Assignment on computer forensics

Technology, Computer

While a relatively new science, computer forensics has gained a reputation for being able to uncover evidence that would not have been recoverable otherwise, such as emails, text messages and document access. The application of computer forensics is given below. Criminal cases: Computer forensics is popularly applied in criminal cases. Computer forensics analysis may provide evidence that a crime has been committed, whether that crime involved computers directly or not. Evidence may be in the form of a document, an email, an instant message, a chat room or a photograph.

This is seen frequently in narcotics cases, stalking, sexual harassment, sexual exploitation, extortion, kidnapping and even murder cases. Domestic cases: Computer forensics also frequently plays a role in domestic cases and is generally centered on proof of infidelity. Examples include recovered emails, chat room transcripts, instant messaging and photographs. Security incidents: The Center for Computer Forensics reports that 92% of all business documents and records are stored digitally and that although hackers are commonly seen as a threat to security, in reality greater risks are found within a company.

Examples include theft of intellectual property (such as customer lists, new designs, company financial or trade secrets) and embezzlement. The fact is that if a person is alone with a computer for less than five minutes, it is enough time to copy a hard drive on a removable storage device. Internal There are many applications of computer forensics that exist within companies to monitor computer usage. While what is being monitored may not be illegal itself, it is tracked because doing so is " illegal" within the confines of the company.

For example, many companies have " acceptable use policies," meaning policies prohibiting personal use of the computers. Common examples of acceptable use violations include online shopping, Internet surfing, online gambling, personal emails and instant messaging or chats. Marketing purposes: Computer forensics is also applicable in marketing. Examples of this can be seen on Amazon. Com when recommendations are provided or " Just for you" from the tunes Store. When a person visits a website, a memory of that website is placed in the computer's memory.

Each site has different meta-tags embedded in it; meta-tags are one or two word descriptions of the site content. The advertisements that person experiences are tailored to the meta-tags of the sites visited, similar to a target demographic. Basic Computer Forensic Techniques: The Basic computer forensic techniques can be divided into two parts For computer networks, the following are the forensic techniques that are most commonly used - Packet Sniffing: Sniffing, in normal language means sensing something and here too it has the same meaning.

Data flows through the network lines Just like oxygen through air, pulling out critical data packets from these networks is called packet sniffing.. IP Address Tracing Internet Protocol Address Tracing means to trace an IP address right down to its real address. IP Address tracing involves reverse address look up, which means, counting the number of servers that lie between source and destination. Email Address Sometimes it becomes important to know where an email came from. This can be achieved by analyzing email headers.

Email headers consist of source machine IP address which could be used for an IP Trace. For Computer Systems File Structure For a physical computer system, the file structure is analyzed and a look out is done for suspicious files which are scattered in every nook and corner of the system. Some of these files may be encrypted, garbled or hashed with some algorithms. Such files are then processed and decrypted for gathering digital evidence. Storage Media Storage media might be in the form of physical or removable disks.

These disks might have been erased (formatted) and it can become almost impossible to recover data from it. However, with the help of advanced utilities and data recovery tools this is possible. Every time data is recovered, it is not necessary that it would be in proper form, so it is seen that whatever data fragments are gathered, are put up together to form formidable digital evidence material. Stenography Stenography is the art of hiding information in images, sounds or any other file format than the routine format.

A piece of data or information hidden into a image or sound file is extremely difficult to catch and this can lead to waste propagation of the material through internet or other media. Stag-Analysis and decryption techniques are applied to get the data back to its original form. Prints Prints are print outs which are taken from a computer printer device. Most of the computer forensic experts forget to concentrate on these print outs. These print outs are taken such that at first glance they are not visible to the naked eye.

They would either be too microscopic or would be garbled or again crypt for deception. So while evaluation and gathering of digital evidence analyzing print out becomes a very important aspect and should not be neglected or handled carelessly. Some of the most common tools of the trade use in Computer Forensics are: Hex Editors Dissemblers Disk Analyzers Descriptors Packet Snifters DNS Tools Computer Forensic Science is a field which is gaining heavy momentum across the world due to rise in cyber crimes and will continue to rise at a tremendous pace in the coming decade.

