer-digital technology in our lives is often discarded by behavior we could have, and should have, controlled. We know better than to completely trust everything that comes over the transom with such devices, but because such information is disseminated by a cell-phone text message, e-mail, fax, phone message, or some other communication form created by the digital gods of the BORG… we don't want to be left out.

The information in this chapter is not "new" certainly, but it is nevertheless common-sense data we must review. Perhaps for some of us we only need to re-examine it once; for others, monthly; for yet others, weekly; and for some of you… every day! Just the same, we will explore methods, techniques, and call-to-action steps to help prevent cyber crime—at work, home, and play. Please understand that everything written and published about "How to Prevent Cyber Crime" is a guide for both sides. Sadly, for some this will serve as a challenge and a way for someone to show up the experts. Hopefully for you, though, you'll listen to protect your identity, your family, your job, and your country. Be confident that you can roam freely and move in and out of cyber space.

ISSN: 2582-6433

Review your habits and be the safe individual you know you should be.

Ways to Prevent Cyber Crime Targeted at You

Anyone connected to the Internet is at risk of being targeted and could become a victim of cyber crime themselves. Some have suggested you are more likely to be threatened, bullied, assailed, or "mugged" online than on your local street corner. With this in mind, you must make active steps to prevent yourself from getting injured, either emotionally, financially, or physically. You must protect you, your identity, your reputation, and your well being. You are the one who will allow others to know information about you directly by responding, or indirectly by not following common-sense guidelines. This section identifies ways you can protect yourself and prevent cyber crime from occurring on a personal level. Often, you will hear cyber cops ask the following questions:

- *Why would someone want to target you?*
- *Who might the culprit be?*
- *What might you have that they want?*
- *How did they gain access to your computer system, PDA, or cell phone?*
- *When could these attacks have occurred?*

Would you have any answers the preceding questions? Have you actually devoted thought to any of it? I'm not suggesting we all become paranoid techno-freaks. When I am asked why I use online banking, I respond "Why wouldn't I?" I have several bank and money accounts. Nevertheless, I have a finite amount that I place in my online account. The monies I leave in that account don't stay there long.And my other accounts are where? That's right, at totally different institutions. Sounds inconvenient to some, but it is safer in today's identity-theft.

Back to the questions, though. Just why would someone target you? Did you offend anyone? Do you have poor online habits that might allow someone to quickly gain access to your bank accounts? Are you in the middle of a divorce or have you given your spouse reason to suspect something is amiss? Are your adult children looking for their supposed inheritance? Have you posted to your Web site inflammatory or inciting comments?

Who might the culprit be? We find that over 90 percent of cyber attacks come from someone you know. Often times, the attack is a result of some trivial or heated disagreement at work with a colleague, or at home with a spouse, child, or relative. Most computers that are randomly compromised are done so to utilize some zombie or peer-to-peer manipulation of your computer's

ISSN: 2582-6433

processing power, not your personal data.

What might you have that they want? Again, are they looking for money? If yes, what information is on your computer that wouldn't be found on your statements in the filing cabinet? Are you taking sensitive data from your workplace home? Is this sensitive data from work on your home computer, or on a laptop, or on a portable media device like a USB thumb-drive, MP3 player, or iPod? Again, why would a complete stranger want to hack your computer system? Sadly, many times there is more information about you in your trash than on your computer.

How did they gain access to your computer system, PDA, or cell phone? Once again, we leave the cyber space for a moment and return to ordinary crime. Was the scene of the crime electronic only, or did you assist by forgetting to address some physical security issues?

- Did you lock your office?
- Did you lock your house?
- Did you leave your laptop in the backseat of your car with the windows down on a warm sunny day?
- Did the USB device fall out of your pocket on the plane or train?
- Did you leave your iPod in the wash room?
- Why was your cell phone left at your favorite restaurant, again?

The following are points to consider in how to better protect yourself from being a target of cyber crime:

- Have your own personal computer log in at home and work.
- Keep your log in information private and secure from others.
- Memorize your password(s).

i. Don't share it or them.
ii. Don't use common dictionary words.
iii. Don't use family names, colors, hobby data, or religious data.

- Always LOCK your system when you walk away from your desk.
- Avoid, or better yet, never post personal photos of you on a nonsecured Web site.
- Never post personal data.
- Never provide your password(s), PIN information, or banking details from a soliciting e-mail, or Web site.
- Install and run a personal firewall.
- Install and run antivirus software.

