A

Seminar report

On

Computer Forensics

Submitted in partial fulfillment of the requirement for the award of degree
Of CSE

www.studymafia.org

SUBMITTED TO:

www.studymafia.org

SUBMITTED BY:

www.studymafia.org

Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

www.studymafia.org

Preface

I have made this report file on the topic **Computer Forensics;** I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

www.studymafia.org

1. INTRODUCTION

1.1 COMPUTER FORENSICS

"Forensic computing is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable."(Rodney Mckemmish 1999).
From the above definition we can clearly identify four components:-

IDENTIFYING

This is the process of identifying things such as what evidence is present, where and how it is stored, and which operating system is being used. From this information the investigator can identify the appropriate recovery methodologies, and the tools to be used.

PRESERVING

This is the process of preserving the integrity of digital evidence, ensuring the chain of custody is not broken. The data needs to preserved (copied) on stable media such as CD-ROM, using reproducible methodologies. All steps taken to capture the data must be documented. Any changes to the evidence should be documented, including what the change was and the reason for the change. You may need to prove the integrity of the data in the court of law.

ANALYSING

This is the process of reviewing and examining the data. The advantage of copying this data onto CD-ROMs is the fact it can be viewed without the risk of accidental changes, therefore maintaining the integrity whilst examining the changes

PRESENTING

This is the process of presenting the evidence in a legally acceptable and understandable manner. If the matter is presented in court the jury who may have little or no computer experience, must all be able to understand what is presented and how it relates to the original, otherwise all efforts could be futile.

Far more information is retained on the computer than most people realize. Its also more difficult to completely remove information than is generally thought. For these reasons (and many more), computer forensics can often find evidence or even completely recover, lost or deleted information, even if the information was intentionally deleted.

www.studymafia.org

The goal of computer forensics is to retrieve the data and interpret as much information about it as possible as compared to data recovery where the goal is to retrieve the lost data.

1.2 WHAT IS COMPUTER FORENSICS?

Computer forensics is simply the application of disciplined investigative techniques in the automated environment and the search, discovery, and analysis of potential evidence. It is the method used to investigate and analyze data maintained on or retrieved from electronic data storage media for the purposes of presentation in a court of law, civil or administrative proceeding. Evidence may be sought in a wide range of computer crime or misuse cases. Computer forensics is rapidly becoming a science recognized on a par with other forensic sciences by the legal and law enforcement communities. As this trend continues, it will become even more important to handle and examine computer evidence properly. Not every department or organization has the resources to have trained computer forensic specialists on staff.

1.3 History of Computer Forensics

Michael Anderson

- ⇨ "Father of computer forensics"
- ⇨ special agent with IRS

Meeting in 1988 (Portland, Oregon)

- ⇨ creation of IACIS, the International Association of Computer Investigative Specialists
- ⇨ the first Seized Computer Evidence Recovery Specialists (SCERS) classes held

www.studymafia.org

2. NEED FOR COMPUTER FORENSICS

2.1 Purpose

The purpose of computer forensics is mainly due to the wide variety of computer crimes that take place. In the present technological advancements it is common for every organization to employ the services of the computer forensics experts. There are various computer crimes that occur on small scale as well as large scale. The loss caused is dependent upon the sensitivity of the computer data or the information for which the crime has been committed.

The computer forensics has become vital in the corporate world. There can be theft of the data from an organization in which case the organization may sustain heavy losses. For this purpose computer forensics are used as they help in tracking the criminal.

The need in the present age can be considered as much severe due to the internet advancements and the dependency on the internet. The people that gain access to the computer systems with out proper authorization should be dealt in. The network security is an important issue related to the computer world. The computer forensics is a threat against the wrong doers and the people with the negative mindsets.

The computer forensics is also efficient where in the data is stored in a single system for the backup. The data theft and the intentional damage of the data in a single system can also be minimized with the computer forensics. There are hardware and software that employ the security measures in order to track the changes and the updating of the data or the information. The user information is provided in the log files that can be effectively used to produce the evidence in case of any crime a legal manner.

The main purpose of the computer forensics is to produce evidence in the court that can lead to the punishment of the actual. The forensic science is actually the process of utilizing the scientific knowledge for the purpose of collection, analysis, and most importantly the presentation of the evidence in the court of law. The word forensic itself means to bring to the court.

The need or the importance of the computer forensics is to ensure the integrity of the computer system. The system with some small measures can avoid the cost of operating and maintaining the security. The subject provides in depth knowledge for the understanding of the legal as well as the technical aspects of computer crime. It is very much useful from a technical stand point, view.

The importance of computer forensics is evident in tracking the cases of the child pornography and email spamming. The computer forensics has been efficiently used to track down the terrorists from the various parts of the world. The terrorists using the internet as the medium of communication can be tracked down and their plans can be known.

www.studymafia.org

There are many tools that can be used in combination with the computer forensics to find out the geographical information and the hide outs of the criminals. The IP address plays an important role to find out the geographical position of the terrorists. The security personnel deploy the effective measures using the computer forensics. The Intrusion Detecting Systems are used for that purpose.

2.2 Why is Computer Forensics Important?

Adding the ability to practice sound computer forensics will help you ensure the overall integrity and survivability of your network infrastructure. You can help your organization if you consider computer forensics as a new basic element in what is known as a "defense-in-depth"1 approach to network and computer security. For instance, understanding the legal and technical aspects of computer forensics will help you capture vital information if your network is compromised and will help you prosecute the case if the intruder is caught.
Two basic types of data are collected in computer forensics.

(a) Persistent data
(b) Volatile data.

2.3 Computer forensics helps the organization in the following way:-

- RECOVER DATA THAT YOU THOUGHT WAS LOST FOREVER:-
  Computers systems may crash, files may be accidentally deleted, disks may accidentally be reformatted, viruses may corrupt files, file may be accidentally overwritten, disgruntled employees may try to destroy your files. All of this can lead to loss of your critical data, but computer forensic experts should be able to employ the latest tools and techniques to recover your data.

- ADVICE YOU ON HOW TO KEEP YOUR DATA AND INFORMATION SAFE FROM THEFT OR ACCIDENTAL LOSS:-
  Business today relies on computers. Your sensitive records and trade secrets are vulnerable to intentional attacks from, for e.g. hackers, disgruntled employees, viruses, etc. also unintentional loss of data due to accidental deletion, h/w or s/w crashes are equally threatening. Computer forensic experts can advice you on how to safeguard your data by methods such as encryption and back-up.

www.studymafia.org

- EXAMINE A COMPUTER TO FIND OUT WHAT ITS USER HAS BEEN DOING:-

  Whether you're looking for evidence in a criminal prosecution, looking for evidence in a civil suit, or determining exactly what an employee has been up to. Your computer forensics expert should be equipped to find and interpret the clues left behind.

