Computer Forensics -An Introduction of New Face to the Digital World

[1]Mohammed Rahmat Ali
[1] Researcher Scholar, Kulliyah Information Communication Technology- Computer Science, International Islamic University Malaysia (IIUM), Gombak Malaysia.

Author Address:
Mr Mohammed Rahmat Ali
Researcher Scholar,
Kulliyah Information Communication Technology
Computer Science,
International Islamic University Malaysia (IIUM).
Gombak, MALAYSIA.
9-8-256, Bada Bazar, Golconda Fort, Hyderabad-500008, Telangana State. Mobile: 91-9985220384
Email: rahmat_ali2u@yahoo.com

Abstract: Computer forensic is the current emerging and the future of the digital world. Computer forensics is the upcoming technology for the crime scene investigation and for the data assessment data discovery and data maintained and data recovery process. Computer forensics can also be used in the retaining the computer technology without major effect to the physical parts of the computer. As the use of technology is increasing day by day and the use of computers to reduce the human efforts and to maximize the efficiency and outcome and also to increase the accessibility of the resources has led others to the misuse of technology. As the technology is increasing the threat to the cyber security and data is also increasing. To reduce the threat for cyber security and to increase the reliability on data and information throughout the network, computer forensics is used as a tool and method to analyse and to reduce the cyber threat to the data and affiliated system on network.

*****

I. INTRODUCTION:

Computer forensics is the emerging technology of the modern day world. Computer forensics also known as the digital forensics is the methodology for identifying, preserving the evidence for the future coursework. The reason computer forensics came into existence or to the study of people is the increase in number of cyber-attacks and increase in the number of infected computer either by hackers or by the effected software by which the computer are been infected. According to a recent industrial survey ninety four percent of the companies did responded with cyber-attack on their company with an approximate loss of $35billions. Hacking or phishing is just a tool which is been used by anyone who has a knowledge of computers and its modes of operations and by learning advancements within a day or night to master in it and start practice. This in turn will result to increase the threats to the data and computer. Technological advancements and open source of information and findings has also lead the internet to find new ways of breaching security and to entering into another's computer without knowing the end users. The user unknowingly or sometimes knowingly the security threats enters a zone wherein the computer which are using will no longer be available but will be under the threat. This creates a crime scene and has to be preserved for identifying the investigation process.

II. WHAT IS COMPUTER FORENSICS?

Computer forensics as the term indicates is a study of scientific tests or techniques used in computers in connection with the detection of crime in digital data and associated computer and network of it with reference to criminal law of offense. Computer forensics involves preservation, identification, extraction and documentation of the evidences. Computer forensics, also been referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. A detailed analysis by a skilled examiner can result in the reconstruction of the activities of a computer user.

Computer Forensics is also been referred to as the solution to the modern world new threat to computer and data with advancements in data investigation and the methods of recovery of the data. Recovery of the data is not only the solution to the crime scene but also to gather the sources of the crime scene and analyse the methods by which crime scenes can be reduced. And also to build the software's and

other application which can reduce the effect of the crime scenes and to improve reliability of the computer and data. Modern method and techniques and increase in research are taking steps in computer forensics experts.

III. WHERE IS COMPUTER FORENSICS USED?

Computer Forensics is used to identify and access and collect information from a crime scene, either from hacking phishing, or from instruction or denial of service attack. The Crime Scene constitutes evidences and details of how system was been attack and data been lost or data to be recovered, such as emails, history of internet, documents been accessed, fraud sites and others.

Computer forensics is not just only to trace the physical loss of the network but also the consequences that might happen after it was ben effected. It also looks after the metadata associated with the files and others such as when was the file been created, who created the file, when it was been last edited, and when it been was last accessed.

