4 (1)

Unit -VI: Understanding Computer Forensics

INTRODUCTION

Cyber Forensics is simply application of computer investigation and analysis techniques in the interest of determining potential legal evidence. Forensic computing is the process of identifying preserving, analyzing and presenting the digital evidence in a manner that is legally acceptable. It is the study of evidence from attacks on computer system in order to learn what has occurred, how to prevent it from recurring and the extent of the damage.

Cyber Forensics is one of the emerging professions of 21st century. It can be thought of as an investigation of computer based evidence of criminal activity, using scientifically developed methods that attempts to discover and reconstruct event sequences from such activity.

The fascinating part of the science is that the computer operating system invariably leaves behind the computer evidences transparently without the knowledge of computer operator. The information may actually be hidden from view. Any enterprise that uses computer networks should have concern for both security and forensic capabilities (Yasinsac and Manzano, 2001). They suggest that forensic tools should be developed to scan continually- computers and networks within an enterprise for illegal activities.

When misuse is detected these tools should record sequence of events and store relevant data for further investigation. Special Forensic software tools and techniques are required in order to recognize and retrieve such evidences. Cyber Forensics involves obtaining and analyzing such digital information for use in civil/criminal or administrative cases. Digital evidence was not considered as tangible evidence in courts until recently but now they are gaining importance.

Terminologies: Types of Computer Forensics

1. Disk Forensics: deals with extracting data/information from storage media by searching active, deleted files and also from unallocated and slack space.
2. Network Forensics: It is a sub branch of digital forensics relating to monitoring and analysis of computer network traffic for the purpose of information gathering, legal evidence or intrusion detection. Unlike other areas of digital forensics, network investigation deal with volatile and dynamic information. It is also called Pro-active forensics.
3. Wireless Forensics: It is a sub part of network forensics. The main goal of wireless forensics is to provide the tools required to collect and analyze the data from wireless network traffic. The data collected can correspond to plain data or with the broad usage of Voice over Internet Protocol (VoIP) technologies especially over wireless technology.
4. Database Forensics: is a branch of digital forensics relating to study and examine databases and their related metadata. A forensic examination of a database may relate to the timestamps that apply to the row (update time) in a relational table being inspected and tested for validity in order to verify the actions of a database user.
5. Malware Forensics: deals with analysis and identification of a malicious code, to study their payload, viruses, worms, Trojans, Keyloggers etc.
6. Mobile Phone Forensics deals with examination and analysis of mobile devices, to retrieve phone and SIM contacts, call logs(Dialled, Missed & Received), incoming and outgoing SMS/MMS, Audio, videos, paired device history and in some smart phones, geolocation and calendar information etc.
7. GPS Forensics is also called SatNav Forensics, is a relatively new discipline with the fast paced world of Mobile Device Forensics. It is used for examining and analysing GPS

devices to retrieve information such as TrackLogs, TrackPoints, WayPoints, Routes, Photos, audio etc.

8. Email Forensics: Deals with recovery and analysis of emails including deleted emails, calendars and contacts.
9. Memory Forensics deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.
10. E-Discovery: E-Discovery is the process of evaluating solutions for organization. A defensible e-Discovery process is repeatable, systemized and meets legal requirements for proper handling and admissibility of computer evidence. Email archiving can be a useful complement e-Discovery. A defensible e-discovery process is repeatable, systematized and meets legal requirements for proper handling and admissibility of computer evidence. An ideal e-discovery process identifies, collects, preserves, processes, reviews and produces relevant electronically stored information. Relevant information may be found in unmanaged, unstructured, semi-structured or structured data sources dispersed across networks on desktops, laptops, servers, share drives, removable storage media and other devices. As the name implies, email archiving is limited to the contents of email system since they work only with the set of emails and do not extend to data on the network. An effective repeatable and defendable eDiscovery response plan requires an organization to proactively anticipate the type of discovery that could be initiated and develop an offensive strategy that employs both technology and human resources (Scott Carlson, 2009).

DIGITAL SPECTRUM

With the advent of new forms of criminality associated with growth of digital technologies, numbers of terms are used within the forensic community. These include cyber crime, high tech crime, e-crime, new technology crime to indicate new and digitized versions of existing crime. Some crimes can be placed on the spectrum depending upon the extent of digital environment.

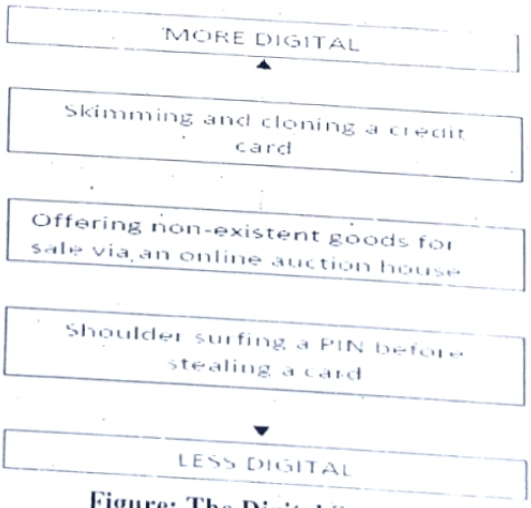


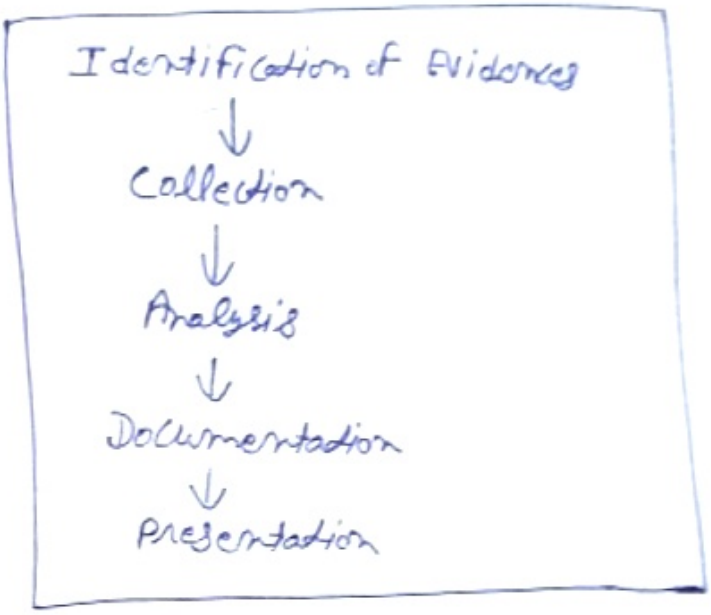
Figure: The Digital Spectrum

Consider a street thief who first observes an unwary user input the PIN in an ATM and then steals the card and later withdraws cash; this is not a crime that appears to be particularly digital and it is therefore placed at the less digital end of the spectrum. On the other hand,

Need For Computer Forensics

4 (3)

1. To Produce evidence in the court which can lead to the punishment.
2. Help the companies gather important Information
3. Efficiently track Cyber Criminals.
4. Protect the organizations.



Cyber Forensics & Digital Evidence

Digital forensics is the practice of identifying, acquiring & analyzing electronic evidence. Digital forensic Data is used in Court Proceedings.