- SWEEP YOUR OFFICE FOR LISTNENING DEVICES:-

  There are various micro-miniature recording and transmitting devices available in todays hi-tech world. The computer forensic expert should be equipped to conduct thorough electronic countermeasure (ECM) sweeps of your premises.

- HI-TECH INVESTIGATION:-

  The forensic expert should have the knowledge and the experience to conduct hi-tech investigations involving cellular cloning, cellular subscription fraud, s/w piracy, data or information theft, trade secrets, computer crimes, misuse of computers by employees, or any other technology issue.

2.4 Advantage of Computer Forensics:-

The main task or the advantage from the computer forensic is to catch the culprit or the criminal who is involved in the crime related to the computers.

Computer Forensics deals extensively to find the evidence in order to prove the crime and the culprit behind it in a court of law. The forensics provides the organization with a support and helps them recover their loss.

The important thing and the major advantage regarding the computer forensics is the preservation of the evidence that is collected during the process. The protection of evidence can be considered as critical.

The ethicality can be considered as an advantage of the forensics in computer systems. At last the computer forensics has emerged as important part in the disaster recovery management

www.studymafia.org

3. COMPUTER FORENSIC METHODOLOGY

3.1 Methods Used:-

According to many professionals, Computer Forensics is a four (4) step process

Acquisition

Physically or remotely obtaining possession of the computer, all network mappings from the system, and external physical storage devices.

Identification

This step involves identifying what data could be recovered and electronically retrieving it by running various Computer Forensic tools and software suites.

Evaluation

Evaluating the information/data recovered to determine if and how it could be used againthesuspect for employment termination or prosecution in court.

Presentation

This step involves the presentation of evidence discovered in a manner which is understood by lawyers, non-technically staff/management, and suitable as evidence as determined by United States and internal laws

3.2 COMPUTER FORENSIC PROCESS:-

As in any investigation, establishing that an incident has occurred is the first key step. Secondly, the incident needs to be evaluated to determine if computer forensics may be required. Generally, if the computer incident resulted in a loss of time or money, or the destruction or compromise of information, it will require the application of computer forensic investigative techniques. When applied, the preservation of evidence is the first rule in the process. Failure to preserve evidence in its original state could jeopardize the entire investigation. Knowledge of how the crime was initiated and committed may be lost for good. Assignment of responsibility may not be possible if evidence is not meticulously and diligently preserved. The level of training and expertise required to execute a forensics task will largely depend on the level of evidence required in the case. If the result of the investigation were limited to administrative actions against an employee, the requirement would be lower than taking the case to court for civil or criminal litigation.

3.3 Approach to retrieve the evidence:-

www.studymafia.org

The following steps should be taken:-

3.3.1 Shut Down the Computer

Depending upon the computer operating system involved, this usually involves pulling the plug or shutting down a net work computer using relevant operating system commands. At the option of the computer specialists, pictures of the screen image can be taken using a camera. However, **consideration should be given to possible destructive processes that may be operating in the background.** These can be resident in memory or available through a modem or network connection. Depending upon the operating system involved, a time delayed password protected screen saver may potentially kick in at any moment. This can complicate the shutdown of the computer. Generally, time is of the essence and the computer system should be shut down or powered down as quickly as possible.

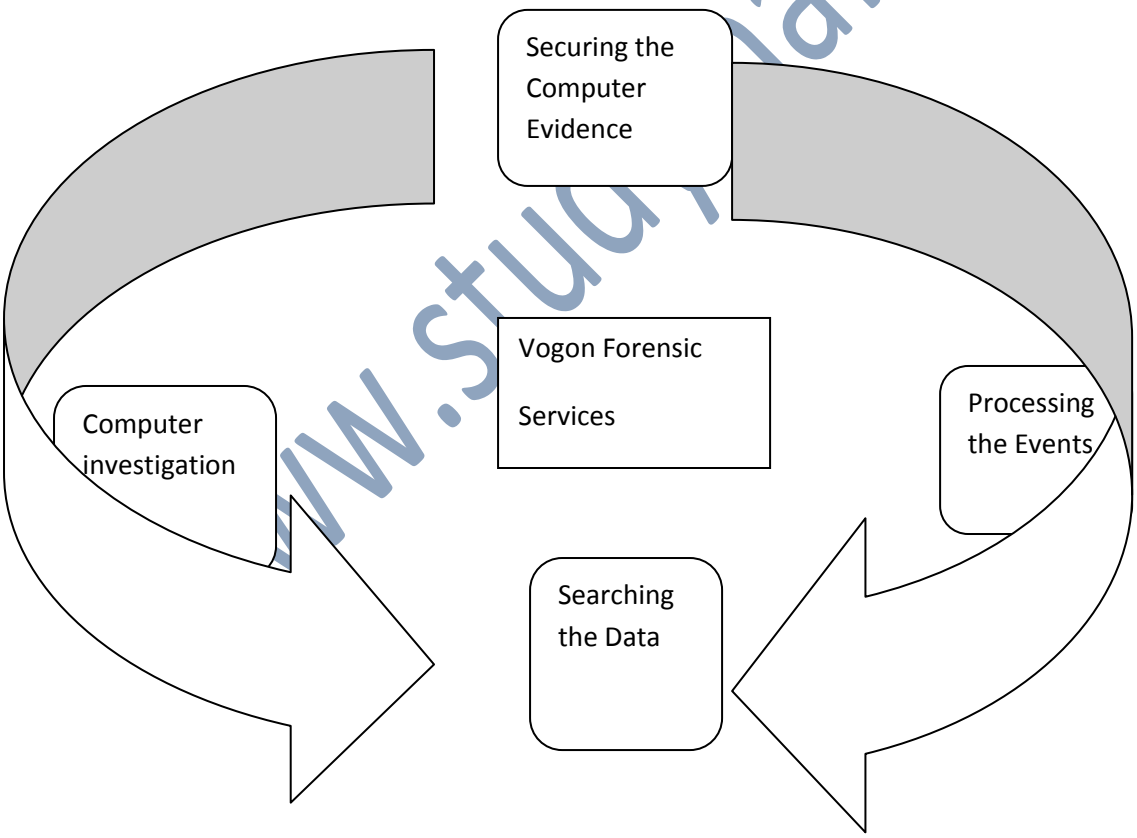

Figure 3.1 Vogon

www.studymafia.org

3.3.2Document the Hardware Configuration of the System

It is assumed that the computer system will be moved to a secure location where a proper chain of custody can be maintained and the processing of evidence can begin. Before dismantling the computer, it is important that pictures are taken of the computer from all angles to document the system hardware components and how they are connected. Labeling each wire is also important so that the original computer configuration can be restored. Computer evidence should ideally be processed in a computer hardware environment that is identical to the original hardware configuration.