ISSN: 2582-6433

- Install and run antispyware software.
- Update your computer frequently with security patches, as well as operating system and application service packs.
- Use encryption for sensitive e-mail and Web transactions.
- If you are a Windows user, use the New Technology File System (NTFS), not FAT32.
- If you have a portable device for storing data, use the Encrypting File System (EFS), part of NTFS. This includes laptops, MP3 devices, and portable drives.
- Make sure your PDA and cell phone have an activation password.
- Report any cyber-harassments and/or cyber threats.
- Purchase a good shredder—a good cross-cut one!
- Don't use your computer for criminal purposes!
- Don't believe you are anonymous on the Web!

Ways to Prevent Cyber Crime Targeted at the Family

The Internet and the World Wide Web contain a wealth of valuable data and information for families. However, with all that good come unwelcome elements, too. Many activities on the Internet are, and can be, very disruptive to the family. Every family unit is unique, and as such, each family must define proper rules of Internet engagement and usage. Everything stated in the previous sections could apply, and perhaps should apply. However, you should define what is right and proper for your family. One main issue to consider is that of access. Internet use and what is posted, shared, and/or accessed on the Internet is one of personal decision making. Too many try to infer moral obligations or arguments of good versus evil. There is one overriding issue, however, and that is the issue of access. My children and your children cannot purchase a pornographic magazine from a store, they cannot attend an NC-17 movie without being of age, and they cannot purchase products restricted for 18- or 21-year-old individuals—however, the Internet does not enforce these same rules and laws. So, you as a family unit need to identify what will be your best roadmap and guidelines for Internet usage in your home.

Popular suggestions for Internet access in the family, and the prevention of inappropriate or dangerous behavior include the following:

- Make sure there is an open screen policy—meaning the computer display faces the doorway and is exposed for all to see.
- Establish time limits on computer use and Internet access.

ISSN: 2582-6433

- Try to separate the game systems from the educational system—many families have a computer for games, and another for homework. Having an Xbox, PlayStation, or similar device helps.
- Talk honestly and frankly about the good, bad, and ugly found on the Internet with your children.
- Limit your exposure, and theirs, by not posting too much personal data on the Web—especially at sites like Myspace, YouTube, and similar spots.
- Chat rooms are full of dirty old men. If you are okay with your 12- year-old communicating with degenerates posing as overly anxious pubescent friends—go for it! Or just say no to chat rooms.
- Let your children know you will read their chats and e-mails, and will contact their friends from time to time. Then, make sure you do so and review those contacts and communications that are inappropriate for your family.
- Let your spouse know you have a key logger and to beware.

Even if your computer is safe and secure, you may have forgotten about your cell phones, iPods, and Xboxes! You must the same conversations with your family regarding text messaging on your cell phones and accessing the Web from your cell phone. This preventive medicine may prove more difficult than with the computer since there are few, if any, tools to assist monitoring behavior or limiting access to sites via a cell phone or PDA.

Likewise, a whole new crop of degenerates are being found at Xbox Live, PlayStation Live, and similar online spaces, where they want to "team-up" with your kids. Don't ignore the dangers. They are the same that exist in chat rooms, e-mail conversations, and instant messaging. Your children can communicate via wireless headsets to any person wishing to join in. Do you know who they are playing with? Have you seen the games they are playing? And when their "friend" requests a face to face to share important details on how
to better play the game, do you know where they are going?

Recognize that the same rules and guidelines are true for cell-phone users. Access to chat rooms, the ability to send and participate in e-mail conversations, and instant messaging exist with cell phone use, too. Do not be afraid to take your children's cell phone for review. Identify unknown or unfamiliar telephone numbers and discuss the dangers of predators in this community. Monitor cell phone use and make sure all is in line and appropriate regarding the guidelines you have established with your family.

Ways to Prevent Cyber Crime Targeted at Personal Property

It is clear problems exist and will persist in the online Internet world. Software, hardware, and Internet vendors continue to clash and blame one another when problems emerge. By now, you

ISSN: 2582-6433

should understand this silly cycle and realize you hold a level of responsibility, too. It is up to you, the end user, to purchase products to help fill the holes the software and hardware vendors have failed to provide. Some of the following items have been mentioned before, but this is what you need to do to protect your digital devices and help prevent cyber crime targeted at your personal property.