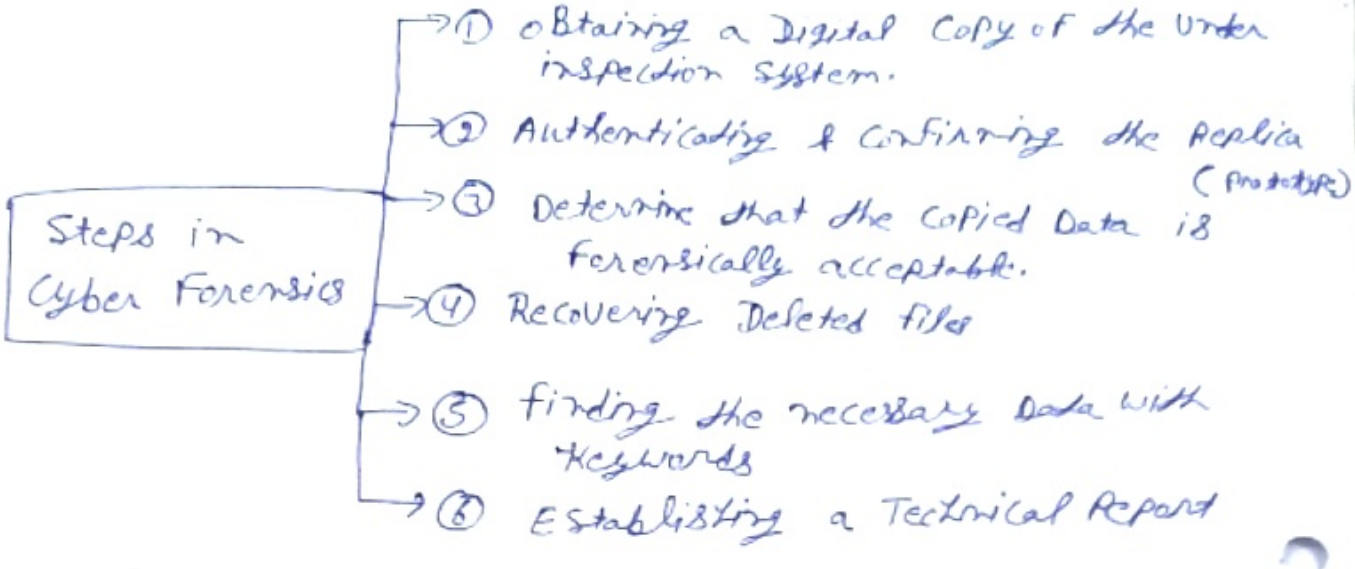
Forensics Analysis of Email

Email Forensics is the Analysis of the content Source of the email message, by identifying the sender & the receiver, the Date & time of the email & analyzing all the activities involved.

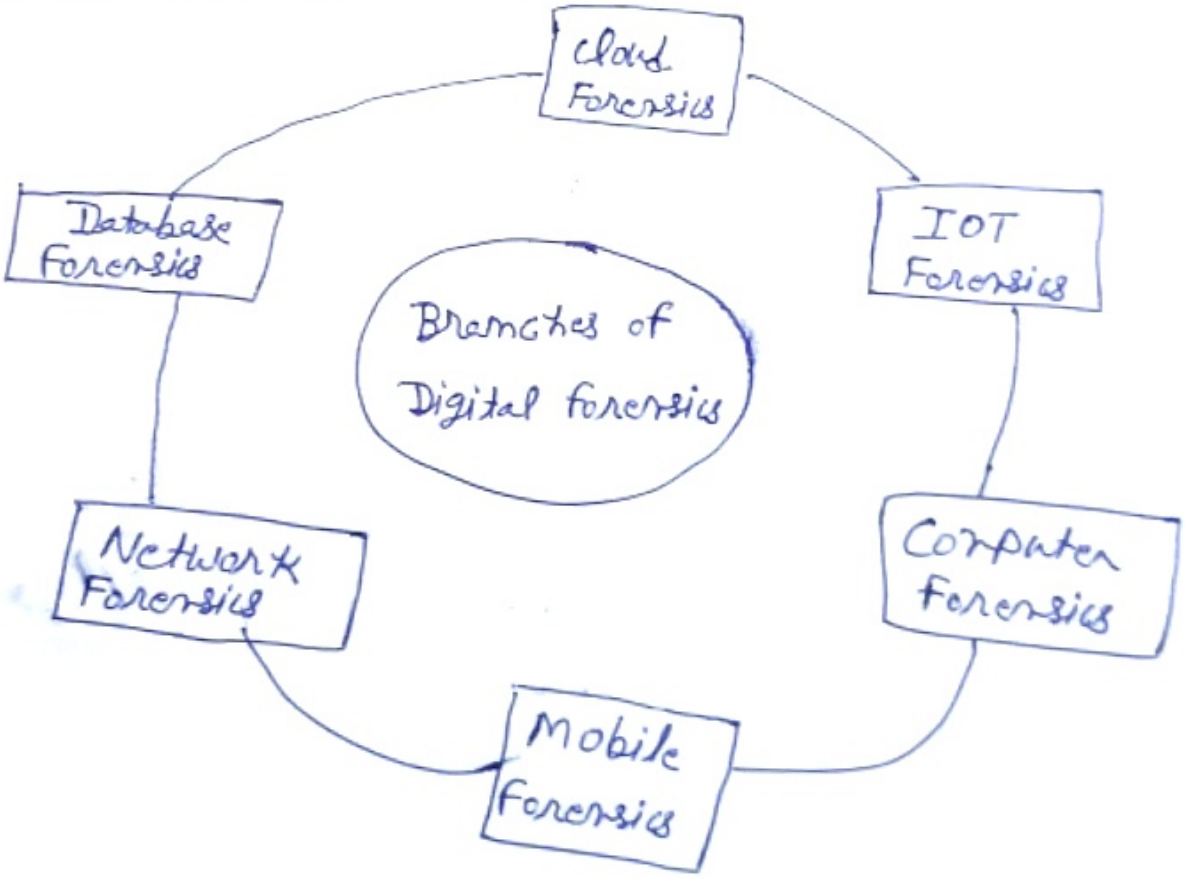
- Header Analysis
- Sender mailer Analysis
- Server Investigation
- Network Device Investigation

Process Involved In Cyber Forensics

4 (4)



Digital Forensics Science



skimming the magnetic strip, cloning a card Skimming and cloning a credit card and then using it to make transactions is clearly a crime unique to digital era and would appear to be placed at the more digital end of the spectrum.

Similarly, some crimes are more likely to have a digital aspect rather than uniquely exploit digital technologies. For example, a fraud enacted via an e-bay, a fraudster may have had planning for the fraud in the internet, setting up temporary and difficult to trace email accounts, surfing the internet for images, descriptions and prices. These are activities which exploit the advantages of digital technologies but nonetheless arise from a conventional and classic form of crime.

GOOD FIELD PRACTICE IN PROCESSING A CRIME SCENE

Crime Scene: It is crucial to understand the definition of crime scene. For practical purpose, a Crime scene is the aftermath of an event that is considered, by law, to be illegal. For basic understanding the crime seene can be considered the apex of an Inverted pyramid that expands to encompass the five phases, Investigation of crime, the recognition, analysis, interpretation of evidence, and finally, court trial. Crime seene should be processed with due diligence, utmost care and by the application of technology because any mistake made in processing the crime scene are impossible to rectify. Both errors of omission and commission made in processing a crime scene can confound the final resolution in two ways to make thing worse. The investigators use general guidelines for processing crime scene and exercise the use of check sheets, forms lists as templates for search and examination to be counterproductive. Each crime scene is unique and must be approached with knowledge, education and experience of the investigator. Crime scene is the apex of an inverted pyramid. This is illustrated in the Figure.

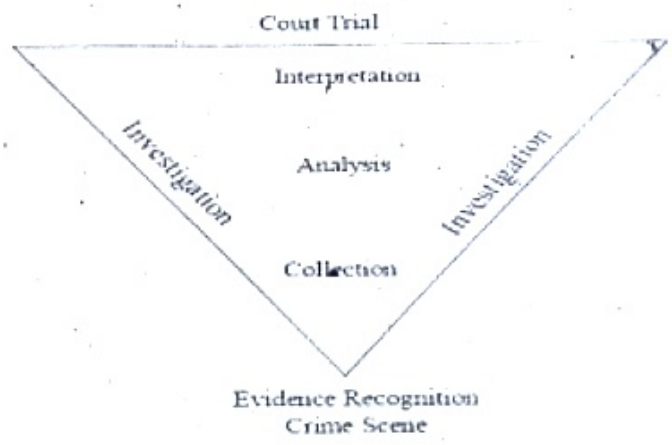


Figure: Crime Scene Pyramid

DIGITAL EVENT AND CASE RELEVANCE

Digital Event is an occurrence that changes the state of one or more objects. If the state of an object changes as a result of an event, then it is an effect of the event. Some types of objects have the ability to cause the events and these called causes (Carrier and Spafford, 2004).

The property of any piece of information, which is used to measure its ability to answer the investigative "who, what, where, when, why and how" questions in criminal investigation

(Rubin and Garrtner, 2005). The authors use this notion to describe the distinction between computer security and forensics even defining degrees of case relevance and the same is given in Figure.