Most of the times and in last few times across, commercial organisations had used computer forensics for their benefit in several of cases like

* Intellectual Property theft
* Industrial espionage
* Employment disputes
* Fraud investigations
* Forgeries
* Bankruptcy investigations
* Inappropriate email and internet use in the work place
* Regulatory compliance

IV. WHEN WOULD COMPUTER FORENSICS BE USED?

Computer forensics is the process of finding what happed to the computer, and from where the computer got effected, moreover when was the computer been effected and how the computer is been effected. And also in addition it, also finds the people who are involved in effecting the computer. All the evidences which are collected are digital evidences and need to be stored as confidential. When compared to physical evidences digital evidences last long, physical evidences cannot be interpreted or changed but there is a provision of digital evidences might be changed or the probability of changing the evidences is high.

As an examples of typical conditions in which computer forensics is used includes:

• When the corporate information of a system is disclosed without authorization, either by accident or by a design.

• When an employee is stealing your employer's intellectual property and will present it to competitors or use it to establish a competing business.

• If the employee violates the basic computer norms, such as when and how to use the Internet, i.e. some organizations have set rules on How to use the computer or the Internet. If the system in the office is used for any illegal activity such as accessing those sites which might harm the security norms of the organization, computer forensics analysis can help determine when and how these illegal entries has occurred.

• Analysis and evaluation of damages after the incident occurred.

• Corporate corruption. This is motivational violence and crime committed by the government or professional business goons. These crimes would be like identity theft, Ponzi schemes and payment schemes in advance. White collar crime can end up with life savings, and can help saving companies or investors impose billions in losses.

• Computer forensics can be used to aid in the investigation of such crimes.

• Industrial espionage. This involves the theft of trade secrets of competitors by recording or copying confidential documents. Examples of documents involved, including the secret formula, product specifications and business plan. Industrial espionage is an illegal activity, and computer forensics can aid in research.

• It is deliberately providing false or misleading information to achieve something that is not fair. Many fraud committed through the internet or with the help of computer forensics and technology can help investigate these crimes.

• The collection of information that can be used to terminate a person's employment in the future.

Competent authorities sometimes require computer forensics to investigate the crime. The teams own system can act as a crime scene in the case of a denial of service and piracy. The computer system may also contain evidence of a crime. Many people can also store information in an inadvertent or accidental computer system. Proof that a forensic investigation conducted in the form of emails, documents and the history of the Internet. Maybe there are also files related to crimes such as kidnapping, drug trafficking, money laundering or fraud.

In addition to the information on the computer, law enforcement officers can use the metadata file to find out more about a particular crime. Computer forensics analyst will determine when a file is first created, when it was edited, and when it is printed or saved last. Forensic examination can also determine which users carry out this activity.

V. HOW COMPUTER FORENSICS WORKS?

According to a survey, when a company in Huston, United States named Enron was declared bankruptcy in December 2001, hundreds of employees were left jobless while some

executives seemed to benefit from the company's collapse. The United States Congress decided to investigate after hearing allegations of corporate misconduct. Much of Congress' investigation relied on computer files as evidence. A specialized detective force began to search through hundreds of Enron employee computers using computer forensics.

The purpose of computer forensics techniques is to search, preserve and to analyse information on computer systems to find potential evidence for a trial and as the basic information for the investigation to start with. Many of the techniques detectives used in crime scene investigations had digital counterparts, but there are also some unique aspects to computer investigations to be known about.

For example, just opening a computer file changes the file, the computer records the time and date when it was been last accessed. If computer forensics expert or a detectives seizes a computer and then start opening files then, there is no way to tell for sure that they didnot change anything. Lawyers can contest the validity of the evidence when the case goes to court.

Some people say that using digital information as evidence is a bad idea. Yes it's true for many of the cases. If it's easy to change computer data, how can it be used as reliable evidence? Many countries allow computer evidence in trials, but that could change if digital evidence proves untrustworthy in future cases. But the fact is that the digital evidences are most trusted as the evidences are seized, it cannot easily be changed because of the fact that it's been stored by different people at different places with no interconnectivity to re-authenticate at the time of re-submitting in the court.

