Unit 4 - Understanding Computer Forensics:

- Introduction
- Historical Background of Cyber forensics
- Digital Forensics Science
- The Need for Computer, Cyber forensics and Digital Evidence
- Forensics Analysis of E-Mail
- Digital Forensics Life Cycle
- Chain of Custody Concept
- Network Forensics
- Approaching a Computer Forensics Investigation
- Setting up a Computer Forensics Laboratory: Understanding the Requirements
- Computer Forensics and Steganography
- Relevance of the OSI 7 Layer Model to Computer Forensics
- Forensics and Social Networking Sites: The Security/Privacy Threats
- Computer Forensics from Compliance Perspective
- Challenges in Computer Forensics
- Special Tools and Techniques
- Forensics Auditing
- Anti forensics.

Introduction and Historical Background of Cyber forensics

*Digital Forensic

*Cyber Forensic

*Computer Forensic

"Forensic computing is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable."(Rodney Mckemmish 1999).

Characteristics Of Forensics

*Identifying

*Preserving

*Analyzing

*Presenting

Needs Of Computer Forensic

*To produce evidence in the court that can lead to the punishment of the actual.

* To ensure the integrity of the computer system.

*To focus on the response to hi-tech offenses, started to intertwine.

History Of Computer Forensic

*Began to evolve more than 30 years ago in US when law enforcement and military investigators started seeing criminals get technical.

*Over the next decades, and up to today, the field has exploded.

*Law enforcement and the military continue to have a large presence in the information security and computer forensic field at the local, state and federal level.

*Now a days, Software companies continue to produce newer and more robust forensic software programs.

*And law enforcement and the military continue to identify and train more and more of their personnel in the response to crimes involving technology.

Two types of crime

*computer to commit a crime

*computer as a target

Goal Of Computer Forensics

*The main goal of computer forensic experts is not only to find the criminal but also to find out the evidence and the presentation of the evidence in a manner that leads to legal action of the criminal.

What is forensic?

*Collection and analysis of evidence

* Using scientific test or techniques

* To establish facts against crime

* For presenting in A legal proceeding

* Therefore forensic science is A scientific method of gathering and examining information about the past which is then used in court of law

What is digital forensic?

* Digital forensics is the use of scientifically derived and proven methods toward

* The preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital devices

Using digital forensics techniques, one can:

1. Corroborate and clarify evidence otherwise discovered.
2. Generate investigative leads for follow-up and verification
3. Provide help to verify an intrusion hypothesis.
4. Eliminate incorrect assumptions.

ROLE

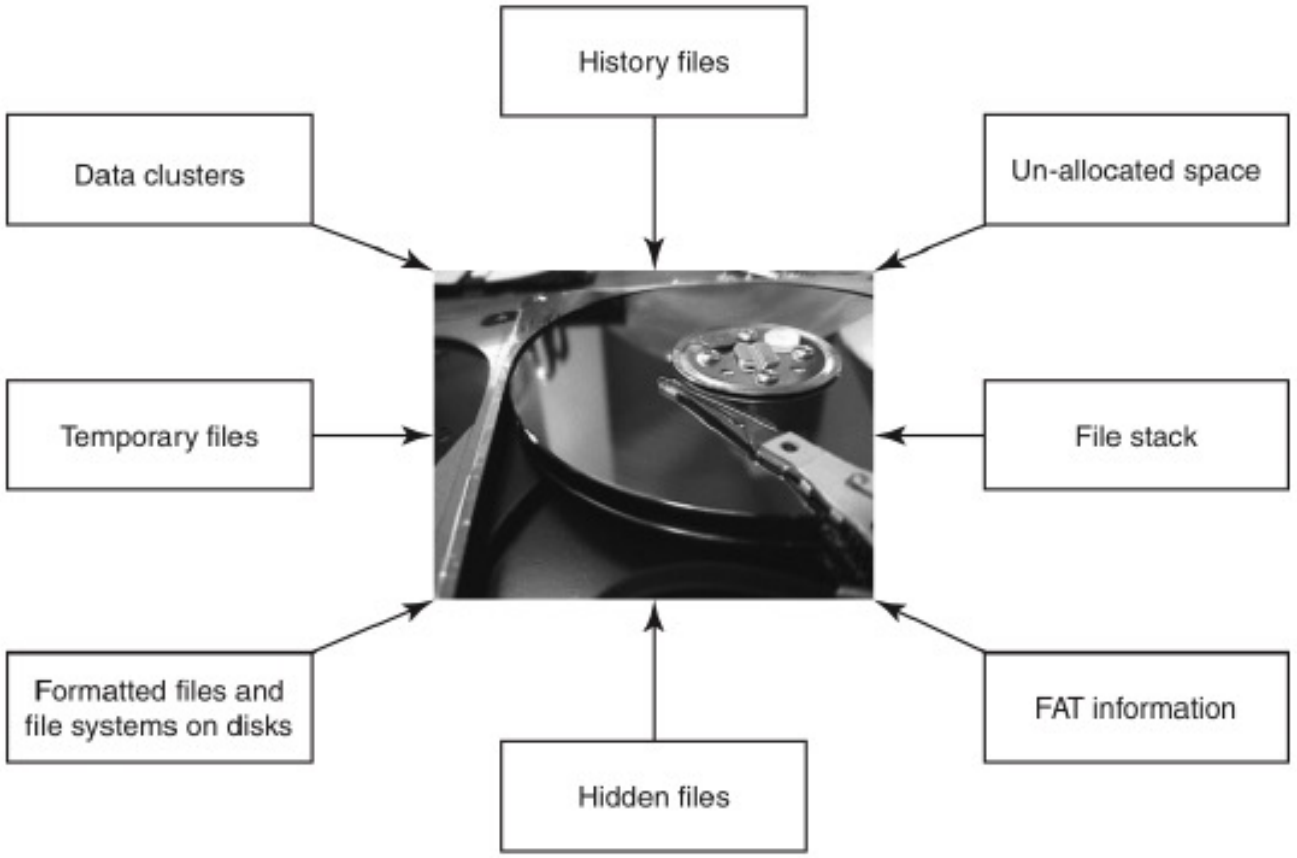
1. Uncover and document evidence and leads.
2. Corroborate evidence discovered in other ways.
3. Assist in showing a pattern of events (data mining has an application here).
4. Connect attack and victim computers.
5. Reveal an end-to-end path of events leading to a compromise attempt, successful or not.