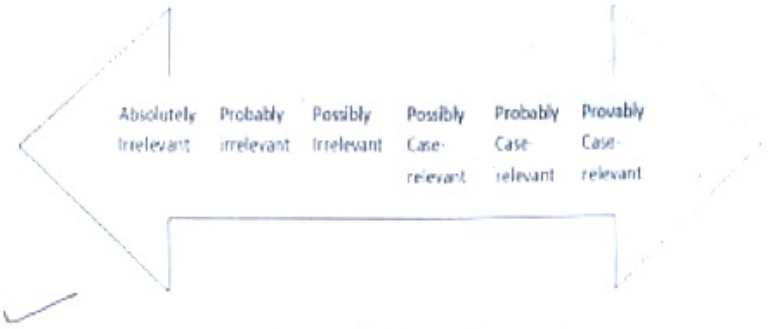


Figure.4. 3: Degrees of Case Relevance

The ultimate purpose of crime scene investigation is to seek to solve the commission of crime inevitably that fall under the umbrella of the six "W" questions:

1. What happened?
2. When did it happen?
3. Where did it happen?
4. Who was involved?
5. How was it done?
6. Why was it done?

In the examination of physical evidence the first five questions are relevant. The question "Why" is irrelevant for laboratory analysis and it is left for the establishment of motive by" "Profilers, "Criminologist" and "Courts".

LOCARDS PRINCIPLE: TRADITIONAL FORENSICS VS. CYBER FORENSICS

Locard's Exchange Principle is often cited in forensics publications, "Every contact leaves a trace." Essentially Locard's Exchange Principle is applied to crime scenes in which the perpetrator(s) of a crime comes into contact with the scene.

The perpetrator(s) will both bring something into the scene, and leave with something from the scene. In the cyber world, the perpetrator may or may not come in physical contact with the crime scene, thus, this brings a new facet to crime scene analysis.

According to the World of Forensic Science, Locard's publications make no mention of an "exchange principle," although he did make the observation *"Il est impossible au malfaiteur d'agir avec l'intensité que suppose l'action criminelle sans laisser des traces de son passage."* (It is impossible for a criminal to act, especially considering the intensity of a crime, without leaving traces of this presence).

CYBER EXCHANGE PRINCIPLE

"Artifacts of electronic activity in digital devices are detectable through forensic examination, although such examination might require access to computer and network resources involving

(Rubin and Gantner, 2005). The authors use this notion to describe the distinction between computer security and forensics even defining degrees of case relevance and the same is given in Figure.

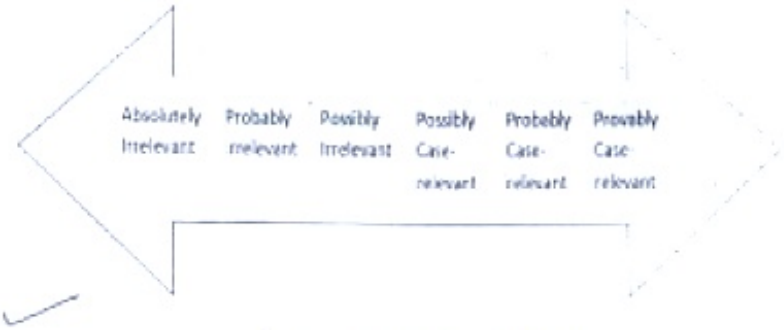


Figure.4. 3: Degrees of Case Relevance

The ultimate purpose of crime scene investigation is to seek to solve the commission of crime inevitably that fall under the umbrella of the six "W" questions:

1. What happened?
2. When did it happen?
3. Where did it happen?
4. Who was involved?
5. How was it done?
6. Why was it done?

In the examination of physical evidence the first five questions are relevant. The question "Why" is irrelevant for laboratory analysis and it is left for the establishment of motive by" "Profilers, "Criminologist" and "Courts".

LOCARDS PRINCIPLE: TRADITIONAL FORENSICS VS. CYBER FORENSICS

Locard's Exchange Principle is often cited in forensics publications, "Every contact leaves a trace." Essentially Locard's Exchange Principle is applied to crime scenes in which the perpetrator(s) of a crime comes into contact with the scene.

The perpetrator(s) will both bring something into the scene, and leave with something from the scene. In the cyber world, the perpetrator may or may not come in physical contact with the crime scene, thus, this brings a new facet to crime scene analysis.

According to the World of Forensic Science, Locard's publications make no mention of an "exchange principle," although he did make the observation *"Il est impossible au malfaiteur d'agir avec l'intensité que suppose l'action criminelle sans laisser des traces de son passage."* (It is impossible for a criminal to act, especially considering the intensity of a crime, without leaving traces of this presence).

CYBER EXCHANGE PRINCIPLE

"Artifacts of electronic activity in digital devices are detectable through forensic examination, although such examination might require access to computer and network resources involving

expanded scope that may involve more than one venue and geolocation." (Zatyko and Bay, 2012)

Locard's Exchange Principle does apply to cyber crimes involving computer networks, such as identity theft, electronic bank fraud, or denial of service attacks, even if the perpetrator does not physically come in contact with the crime scene. Although the perpetrator may make virtual contact with the crime scene through the use of a proxy machine, we believe he will still "leave a trace" and digital evidence will exist.

Breaking apart the principle into its parts and analyzing the application of Locard's Exchange Principle, one has to determine whether or not the following occurs:

- Are there two items?
- Is there contact?
- Is there an exchange of material?

To illustrate the application of Locard's Exchange Principle to a cyber crime, we take the example of identity theft where someone's identity is stolen and the perpetrator intends to use the stolen information for criminal gain. Let us further suppose the perpetrator steals the identity through the use of a Trojan horse and keyboard logger on the victim's computer. One could contend that during this type of cyber crime Locard's Exchange Principle does not apply. The rationale is that because a human is not at the crime scene there is no trace evidence from the human on the computer or digital media at the scene.

However, in actuality there may be lots of digital evidence such as the Trojan horse itself, changed passwords, digital logs, and so on. Thus, in this example, there is a trace at and from the scene. It may involve finding the trace evidence at other physical locations than just the one scene of the crime. The key logger could be added software or hardware or both, but in both cases it remains behind for an investigator to discover. This examination typically involves bits and bytes of information.

GOALS OF CYBER FORENSICS

In pursuit of finding the truth, the goal of digital forensics moves from specific to abstract. This can be from acquiring the evidence from the storage media in the form of data or information. This information could be represented inside the media as an encoding (i.e) ASCII or binary. The encoded data in the form of information may be involving incidents that transpired in an organization and event reconstruction needs to be made on timeline basis. The correlation or the relationship between events must be established specific to the context for e.g.: an unauthorized exploit. After acquiring the data must be relevant or coincidental to the questioned occurrence. This incident may involve the motivation or the malicious intent of the attacker. The intent may be *information component* or *human component*. It requires the skill, knowledge and ability of the investigator in the process of unraveling the truth. Incident and response time have inverse relationship. Severity and number of attacks/penetrations are high when compared to earlier years as against the time to respond is very low. A graphical representation of the goal from specific to abstract is represented in the Figure.

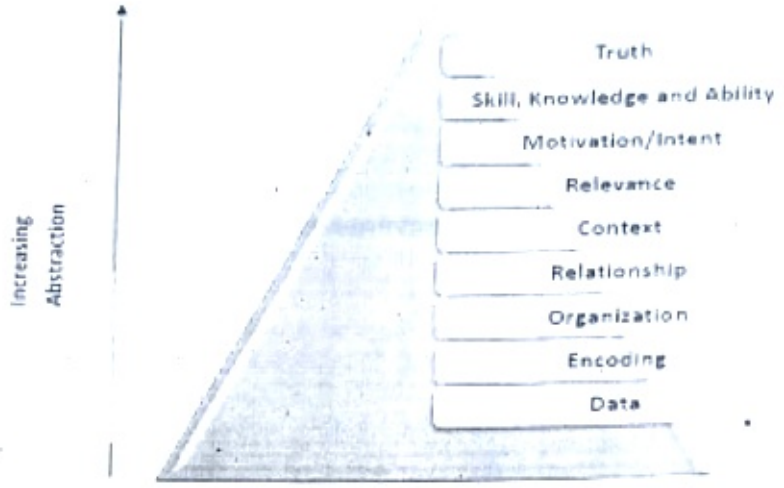


Figure: Goals of Cyber Forensics

EVOLUTION OF CYBER FORENSICS

The field of computer forensics began in the 1980s, shortly after personal computers became a viable option for consumers. In 1984, an FBI program was created. Known for a time as the Magnetic Media Program, it is now known as the Computer Analysis and Response Team (CART). Shortly thereafter, the man who is credited with being "the father of computer forensics" began work in this field. His name was Michael Anderson, and he was a special agent with the criminal investigation division. Anderson worked for the American government until the mid 1990s, after which he founded New Technologies, Inc., a leading computer forensics firm.