Future Prospects of Computer Forensics: 1: Hardware -The size of storage media & memory and the speed of processors. We can expect that in upcoming years, computers will come standard with TPTB or more of storage and that portable media like flash drives will carry something like BIBB of ATA - what the average hard drive was holding one or two years ago. After some years, computers will probably be 7 or 8 times faster. So these things will hold lots and lots more data and people will fill them up with lots & lots more data.

Therefore, each computer forensics Job will require sorting through and analyzing many times more data than today. 2: Computer Forensic Tools - The capabilities, automated nature and cost of computer forensic tools. We can expect that in upcoming years, computer forensic tools will be about 5 times as fast, and twice as sophisticated. That means that even with all the additional data, the average, non-automated Job will take about the same effort as it does now. However, a lot of automated tools for collection and initial processing are starting to be released.

These tools can be used by less-trained people, so it may be that data collection and preliminary processing will be faster due to automation. We expect that the cost of computer forensic tools will not go down in relative terms. However, more Open Source forensic tools will be available for free for those willing to learn to use them. 3: Bad guys - Ann-forensics lolls & schemes, sophistication of hackers There's always a race between how harmful software and cyber-marauders can be and the defenses against them. There is also software constantly being developed to stump investigation by erasing or scrambling traces of wrongdoing.

This trend will continue to accelerate and there will continue to be an uneasy balance between the two sides, with lots of collateral damage. In most cases, people will continue to forget to hide or cover all of their tracks and there will still usually be evidence to find. Over recent years, computers have penetrated almost every area of business and arsenal life. Its resources for organizations are available 24 hours a day and enable electronic business activities between clients, other organizations or state administration during which important data is exchanged.

A negative consequence for such development in technology and society is the increasing number of mobile devices, portable and desktop computers and servers from which information may leak, or which may even be used for criminal activities - whether done by malicious employees of the organization or other malicious individuals. Thus it is important hat all those who manage or administer information systems and networks be familiar with the

protocols foreseen in case of security incidents together with the principles of computer forensics.

Here we explain the requirements for the implementation of computer forensics in a business environment in an efficient and legal way. Keywords: security incidents, computer safety, data collection and analysis, security policies, legal framework 1 . Security incidents The protection of vital IT resources requires not only the implementation of cautionary measures and security policies aimed at their protection but also the usability of a quick and efficient reaction, should such security incidents occur. However, it is not easy to respond to security incidents.

The appropriate answer to the security incident requires technical knowledge as well as communication and coordination between the staff responsible for intervention. Within organizations, often the system and network administrators are the first to face such an incident and are also the first responders, so it is essential that they know the basic areas of computer forensics and the procedures they have to take care of during interventions on the compromised computer system or network. Adequately to incidents, it is necessary to be able to recognize them.

In the following text there is a list and explanation of security incidents for which the correct response is to use computer forensics methods. Attack by malicious programs Malicious programs are called viruses, Trojan horses, worms and scripts by which malicious users obtain permission from the organization computers or computer networks, to obtain possession of authorized users" passwords or to change log files for the purpose of hiding

unauthorized activity. Malicious programs that are programmed to hide their presence create great problems as their presence on the computer is very hard to discover.

Besides this, malicious programs such as viruses or worms have the possibility of multiplying in great numbers, so stopping their spreading is quite a challenging Job to be undertaken. Unauthorized access: Unauthorized access includes a set of security incidents, starting from irregular user log-in within the system itself. In the case when a malicious user logs into the system with the surname and password of an organization employee, to the unauthorized access of a malicious user to files and directories situated on local or network disks users which are transferred through the network, and use them for further malicious activities.