Extract data that may be hidden, deleted or otherwise not directly available.

The typical scenarios involved are:

1. Employee Internet abuse.
2. Data leak/data breach.
3. Industrial espionage.
4. Damage assessment.
5. Criminal fraud and deception cases;
6. Criminal cases.
7. Copyright violation – more about this is mentioned.

Data Can Be Seen Through Forensic Tools



The Need for Computer Forensics

*computers worldwide together have brought about many advantages to mankind.

*devices provides avenues for misuse as well as opportunities for committing crime.

*Chain of custody means the chronological documentation trail, etc. that indicates the seizure, custody, control, transfer, analysis and disposition of evidence, physical or electronic.

*“Fungibility” means the extent to which the components of an operation or product can be inter- changed with similar components without decreasing the value of the operation or product.

*Chain of custody is also used in most evidence situations to maintain the integrity of the evidence by providing documentation of the control, transfer and analysis of evidence.

Cyber forensics and Digital Evidence

Cyber forensics can be divided into two domains:

1. Computer forensics.

2. Network forensics.

Network forensics is the study of network traffic to search for truth in civil, criminal and administrative matters to protect users and resources from exploitation, invasion of privacy and any other crime fostered by the continual expansion of network connectivity.

As compared to the “physical” evidence, “digital” evidence is different in nature because it has some unique characteristics.

Digital evidence is much easier to change/manipulate! Second, “perfect” digital copies can be made without harming original.

There are number of contexts involved in actually identifying a piece of digital evidence:

1. Physical context: It must be definable in its physical form, that is, it should reside on a specific piece of media.

2. Logical context: It must be identifiable as to its logical position, that is, where does it reside relative to the file system.

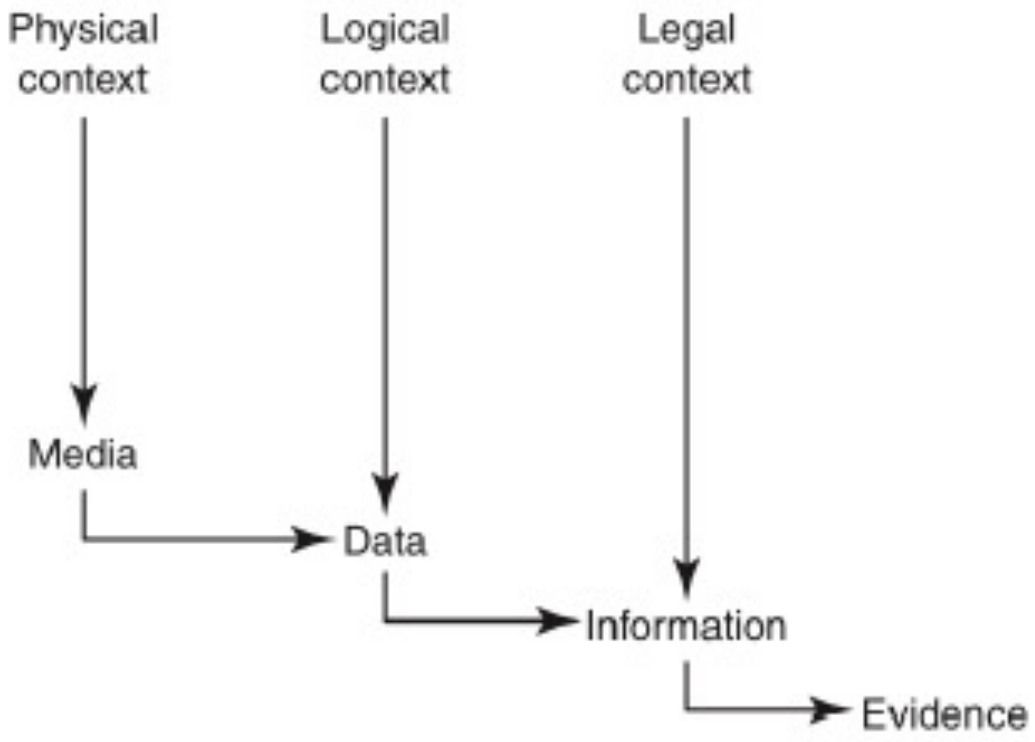
3. Legal context: the evidence in the correct context to read its meaning.

