How does Forensic work?

The purpose of computer forensics is to search, maintain and analyze information on computer systems to find evidence of a crime for a case.

***TipsMake.com* - When Enron energy group declared bankruptcy in December 2001, hundreds of employees lost their jobs, while some officials seemed to benefit from the collapse of the company. The US Congress decided to investigate after rumors of a fraud in the company. Most US Congress investigations focus on computer files to find evidence. A professional force began searching through hundreds of Enron employees' computers with forensic computers - finding evidence of high-tech crime.**

The purpose of computer forensics is to search, maintain and analyze information on computer systems to find evidence of a crime for a case. Many investigative methods used in criminal investigations have a combination of digital, but there are some special cases that use computer surveys.

For example, just open a file in the computer and change it, the computer will record the time and date it accessed the file. If an employee has a computer and starts opening files, no one can be sure they haven't changed anything. Since then, the lawyer can argue the validity of these evidence if the case is brought to court.

Some argue that using digital information is evidence is a bad idea. If it is easy to change computer data, how can it be used as reliable evidence? Many countries allow the use of computer evidence in court hearings, but this can also be altered if digital evidence proves to be unreliable evidence.

Computers are becoming more and more powerful, so computer forensics must also have adequate development. In the early days of computers, it was easy for investigators to find a file because of low storage capacity. Today, with disk storage capacity up to gigabytes, even terabytes of data, work is even more difficult. Investigators will have to find different ways to find evidence without using too many sources for the investigation process, improving the efficiency of the process.

So, what are the basics of forensic computer - finding high-tech crime evidence? What do investigators look for? Where do they search?

The basics of Computer Forensic

Forensic computer field is still quite new. In the early days of computers, the court considered the evidence from computers no different from other types of evidence. As computers became more and more developed and complicated, this thought changed - the court learned that evidence of crime could easily be altered, deleted or destroyed.
Investigators realized that it was necessary to develop a tool that could help investigate evidence in computers without compromising information. They have begun working with computer scientists, creating volunteers to discuss the appropriate methods and tools they need whenever they have to retrieve information from a computer. Since then, they have developed a method to form a forensic computer field.

Often, investigators must have a court order to find information on a suspect computer. This order will include where the investigator is allowed to search and the type of evidence they can find. In other words, investigators can only follow orders and look for what they think is suspicious. In addition, the commands in the command must not be too general. Most courts require very specific things when giving an order to investigators.

For this reason, investigators will have to search for as many sources of suspicion as possible before requesting a court order. For example, an investigator has an order to investigate a suspect laptop. This person comes to the home of the suspect to follow the order. When they arrived, the investigator saw a desktop computer. This investigator cannot search for evidence on this computer because it is not included in the terms of the search order.

Plain View

Plain view rules - allow investigators to collect any evidence available during the search process. If the investigator in the previous example discovers evidence on the computer screen of the person in question, the employee can use this computer to search for evidence even though it is not included in the command. examination. If this desktop computer is not enabled, the investigator has no right to inspect it.

Each survey on the machine has its own difference. Some surveys may take a week to get results, but others may occur monthly to complete. Here are some things that may affect the timing of an investigation:

• Qualifications of investigators

• Number of computers to check

• All of the space that investigators need to check (hard drives, CDs, DVDs and external storage devices)

• Whether the suspect is deleting or hiding the information

• Handle encrypted files or password-protected files.

The stages of investigating Computer Forensic

Judd Robbins, a computer expert and forensic computer leader, has listed some of the steps investigators need to do whenever they want to retrieve evidence from a computer:

1. Control the computer system to make sure the device and data are safe. This means the investigator needs to have security so that no individual can access the computer and the storage device is being checked. If the computer system is connected to the Internet, the investigator must control this connection.

2. Search all files contained in the computer system, including encrypted files, password protected, hidden or deleted but not overwritten. Investigators should reproduce all system files, including those contained in the computer's drive or files from external hard drives. Since accessing files can change it, investigators should only work with copies of files when searching for evidence. The original should be preserved and not be touched.

