International Journal of advanced studies in Computer Science and Engineering
IJASCSE, Volume 3, Issue 11, November 2014

Managing Digital Evidences for Cyber Crime Investigation

Dr. Ajeet Singh Poonia
Associate Professor, Department of Computer Science and Engineering
Govt. College of Engineering and Technology, Bikaner, India

Abstract: **At the one end cyber system provides incomparable opportunities to communicate and learn and at the other end some individuals or community exploit its power for criminal purposes. Criminals exploit the Internet and other network communications which are international in scope. Cyber attacks may originate from anywhere in the world and transit a number of jurisdictions on the way to their destination. They launch cyber attacks from foreign countries; conceal evidence of their crimes in foreign locations. They take advantage of the weaknesses in international law enforcement co-operation. Numerous reasons are there for the lack of successful prosecutions. It is very difficult in identifying the offender and connecting that person to a cyber attack, especially where the attack is based offshore. This raises the issue of digital evidence which poses significant problems for the prosecution of cyber crime. Digital evidence is different from evidence created, stored, transferred and reproduced from a non-digital format. It is temporary in nature and susceptible to manipulation. These characteristics of digital evidence raise issues as to its reliability. Even more is at stake when the cyber attacker is a trusted insider who has intimate knowledge of the computer security system of the organization.**

Keywords: Digital Evidence, Cyber Attacks, Cyber Security.

I. INTRODUCTION

The beginning of digital technology and the union of computing and communications have begun to change the way we live. These trends have also created unprecedented opportunities for crime. Criminal activities that were not expected two decades ago have become facts of life today. Digital technologies now provide ordinary citizens, with the capacity to cause massive harm. The continued uptake of digital technology will create new opportunities for criminal exploitation. It is essential for public prosecutors, IT managers, security and law enforcement agencies to equip themselves with the knowledge that will permit an effective response as, cyber crime is routinely trans-border/ transnational in nature, which means there is usually not a single, localized crime scene that becomes the focus of an investigation. Also the cyber crime is routinely committed on a scale vastly exceeding the scale on which it is possible to commit crimes, also the cyber attackers are rarely held accountable for their criminal actions.

One explanation for the lack of successful prosecutions of cyber intruders is the dependence on digital evidence. Digital evidence is different from evidence created, stored, transferred and reproduced from a non-digital format. It is temporary in nature and susceptible to manipulation. These characteristics of digital evidence raise issues as to its reliability. Network-based evidence – i.e. digital evidence on networks – poses additional problems because it is volatile, has a short life span, and is frequently located in foreign country [1].

Absolute security is unattainable. However, it is possible to obtain effective results by involving good management, enforced procedures, and the adequate technical tools, with an appropriate policy framework [2].

II. CYBER CRIME

Cyber crime is any illegal activity arising from one or more Internet components done by the cyber criminals. Cyber Criminal is a person who commits an illegal act with a guilty intention or commits a crime in context to cyber crime. Cyber criminal can be motivated criminals, organised hackers, organised hackers, discontented employees, cyber terrorists.

Cyber crime can include everything from non-delivery of goods or services and computer intrusions (hacking) to intellectual property rights abuses, economic espionage (theft of trade secrets), online extortion, international money laundering, identity theft, and a growing list of other Internet-facilitated offenses. Further, it is not easy to identify immediately about the crime method used, and to answer questions like where and when it was done. The anonymity of the Internet makes it an ideal channel and instrument for many organized crime activities [3].

Cyber crime has high potential and thus creates high impact when it is done. It is easy to commit without any physical existence required as it is global in nature due to this it has become a challenge and risk to the crime fighter and vice versa. The borderless nature of ICTs may not allow for rigid regulations and instead challenges the principle of criminal laws. As such, international laws and regulations combined with reliance on technologies are crucial to counter the crime race.

III. CYBER CRIME ISSUES

ICT is booming at the enormous speed which is a matter of pride but the drawbacks associated with them are also coming at the alarming stage. The development of information technology and the widening usage of the Internet have made it possible for cyber crimes to happen. It opens more opportunities for crime and draws people into committing crime, leading to an unprecedented growth in the crime rate. While the offence committed may be recognizable, cyber crime poses a number of significant issues for traditional policing across all types of crime

committed on the internet. Unfortunately, it is not possible to calculate the true social and financial impact of cyber crime. This is because most crimes go unreported .Cyber crime is hard to detect, thus giving the culprit plenty of time to flee the area in which the crime was committed. The nature of cyber crime shows that investigations are often technically complex, requiring access to specialist skills and / or the support of the private sector. Evidence gathering is difficult and time-consuming, especially when the data evidencing the crime has been routed through a number of countries. Cyber crime differs from the conventional crimes in many ways i.e they are easy to learn, they require few resources, Creates high Impact, High Potential, Silent in Nature, Global in character, Non existence of Physical Evidence, and they are often not clearly illegal.