Computers are getting more powerful and intelligent, so the field of computer forensics must constantly evolve. In the early days of computers, it was possible for a single detective to sort through files because storage capacity was so low. Today, with hard drives capable of holding gigabytes to terabytes of data and even petabytes of data, that's a daunting task. Detectives must discover new ways to search for evidence without dedicating too many resources to the process and with less amount of time to spare for only investigating the data. But also should have advancement is detecting the evidences and sources of attack.

VI. WHY COMPUTER FORENSICS IS BEING USEFUL

Although, it is the most commonly used in computer crime investigation. Computer forensics can also be used in public affairs investigations. The computer forensic process is very similar to data recovery, but with additional guidelines and rules to create legal pathways for audit data. Computer forensics are widely accepted in the United States, Latin America and throughout Europe, as it is believed to be in the investigation of many high profile evidence cases.

Or might be able to thoroughly investigate digital crime today. Computer forensics are required to access encrypted and hidden digital information typed or stored on computer hard drives and other digital storage. In a world of professional hackers and clever hacking techniques, it would be impossible to find the necessary evidence for digital types and other crimes, without this form of forensic science.

Proof are disclosure by computer forensics is subject to the same as any other evidence of criminal law guidelines. It must follow the law that is acceptable in court. Each country also has a unique set of guidelines for the use of computer forensic evidence and this science has been used in several important criminal court cases since the mid-eighties.

In the digital age we live today, it would be impossible to retrieve the kind of evidence required to solve many cases submitted to the judicial system in the digital era. Computer forensics is a very reliable and useful resource necessary to try those cases in court.

VII. COMPUTER FORENSICS SERVICES

Data and Information is though much secured but it's always been in a peak of threat that any point of time the data can be stolen. The data might be from any of the bank that constitutes usernames and passwords of the data might be a highly confidential to any of the firm. No matter how concern you are about the data or how much the data is secured the data will get stolen or been copied to unauthorized personals.

There can any one of the either way that the system will be effected or a crime scene will be created, if the system is been accessed and some data is copied and some damage is been to the system either with software or with hardware interference. Or the system is been accessed through an unauthorized network and the system is been effected with some of the denial of services attack or some kind of virus in been injected to the computer system. This Creates a crimes scene, and investigation starts from here, but for the computer forensics expert they should be able to perform the following services:

- Data seizure
- Data duplication and preservation
- Data recovery
- Document searches
- Media conversion
- Expert witness services
- Computer evidence service options
- Other miscellaneous services

 ISSN: 2321-8169
453 – 456

There are many of the upcoming sector who is using computer forensics in there firm. Computer forensics has evolved and occupied the market with its effectiveness and with its ability to identify, preserve, store and restore the evidences with modern amenities and with modern way of resolving the digital world problem. Banking sector and many private firms are hiring computer forensics expert to look after the data and to monitor the data across the network.

REFERENCES

[1] https://www.lgms.global/forensic/?gclid=CPavysLFmdUCFdiFaAodZvAM7g
[2] https://en.wikipedia.org/wiki/Computer_forensics
[3] https://www.criminaljusticedegreeschools.com/criminal-justice-careers/computer-forensics-investigator/
[4] https://forensiccontrol.com/resources/beginners-guide-computer-forensics/
[5] https://www.edx.org/course/computer-forensics-ritx-cyber502x-0
[6] http://searchsecurity.techtarget.com/definition/computer-forensics
[7] http://computer.howstuffworks.com/computer-forensic.htm
[8] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwiWnpCwxpnVAhWCoJQKHcftAeUQFgg4MAE&url=https%3A%2F%2Flib.lhu.edu.vn%2FViewFile%2F5788&usg=AFQjCNGeOZUntx_e-BBXO-1ndMGJk765vQ&cad=rja
[9] https://docs.google.com/viewer?a=v&pid=forums&srcid=MDMxNjI0Nzk4MjMzOTkxMjIxNDABMTc0MjE0NTg5NjQzNjAxNzc2ODUBMXd0My1ac0QtczBKATAuMQEBdjI