UNIT-3

DISCOVERY OF ELECTRONIC EVIDENCE

Many types of information that can play a useful role in litigation are no longer printed on paper and stored in paper files, but rather are stored in a computer system or in computer-readable form.

As companies have increased their reliance on their computer systems, lawyers have begun to be aware of the valuable electronic treasures that are now being kept in these systems and have started aggressively to target electronic data for discovery in all types of litigation cases. The discoverability of these electronic files is referred to as discovery of electronic evidence or DEE.

Competition Act, peace officers with, or in exigent circumstances without, a search warrant, may enter the premises, examine records, and copy or seize them. They may use the computer system on the premises to search data and produce printouts, which they may then seize for examination or copying.

Today, documents are rarely typed or handwritten. Most documents are created using personal computers with word processing applications or email programs. Most professionals rely on personal computers to maintain schedules and to create their written communications.

ELECTRONIC DOCUMENT DISCOVERY

The computer user is usually not aware of this situation. Furthermore, when computer-created documents are updated or erased, remnants of the original version and drafts leading up to the creation of the original version remain behind on the computer hard disk drive. Most of this data is beyond the reach or knowledge of the computer user who created the data.

AN AGENDA FOR ACTION FOR DISCOVERY OF ELECTRONIC EVIDENCE

The following are list of actions for discovery of electronic evidence

1. Do not alter discovered information.

2. Always back-up discovered information.

3. Document all investigative activities.

4. Accumulate the computer hardware and storage media necessary for the search circumstances.

5. Prepare the electronic means needed to document the search.

6. Ensure that specialists are aware of the overall forms of information evidence that are expected to be encountered as well as the proper handling of this information.

7. Evaluate the current legal ramifications of information discovery searches.

8. Back-up the information discovery file or files.

9. Start the lab evidence log.

10. Mathematically authenticate the information discovery file or files.

11. Proceed with the forensic examination.

12. Log all message digest values in the lab evidence log.

13. When forensic work is complete, regenerate the message digest values using the back-ups on which work was performed; log these new values along-side the hashes that were originally generated. If the new values match the originals, it's reasonable to conclude that no evidence tampering took place during the forensic examination of the information file.

15. Briefly compare the physical search and seizure with its logical (data-oriented) information discovery, counterpart, and information discovery.

IDENTIFICATION OF DATA

INTRODUCTION

Internet gives computer users access to a wealth of information. It is also a wonderful mechanism for the exchange of email communications and file attachments globally. International boundaries no longer exist when it comes to the exchange of information over the Internet.

Law enforcement agencies are encountering computers at crime scenes. These computers are used to store the secrets of criminals and are used in the commission of crimes.

Keeping an accurate and consistent sense of time is critical for many computer-forensic-related activities such as data identification. In other words, being able to investigate incidents that involve multiple computers is much easier when the timestamps on files (identified data) and in logs are in sync.

TIME KEEPING

It seems that, although every computer has a clock, none of them appear to be synchronized—unless the computer in question is running the Network Time Protocol (NTP). With NTP, you can synchronize against truly accurate time sources.

NTP is a protocol built on top of transmission control protocol/Internet protocol (TCP/IP) that ensures accurate local timekeeping with reference to radio, atomic, or other clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long periods of time.

Keeping a consistent sense of time is critical for many computer-forensic-related activities. Financial organizations rely on accurate timekeeping for their transactions. Many authentication systems, Kerberos being the most prominent example, use dated tickets to control access to systems and resources.

NTP a tool a tool that permitted researchers to synchronize workstation clocks to within milliseconds or better. With the growth of the Internet, the mechanisms that enabled NTP clients and servers to securely exchange time data have gone from sufficiently secure to not nearly secure enough. Newer versions of NTP fixed the problem by providing a model for automatic configuration.

TIME MATTERS

Programmers have developed different techniques for synchronizing clocks over TCP/IP or other network protocols. The time protocol provides a server's notion of time in a machine-readable format, and there's also an Internet Control Message Protocol (ICMP) timestamp message.

The Unix r commands include rdate, which permits setting a local clock based on a remote server.