3.3.3 Transport the Computer System to A Secure Location

This may seem basic but all too often seized evidence computers are stored in less than secure locations. It is imperative that the subject computer is treated as evidence and it should be stored out of reach of curious computer users. All too often, individuals operate seized computers without knowing that they are destroying potential computer evidence and the chain of custody. Furthermore, a seized computer left unintended can easily be compromised. Evidence can be planted on it and crucial evidence can be intentionally destroyed. A lack of a proper chain of custody can 'make the day' for a savvy defense attorney. Lacking a proper chain of custody, how can you say that relevant evidence was not planted on the computer after the seizure? The answer is that you cannot. **Do not leave the computer unattended unless it is locked in a secure location!** NTI provides a program named Seized to law enforcement computer specialists free of charge. It is also made available to NTI's business and government in various suites of software that are available for purchase. The program is simple but very effective in locking the seized computer and warning the computer operator that the computer contains evidence and should not be operated

www.studymafia.org

3.3.4 Make Bit Stream Backups of Hard Disks and Floppy Disks

The computer should not be operated and computer evidence should not be processed until bit stream backups have been made of all hard disk drives and floppy disks. All evidence processing should be done on a restored copy of the bit stream backup rather than on the original computer. The original evidence should be left untouched unless compelling circumstances exist. Preservation of computer evidence is vitally important. It is fragile and can easily be altered or destroyed. Often such alteration or destruction of data is irreversible. Bit stream backups are much like an insurance policy and they are essential for any serious computer evidence processing.

3.3.5 Mathematically Authenticate Data on All Storage Devices

You want to be able to prove that you did not alter any of the evidence after the computer came into your possession. Such proof will help you rebut allegations that you changed or altered the original evidence. Since 1989, law enforcement and military agencies have used a 32 bit mathematical process to do the authentication process. Mathematically, a 32 bit data validation is accurate to approximately one in 4.3 billion. However, given the speed of today's computers and the vast amount of storage capacity on today's computer hard disk drives, this level of accuracy is no longer accurate enough. A 32 bit CRC can easily be compromised. Therefore, NTI includes two programs in its forensic suites of tools that mathematically authenticate data with a high level of accuracy. Large hashing number, provides a mathematical level of accuracy that is beyond question. These programs are used to authenticate data at both a physical level and a logical level. The programs are called CrcMD5 and DiskSig Pro. The latter program was specifically designed to validate a restored bit stream backup and it is made available free of charge to law enforcement computer specialists as part of NTI's Free Law Enforcement Suite. The programs are also included in our various suites of forensic software which are sold NTI's clients.

3.3.6 Document the System Date and Time

The dates and times associated with computer files can be extremely important from an evidence standpoint. However, the accuracy of the dates and times is just as important. If the system clock is one hour slow because of daylight-saving time, then file time stamps will also reflect the wrong time. To adjust for these inaccuracies,

www.studymafia.org

documenting the system date and time settings at the time the computer is taken into evidence is essential.

3.3.7 Make a List of Key Search Words

Because modern hard disk drives are so voluminous, it is all but impossible for a computer specialist to manually view and evaluate every file on a computer hard disk drive. Therefore, state-of-the-art automated forensic text search tools are needed to help find the relevant evidence.

3.3.8 Evaluate the Windows Swap File

The Windows swap file is potentially a valuable source of evidence and leads. The evaluation of the swap file can be automated with several of NTI's forensic tools, e.g., NTA Stealth, Filter_N, FNames, Filter_G, GExtract and GetHTML. These intelligent filters automatically identifies patterns of English language text, phone numbers, social security numbers, credit card numbers, Internet E-Mail addresses, Internet web addresses and names of people.

3.3.9 Evaluate File Slack

File slack is a data storage area of which most computer users are unaware. It is a source of significant 'security leakage' and consists of raw memory dumps that occur during the work session as files are closed. The data dumped from memory ends up being stored at the end of allocated files, beyond the reach or the view of the computer user. Specialized forensic tools are required to view and evaluate file slack and it can prove to provide a wealth of information and investigative leads. Like the Windows swap file, this source of ambient data can help provide relevant key words and leads that may have previously been unknown.

3.3.10 Evaluate Unallocated Space (Erased Files)

The DOS and Windows 'delete' function does not completely erase file names or file content. Many computer users are unaware the storage space associated with such files merely becomes unallocated and available to be overwritten with new files. Unallocated space is a source of significant 'security leakage' and it potentially contains erased files and file slack associated with the erased files. Often the DOS Undelete program can be used to restore the previously erased files. Like the

www.studymafia.org

Windows swap file and file slack, this source of ambient data can help provide relevant key words and leads that may have previously been unknown to the computer investigator.

3.3.11 Search Files, File Slack and Unallocated Space for Key Words

The list of relevant key words identified in the previous steps should be used to search all relevant computer hard disk drives and floppy diskettes. There are several forensic text search utilities available in the marketplace. NTI's forensic search TextSearch NT can be used for that purpose and it has been tested and certified for accuracy by the U.S. Department of Defense. This powerful search tool is also included as part of NTI's suites of software tools.

3.3.12 Document File Names, Dates and Times

From an evidence standpoint, file names, creation dates, last modified dates and times can be relevant. Therefore, it is important to catalog all allocated and 'erased' files. NTI includes a program called File List Pro in its various suites of forensic tools. The File List Pro program generates its output in the form of a database file. The file can be sorted based on the file name, file size, file content, creation date, last modified date and time. Such sorted information can provide a timeline of computer usage.

3.3.13 Identify File, Program and Storage Anomalies

Encrypted, compressed and graphic files store data in binary format. As a result, text data stored in these file formats cannot be identified by a text search program. Manual evaluation of these files is required and in the case of encrypted files, much work may be involved. NTI's TextSearch Plus program has built in features that automatically identify the most common compressed and graphic file formats. The use of this feature will help identify files that require detailed manual evaluation. Depending on the type of file involved, the contents should be viewed and evaluated for its potential as evidence.