This may require looking at the evidence as machine language, for example, American Standard

Some guidelines for the (digital) evidence collection phase:

1. Adhere to your site's security policy and engage the appropriate incident handling and law enforcement personnel.

2. Capture a picture of the system as accurately as possible.



Rules of evidence:

* Indian evidence act 1872→ oral evidence , documentary evidence

Guidelines To Collect The Evidence

*keep detail notes with date and time

*Notes and printout should be signed.

* Note difference between the system clock and universal time.

* Outline all action you took and at what time -detail notes .

* minimize changes to the data as you are collecting it – avoid changes .

* Remove the external changes.

* Collect first and analysis later.

* Possible automate .

* spread the work among the team.

* Less volatile - power off data erase.

* Bit level copy .

Digital Forensics Life Cycle

* cardinal rule :

1.Is admissible.

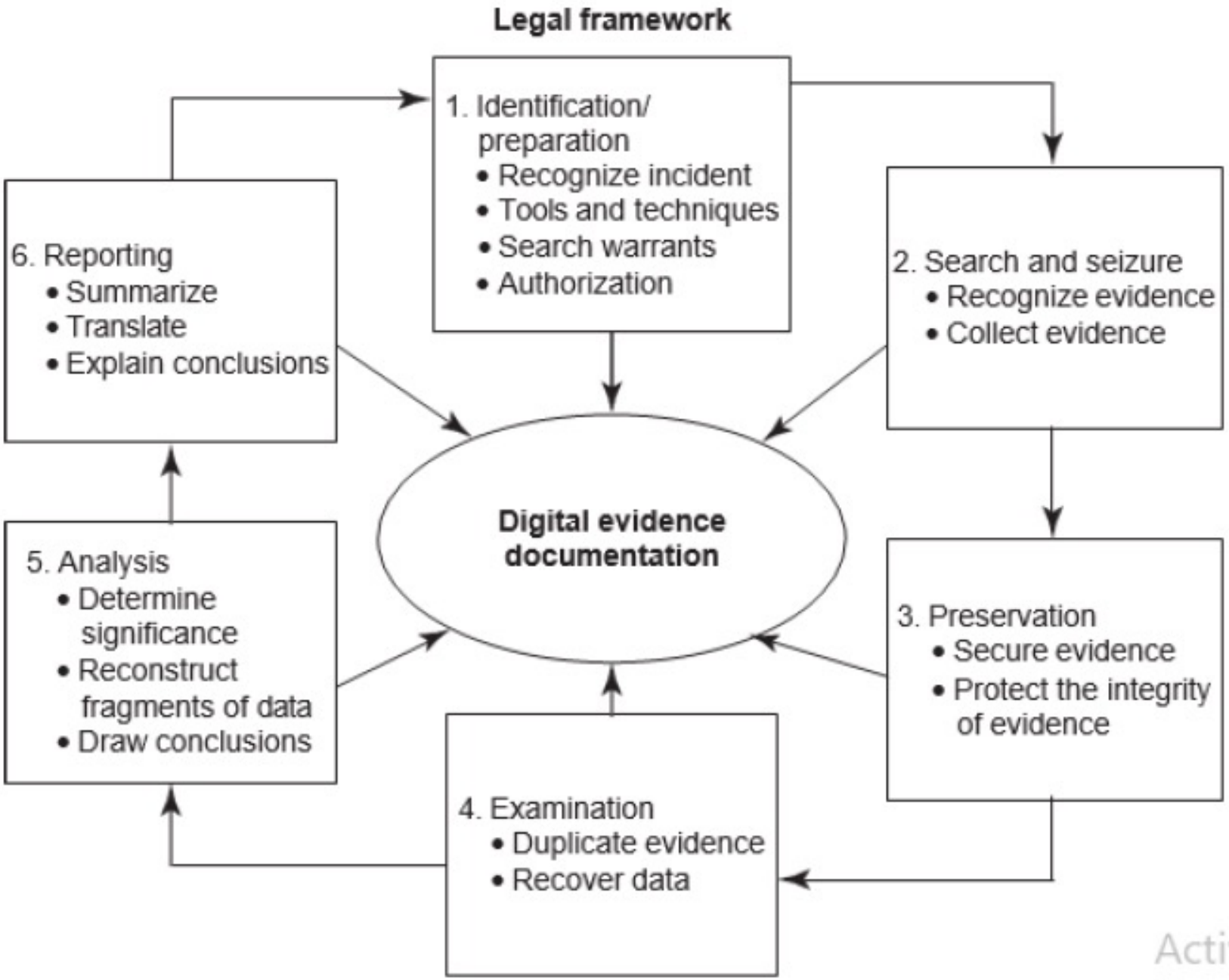
2. Is authentic.