CLOCK FILTERS

NTP goes beyond this by collecting timestamps from many servers. NTP maintains a queue composed generally of eight samples and uses carefully crafted algorithms to compute the best approximation of exact time.

AUTOKEY

A system called the autokey uses public key algorithms combined with a list of one-way hashes.

The key ids are used with session keys to perform a quick digital signature check based on Message Digest 5 (MD5).

Version 4 NTP also supports the Diffie-Hellman key exchange for peers, so that peers can exchange private session keys.

Forensic identification and analysis of technical surveillance devices

Computer forensics analysis is widely not done only in crime investigation but also for expansion of business.

CORPORATE INFORMATION

What is corporate information?

Everything from illegal spying and theft of trade secrets to classic intelligence-gathering—whatever it takes to provide executives with a systematic way to collect and analyse public information about rivals and use it to guide strategy.

Its goal is to anticipate, with razor-sharp accuracy and speed, a rival's next move, plot new opportunities, and help prevent disasters.

CI is in the pharmaceuticals, telecom, petrochemicals, and consumer products industries, where consumers are the most fickle and where speed and flexibility are especially critical for success.

INFORMATION OVERLOAD

The growing information makes it critical for CIOs to start thinking about how they can support their company's CI snoopsters.

It is recommended that you now start recruiting the technology executives who can build systems that will give your company the ability to react in real time to what its rivals are doing. Build such systems, and your company also will be able to respond faster to customers. The goal is to tie technology and business together in a common pursuit of becoming more competitive and responsive to rivals and customers in the marketplace.

CIOs (Chief Information Officers) can help marketing and sales strategies turn on a dime (small amount of money). CI teams should spend one-third of their time gathering information on a project, one-third in analysis, and one-third discussing their findings. Instead, many companies spend 80% of their CI time on collection, most of the rest on analysis, and very little on communication that reaches everyone.

CIOs also can help determine what the company considers junk. Often the best competitive information does not appear as highly structured data, such as financial information. More likely, it's something like an offhand comment in a press release, a photograph in a rival's advertisement, or a soundbite from a television news show.

BUILDING TEAMS

You need to build teams with diverse membership. People who understand the concept of organizing information and indexing it could be paired with someone who understands different technology capabilities, such as a relational database showing connections between different terms or items.

No company should buy a software package in the hope it will build an intelligence process for the corporation. CIOs need to help build that. It won't come off the shelf.

Reconstructing past events

Recovering electronic data is only the beginning. Once you recover it, you need to determine how to use it in your case. In other words, how do you reconstruct past events to ensure that your findings will be admissible as evidence in your case?

If You Need Help, Get Help

When you receive the package of evidence containing a Zip disk and cover letter stating, "Enclosed and produced upon your request, please find ...," you may not know what to do with the disk. If you don't know, get help.

If you have a litigation support group, consider contacting them. They may have the tools you need to look at and start working with the data you just received. Even if there is no formal entity within your office dedicated to dealing with technological issues, there may be informal resources.

Convert Digital Evidence

Before you can reconstruct past events and present the data, you need it on a medium and in a format you can work with.

Today, data can come on a variety of media, such as holograms, video, data tapes, Zip disks, CD-ROM disks, and even 3.5-inch floppy disks.

Put the Evidence in a Useable Format

If the data comes in a format that you already use, then you can begin to work with it as soon as you get it off the media. The formats most likely to be useable without conversion are word processing files (principally WordPerfect and Word files), spread sheet files (principally Excel and Lotus), and presentation files (principally PowerPoint files).

Useable file formats

Even if the data is in a format that appears to be one you already use, conversion still may be necessary. The format may be too new. The problem is a basic one.

In a similar vein, you may have to get the data converted if it comes to you in a format that is too old or runs on a different operating system.

Although simple files created with one company's software generally can be opened without a problem using a competitor's comparable product, this often does not hold true for more complex files.

Unusable file formats

When that happens, you have to convert the files to a format you can use or find someone to do the conversion for you. You may have already encountered these issues with a variety of files including email files, database files from mainframe systems and ".txt" files containing data dumped from database files. Anyone who has undertaken this task can attest that it is potentially a difficult and painstaking process.