IV. DIGITAL EVIDENCE COLLECTION

In case of Cyber Crime Investigation, Digital Evidence Collection is the important phase as compare to other one, as the errors or poor practices at this stage may leads to evidence useless. This is all because that digital evidence is delicate and can easily be lost, i.e. it can change with usage, it can be maliciously and deliberately destroyed or altered, it can be altered due to improper handling and storage.

For these reasons, evidence should be expeditiously retrieved and preserved. Also consider that when investigating offences' involving the Internet, time, date, and time zone information may prove to be very important. Server and computer clocks may not be accurate or set to the local time zone. The investigator should seek other information to confirm the accuracy of time and date stamps.

Photographing to record the evidence of the damaged scene is the initial step towards the evidence collection.

The investigators collect the evidences generally which is damaged/deleted evidences. are recorded in main memory or temporary file on hard disk. Volatile evidence are collected using program for examining processes, system state in live computer system, as they are lost after the system is shut off. Non-Volatile evidence is collected using auxiliary storage Medias such as hard disk, zip disk, floppy disk, and USB memory.

Profile of any criminal is another method through which we can know the nature of criminal suspects based on information collected from the crime scene. The profiling can reduce the cyber investigators' scope of the investigation and can provide the clues for cyber crime. The profiling data can solve a lot of crime, can reduce time and cost of the investigation.

A. *Possible Range of Evidences*

There are numerous resources through which the evidences can be collected for investigation of the cyber crime held. Below mentioned are some of the sources but not limit too.

- Hardware such as routers, firewalls, servers, clients, portables, and embedded devices.
- Software such as ERP packages for employee records and activities (e.g. in case of identity theft), system and management files. Monitoring software such as Intrusion Detection Software, packet sniffers, keyboard loggers, and content checker.
- Other sources, such as CCTV, door access records, phone logs, PABX data, telecommunication records and network records, call centre logs or monitored phone calls, and recorded messages.
- Back-ups and archives, for example, laptops and desktops.
- Files those are either contraband or illegally possessed. Configuration files showing server or user information, connection history, shared drives on a network, or Internet sites that provide offsite data storage space
- Data files showing file sharing locations with user names, passwords, search terms, file listings, and date and time information.
- Log files that show transfers and network activity. Dynamic Host Configuration Protocol (DHCP), and RADIUS logs, which may assist in connecting the suspect to the illegal activity.
- E-mail server logs, payment records, and subscriber information, which may assist in identifying the suspect and in connecting the suspect to the illegal activity.
- External network service providers.
    i. Offsite storage.
    ii. Application service providers.
    iii. Offsite backup service providers.
- Information that may be obtained from the ISP includes—
    i. Subscriber information such as the registered owner, address, and payment method.
    ii. Transactional information such as connection times, dates, and IP address used. Some of the information used in tracing an IP address or end user may be obtained from ISPs or network administrators. This information typically includes account information, e-mail address information, IP address, and domain name.

B. *Evidence Collection Tools*

Numerous tools are available in the system for collecting the evidences. Many tools have common features but they all have their own characteristics. Utility of the tolls vary from case to case. Below mentioned are some of the evidence tools which are basically used in general.

- *SafeBack*

First step at a client site is to obtain a bitstream backup of the compromised systems. A bitstream

backup is different from the regular copy operation. When performing a bitstream backup of a hard drive, you are obtaining a bit-by-bit copy of the hard drive, not just files. Every bit that is on the hard drive is transferred to your backup medium. During a copy operation, you are merely copying files from one medium to another. Hidden data exists on your hard drive means that more is present in the hard drive than just the file names you see [4].

- *GetTime*

GetTime is used to document the time and date settings of a victim computer system by reading the system date/time from CMOS. Compare the date/time from CMOS to the actual current time [4].