3.3.14 Evaluate Program Functionality

Depending on the application software involved, running programs to learn their purpose may be necessary. NTI's training courses make this point by exposing the students to computer applications that do more than the anticipated task. When destructive processes are discovered that are tied to relevant evidence, this can be

www.studymafia.org

used to prove willfulness. Such destructive processes can be tied to 'hot keys' or the execution of common operating commands tied to the operating system or applications. Before and after comparisons can be made using the FileList Pro program and/or mathematical authentication programs. All these tools are included in most of NTI's suites of forensic tools

3.3.15 Document Your Findings

As indicated in the preceding steps, it is important to document your findings as issues are identified and as evidence is found. Documenting all of the software used in your forensic evaluation of the evidence including the version numbers of the programs used is also important. Be sure that you are legally licensed to use the forensic software

www.studymafia.org

4. COMPUTER FORENSIC TECHNOLOGY

Computer forensics tools and techniques have proven to be a valuable resource for law enforcement in the identification of leads and in the processing of computer-related evidence. Computer forensic tools and techniques have become important resources for use in internal investigations, civil law suits, and computer security risk management.

Forensic S/w tools and methods can be used to identify passwords, logons, and other information that is automatically dumped from the computer memory. Such forensic tools can be used to tie a diskette to the computer that created it. Some of the tools used are as follows:-

4.1 Get Free - Forensic Data Capture Tool:-

When files are 'deleted' in DOS, Windows, Windows95 and Windows 98, the data associated with the file is not actually eliminated. It is simply reassigned to unallocated storage space where it may eventually be overwritten by the creation of new files over time. Such data can provide the computer forensics investigator with valuable leads and evidence. However, the same data can create a significant security risk when sensitive data has been erased using DOS, Windows, Windows 95 and Windows 98 file deletion procedures and commands.

GetFree software is used to capture all of the unallocated file space on DOS, Windows, Windows 95 and Windows 98 based computer systems. The program can be used to identify leads and evidence. It is also effectively used to validate the secure Scrubbing of unallocated storage space with programs like NTI's M-Sweep ambient data deletion software.

www.studymafia.org

When GetFree software is used as an investigative tool, it eliminates the need to restore potentially hundreds or thousands of files on computer hard disk drives and floppy diskettes. The software was primarily developed as a computer forensic tool for use in computer related investigations and internal audits. However, GetFree has also proven to be an ideal tool for use in computer security risk assessments because the software automatically captures the data associated with unallocated file space. Such data can be reviewed and analyzed using other NTI forensic tools, e.g., Filter_I, Net Threat Analyzer and Graphics Image File Extractor.

GetFree Software - Primary Uses:

- Calculates the amount of unallocated storage space on a computer storage device.
- Automatically captures all logical unallocated storage space on one or more computer hard disk drives and floppy diskettes.
- Captures the contents of a dynamic Windows swap file for analysis with other tools.
- Used in internal audits, security reviews and computer-related investigations.
- Validates the effectiveness of computer security data scrubbers.
- Identifies classified data spills in unallocated data storage areas.
- Identifies violations of company policy through the identification of sensitive data leakage into unallocated storage space.
- Used very effectively with NTI's Image File Extractor in investigations involving computer generated graphic file images, e.g., child pornography investigations.

GetFree - Program Features and Benefits:

- DOS-based for speed and ease of use.
- Compact program size easily fits on one floppy diskette with other forensic software tools.
- Non-printable characters (ASCII values 0-31 and non ASCII values 127-255) are replaced by a space character, at the option of the user.
- Does not alter any data on the target computer and can therefore be operated covertly.

www.studymafia.org

- Captures unallocated clusters marked as bad (by a user or the operating system) in the event that sensitive data is stored in sectors associated with such clusters.

- Compatible with DOS, Windows 3.x, Windows 95 and Windows 98.

- Estimates the output storage space needed for the data capture prior to use.

- Processes more than one logical drive in one work session.

- Automatically increments the output file names and prompts the user for additional removable media in the event additional storage space is needed in achieving the data capture.

- Supports 12 bit, 16 bit and 32 bit FAT types (32-bit FATs).

- If 32 bit FAT (FAT32) file systems are involved, GetFree should be run with a FAT 32 aware version of DOS, e.g., DOS 7x.

- Automatically creates output files which are less that 2 gigabytes in capacity. This aids in the analysis of the output files and avoids the 2 gigabyte DOS file limitations.

4.2 Get Slack - Forensic Data Capture Utility:-

This software is used to capture all of the file slack contained on a logical hard disk drive or floppy diskette on a DOS, Windows, Windows 95 and/or Windows 98 computer system. The resulting output from GetSlack can be analyzed with standard computer utilities or with special NTI tools, e.g., Filter_I and Net Threat Analyzer software. GetSlack software is an ideal computer forensics tool for use in investigations, internal audits and in computer security reviews. NTI places special importance on the use of this tool in computer security risk assessments because memory dumps in file slack are the cause for security related concerns. Typically, network logons and passwords are found in file slack. It is also possible for passwords used in file encryption to be stored as memory dumps in file slack.

From an investigative standpoint, file slack is a target rich environment to find lead sand evidence. File slack can contain leads and evidence in the form of fragments of word processing communications, Internet E-mail communications, Internet chat room communications, Internet news group communications and Internet browsing

www.studymafia.org

activity. As a result, this program is a good tool for use in computer related investigations. It also acts as a good validation tool for use with computer security programs which are designed to eliminate file slack, e.g., NTI's M-Sweep ambient data scrubbing software.

GetSlack Software - Primary Uses:

- Quickly calculates the amount of storage space which is allocated to file slack on a logical DOS/Windows partition.
- Captures all file slack on a logical DOS/Windows drive and converts it into one or more files automatically.
- Used in covert and overt internal audits, computer security reviews and computer investigations.
- Validates the results of computer security scrubbers used to eliminate sensitive or classified data from file slack on computer storage devices.

GetSlack Software - Program Features and Benefits:

- DOS based for speed.
- Compact program size easily fits on a single floppy diskette with other forensic software tools.
- At the option of the user, non-printable characters (ASCII values 0-31 and127-255) can be replaced with space characters.
- Does not alter or modify the data stored on the target computer.
- Does not leave any trace of operation. Therefore, it can be used coverly when laws permit such use.
- Does not alter evidence on the target drive. Therefore, this tool is ideal for the processing of computer evidence.
- Compatible with DOS, Windows 3.x, Windows 95 and Windows 98.
- Estimates the output file space needed prior to use.
- Multiple logical storage devices can be specified in one operating session.
- Configures the output files to fit on one or more removable storage devices depending on the volume of the computed output.
- Supports 12 bit, 16 bit and 32 bit FAT types (32-bit FATs are currently found on Windows 95B/98/OSR2/NT).

www.studymafia.org

4.3 DiskScrub - Hard Drive Data Elimination Software:-

It is becoming standard practice in corporations, government agencies, law firms and accounting firms to reassign computers and to donate older computers to charity. Millions of personal computers have been put to use since 1981 when the IBM Personal Computer came into existence. Many of the older personal computers have been reassigned or donated to charity and many more will fall into this category in the future. However, data security is often ignored when computers change hands.