3. Restore as much deleted information as possible by using applications that can search and retrieve deleted data.

4. Search for information of all hidden files

5. Decode and access protected files

6. Analyze special areas on computer drives, including sections that are often hard to reach.

7. Record all steps of the process. This is very important for investigators to provide evidence that their investigation work has protected the information of the computer system without altering or damaging them. An investigation and trial may take years, if there is no authentic document, evidence is not even acceptable. Robbins argues that these authentication documents include not only files and data recovered from the system, but also system drawings and where files are encrypted or hidden.

8. Prepare to be a witness in court for computer forensics. Even when the investigation process is complete, their investigation work is not done. They may still have to testify in court.

Do not delete the file as you think

Every time you delete a file, your computer will transfer this file to a new directory. When emptying the recycle bin, the computer will notify you that the space used for the file has been empty. The file remains there unless the computer writes a new data to that part of the drive. With the right software, you can retrieve deleted files if they have not been overwritten.

All these steps are important, but the first step is the most important. If investigators cannot control the entire computer system, the evidence they find will not be recognized. This is also very difficult. During the early days of the computer, the system consisted of only one device with several floppy disks. Today, it includes a lot of computers, drives, external hard drives, .

Some bad guys have tried to make it difficult for investigators to find information in their systems. They use programs and applications called anti-forensic. Investigators will have to watch out for these programs and find ways to remove them if they want to access information in the system.

So, what is anti-forensic? What is their purpose?

Anti-Forensic

Anti-forensic may be a nightmare for computer investigators. Developers design anti-forensic tools to make it difficult or even impossible to retrieve information during the investigation process. In essence, anti-forensic refers to any method or tool or software designed to make it difficult to investigate computers.

There are many different ways for people to hide information. Some programs can trick a computer by changing the file header information. A header is usually hidden from everyone but it is really important when it notifies the computer the type of file it is being attached to. If you just changed the name of an mp3 file to a '.gif' file, the computer still knows that it is an mp3 file by the header information. Some programs allow you to change the header information so that the computer recognizes it as another file. The investigator looking for a specific file format can ignore important information because it does not look relevant to the information to be searched.

Other programs can split files into different small items and hide each item in a different file. Files that do not use capacity are called slack space. With the right program, you can hide these files using slack space. This makes it very difficult to retrieve and gather hidden information.

Also, it is possible to hide a file inside another file. Executable files - are computer files identified as a program that can cause problems. Programs called packers can nest executable files to files of other types, while binder tools can mount many executable files together.

Encryption is also a way to hide other data. When you encrypt data, you can use complex algorithms to make data difficult to read. For example, the algorithm can change a text file into a set of meaningless numbers and characters. Someone who wants to read the data needs to be able to open the password, helping to convert numbers and characters into text. Without a password, the investigator will have to use computer programs to unlock the password. The more complex the algorithm, the more time it takes to decode it without a password.

Another anti-forensic tool can change metadata - data history - attached to a file. Metadata includes the same information as when a file was created or the file was last changed. Normally, you cannot change this information, but there are programs that help users to change the metadata attached to the file. Imagine checking a data calendar and discovering that it said the file didn't exist in the next 3 years and the last visit was a century ago. If the metadata has been destroyed, it makes proving evidence more difficult.

Some applications will delete data if someone is not authorized and still deliberately access the system. Some developers have tested how forensic computer programs work and try to create applications that can both block and attack programs. If forensic computer experts face such people, they will have to be very careful and skillful to retrieve data.

Some people use anti-forensic to prove that computer data can be easily attacked and unreliable. If you are not sure when a file was created, the last time it was accessed, or even if it ever existed, how can you prove that the evidence is legitimate before the court? While this is still a valid question, many countries still accept computer evidence in trials, despite the standards of evidence in different countries.

So, what is the standard of evidence?