- *FileList, FileCnvt*

Now that you have restored your bitstream backup to drive C of your analysis computer , use FileList to catalogue the contents of the disk. FileCnvt and Excel are used to properly read the output of the FileList program. Using FileList, it is simple to review the chronology of usage on a computer hard drive, several computer hard drives, or a collection of diskettes [4].

- *GetFree*

Now we want to obtain the content of all unallocated space (deleted files) on drive C of your analysis computer and place this data in a single file. This single file can be placed on a diskette or on any media. Any files that were deleted from drive C can be obtained in a single file by this utility [4].

- *Temporary Files*

When working with a Microsoft Windows operating system, it copies the Windows temporary files to your Zip Drive D. These files have a .tmp extension.

- *CRCMD5*

CRCMD5 calculates a CRC-32 checksum for a DOS file or group of files and a 128-bit MD5 digest. The purpose of having the CRC checksum and MD5 digest is to verify the integrity of a file or files. For instance, once you have collected a file for evidence, run CRCMD5 on it to obtain the CRC checksum and MD5 digest. As long as the file contents are not changed, these values remain unchanged. If they do change, then the integrity of the file has been compromised, and the file may no longer be admissible in a court of law [4].

- *DiskSig*

DiskSig is used to compute a CRC checksum and MD5 digest for an entire hard drive. The checksum and digest include all data on the drive, including erased and unused areas. By default, the boot sector of the hard drive is not included in this computation. Similar to CRCMD5, the purpose of DiskSig is to verify the integrity of a hard drive. Running DiskSig on a hard drive held for evidence provides a CRC checksum and MD5 digest. If the hard drive data is altered in any way, the values of the CRC and MD5 will change [4].

- *Mcrypt*

The purpose of Mcrypt is to encrypt and decrypt files. Various levels of encryption are available. If you are also using file compression techniques, the proper procedure is to first compress the file and then encrypt it using Mcrypt [4].

i. Micro-Zap

When a file is erased or deleted using standard DOS (delete, erase) or Microsoft Windows (95/98/NT/2000) techniques, the file is not actually deleted. The file is still there and can be recovered by those who know how. Micro-Zap actually eliminates the file names and the file content associated with them. Micro-Zap deletes files by overwriting them with a hex F6 pattern. One overwrite is the default, but an even higher level of security is afforded through the seven overwrites option [4].

ii. Map

Map is used to find and identify TSR (Terminate and Stay Resident) programs. TSR is a program that is running in computer memory, but you may not realize it [4].

C. Check Records, Logs and Documentation.

They are an electronically generated and stored file of information about activities occurring in a system. They are usually in the form of a series of entries each containing descriptive attributes about a past event. Logs provide factual material which assist in the reconstruction of events, such as cyber attacks. There are many different types of logs. For example General logs, such as access logs, printer logs, web traffic, internal network logs, Internet traffic, database transactions, and commercial transactions; every application and operating system on every device on a network may be logged. Logs have been described as the “digital witnesses to transactions between computers and humans.” Unlike human eyewitnesses, logs do not

contain human statements which may suffer from bias, prejudice or faulty human recollection. There is an assumption that computer logs are more likely to be accurate as to their content, provided that the logs are authentic and reliable.

Examples of information that can be obtained from logs includes—

- Files were added, modified, copied, or deleted.
- Security settings were reconfigured or backdoors added.
- Virus or Trojan activity is indicated.
- Intrusion and sniffer tools were copied to the network.
- Internet Protocol addresses of the evident perpetrators was logged or not.
- Services were stopped or started.
- Ports were closed or opened.
- Other relevant activity occurred.
- Address translations
- Date and time stamps
- User names and passwords
- Connection information
- IP addresses
- Node names

V. MANAGING EVIDENCES FOR CYBER CRIME INVESTIGATION

Managing evidences is carried out after conducting collecting all necessary evidences for identifying the crime and criminal. In this phase, the investigating team collects relevant evidences for providing the crime's effect and to reach the criminal/conclusion. These evidences are collected from various sources inside the organization and from the records available and also from the site of the crime.

In this phase, all the evidences are collected together, stored, packaged, transported, backed up and analyzed. Evidences are basically required for Criminal Prosecutors, Civil litigators, Insurance Companies, Corporations, Law Enforcement Officials or Individuals.