Anti-Virus software

Most computer systems come with two or three 90-day trial copies of antivirus software. This isn't an option; it is a must. Make sure you are using some tool to protect your computer system from viruses. Viruses typically cause damage, often referred to as the "payload. "The role of most computer viruses is to spread like a germ from one host to another. These self-replicating viruses are typically instructed to infect as many hosts as they can, and to possibly extract, move, or delete your files or completely destroy the operating system, rendering your computer helpless. Damage to your system will occur if you do not use an anti-virus software tool. Some anti-virus products also look for spyware and/or Trojans. In the end, you will need several tools, and definitely anti-virus software.

Anti-Spyware Software

Spyware is relatively new and comes in a variety of deployed methods. The primary goal of a piece of spyware code is to get into your computer without your knowledge and/or permission. Once in, spyware instructs the computer to relay information to some other system about your internet use or redirect you to a website. Some spyware is relatively harmless, perhaps a set of marketing instructions. Other spyware is more annoying by constantly redirecting your browser and/or displaying pop-up windows. It is very unfortunate that there are people and instructions of code placing instructions on your computer without your approval. As a result of these actions, we must all have anti-spyware software on our computers.

Occasionally, anti-spyware software provides false positives and other misleading data to scare you into purchasing the tool. Some anti-spyware software is actually fake and completely ineffective. For a good independent review and a list of trusted anti-spyware tools, go to www.spywarewarrior.com/rogue_anti-spyware.htm#trustworthy.

Both malware viruses and spyware tend to be installed by you, the user. Perhaps you have been guilty of the following:

ISSN: 2582-6433

- A friend sends you an e-mail with a video or sound clip, a game of some sort, or a cool desktop image, and you listen or install the attached file. The intention of your friend was pure, merely sharing some joyful or funny moment. Unfortunately, for both of you, the virus or spyware was installed simultaneously.
- A "Security Window" pops up, instructing you to download a needed file—and you blindly follow the instructions. Ironically, one of the biggest culprits of these is fake spyware information windows, which often claim to be part of Microsoft Internet Explorer, and so you install it.
- Some browsers have "add-on" functions that are really just spyware or virus executables. However, they appear to be needed, so once again you install them.
- Occasionally, you get the virus or spyware from a legitimate software vendor that has been infected and is inadvertently shipping the virus or spyware with their software.

Personal Firewall Software

This tool is intended to protect in-coming and out-going communications. The role of a personal firewall is to prevent intrusion from uninvited Internet traffic. It also serves as a facilitator in that it provides information about applications or users attempting to contact or communicate with the computer. It also acts as a personal firewall, providing information about the other computer system or server. Like the two aforementioned tools, every homeowner should have a personal firewall to protect their data and their family, and to prevent their computer from being manipulated.

The guidelines to prevent property damage to your computer are quite exhaustive. The following reviews the steps you should take to protect your computers:

- *Choose one anti-virus tool. Running two such tools simultaneously is not a good idea.*
- *Choose one personal firewall tool. Running two such tools simultaneously is not advisable.*
- *Plan to have two or more anti-spyware tools. Because there are so many unknowns in this category, it is required to have at least two, or ideally three or more, installed and running on your personal computer*
- *Anti-virus, anti-spyware, and personal firewall software are only useful if you're using the most recent version. Get regular updates!*
- *Consider getting help from your ISP or online provider to supply services that include anti-virus and anti-spam software, and e-mail filtering.*
- *Read the end-user license agreement (affectionately known as EULA) for all of these tools, but especially for the anti-spyware software. Some of the anti-spyware licenses provide a clause for them to spy on you! Or to provide an endless stream of pop-up advertisements.*

ISSN: 2582-6433

- *Find the programs that best match your privacy and security needs.*
- *Make sure you test your tools. It is the only way to ensure your computer system is being protected.*
- *Use a wiping tool like WhiteCanyon's WipeDrive to completely erase and sanitize your used or donated hard drives, thumb drives, or cell phones.*
- *Delete all data from your cell phones and PDAs before donating them or throwing them away.*
- *Destroy CDs, DVDs, floppies, or similar storage devices before discarding. Most shredders will shred these.*

The Internet is not a kind and gentle world. Too many discontent and probing users are waiting out there. Every time a fix is devised to prevent unwelcome intrusions, a new door is found. Managing these tools requires diligence on your part. Yours is not an optional role in preventing cyber crime. Updating these tools and properly maintaining them is a burdensome requirement for us all.

Ways to Prevent Cyber Crime Targeted at a Business

The next three sections are closely related. Your role in each of these will differ. Some of you will have more direct responsibilities and obligations, while others will merely be the recipients of what has been determined.