EMERGENCE OF CYBER FORENSIC INVESTIGATING AGENCIES

A meeting held in 1988 in Oregon led to the formation of the International Association of Computer Investigative Specialists (IACIS). Shortly after that, the first classes were held to train SCERS (Seized Computer Evidence Recovery Specialists).

Computer Forensic Timeline is illustrated in Figure and it represents the evolution of digital forensics domain as such.

Figure: Computer Forensics Timeline

Different Phases of Cyber Forensics are:

1. Ad-hoc phase -which was characterized by lack of structure, lack of clear goals, lack of adequate tools, processes and procedures. Further huge legal issues on how to proceed with digital evidence were seen.
2. Structured Phase- is complex solution for computer forensic from accepted procedures, special tools developed and what is more important enabling criminal legislation to wide use of digital evidences.
3. Enterprise phase –Three areas of this phase are real-time collection of evidence, developing field collection tools and forensic becoming a service in companies.

- **International Organization on Computer Evidence:** The discipline continued to grow in the 1990s, with the first conference on collecting evidence from computers held in 1993. Two years later, the International Organization on Computer Evidence (IOCE) was established.
- **Digital Forensic Research Workshop (DFRWS):** DFRWS is a non-profit, volunteer organization dedicated to the sharing of knowledge and ideas about digital forensics research. DFRWS organizes an annual conference and sponsors technical working groups and annual challenges to help drive the direction of research and development.
- **Scientific Working Group on Digital Evidence (SWDGE):** The federal Crime Laboratory Directors group formed SWGDE in 1998. It was noted that the traditional audio and video examination processing was becoming digital and along with digital still photography, was converging with computer forensics. As a result, they formed a group to explore digital evidence as a forensic discipline. This group comprised of members of prominent organizations such as American Association of Forensic Science , Internation Association of Computer Investigative Specialist, High Technology Crime Investigation Association and International Organization on Computer Evidence. SWGDE is focused on the practice of digital evidence forensics primarily in the laboratory setting.
- **Association of Chief Police Officers (ACPO):** Association of Chief Police Officers functioning from Northern Ireland have designed and published a guide with procedures to be followed while collecting computer based evidence to ensure good field practice.

DEVELOPMENT OF CYBER FORENSICS

Computer forensics is the study of extracting, analyzing and documenting evidence from a computer system or network. It is often used by law enforcement officials to seek out evidence for a criminal trial. Government officials and business professionals may also have need of a specialist familiar with computer forensic techniques. The discipline of computers forensics is relatively new, having been founded in the 1980s. This digital evidence consists of data from storage media like hard disk, floppy disks, zip disks, Compact dises, DVDs, emails, data transmitted over communication links (wired and wireless), log files generated by the operating system, logs from perimeter devices like router and switch, PDA, Mobile Phones, MP3 players, USB devices, and even plethora of devices which do not fit into the original concept of computers like the washing machines, engine management system in cars, GPS devices.

In order for evaluation and acceptance of Digital evidence – a new type of evidence, previously not considered by courts, certain basic principles are suggested by research scholars and these are given below:

- Authenticity – the evidence should be authentic that is "it should specifically linked to the circumstances and persons alleged – and produced by someone who can answer questions about such links"
- Accuracy – the evidence should be free from any reasonable doubt about the quality of procedures used to collect the material, analyze the material if that is appropriate and necessary and finally to introduce it into court and produced by someone who can explain what has been done. In the case of exhibits which themselves contain statements – a letter of other document, for example – 'accuracy' must also encompass accuracy of content and that normally requires the document's originator to make a witness statement and be available for cross examination"
- Accuracy – when presented evidence contains statements created in a computer "accuracy must encompass the accuracy of the process which produced the statement as well as the accuracy of the contents
- Completeness - " tells within Its own terms a complete story of a particular set of circumstances or events"

In addition to these considerations, forensic evidence must exhibit the following properties:

- Chain of custody, transparency and explainable are the other basic principles the needs to be followed among the other principles.

Unlike the physical evidence, the digital evidence, by itself has no informational value. It requires skill and talent in interpreting the latent information which is dependent on the process by which it is unraveled and the process in turn depends on the basic principles of computer science. In order to be legally acceptable in the court of law, it requires a motivated skilled expert who will apply appropriate tools to achieve, efficiency and reliability. Cyber Forensics focuses on three kinds of data namely active data, latent data and archival data.

- **Active Data:** An active data is one that is currently available, visible and that which can be understood using an application within a computer. Active data might also be protected using passwords or some means of encryption. Some of the active data are word processor files, spread sheets, files and directories, email content, database programs, system files, history files, temporary internet files, cookies, recycle bin and the like.
- **Latent Data:** Latent data also called as ambient data, volatile data may be in the form of deleted files, memory dumps and similar data which reside in swap files, temporary files, printer spool files, metadata, shadow file and so on. It requires an expert talent to bring to light the latent data using specialized tools and techniques.
- **Archival data:** Data that has been stored or backed up to external storage media such as tapes, CDs, DVDs, external hard disks, pen drive, zip disks, network servers or the internet is archival data. Necessary precautions have to be taken while performing forensic examination since the backup peripheral devices do not have all the information. Hence, it is always better to perform forensic examination on original source media because backups do not store latent data.

CARDINAL RULES IN CYBER FORENSICS

The cardinal rules of computer forensics can be expressed as the five 'A's

1. Admissibility must guide actions: document everything that is done;

2. Acquire the evidence without altering or damaging the original;
3. Authenticate your copy to be certain it is identical to the source data
4. Analyse the data while retaining its integrity and
5. Anticipate the unexpected.
6. The cardinal rules are designed to facilitate a forensically sound examination of computer media and enable a forensic examiner to testify in court as to their handling of a particular piece of evidence. A forensically sound examination is conducted under controlled conditions, such that it is fully documented, replicable, and verifiable. A forensically sound methodology changes no data on the original evidence, preserving it in pristine condition. The results must be replicable such that any qualified expert who completes and examination of the media employing the same tools and methods employed will secure the same results.

CYBER FORENSIC LAB

The role of cyber forensics will be increasing importance to the legal system as information continues to evolve into purely a digital form and the systems on which such digital information is stored becomes more technologically advanced. Strategic planning for setting a laboratory involves in developing a forensic practice: Operational Perspective, Technological perspective/venue, Scientific Perspectives an artistic perspective. Other areas of significance are Core Mission and Services, Budget and Standard operating procedures.

Cyber Forensics Lab requires adequate infrastructure for examination and analysis of Digital Evidence. Adequate Infrastructure not only includes technical infrastructure but also assets such as workspace, dedicated communication lines, 24/7 internet connection among others which should be made available to the cyber forensic experts.

- **Operational Perspective:** All business venue must have sound business management, financial profitability, core service etc. a police cyber forensics lab may not have profit perse, but the lab has to demonstrate value of service and return of Investment in order to acquire annual budget allocations and training in new technologies to continue fighting crime.
- **Technological Perspective:** Technological advancement calls for sophisticated knowledge in data and data storage technologies. More complex techniques are used by criminals to hide their criminal activity. The commercial market is rolling out a new wave of newest and shiniest technologies available to upkeep the demand for progress; again forensics community is at the front of the line, dismantling and investigating every new gadget that hits the shelves in order to reveal its secrets.
- **Scientific Perspective:** In order reveal facts objectively through empirical observation, deductive reasoning and conversion of hypothesis to demonstrable proof of the fact, examiners have to perform their duties according to reliable, repeatable, valid, objective, consistent and accurate methodologies, thereby enabling the presentation of the findings as acceptable in court of law.
- **An Artistic Perspective:** A great degree of technological prowess or expertise and competency is required in fact finding. Although the investigative process involves a rigid set of procedures, intuitive and creative skills of the forensic examiner is also required. Raw technological skill does not empower an examiner to understand the man and the machine. More artistry and creativity is required to enable a better understanding of how the tools of technology and human nature and thought process interact.

forensics, the standalone system and other storage media are examined offline. Choice of the tools should take into consideration the performance, reliability and repeatability and also the caveats. Having considered all these factors, examination should be performed utilizing these tools in a forensically sound manner following the best practices so as to enable admissibility of the evidence in the court of law.