You must be aware that personal computers were never designed with security in mind. Potentially anything that transpired on a used computer still exists. Multiply that by the number of computers your organization will reassign or surplus this year, and you get the point. Computers should be reassigned and donated to charity but the contents of the hard disk drives should not be ignored.

With computer technology changing almost daily, corporations and government agencies have to stay current while still making the best uses of aging computer resources. Advancements in hard disk drive storage capacities, operating systems and software applications cause corporations to buy or lease new computers every year. But what is done with the old computers? What is done about the sensitive data still existing, essentially "stored" on these computers when they are sold, transferred or donated? That is a serious problem, and NTI's Disk Scrub software was specifically designed to deal with these risks, for corporations, government agencies, hospitals, financial institutions, law firms and accounting firms.

4.4 Forensic Graphics File Extractor:-

NTI's Forensic Graphics Image File Extractor is a computer forensics software tool which was designed to automatically extract exact copies of graphics file images from ambient data sources and from SafeBack bit stream image backup files. The latter process has the potential of quickly identifying all graphics file images stored on a computers hard disk drive. The resulting output image files can be quickly evaluated using a graphics file viewer, e.g., Firehand Ember Millennium by Firehand Technologies which NTI recommends. Firehand Ember Millennium fits limited law enforcement budgets, e.g., priced at under $50 and it is an ideal product for investigations involving computer graphic images.

NTI’s Image File Extractor software was developed with our law enforcement friends in mind and it has been priced accordingly. Law enforcement computer crime specialists spend much of their valuable time in the investigation of computer crimes involving the possession and distribution of graphic image files which involve child pornography. This computer forensics tool saves time and it was specifically created to accurately and quickly reconstruct evidence grade copies of "deleted" image files.

www.studymafia.org

The software can also be used effectively to identify and reconstruct residual graphics file images which passed through Windows Swap and Windows Page files during Internet web browsing sessions. An "after the fact" analysis of such files can quickly determine how a computer may have been used. Such information is invaluable to corporate investigators and law enforcement computer crime specialists alike. NTI's Graphics Image File Extractor also provides benefits in internal audits involving them issues of corporate computers by employees and corporate due diligence reviews of computers.

Forensic Graphics File Extractor - Primary Uses:

- Used to find evidence in corporate, civil and criminal investigations which involve computer graphics files, e.g., investigations which potentially involve child pornography and/or inappropriate Internet web browsing in a corporate or government setting.
- Used with other computer forensic software to quickly reconstruct previously deleted BMP, GIF and JPEG graphics files stored on computer storage media.
- Used to quickly identify and preview BMP, GIF and JPEG image files stored on a computer hard disk drive when used with SafeBack and Firehand Embers.
- Used effectively in computer investigations involving the distribution of child pornography.
- Used "after the fact" to determine what files may have been viewed over or downloaded from the Internet.
- Used very effectively with NTI's GetFree software this can be purchased separately.

Forensic Graphics File Extractor - Program Features and Benefits:

- Operates under DOS/WIN9x/WINNT/WIN2000/WINXP for ease of operation and speed.
- Compact program size which easily fits on one floppy diskette with other forensic software utilities for portability.
- Searches a targeted Windows Swap File or a file created from erased file space for patterns of BMP, GIF and JPG file images and it reconstructs partial or complete image files in one highly accurate operation. The accuracy of this process is dependent upon the degree of fragmentation involved, etc.
- When complete image files are identified and reconstructed by the program the output of restored graphics images files is exact. Our tests indicate that a majority of reconstructed files will pass a CRCMD5 hash test when restored

www.studymafia.org

image files are compared with the original files prior to deletion. This feature makes the software ideal for evidence reconstruction in criminal cases. It also allows for the exact reconstruction of graphics image files which may contain hidden files or other messages through the use of steganography.

- Partial image file patterns (caused due to fragmentation and/or file corruption) can be automatically reconstructed and viewed.
- The highly accurate graphics file identification search engine ensures that every byte is checked for integrity.
- The software operates in batch file mode for automatic processing when combined with other NTI software processes.
- It automatically creates a complete log of the processing steps taken by the program to aid in expert witness testimony.
- Priced to easily fit limited law enforcement budgets.
- Operation of the software is easy and is not hampered by hardware anti-theft software protection.
- Free Upgrades for one year from the date of purchase.
- Quantity discounts are available.

www.studymafia.org

5. REQUIRMENTS AND ANALYSIS

5.1 The Tools:-

The tools developed perform the following functions:

- Analysing a hard disk and detecting HPAs, DCOs and bad sectors with a reasonable degree of accuracy
- Creating a bit stream image of a hard disk and verifying the copy
- Mapping the systems logical partitions and locating hidden data with a reasonable degree of accuracy.
- Locating file contained in a file system, recovering deleted file where possible, and recon-structing fragmented files.
- Displaying the contents of an encrypted file (where possible) and at least identify that the file is encrypted,
- Reconstructing computer events which occurred before a crime was committed.
- Detecting the use of steganographic methods, with reasonable accuracy, and extracting the data hidden using those methods.

5.1.1 Partition Analysis:-

Once an image has been acquired it is then necessary to find and recover deleted (and undeleted) files. However these files will be contained inside a file system so it is obviously necessary to find the file system before this can happen. File systems, on most systems, are contained inside partitions of which there may be several so the first step is to be able to analyse the partitioning formation. This is why the next tool to be developed will be a partition analysis tool.
The first, and most obvious, requirement of the partition analysis tool is that it must be able to map the partitions and present the information to the user. However the partition table (for many systems) is contained inside the first sector of the disk, therefore it will be necessary for the tool to know how many bytes are in a sector so that it knows how many bytes to read. This information will have been gathered and stored by the disk imaging tool so the first step of analyzing a partition will be to parse the disk information file to find the information required for the analysis. It will also be necessary to find the size of the disk from this file for use when finding slack space.
During a computer forensics investigation every procedure and result must be well documented. The tool should therefore also be able to store the partition information

www.studymafia.org

in a log file along with the date and time the analysis was carried out. When presenting the information to the user it might be helpful to display the information in a diagram to make the data easier to understand although this isn't a critical requirement.