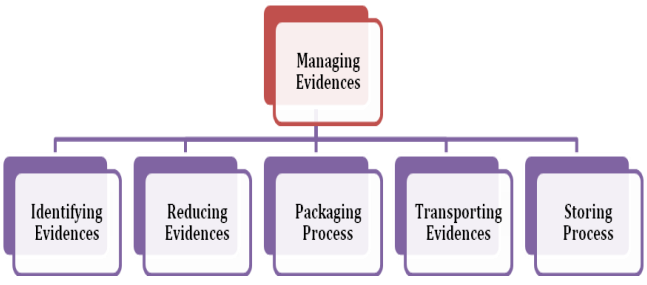

Figure 1.1: Sub-phases of Managing Evidences phase

A. Identifying Evidences

In this phase, the evidences collected are analyzed initially and all the evidences are classified into decreasing order of importance or relevance. The more relevant evidences need to be handled with extreme care and stored accordingly. The evidences are preserved according to their category to avoid any confusion and for facilitating investigating procedure. It is important that the more important evidences are not at all altered and less relevant evidences may prove out to be highly relevant at later instance so they are also conserved separately.

B. Reducing Evidences

In this sub-phase, the evidences collected and classified in previous phases are reduced or filtered. This means that some evidences which seem to be of no use to the investigating team are filtered and the set of evidences is reduced. Reduction of the evidences will involve the use of a potentially large number of techniques to find and interpret significant data. It may require, repair of damaged data in ways which preserve its integrity. This process leads to a filtered set of evidences which are relevantly used in the hypothesis phase. Depending on the outcomes of the search/identification and collection activities, there may be very large volumes of data to be examined so automated techniques to support the investigator are required. Various techniques such as Data Mining could also be implemented here where filtering, separation, categorization etc is implemented.

C. Packaging Process

Before the transportation of the evidences the auditor should check first that the packaging of the evidences is according to the norms, so that the evidences are sent safe and secure with their originality.

- Assure that all collected electronic evidence is properly documented, labeled, and inventoried before packaging.
- Magnetic media should be packed in antistatic packaging and avoid using materials that can produce static electricity.
- Folding, bending, or scratching computer media such as diskettes, CD–ROMs, and tapes should be strictly avoided.
- Ensure that all containers used to hold evidence are properly labeled.

D. Transporting Evidences

The evidences collected from the site may be digital or physical so both type of evidences need to be securely transported. Transportation could be simply the physical transfer of seized computers to the transmission of data through networks. The

evidences are named and numbered or some form of identity is provided to the evidences so that these may be securely handled and carried away with care. All security checks in all aspects should be there confirming that no alteration can be possible in the evidences, once sealed.

Some basic rules of transporting the evidences are mentioned as below:

- Keep electronic evidence away from magnetic sources. Radio transmitters, speaker magnets, and heated seats are examples of items that can damage electronic evidence.
- Avoid storing electronic evidence in vehicles for prolonged periods of time. Conditions of excessive heat, cold, or humidity can damage electronic evidence.
- Ensure that computers and other components that are not packaged in containers are secured in the vehicle to avoid shock and excessive vibrations.
- Maintain the chain of custody on all evidence transported.

E. Storing Process

Storage of the evidences is another important issue. Along with transporting the evidences, these need to be securely stored so as to avoid any loss of evidences or important data. Examination of evidences does not start immediately after the collection itself. The digital evidences are backed up double or triple times over disk in read only form. This prevents loss of any digital evidences. Physical evidences need to be forensically stored to prevent any changes in their form and content of information. Ensure that evidence is inventoried in accordance with departmental policies. Store the evidences in a secure area away from temperature and humidity extremes. Protect the evidences from magnetic sources, moisture, dust, and other harmful particles or contaminants. These stored evidences are then worked upon to generate hypothesis. All security checks in all aspects should be there confirming that no alteration can be possible in the evidences, once sealed.

REFERENCES

[1] Chaikin, D., Network investigations of cyber attacks: the limits of digital evidence. Crime, Law and Social Change, 2006. **46**(4): p. 239-256.

[2] Luna-Reyes, L.F., et al., eGovernment & internet security: some technical and policy considerations, in Proceedings of the 2003 annual national conference on Digital government research. 2003, Digital Government Society of North America: Boston, MA. p. 1-4.

[3] Govil, J., Ramifications of Cyber Crime and Suggestive Preventive Measures, in International Conference on Electro/Information Technology, 2007 IEEE. 2007: Chicago, IL. p. 610-615.

[4] B.Middleton (2006) Cyber Crime Investigator's Field Guide.