A survey of forensic tools has been compiled by Dr. Peter Stephenson, in July 2006 has been published in the SC Magazine (Marcella and Menendez, 2008). A summary of the findings as to the "best of breed" of forensic tool has been listed in the Table. According to the survey the computer forensic tools sets are categorized as good, the better and best.

Table: Specification for Forensics Tools
(Source: Marcella and Menendez, 2008)

S No.	Product	Supplier	UNIX Linux	Windows	Analysis W=Windows U=Unix Linux	Remote capture	GUI	Requires remote agents	Pre-Forensic Audit
1	Coroners Toolkit(TCT)	Open source	Yes	No	U	No	No	No	No
2	Encase	Guidance Software	No	Yes	W U	No	Yes	No	Yes
3	Forensic Toolkit	Access Data	No	Yes	W U	No	Yes	No	Yes
4	i2 Analyst Notebook	i2 Inc	No	Yes			Yes	No	No
5	LogLogic LX-2000	LogLogic	Yes	No	-	Yes	Yes	No	No
6	Mandiant First response	Mandiant	No	Yes	W	Yes	Yes	Yes	Yes
7	Net witness	Man Tech Intl.	Yes	No	-	-	No	No	No
8	Pro Discover Incident response	Technology Partners	No	Yes	W,U	Yes	Yes	No	Yes
9	Sleuthkit and Autopsy Browser	Open Source	Yes	No	W, U	No	Yes	No	No

- **Forensic Hardware:** Forensic hardware includes workstation, write blockers, and forensic devices.
- **Forensic Workstations:** Forensic Recovery of Evidence Device **(FRED, Digital Intelligence)** family of workstations consists of integrated forensic processing platforms capable of handling the most challenging computer case. FRED is available in Mobile, Stationary and laboratory configurations. These systems are designed for both the acquisition and examination of Digital evidence. FRED professional forensic systems and the Digital Intelligence Ultrabay universal write protected imaging bay, deliver the ability to easily duplicate evidence directly from IDE/SCSI/SATA hard drives, USB Devices, Firewire devices, floppies, CDs, DVDs, ZIP cartridges, DLT-V4 tapes and PC Card/smart card/SD – MMC/Memory stick/Compact Flash Media in a forensically sound environment. Various categories of FRED workstations are:

- **Budget:** Every forensic facility be it business organization or government, require funds to function. It has to spend on building, staff, and stock. It has to operate, maintain and grow a facility. Every operation needs to demonstrate return of investment in order to prove viability of the venture.
- **Core Missions and Services:** Primary consideration of forensics facility is the design plan and what services are to be rendered and the scope at which it is to be provided. A firm grasps of a prospective lab core mission and range of service will provide guidance on every aspect of building, functional forensic facility, touching on everything from annual budget to furniture ergonomics. The technical aspects would include the requisite hardware and software tools for examination and analysis. The cyber lab should possess robust operating system software like Microsoft Windows, MAC OS, Linux, SOLARIS etc. It must also have powerful computer workstation with standard peripherals. Another vital requisite would be Uninterruptible Power management software is also required for extensive control and monitoring capabilities. In general, the infrastructure is layered and the same is illustrated in Figure.

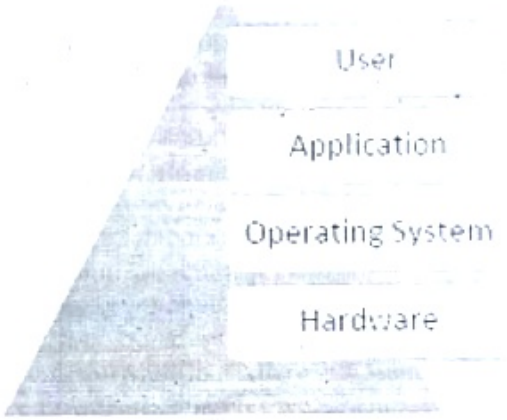


Figure: Layered Infrastructure

CYBER FORENSIC TOOLS

Software packages and hardware devices that qualify as forensic fraternity an there is utilizing cyber forensics tools are hoards of them. The main responsibility lies in the hands of the cyber forensic examiner to have a thorough understanding of this software, hardware and other utilities. Quite often, a combination of tools has to be employed in order to obtain a complete picture. Two-way approach in utilizing the tools exists.

One way is Proactive Forensics and the other is Post Incident Forensics. In another sense, in the current scenario, with increased volume of storage devices and multiple terabytes of data running across in the network or on such devices invites the live examination that is proactive forensics which relates to electronic discovery.

The other way is examining the storage devices after the incident has happened to find out what has actually happened in storage medium like hard disk, memory card, etc,. In proactive forensics, live examination is required without disrupting the business, whereas in post incident

4 (14)

a. FRED – Forensic Recovery of Evidence Device an ideal tool for laboratory for imaging and processing
b. FREDDIE – a highly portable solution which meets both imaging and processing requirements FRED interrogation Equipment.
c. FRED- L – The Laptop of FRED family of tools
d. µRED- microFRED the smallest, full powered Forensic Workstation
e. FRED Systems: is the complete forensic hardware and hardware solution. The 19" LCD monitor is included. The available OSs on this system is MS 6.22, Wins 98, Wins XP Pro, and Linux 9.1 Pro. Some software such as Norton GHOST 10.0 & 2003, Nero DVD/CD Authoring Software, DriveSpy, Image, PDWipe, PDBlock, and PART are included

- **Forensic Network:** Forensic Network is a series of processing and imaging computers connected and integrated directly with a high speed, high capacity server to share resources. The file server operates as the core of the Forensic Network and can be used as a central storage facility for Forensic Images as well as the applications software for use by the client processing and imaging stations.
- **Forensic Write Blockers:** ATA and SCSI hardware write blockers, as well as other custom solutions, to effectively address specific write blocking requirements. Learn how our UltraKit, FireFly, FireBlock, SCSIBlock and FireChief devices can maintain the integrity of evidence.
- **Forensic Devices:**
  1. Fannie - forensic area network numerous imaging enclosure
  2. Rack-a-Tacc password decryption
  3. Tacc1441 Hardware Accelerator
  4. Modular Accessories
  5. Forensic Duplicator
  6. Hardcopy 3 & Hardcopy 2
  7. Shadow 2
- **Forensic Software Tools:** The forensic software tools frequently used for cyber forensics include imaging tools, examination and analysis tools, visualization tools and the like.
- **Digital Intelligence Software:** Digital Intelligence has created several forensic software tools in-house specifically for Forensic use. These tools include DriveSpy, Image, Part, PDBlock and PDWipe.
- **Accessdata:** The forensic tools available are Ultimate Toolkit, Forensic Toolkit, and specialized password recovery based on applied cryptography – Password Recovery Toolkit and Registry Viewer.
- **Guidance Software:** EnCase Forensic Edition, by Guidance Software, is the worlds leading solution for computer investigations and forensics. It is the oldest of GUI Basted IT Forensic Tools, and it includes other useful features including the ability to preview and acquire disks through many types of connections.
- **The Sleuth Kit and Autopsy Browser** powerful forensic tools to work in UNIX or Linux Environments.
- **The Coroner's Toolkit (TCT)** is an open source set of forensic tools for performing post mortem analysis on UNIX system.