Each business, company, and/or corporation has policies or procedures, or at least they should, for installing and maintaining software to protect their intellectual data and property, the information regarding their employees, and the communications of their employees. We have discussed several of these tools, anti-virus, anti-spyware, e-mail spam filters, and firewalls. In addition, many businesses utilize some form of network intrusion detection software (NIDS). Unlike individual or family users, however, corporate users are targets

of malware or malicious software. Malware is intent-driven and includes viruses, Trojans, worms, spyware, or some other type of destructive software. These unwanted and undesirable software programs are designed to penetrate and damage computer systems—in short, to bring a network or Web site server down.

One of the most infamous instances of malware was the Slammer virus that was released in January of 2003.The Slammer virus spread faster than any other known attack, including the Code Red or Blaster viruses and the Klez or Nimda worms. This Microsoft SQL virus started creating millions of clones, and doubled almost every 8.5 seconds. By the time the Internet world

ISSN: 2582-6433

started to realize the problem, over 300,000 cable modem users in Portugal were down. South Korea's cell phone and Internet service providers were in total chaos, and many were shut down for over 24 hours. Many airlines, including Continental, had to cancel flights. The price tag estimated to recover worldwide was over $1.2 billion. It was not a "good" day for those network administrators who had failed to update their MS-SQL software. Had they followed their policies and procedures, they could have avoided and averted the entire episode.

Many believe more losses exist than reported. Too many businesses choose not to report cyber crime for fear of loss of income from customers, bad press, or loss of employment. It is time for stiffer penalties to be imposed on those corporate leaders that elect to hide cyber crimes.

Make a difference. Be observant and helpful, and establish guidelines like the following:

- Understand what your business's appropriate and inappropriate use policies are, and then follow them.
- Continue to use the prevention methods discussed for individuals, families, and property.
- Follow and enforce strict password management policies.
- Clearly communicate security solutions to all employees.
- Establish proper audit policies for user accounts, computer accounts, and management tools for server communication.
- Do not possess unauthorized information or corporate intellectual property.
- Do not distribute or use pirated software.
- Do not provide access to your computer to any unauthorized individual.
- Stay informed about changes to your phone, Internet, intranet, and computer access.
- Report any cyber threats, intimidation, stalking, or harassment.
- Don't assume your Web use or e-mail communication is private and confidential at work. It isn't and it can be used against you. So, DO NOT commit crimes at work.

Ways to Prevent Cyber Crime Targeted at an Organization

Like businesses, nonprofit and academic organizations need to employ policies and procedures to protect the rights of the organization, the employees, volunteers, students, and members. The best way to prevent cyber crime is to educate members on the unique rules and guidelines of your organization. Organizations need to identify potential vulnerabilities and possible exploits.

Understand who is working for you and why. Do background checks on your volunteers, and do not provide access to any system without knowing some history about the members of your organization. Follow the guidelines as outlined in the Business section.

ISSN: 2582-6433

Conclusion

Better legislations with increasing Ambit of Cyber internet space is very necessary such legislations should be governing nationally as well as internationally to avoid the issues and contradiction of laws between the Nations having cyber crime problems.

As the growing number of Cyber crime in the country, it is very necessary that the present dispute resolution structure given under information and technology act of 2000 maybe strengthened. The authorities of IT act are responsible for a huge range of concerns which includes data privacy cyber offences cyber security concerns and responsibility of keeping the data of every internet user safe. Such authorities must be developed so that they can bring a well developed and better regulatory structure for the increasing number of Cyber attacks in the nation.

Cybercrime is a significant threat that can bring huge loss to the individual and the organization. It is essential to follow basic online rules to ensure the safety of self and the organization. The Internet is often described as a wonderful tool, an engaging place and a liberating experience…… but for whom? There is the potential for many of us to become victims to the growing pool of criminals who skilfully navigate the Net. Cyberspace often known as Web is an environment that is intangible and dynamic.

Criminal behavior on the Internet, or cyber crime, presents as one of the Major challenges of the future to India and International law enforcement. As ICT become even more pervasive, aspects of electronic crime will feature in all forms of criminal behavior, even those matters currently regarded as more traditional offences. It already feature in many international crime involving drug trafficking, people smuggling, terrorism and money laundering. Digital evidence will become more commonplace, even in traditional crimes, and we must be prepared to deal with this new challenge.

Law enforcement agencies around the world are working together to develop new partnerships, new forensic methodologies and new responses to cyber crime in order to ensure safety and security on the Internet. New skills, technologies and investigative techniques, applied in a global context, will be required to detect, prevent and respond to cybercrime.