The tool must be able to detect volume and partition slack, record the location of this slack space and record this information in the appropriate log file along with the reason for identifying it as slack space. This reason would consist of the total size of the partitions in the volume compared to the total size of the volume.

There may be occasions when one or more of the partition tables are corrupted and can't be used. The tool should be able to identify that some of the tables are unusable, make a note of which tables are missing, and then recover the partition information using other methods such as searching for known signatures. In the literature review I mentioned that searching for signatures often yields many false results. The tool should make a note of all the results in the appropriate log and then filter out the results which are definitely false, again noting these results in the log along with reasons why they're false. The remaining results which may be positive should be recorded in a log.

There are many different partitioning systems and MS-DOS is just one example, modern 64-bit systems and some Unix/Linux systems use completely different methods. The system being developed is simply an example system so only be initially able to analyze DOS partition systems is acceptable.

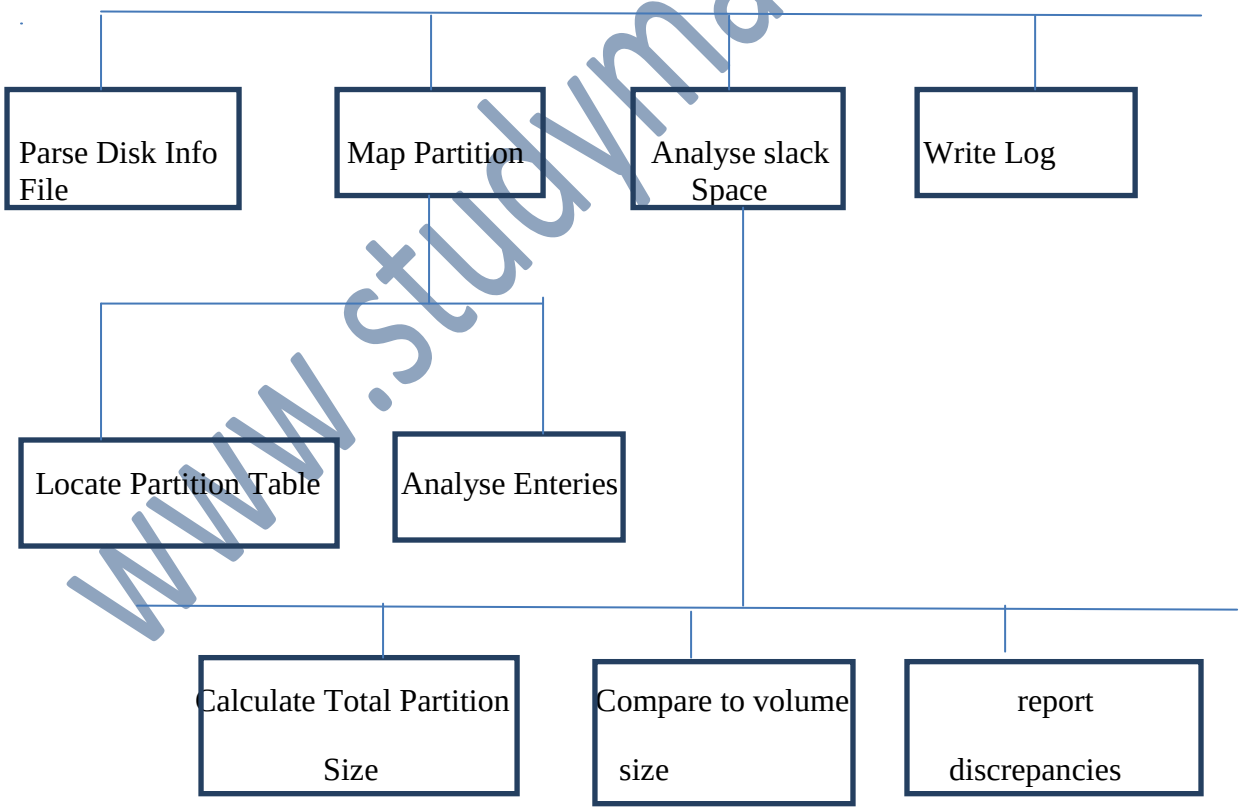

Fig 5.1.Task Hierarchy for the Partition Analysis Tool

Requirement No.			ype

www.studymafia.org

1	Get Partition Info.	The system must be able together the partition information from the specified disk image. This information must include the type and address of each partition the image contained. The gathered data should be displayed to the user if requested and also saved in a specified file.	Essential
2	Create Analysis Log.	The system should be able to create a log of the analysis highlighting why particular results were obtained.	Optional

Table 5.1. Partition Analysis Tool Requirements

5.1.2 File System Analysis:-

Now that the file systems have been found the tool should now be able to analyze them and recover files. There may be many file systems and the user may only want to analyze data from one of these file systems. Therefore the first requirement of the tool will be to parse the partition information file created by the partition analysis tool and present the user with a choice of file systems to analyze.
The initial requirement for the file system tool is to be able to record the type of file system(i.e. FAT, NTFS etc.) and the directory structure it contains for all current non-deleted files. This information should both be stored in the log file and presented to the user. Again it could be helpful if the information was presented to the user in the form of a diagram but this isn't a critical requirement as the user should be able to quite easily understand directory listings. The tool must also record basic file system information such as the number of sectors per cluster, the size of the file system and other file system specific information.
The tool must record which clusters are marked as good and which are marked as bad. The bad clusters should be analyzed for possible evidence although this will depend on the kind of information the user is searching for. In other words the tool should include bad sectors in any searches.
One problem is that many file systems, such as FAT and NTFS, store files in clusters rather than sectors and it will be necessary to identify these clusters before the files can be recovered. File system generally have data structures which contain this information along with other general file system information such as the date it was created that might be useful to an investigation. It is therefore necessary for the tool to be capable of analyzing the appropriate data structure(s) and presenting the information to a user.
Now that the basic file system information is known files containing evidence can be recovered. Whilst there has been some work on creating models for automated

www.studymafia.org

analysis of file systems some user interaction is still required. The user must be able to search the directory structure for files with names containing specified keywords or files with contents matching specified keywords. The tool must also provide the option of searching for specific file types which should be located byusing both the extension in the file name and the file's signature, although if the values don't match then the signature should be trusted rather than the extension. The details of the search should be noted in the log (i.e. the keywords, the file types searched for, the date and time of the search etc.) along with the results which will contain the file name and directory address. It is necessary to be able to search for files because a typical system could contain hundreds, or thousands, of files which may need to be analyzed in detail to determine if they can be considered as evidence. If an investigator could fully examine a text/pdf file in 30 minutes and the system contained 1000 files, many of which are irrelevant for the investigation, then it would take over 20 days to be able to gather the required evidence. Alternatively searching for files containing certain keywords is more likely to find the relevant files more quickly than manually searching.