4 (15)

- **Mandiant First Response** as a first response tool for gathering snapshot of the network with very limiter intrusiveness prior to a detailed forensic examination.
- **ProDiscover** is a complete IT forensic tool that can access over the network to enable media analysis and network behaviour analysis.
- **i2 Analyst Notebook:** This a very different type of analysis tools from those information security professionals are used to perform Link Analysis, a crucial aspect of incident response is usually done manually or by trying to use log correlators. This is a true link analyser in analysing complex crimes an security incidents. Link analysis is applied to incident response and it is used as a visualization software to link inter relationship between displayed.
- **Nuix Email Investigation** Software is a powerful email investigation software tool that performs link analysis, email information visualization, hierarchical relationship between chain of emails.
- **Paraben Forensic Tools** is a Forensic Software for PDA, Mobile Phone, text searching, data acquisition and email examination.
- **Netwitness** is a network traffic security analyzer (security intelligence) is used as a forensic incident response tool to gather information from connected computers.
- **Forensic Network** is a series of processing and imaging computers connected and integrated directly with a high capacity server to share resources. The file server operates as the core of the Forensic Network and can be used as a central storage facility for Forensic Images as well as applications software for use by the client processing and imaging stations. Workstation clients on the network perform the actual imaging and processing tasks, while the central file server stores the images and case work.
- **CyberCheck Suite** is a suite of forensic software tools to perform data analysis which has a capability of analysing storage media such as hard disks, and optical media images and analyses images for evidences developed by C-DAC Thiruvanathapuram.
- **Hot Pepper Technology:** Authors of EMAIL Detective, a dedicated software solution for recovering and reconstructing AOL email. EMD is the most comprehensive AOL extraction tool available to forensic agencies
- **Stepanet DataLifter:** Suite of products based on investigative experience. These tools have been specifically designed to assist with Computer Forensics, Information Auditing, Information Security and Data Recovery.

DIGITAL FORENSIC LIFE CYCLE

The major issues of cyber forensics involves Identification of potential digital evidence and determine as to where might the evidence be. Which devices were used by suspects? reservation of evidence on the electronic crime scene, prevent loss and contamination and ensure proper documentation and further extract the evidence and present in a legally acceptable manner, taking due care to privacy related issues. The next step is to ensure integrity of evidence. The aim is to try to make an identical copy of the evidence so that it can be analyzed without destroying the original evidence. As a thumb rule, according to various standards, one should never work on the original disk or the storage medium, always make multiple copies and work only on the copies, ensure chain of custody. Different methods of forensic copying are available.

A special device called a write blocker is commonly used. Both Software based write blockers and hardware based write blockers are available. The hardware based write blocker is a small device or a bridge that is connecting the suspect hard disk and the computer system

4 (16)

through the hard disk interface. The write blocker functions by analyzing the commands sent from the Hard Disk controller on the motherboard to the hard drive and it filters all the commands that instruct the drive to change its content. That is, it allows the system to "read only" mode. Generally Hardware write blockers are preferred over software based write blockers. Integrity of the evidence can be verified with message digest (MD5) or Secure Hashing Algorithm (SHA) hash algorithm and may be a Global Position System may be used to provide for more reliability indicating the location of imaging process.

The digital forensic life cycle is represented in the Figure.

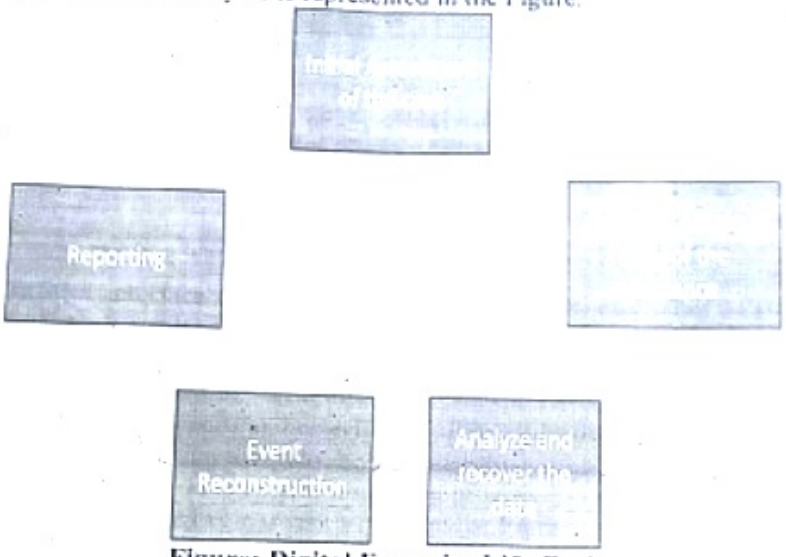


Figure: Digital Forensics Life Cycle

DIGITAL FORENSIC EXAMINATION

Digital Forensic examination may be sought for either public or private investigation. What is possible is recovery of deleted data, discovery of when the files were created, modified or deleted, installed and uninstalled application, web browsing habit s of the user etc. What is not possible is recovery of digital media that is physically damaged or destroyed or securely overwritten.

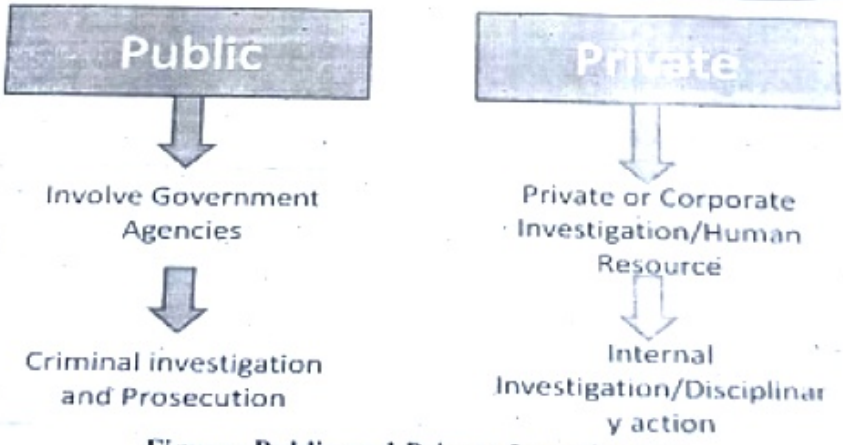


Figure: Public and Private Investigation

LATENT DEMAND FOR COMPUTER FORENSIC SERVICES IN INDIA

A survey had been done for the "Latent Demand for Computer Forensic Services in India" (Parker P, INSEAD, 2009) Based on the methodology described above, the latent demand for computer forensic services in India is estimated to be $278.1 million in 2009. The distribution of the latent demand (or potential industry earnings) in India, however, is not evenly distributed across regions. Maharashtra is the largest market with $37.8 million or 13.60 percent, followed by Uttar Pradesh with $32.3 million or 11.60 percent, and then Gujarat with $22.9 million or 8.22 percent of the latent demand in India. In essence, if firms target these top 3 regions, they cover some 33.42 percent of the latent demand for computer forensic services in India.

- **The Latent Demand in India Territory Wise** A Study conducted on the latent demand for computer forensic services in India recently **(Philip M. Parker. 2009)** has predicted that the requirement for computer forensic services in India and presents state wise percentage for industry earnings amounting in USD. Table.4.2 represents the latent demand state wise for the year 2009 and in Table.4.3 shows the year wise latent demand and Table 4.3 represents the latent demand for industry earnings in Tamilnadu.

Table.4.2: Latent Demand for Computer Forensic Services in India (2009)
(Source: Philip M. Parker, INSEAD, © 2008, www.icongrouponline.com)

S No	State	USD in millions	Percentage in India
1	Maharashtra	37.816	13.6%
2	Uttar Pradesh	32.260	11.6%
3	Tamil Nadu	26.058	9.4%
4	Gujarat	22.861	8.2%
5	West Bengal	21.716	7.8%
6	Andhra Pradesh	20.216	7.3%
7	Madhya Pradesh	15.935	5.7%
8	Karnataka	14.286	5.1%
9	Rajasthan	12.894	4.6%
10	Delhi	9.804	3.5%
11	Kerala	9.123	3.3%
12	Haryana	8.639	3.1%
13	Orissa	8.066	2.9%
14	Punjab	8.009	2.9%
15	Chhattisgarh	5.661	2.0%
16	Bihar	4.884	1.8%
17	Assam	4.305	1.5%
18	Jharkhand	4.192	1.5%
19	Uttaranchal	2.220	0.8%
20	Himachal Pradesh	1.988	0.7%
21	Jammu & Kashmir	1.689	0.6%
22	Goa	.969	0.3%

23	Chandigarh	.839	0.3%
24	Pondicherry	.735	0.3%
25	Nagaland	.632	0.2%
26	Tripura	.509	0.2%
27	Meghalaya	.506	0.2%
28	Manipur	.427	0.2%
29	Mizoram	.310	0.1%
30	Arunachal Pradesh	.256	0.1%
31	Andaman & Nicobar Islands	.142	0.1%
32	Sikkim	.056	0.0%
33	Daman & Diu	.042	0.0%
34	Dadra & Nagar Haveli	.036	0.0%
35	Lakshadweep	.026	0.0%
	Total	278.109	100.0%

Table.4.3: Year wise Latent Demand/requirement for Computer Forensic Services: 2004 – 2014.