REFERENCES:

- https://www.kaspersky.com/resource-center/threats/what-is-cybercrime
- https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-anoverview.html
- https://hbr.org/2023/04/cyber-thieves-are-getting-more-creative
- https://www.drishtiias.com/daily-updates/daily-news-analysis/cyber-crime-4

ISSN: 2582-6433

- https://journals.sagepub.com/doi/10.1177/0032258X221107584
- https://www.infosecurity-magazine.com/cybercrime/
- https://www.un.org/en/chronicle/article/fighting-industrialization-cyber-crime
- https://rjhssonline.com/HTMLPaper.aspx?Journal
- Aggarwal, Gifty (2015), General Awareness on Cyber Crime. International Journal of Advanced Research in Computer Science and Software Engineering. Vol 5, Issue 8
- https://cybertalents.com/blog/cyber-crime-investigation
- https://economictimes.indiatimes.com/wealth/personal-finance-news/cyber-criminals-stole-rs-1-2-trillion-from-indians-in-2019 survey/articleshow/75093578.cms
- https://www.tandfonline.com/doi/abs/10.1080/13691180802007788#:~:text=Reactions%20which%20heighten%20the%20culture,the%20subsequent%20interpretation%20of%20justice.
- https://www.researchgate.net/publication/228264135_Cybercrime_and_the_Culture_of_Fear_Social_Science_Fictions_and_the_Production_of_Knowledge_about_Cybercrime_Revised_Feb_2011
- https://www.vedantu.com/english/cyber-crime-essay
- https://www.britannica.com/topic/cybercrime
- https://vc.bridgew.edu/ijcic/
- N. Roshan, 'What is Cyber Crime- Asian School of Cyber Laws', available at: www.aclonline.com
- Ashabhari Thakur, 'Determination of jurisdiction in cyber crimes- issues & classification', 2019, available at: www.legalpedia.in
- www.mondaq.com/india/securty/623820/cyber-laws-in-india
- Ikigai law, 'DRM framework of cyber crimes under IT act, 2000,' available at: www.ikigailaw.com
- Dr. S. Poonia, 'Cyber Crime: Challenges & its Classification', Vol. 6, issue 10, available at: www.ijettcs.org
- Ajzen, I., "The theory of planned behavior," Organizational Behavior and Human Decision Processes 50X, 1991, 179--211Google Scholar
- Alshalan, A. (2009). Cyber-Crime Fear and Victimization: An Analysis of a National Survey.Google Scholar
- Saarbrücken: VDM Verlag Dr. Müller Chin, W. W. (1998) "The partial least squares approach for structural equation modelling," In Modern Methods for Business Research (Ed, Marcoulides, G. A.) Lawrence Erlbaum Associates, Hillsdale, 295--336Google Scholar.

ISSN: 2582-6433

- Alshalan A. (2006). Cyber-Crime Fear and Victimization: An Analysis of a National Survey. Mississippi: Mississippi State University. [Google Scholar]
- Clememte F., & Kleiman M. B. (1976). Fear of crime among the aged. The Gerontologist, 16(3), 207–210. [PubMed] [Google Scholar]
- Collins R. E. (2016). Addressing the inconsistencies in fear of crime research: A meta-analytic review. Journal of Criminal Justice, 47, 21–31. [Google Scholar]
- Empirica (2007). Benchmarking in a Policy Perspective: Security and Confidence. Empirica. [Google Scholar]
- European Commission (2013) Eurobarometer 79.4: Social Climate, Development Aid, Cyber Security, Public Transport, Anti-Microbial Resistance and Space Technology. ICPSR36038-v1. Cologne, Germany: GESIS/Ann Arbor, MI: Inter-university Consortium for Political and Social Research [distributors], 2015-07-08 10.3886/ICPSR36038.v1 [CrossRef] [Google Scholar]
- European Commission (2016) A digital single market in Europe: Bringing down barriers to unlock online opportunities. The European Union Explained. Luxembourg: Publications Office. [Google Scholar]
- Ferraro K. F. (1995). Fear of crime: Interpreting victimization risk. Albany: State University of New York Press, Albany. [Google Scholar]
- Killeas M. (1990). Vulnerability: Towards a better understanding of a key variable in the generis of fear of crime. Violence and victims, 5, 97–108. [PubMed] [Google Scholar]
- LaGrange R. L., & Ferraro K. F. (1989). Assessing age and gender differences in perceived risk and fear of crime. Criminology, 7(4), 697–720. [Google Scholar]