Standard of evidence from computer

" *Thinking globally, acting in the region* "

One challenge faced by computer investigators is that while computer criminals operate without borders, so does the law. One thing is considered illegal in this country but is legal in another. Moreover, there is no general international standard for collecting information on computers. Some countries try to change this. The G8, including the United States, Canada, France, Germany, Britain, Japan, Italy and Russia, unified six common

things about finding high-tech crime evidence. These things focus on keeping the original evidence.

In the US, laws cover the control and use of evidence on computers. The US Department of Justice has a handbook called "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (searching for, controlling computers and collecting electronic evidence in what we are criminals). This book explains when an investigator is allowed to use the computer while searching, what kind of information is acceptable, hearsay law - a testimony heard from others speaking - is applied when conducting looking for evidence.

If investigators believe that the computer system only functions as a storage device, they are not allowed to seize the hard drive. This will limit the evidence for the incident. Alternatively, if the investigator thinks that the hard drive is proof, they can seize the hard drive and bring it to the office. For example, if the computer is a proof of theft of the property, the investigator may seize the hard drive.

In order to be able to use evidence from a computer in court, the plaintiff must verify this evidence. That is, the plaintiff must certify that the information presented before the court is evidence from the defendant's computer and that the information is retained.

Although people often admit that tampering with computer data is possible and very simple. However, US courts do not completely remove evidence from computers. Instead, they asked to prove these evidence to be false before removing it.

Another thing that the trial is considering with evidence from the computer is hearsay. This is a term about the statements spoken outside the court. In most cases, the court does not allow hearsay as evidence. The court has considered information on a computer that is not hearsay in the case and therefore it is accepted. If the computer records statements as an email, the court must consider whether these statements are considered reliable or not, before taking them as evidence. The court will determine these on a case-by-case basis.

Computer forensics uses some interesting tools and applications during the investigation process. Let's learn about these tools in the next section.

Tools of forensic computer

Programmers have created a lot of forensic computer applications. For police headquarters, the choice to use these tools is based on budget as well as human resources.

Here are some forensic computer programs and devices useful during the investigation process:

• Disk imaging software records the structure and content of a hard drive. With this software, it is easy to copy the information of a drive and it also provides the way the files are organized and the relationship between files.

• Software or hardware write tools copy and reset a hard drive bit by bit. Both types of tools can avoid changing information. Some tools require an investigator to remove the hard drive from the suspect's computer first, then copy it.

• Hashing tools are used to compare originals in hard drives with copies. The tool will analyze the data and assign it a separate number. If this number is on the original and the duplicate is the same, this is the original copy.

• Investigators use data recovery programs to search and recover deleted data. These programs locate the data that the computer has marked for deletion but has not been overwritten. Sometimes, this also affects files that have not been finalized, making it difficult to analyze.

• There are several programs designed to protect information stored in RAM. Unlike information on the drive, data stored in RAM is lost after shutdown. Without appropriate software, this information will be easily lost.

• Analysis software filters all information on a drive to search for specific information. Because modern computers can store gigabytes of data, it is difficult and time-consuming to search files on a computer manually. For example, some analytics programs search and evaluate Internet cookies, helping investigators find suspicious activities on the Internet. Some other programs allow investigators to search for specific, questionable information in the computer system.

• The decryption program and password cracking software are useful when investigators face protected data.

Cellular phone

Mobile phones can also store important data. In essence, a mobile phone can be considered a small computer. A handful of forensic computer sellers that provide devices can copy all data in mobile memory and print it out into a report. These devices can retrieve everything from messages to ringtones.

These tools are only really useful when the investigator follows the procedures properly. Otherwise, a good defense lawyer can argue that all evidence collected while investigating the computer is unreliable. Of course, there are still a few anti-forensic experts who argue that no evidence on any computer is completely reliable.

Will the court continue to accept evidence from the computer that is reliable for use in court sessions as well? Anti-forensic experts still argue that there is only a matter of time before someone can prove to the court that these data are legitimate and can be protected. If this happens, the court will be very difficult to verify evidence from a case's computer or an investigation.