(Source: Philip M. Parker, INSEAD, 2008, www.icongrouponline.com)

Year	India Market US$ Million
2004	103.152
2005	137.641
2006	173.446
2007	208.279
2008	243.141
2009	278.109
2010	313.708
2011	349.845
2012	384.546
2013	421.925
2014	463.050

The data in Table 4.4: represents the requirement in USD demand for computer forensic services in Tamilnadu.

Table.4.4: Latent Demand for Computer Forensic Services in Tamil Nadu: 2004 – 2014

(Source: Philip M. Parker, INSEAD 2008)

Year	US$ Million	Percent in India
2004	10.669	10.34
2005	13.925	10.12
2006	17.186	9.91
2007	20.222	9.71
2008	23.150	9.52

2009	26.058	9.37
2010	28.930	9.22
2011	31.741	9.07
2012	34.308	8.92
2013	37.005	8.77
2014	39.914	8.62

Figure.4.9. represents the district wise requirement in percentage. Accordingly, in Chennai it is 14% followed by Coimbatore, 12%, Trichy and Madurai 4% each

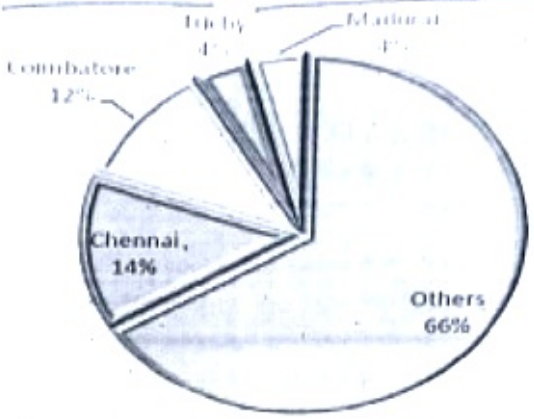


Figure.4.9: Latent Demand for computer forensic services in Tamilnadu

CONCLUSION

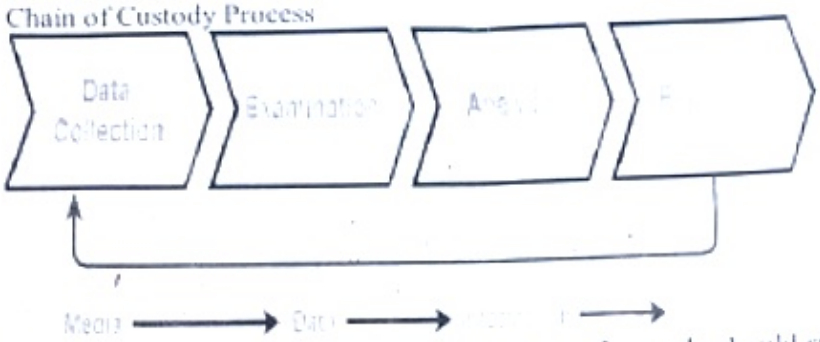
Cyber Forensics puts the wheels in motion between the cyber forensic professionals (humanware), the software and the hardware tools of cyber forensics as there is a dire need to develop new methods for analysis and assessment thereof to reflect the focus on competencies. A high quality interdisciplinary collaboration is the need of the hour. In this regard combination of the said factors is envisaged for achieving best practices in cyber forensic investigation. The cyber forensic investigation is confronted with cyber crimes which are heterogeneous in nature. In the next chapter pattern recognition techniques in order to highlight the possible relationships between occurrences of particular crime has been discussed using application of practical forensic methods.

Chain of Custody Concept

- Chain of Custody refers to the logical sequence that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence in legal cases. Each step in the chain is essential as if broke, the evidence may be rendered inadmissible.
- Thus we can say that preserving the chain of custody is about following the correct and consistent procedure and hence ensuring the quality of evidence.
- Chain of custody indicates the collection, sequence of control, transfer and analysis.
- It also documents details of each person who handled the evidence, date and time it was collected or transferred, and the purpose of the transfer.

4 (20)

- It demonstrates trust to the courts and to the client that the evidence has not tampered.
- Digital evidence is acquired from the myriad of devices like a vast number of IoT devices, audio evidence, video recordings, images, and other data stored on hard drives, flash drives, and other physical media.
- Chain of Custody Process



- In order to preserve digital evidence, the chain of custody should span from the first step of data collection to examination, analysis, reporting, and the time of presentation to the Courts. This is very important to avoid the possibility of any suggestion that the evidence has been compromised in any way.
- Data Collection: This is where chain of custody process is initiated. It involves identification, labeling, recording, and the acquisition of data from all the possible relevant sources that preserve the integrity of the data and evidence collected.
- Examination: During this process, the chain of custody information is documented outlining the forensic process undertaken. It is important to capture screenshots throughout the process to show the tasks that are completed and the evidence uncovered.
- Analysis: This stage is the result of the examination stage. In the Analysis stage, legally justifiable methods and techniques are used to derive useful information to address questions posed in the particular case.
- Reporting: This is the documentation phase of the Examination and Analysis stage. Reporting includes the following:
  - Statement regarding Chain of Custody.
  - Explanation of the various tools used.
  - A description of the analysis of various data sources.
  - Issues identified.
  - Vulnerabilities identified.
  - Recommendation for additional forensics measures that can be taken.
- The Chain of Custody Form
  - In order to prove a chain of custody, you'll need a form that lists out the details of how the evidence was handled every step of the way. The form should answer the following questions:
  - What is the evidence?: For example- digital information includes the filename, md5 hash, and Hardware information includes serial number, asset ID, hostname, photos, description.
  - How did you get it?: For example- Bagged, tagged or pulled from the desktop.
  - When it was collected?: Date, Time
  - Who has handle it?
  - Why did that person handled it?

Computer Forensics Investigation

Computer Forensics is a field of Technology that uses investigative techniques to identify & store evidence from a computer device.

it has 5 basic stages

- (A) — Identification
- (B) — Preservation
- (C) — Collection
- (D) — Analysis
- (E) — Reporting

The first stage identifies potential sources of relevant information as well as key & locations of data

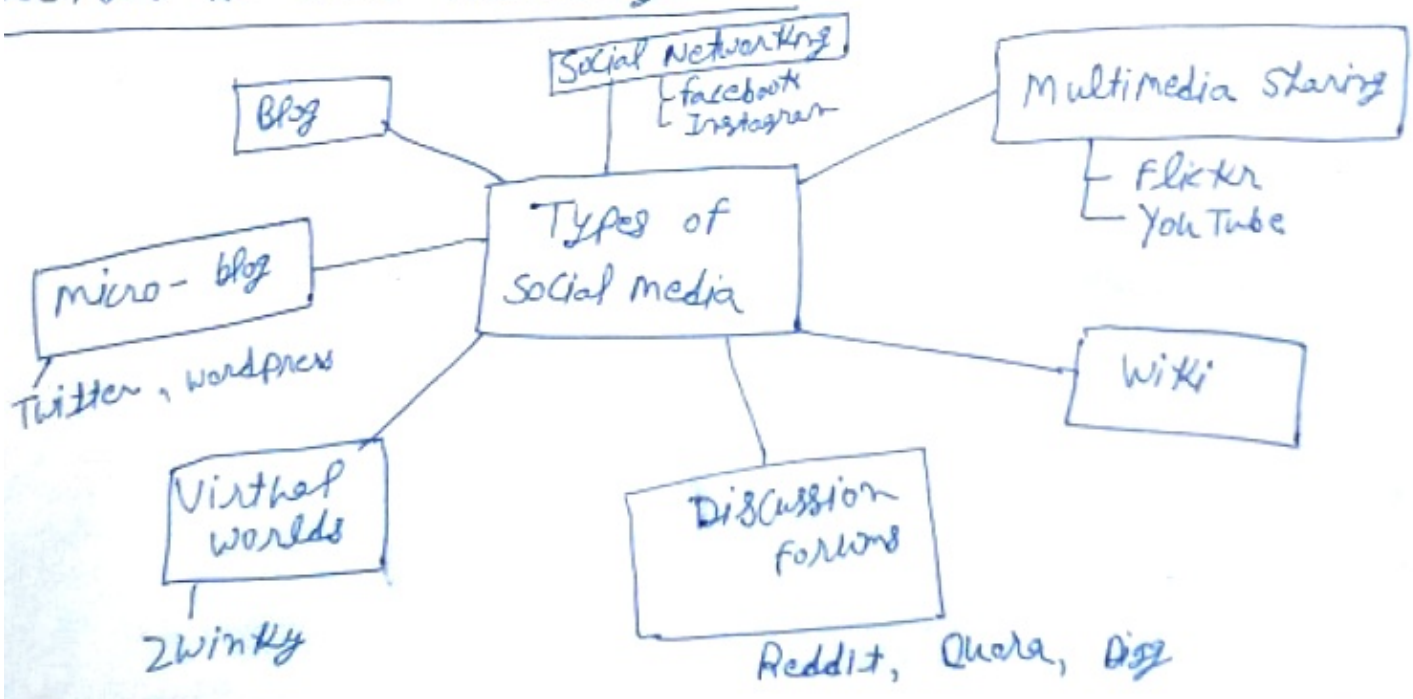
The Process of preservation relevant electronically stored Information [ESI] by protecting the crime or incident scene, Capturing visual images of the scene.