Malicious use of the service: Entering into possession of information within the organization can be achieved by abusing the server and programs that provide the service using the security failures within them. Examples of this are the abuse of web or FTP server services - by taking over control, the malicious user can enter inappropriate content and use the server for their further distribution. Inappropriate usage of information resources:

It can be said that the inappropriate usage of information resources is using the information resource for purposes not determined by security policies, such as using the official computer for saving inappropriate (e. G. Pirate) software. Spying: Confidential information of organizations and state administration bodies can be of great value to other organizations and governments, so intrusion into information systems for the purpose of spying

and stealing information is a serious security incident. Hoaxes: Hoaxes refer to the spreading of false information regarding the presence of security errors in programs.

Users are misled by false information and alerted to particular false threats and on occasion are also asked to delete important programs on the computer they are working on, thus causing damage. 2. Organizational policies, security and computer forensics: Implementing adequate tools and security policies and enabling computer forensics when necessary, helps organizations to create integrity and sustainability of their infrastructure. It is important that each organization consider computer forensics as a new basic element in the so-called defense in-depth " strategy to insure the computers and network infrastructure of he organization.

Shows the international framework of organizational structures that enables a more rapid undertaking of investigations in the case of security incidents and a higher quality of electronic evidence. During these procedures, employees are exposed to multiple authorities and must, as well as laws respect all organizational and security policies established on the basis of the mission and targets of the organization, and which, in turn, they must reconcile with the legal regulations. The wider definition of the aim of computer security is to ensure that the system unction as defined by the security policies.

The purpose of computer forensics is to discover and explain how a particular security policy has been breached. Policies in the implementation of computer systems security and forensics: There is a specific overlap

between the data that is necessary for computer systems security and that which can be used for computer forensics. Many security measures, if implemented completely, facilitate computer forensics: Event logs, computer systems access logs, error logs, traces of attempts to access computers, etc. Re Just some of these. Countermeasures for unauthorized access to the computer, such as smart cards for access to the computer itself, security policies for the complexity of passwords or a limited number of unsuccessful logins, together with the policy of registering the unsuccessful login, leave traces for further analysis. Nevertheless, in practice, only minimal measures of recording are used, because of the influence they could have on the system performances.

Files with event logs have configured fixed sizes in order to avoid filling up the disk space, whilst the logic of recording within them is forensics investigation is lost. Numerous security countermeasures are based on cleaning the computer system of data which is unnecessary for normal operation, such as deleting the history of web pages which have been viewed, in addition to temporary files. Procedures for accelerating system performance can also delete forensic data.

One of these procedures is disk differentiation, by which data on the disk is reorganized and disk content is overwritten in spaces where incompletely deleted files may be situated. Antivirus programs, when performing automatic virus cleaning, may also effect data, so it is important that all automatic activities are corded in files with event logs and when viruses are found, that they are not deleted, but put, e. G. into quarantine". Managing

security risks and estimating security threats are generally effective in protecting the computer system.

However, as the majority of organizations are focused on prevention and system performance rather than on enabling procedures of computer forensics, it is more than obvious that due to this, data collected in the case of security incidents will be either incomplete or there will be no collected data. Therefore, it is necessary to determine leslies within the organization by which the system will work optimally and all security policies needed for the implementation of computer forensic procedures in cases of security incidents will be implemented. . Important legal frameworks necessary for computer forensics: Nowadays people are more and more conscious of protecting their privacy. However, the protection of Applicable law and regulations Organizational policy Computer security policy Computer security enforcement Users Organizational mission and objectives Company operations Privacy and resolving security incidents or computer crimes are two almost inflicting activities.

Legal implementation agencies have to have access to as much of the data as possible stored in an electronic form, such as for Internet banking, a list of telephone calls, electronic mail, internet connections, etc. Whilst citizens are concerned about the abuse of their private data and privacy. So, one part of the law takes care of the protection of privacy and private data, whilst the other part of legislation consists of laws punishing the computer criminal and determining punishments for those who provoke security incidents.