The tool should be able to find and recover a reasonable amount of hidden data from the file system. It will do this by first identifying possible locations in which data could be hidden and then recording these locations in the log along with reasons why they were identified. One example of this might be when the number of sectors in the file system isn't divisible by the number of sectors per cluster. These locations will also be used during the searches conducted by the user.

As the data being analyzed is simply a binary file containing the disk image it will be difficult for the user to view a file's contents by just using this image file. The tool must therefore be capable of extracting the bits from the image which correspond to the file the user wants to view and place them in a file of an appropriate type, e.g. extract the bits of a jpeg image and place them into an empty jpeg file. I have managed to create a program which can place extracted bit into an empty file although it is currently necessary for the user to input the type of the file.

The tool must be capable of recovering a reasonable amount of deleted data from the system. The term reasonable is used here as some data cannot be recovered without use of specialist equipment which I won't have access to. The details of the recovered files, including their original directory address, must be stored in the log and be presented to the user. It should be noted that some of the data may have originated from other locations such as slack space or the windows swap file in which case the directory address stored would refer to these locations. The tool must allow the user to conduct the same sort of searches as with non-deleted data. It must also identify cases where data wiping software has been used and record the signature of the tool and locations which the tool has wiped.

If fragments of files are recovered then the tool should ideally be capable of reconstructing the files using various methods. However as it isn't known whether this is possible I won't make it a critical requirement.

Their are many different types of file systems (FAT, NTFS, UFS, Ext, HFS, Reiser etc.) and ideally the tool should be capable of analyzing all of them using their known data structures.

However this may not be possible in the limited time available and only an example system is being developed so limited capabilities are acceptable. I will make it a requirement that the tool is capable of analyzing FAT systems and is also capable of being expanded to support other file systems.

www.studymafia.org

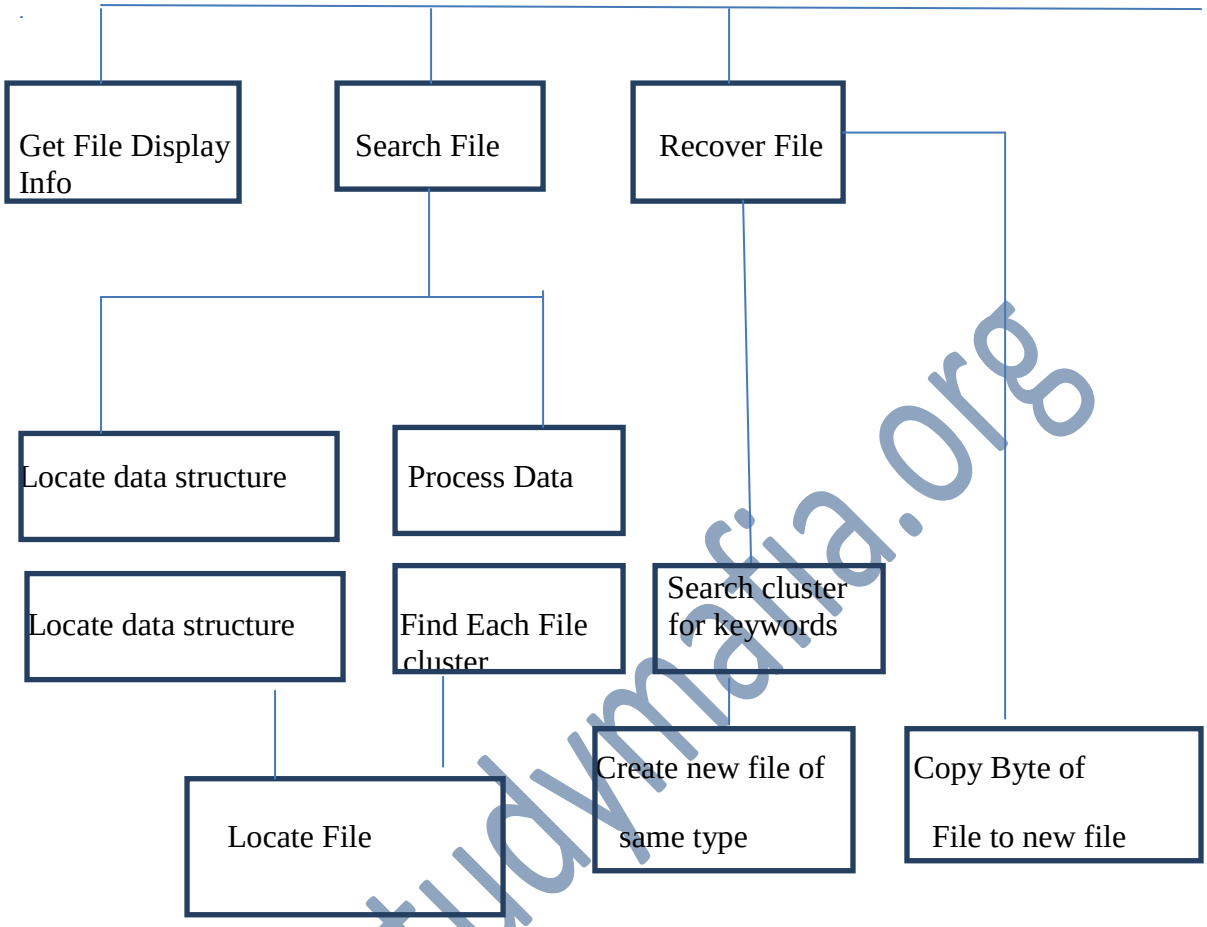

Fig5.2. Task Hierarchy for the File System Analysis Tool

www.studymafia.org

Requirement No	Name	Description	Type
1	Get File System Info	The system must be able to gather information about a specified file	Essential

		system. The file system will be chosen by the user selecting a partition after loading the partition information file already created using the previous tool. The retrieved information should be displayed to the user if requested and also saved to a specified file.	
2	Search File	The system must allow the user to search the specified file system for files whose contents contain given keywords or whose name matches the string entered. Another option must be to list all files. It should be possible to filter all searches to only include files of certain types or all deleted files etc. Results of the search must be displayed on the screen and it should also be possible to save the search criteria and results in a given file.	Essential
3	Recover File	It must be possible for a user to recover files from the image into another file on another volume (possibly thesame volume). The system must allow the user to select a file by entering its name.	Essential
4	Event Reconstruction	The system should be capable of using the accessed, modified and created times of all the files in the specified file system to create a timeline of system activity. This timeline should be easy to understood and displayed to the user if requested. The data should also be stored in a specified file.	Desirable
4	Create Analysis Log	The system should produce a log of any analysis done using the functions described above. This log will include details of the analysis performed along with the necessary time stamps and should be saved in a file specified by the user.	Optional