Whenever you suspect that you will have to convert data, there are some steps you can take to facilitate the process. Initially, try to get as much information about how the files were created and maintained as you can. Whether you intend to try the conversion yourself or rely on outside resources to get the work done, the more you know about the files, the better your chances of a successful conversion.

For example, if you receive a ".txt" file that appears to contain information from a database file, try to find out, among other things, the make and model of the computer the file came from; the name and version of the operating system the computer ran; the name and version of the database program used; the name of the database file; a list of all fields in the database; and descriptions of each field with the descriptions including the type, length, and other characteristics of the field.

Converting Files

If you are going to attempt converting the data yourself, you may be fortunate enough to have received electronic data that you can covert directly into programs such as Access or Excel using the wizards built into those programs. This can be the case with ".txt" files. Sometimes the first line in a file you are converting may even contain the names of the fields that need to be created, further simplifying your task. If that information is not in the file, then try to get the field names and descriptions from the producing party. If you fail at that, you may have an exceedingly difficult time carrying out a meaningful conversion. Sometimes data will not be in a format amenable to immediate conversion. Email files are a common example.

Networks: A technical approach

As information systems become cheaper and cheaper, companies are rapidly automating not only their overhead processes such as purchasing, payables, hiring, and payroll, but also their value by adding processing such as marketing and sales.

The result of this rush to automate and, with the explosion of the Internet, a rush to publish, is the highest level of dependency on information systems. The ability of corporations to conduct their business is dependent on technology that was designed to be as open as possible and that only a minority of engineers and scientists understand.

When connected to the Internet, what managers need to do is create barriers that prevent cyber-based or internal perpetrators from attacking their systems. The first way to do this is to analyse corporate resources for known vulnerabilities. That is, systems need to be checked to ensure that they are correctly configured and have the most up-to-date security patches in place. This is what security scanners do. When the malicious act is discovered, the question immediately comes to mind: How did they do this? And sometimes: What did they do?

Destruction of email

We need to recognize email as more than simply an informal, casual means of communication. The courts treat email as formal records not different than print communication is prepared for the legal consequences, including the fact that your company's email is discoverable in litigation.

For example, just ask Bill Gates about the significance of this treatment. Reams and megabytes of Microsoft email messages dating from the 1990s (including Gates' own) were used skilfully by the government in its antitrust case against Microsoft. As with any other printed documents, these email messages were deemed records discoverable under the federal rules of civil procedure.

Hitting the Delete button on your keyboard is not a remedy. Oliver North's deleted email messages from the White House were retrieved from a main frame backup tape during the Iran-Contra investigation.

If information that has been deleted has not yet been overwritten by the computer system or is stored on back-up tapes or archive tapes, the information may still be accessible.

Employers beware, for even prelitigation correspondence has been found sufficient to impose a duty to preserve relevant documents.

To avoid these litigation nightmares, you should implement a consistent retention policy that includes one or more of the following:

- ✓ Routinely archive all email as it is received on your server for a certain period of time (for example, 30–60 days).
- ✓ Clear the archives after an additional specified time.
- ✓ Physically segregate the backup copies of the email system from backups of the rest of the computer system.
- ✓ Automatically erase email from the computer system, including backups, after a short period (15–30 days).
- ✓ Apply uniform retention and deletion standards and features outside the server to workstations and laptops and formulate and distribute a statement that the automatic deletion of electronic records will be suspended and steps taken to preserve records in the event of investigation or litigation.

Damaging Computer Evidence

To ensure that digital evidence is collected, preserved, examined, and transferred in a manner that safeguards its accuracy and reliability, law enforcement and forensic organizations must establish and maintain an effective quality system.

Rapid technological changes are the hallmark of digital evidence, with the types, formats, and methods for seizing and examining digital evidence changing quickly.

To ensure that personnel, training, equipment, and procedures continue to be appropriate and effective, management must review and update SOP documents annually.

Case notes and records of observations must be of a permanent nature.