Collection of Digital Information that may be relevant to the investigation Collection may involve removing the electronic device from the crime or incident scene and then imaging, copying or printing out its content.

Analysis means search of evidence relating to the incident being investigated. The outputs of examination are data objects found in the collected Information.

Reporting — makes a report based on techniques & methodology.

rensics & Social Networking Sites



Types of Social Media Crime

Social media need no Introduction. At Present it has over 3.377 billion users are active on social media who spend over 116 minutes Perday on an average.

Social media is any application or website that facilitates users to interact & socialize, share ideas & Information, upload Photos & Vids Participate in Various activities / events & engage in real time conversations

Social media statistics

1. facebook adds 6 new profiles every seconds
2. 1.3 billion accounts on Twitter
3. ~~Linkedin~~ Contain 500 million users.
   Linkedin
4. Snapchat contain 187 million users.
5. Pinterest - 200 million active user.
6. Youtube 1148 billion mobile video views each days.

"The Black Hole Called Social media"

"A Place in the network where incoming or outgoing traffic is Silently Discarded"

Types of Social Networking Platforms

1. Social Networks → Facebook, Twitter, Whatsapp, Linkedin
2. Media Sharing Networks → Instagram, Snapchat, Youtube
3. Discussion forums → Reddit, Quora, Digg
4. Bookmarking & Content Curation Networks → Pinterest Flipboard
5. Consumer Review Network → Yelp, Zomato, TripAdvisor
6. Blogging & publishing Networks - wordpress, Tumblr, medium
7. Sharing Economy Networks → Uber, Airbnb
8. Anonymous Social Network → Ask.fm, Afterschool

Types of Social media crime

- Hacking
- photo morphing
- offer & shopping scam
- Dating scams
- Cyber bullying (Cyber stalking)
- Link Baiting
  (Victim gets a message "somebody just put up these pictures of you drunk at the party! check out here"
- Information Theft

The Security / Privacy Threats

Information security threat can be many like Software attacks theft of Intellectual property, Identity theft, theft of equipment or information & extortion of Information.

Threats can be anything that can take advantage of a vulnerability to breach security.

Malware is a combination of malicious & Software

malicious S/W can be an Intrusive program code or a anything that is designed to perform malicious operations on system.

Malware may be

- Virus
- Worms
- Trojan
- Bots

Malware Based on Actions

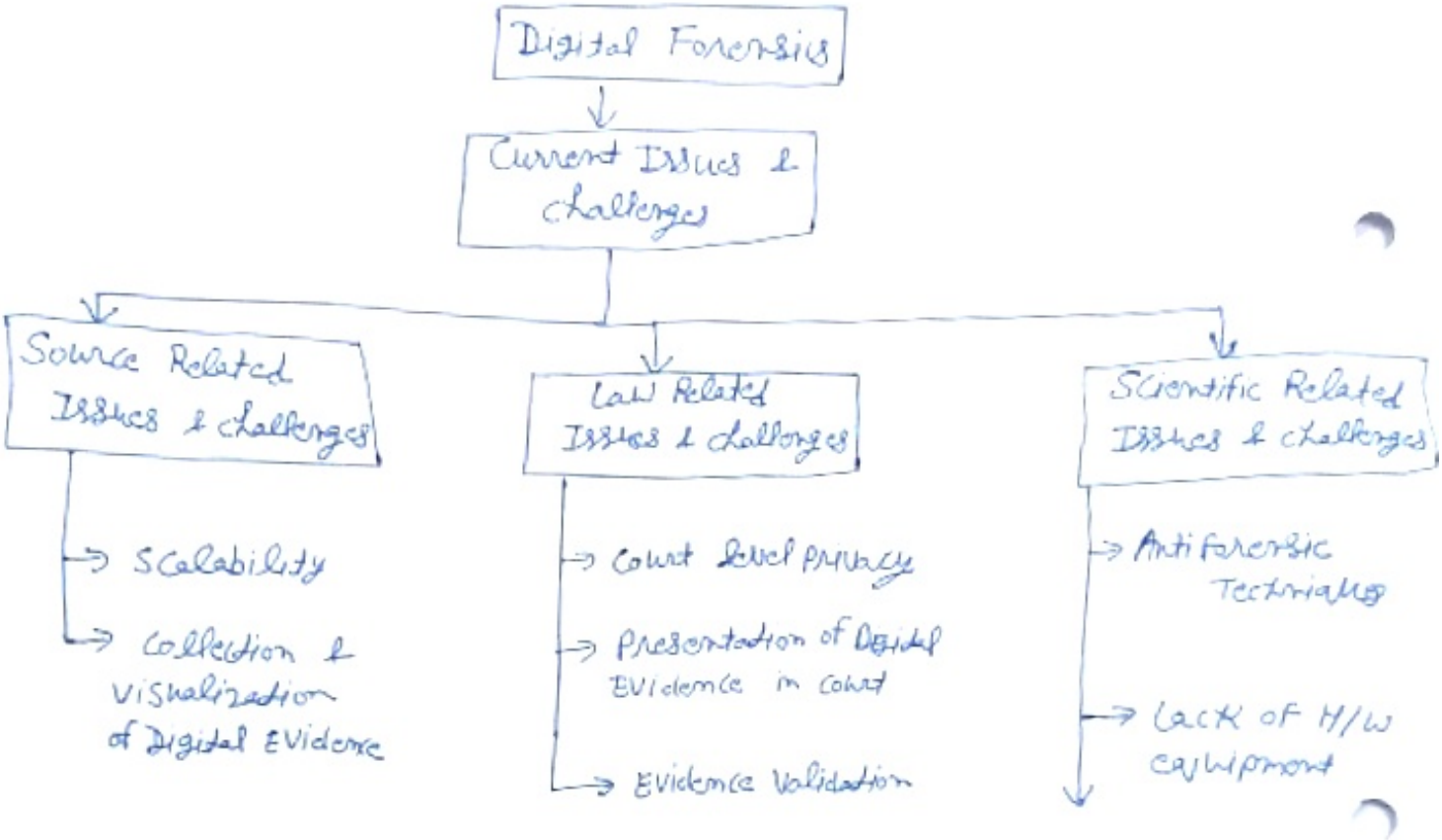
- Adware
- Spyware
- Keylogger

Ransomware – it is type of malware that will either encrypt your file or will lock your computer. a screen display asking for money.

Scareware – The S/W will display to force to take some action.

Root Kits – Design to gain root access for administrative Privileges

Challenges for Digital forensics



Challenges

- Legal Issues
- Nature of Digital Evidence
- Alteration of Evidence
- Size & Distribution of Evidence
- malware presents in Evidence
- Steganography
- Encryption

4 (25)

- Digital forensic requires a high level of technical expertise Shortage of trained forensic analysts.
- Difficult to analysis of large amount of data
- Case complexity
- if Data is encrypted then Data recovery is difficult.
- Digital Data can become corrupted or lost over time making it difficult to retrieve and analyze.
- Need new tools for analysis