Table 5.2.Requirements for the File System Analysis Tool

5.1.3 General Requirements:-

By definition the whole point of computer forensics analysis is that the evidence recovered will be used in a court of law. There are various rules and procedures which

www.studymafia.org

must be followed in order for evidence to be deemed admissible. I have briefly highlighted some of these procedures in the literature survey such as verifying that an image is identical to the original disk data. Following on from this a requirement of the tools developed will be that they adhere to the appropriate procedures so that the output they produce can be used.

5.1.4 Non Functional Requirements:-

The tool kit developed will need to be portable as it could be necessary to use it on a variety of machines. For the most part I will therefore be using the Java programming language as the programs developed could be used on any machine which has the java virtual machine installed. However there will be a problem with the disk imaging tool as Java would be unable to perform the necessary low level disk access. For this tool I will use the C++ programming language as it overcomes these difficulties but I would need to make sure this tool still has the required portability.
The system developed would obviously need to be secure although this can be achieved by using a standalone machine which isn't connected to any outside sources such as the internet.
However where this isn't possible I will aim to make the tools as secure as I can. It is very difficult to develop nonfunctional requirements related to the time taken to complete the analysis as every case could be different in terms of the amount of analysis necessary and the amount of time available to conduct the investigation. These requirements may be added at a later date. The system will need to be reliable as any analysis interrupted by system failure will need to be repeated and some of the analysis could take a long while, e.g. disk imaging may take a few hours depending on the size of the disk

5.2 Specific Requirements:-

Requirement No	Name	Description	Type
1	Analyze Disk	See Disk Imaging Tool Requirements	Essential
2	Analyze Partitions	See Partition Analysis Tool Requirements	Essential
3	Analyze File System	See File System Analysis Tool Requirements	Essential
4	Analyze File	See File Analysis Tool Requirements	Essential

Table 5.3. General Project Requirements

www.studymafia.org

6. COMPUTER FORENSICS SERVICES

There are many different areas of computers where in the services of computer forensics is employed. Most of computer forensics services provide useful services to an organization. It is very much useful in professional environment where the requirement is quite high. Computer forensics services also include investigative assistance. The computer forensics is also important in corporate consulting. Forensic data recovery – FDR is also a part of computer forensics. Incident Response Systems also play a part of computer forensics. The services of computer forensics are availed in private as well as government organizations.

The secrecy or the privacy of organization is important in some cases where it is maintained as per expectations. Some of important fields where in the services of computer forensics can be applied include the following. Incident response systems and internal investigations can be done using the computer forensics. Computer forensics is extensively used in criminal as well as civil litigations. There are many laws that provide the support to a computer forensic.

Another aspect of computer forensics is the electronic document discovery. Data recovery in itself is a large topic. But some times it is referred to as a part of computer forensic. Security risk management can also be carried out using the computer forensic tools. The services provided by the computer forensics are the development of the plans to gather the electronic evidence. Computer forensic can be used for its services to support criminal and civil warrants.

Also the computer forensics is useful in electronic discovery requests. Even computer forensics investigation is beneficent for the purpose of identification, acquisition, preservation, analysis and reporting of digital evidence. The digital evidence may be from desktop computers, laptops, storage servers, or any type of removable storage devices. The services are also available for dispute resolution and to provide an expert witness testimony. In the event of conducting the audits also its services can be availed. These audits may involve remote or even network analysis.

The compliance of proactive reviews as well as risk assessment and even for the investigation of specific allegations the services of computer forensics can be availed. In case of corporate consultations the services provided by the computer forensics professional include the development of in house standards. Also the protection of intellectual property is a major service.

The protection of corporate assets is also a service of computer forensics. The consultation of computer forensic can be provided to adhere to the legislation involving federal and provincial privacy. The electronic file retention policies are also a part of consultancy services of computer forensics.

www.studymafia.org

Apart from all these services, the computer forensics can be even applied for individual case studies involving personal issues. Even the services of computer forensics can be used for data recovery problems. Intentional misuse of privacy or personal information can be considered as a legal case with the help of computer forensics.

www.studymafia.org

7. APPLICATION OF COMPUTER FORENSICS

System forensics is not different from any other forensic science when it comes to application. It can be applied to any activity, where other mainstream traditional forensics such as DNA mapping is used, if there has been an involvement of a system or computer in the event.

Some of the common applications of computer forensics are:-

- FINANCIAL FRAUD DETECTION:-
  Corporates and banks can be detect financial frauds with the help of evidence collected from systems. Also, insurance companies can detect possible fraud in accident, arson, and workman's compensation cases with the help of computer evidence.

- CRIMINAL PROSECUTION:-

www.studymafia.org

Prosecutors can use computer evidence to establish crimes such as homicides, drug and false record-keeping, financial frauds, and child pornography in the court of law.

- CIVIL LITIGATION:-

  Personal and business records found on the computer systems related to fraud, discrimination, and harassment cases can be used in civil litigations.

- "CORPORATE SECURITY POLICY AND ACCEPTABLS USE VIOLATIONS":-

  A lot of computer forensic work done is to support management and human resources (HR) investigations of employee abuse.

Besides cyber crimes and system crimes, criminals use computers for other criminal activities. In such cases, besides the traditional forensics, system forensic investigation also plays a vital role.

www.studymafia.org

8. CONCLUSION

With computers becoming more and more involved in our everyday lives, both professionally and socially, there is a need for computer forensics. This field will enable crucial electronic evidence to be found, whether it was lost, deleted, damaged, or hidden, and used to prosecute individuals that believe they have successfully beaten the system.

The computer forensic needs and challenges can be accomplished only with the cooperation of the private, public, and international sectors. All stakeholders must be more willing to exchange information on the effect economic and cyber crime has on them and the methods they are using to detect and prevent it.

www.studymafia.org

10. REFERENCES

- www.google.com
- www.wikipedia.com
- www.studymafia.org

www.studymafia.org