Notes and records should be authenticated by handwritten signatures, initials, digital signatures, or other marking systems. Evidence has value only if it can be shown to be accurate, reliable, and controlled. A quality forensic program consists of properly trained personnel and appropriate equipment, software, and procedures to collectively ensure these attributes.

International Principles against Damaging of Computer Evidence

The International Organization on Computer Evidence (IOCE) was established in 1995 to provide international law enforcement agencies a forum for the exchange of information concerning computer crime investigation and other computerrelated forensic issues.

The international principles developed by the IOCE for the standardized recovery of computer-based evidence are governed by the following attributes:

- ✓ Consistency with all legal systems
- ✓ Allowance for the use of a common language
- ✓ Ability to cross international boundaries
- ✓ Ability to instill confidence in the integrity of evidence
- ✓ Applicability to all forensic evidence
- ✓ Applicability at every level, including that of individual, agency, and country

Furthermore, the following international principles were presented, approved, and approved again at the IHCFCs (International Hi-Tech Crime and Forensics Conference) in October 1999 and 2001, respectively.

- ✓ Upon seizing digital evidence, actions taken should not change that evidence.
- ✓ When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- ✓ All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- ✓ An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in his possession.
- ✓ Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles

Tools needed for intrusion response to the destruction of data

It is very important to document and inventory the tools needed for intrusion response to the destruction of data—including intrusion detection software, backups, and file-system-recovery tools. There is also a need to have written requirements for training IT staff on how to deal with intrusions. This can be System Administration, Networking, and Security Institute (SANS) courses, Computer Emergency Response Team's (CERT) Software

Engineering Institute, training offered for your intrusion detection tools, or even custom training developed in-house.

Incident Reporting and Contact Forms

Documenting the intrusion (incident) on destruction of data is very important, not only as an aid for solving the intrusion problem, but also for an audit trail that may even be used in criminal proceedings. It is critical to capture as much information as possible and create forms enabling users who are not intrusion detection specialists to provide as much information as possible. Some of the important elements of incident reporting forms are

- ✓ Contact information for person(s) discovering problem and responsible parties.
- ✓ Target systems and networks. Know all about the systems under attack, including operating system versions, IP addresses, and so on.
- ✓ Purpose of systems under attack. Know what the systems are used for (payroll, R&D, and so on), as well as some kind of a ranking of the importance of the system.
- ✓ Evidence of intrusion. Discover anything that is known about the intrusion, method of attacks used, source IP address of attacker, and network contact information for this address.
- ✓ List of parties to notify. This can include the technical contacts, internal legal contacts, and possibly the legal authorities.

System Testing

Statistics show that more than 82% of successful hacks occur because Web technicians fail to install patches for known and publicized bugs. In other words, a little effort can go a long way toward securing your network.

Domain Name Service

If you've ever used a URL to represent an IP address, you've used domain name service (DNS)—a distributed database that provides translation capabilities between domain names and IP addresses. DNSs also provide a standard Internet mechanism for storing and accessing other types of data, such as MX (mail exchange) records.

First, if yours is one of the many companies that run outdated DNS software, an upgrade is definitely in order. Install the latest version of your DNS software immediately.

Your next step should be to limit your access to port 53 (the DNS port) on your firewalls. Although User Datagram Protocol (UDP) packets are required for requests to and from the Internet DNS, your network's transmission control protocol (TCP) transport layer should be locked down except in cases when it's absolutely required, such as on primary and secondary servers at opposite sides of the firewall.

Services and File Sharing

Although services and file sharing capabilities are available on both Windows and UNIX, Windows computers receive the brunt of file sharing attacks from trojan horses and share compromises.

Many network administrators use share services to make data access more convenient, but hackers will often compromise healthy machines by installing backdoor programs that

register themselves as share services when users start their systems. These shares can then be run from any client machine with "log on as service" rights.

To prevent unauthorized access through your network services, identify and remove all services that are not absolutely necessary.

File shares present another potential vulnerability to your network because, when improperly configured, they can expose critical system files or even give full file system access to any party that is able to connect to your network.