3. Is complete.

4. Is reliable.

5. Is understandable and believable.

The digital forensics process needs to be understood in the legal context starting from preparation of the evidence to testifying.


Legal framework
1. Identification/ preparation
• Recognize incident
• Tools and techniques
• Search warrants
• Authorization
2. Search and seizure
• Recognize evidence
• Collect evidence
3. Preservation
• Secure evidence
• Protect the integrity of evidence
4. Examination
• Duplicate evidence
• Recover data
5. Analysis
• Determine significance
• Reconstruct fragments of data
• Draw conclusions
6. Reporting
• Summarize
• Translate
• Explain conclusions
Digital evidence documentation

The Phases in Computer Forensics/Digital Forensics

*The investigator must be properly trained to perform the specific kind of investigation that is at hand.

* Tools that are used to generate reports for court should be validated.

* There are many tools to be used in the process.

* One should determine the proper tool to be used based on the case.

1. Preparation and identification

2. Collection and recording

3. Storing and transporting

4. Examination/investigation

5. Analysis, interpretation and attribution

6. Reporting

7. Testifying.

The process involves the following activities:

1. **Prepare**: case briefings, interrogatories, spoliation prevention, disclosure and discovery planning, discovery requests.

2. **Record**: drive imaging, indexing, profiling, search plans, cost estimates, risk analysis.

3. **Investigate**: triage images, data recovery, keyword searches, hidden data review, communicate, iterate.

4. **Report:** oral vs. Written, relevant document production, search statistic reports, chain of custody reporting, case log reporting.

5. **Testify**: testimony preparation, presentation preparation.

Preparing for the Evidence and Identifying the Evidence

*Evidence must first be identified as evidence.

*It can happen that there is an enormous amount of potential evidence available for a legal matter

*sequence of event in the single time stamp

*vast majority of the potential evidence may never get identified.

Collecting and Recording Digital Evidence

*Digital evidence can be collected from many sources.

*Obvious sources include computers, cell phones, digital cameras, hard drives, CD-ROM, USB memory devices and so on.

* Non-obvious sources include settings of digital thermometers, black boxes inside automobiles, RFID tags and webpages

*which must be preserved as they are subject to change.


HD
INDEX


LOCK
SD
HC
CLASS 6
8GB


DAT
Digital Audio Tape
120


OK
MODE
DISPLAY
LETSGODIGITAL


DAT
DM 46


Mini DV
Master
83

Storing and Transporting Digital Evidence

1. Image computer media using a write-blocking tool to ensure that no data is added to the suspect device

2. establish and maintain the chain of custody.

3.Storage : (a) Read-only memory (ROM) chips; (b) erasable programmable read-only memory (EPROM) chip; (c) programmable read-only memory (PROM) chips; (d) electrify erasable programmable read-only memory (EEPROM) chips.

4.tools and methods -> tested

5.Some of the most valuable information obtained in the course of a forensics examination will come from the computer user.

6. special care – chain of custody

Examining / Investigation Digital Evidence :

*Live and dead analysis = live →shutdown process

* Exact duplicate data

* To prevent tampering

* starts OS investigation

*evidence verified by forensic specialist

* imaging for the original data is done

Analysis ,interpretation and attribution

suspect information in order , discovering fact , cracking password, performing keyword search

Types of analysis

* Media analysis - s
* Media management analysis-
* File system analysis p
* Application analysis- con
* Network analysis- com,pack,tra
* Image analysis -hidd
* Video analysis –

Reporting

→ oral , written format , complex, tricky process, beyond the scope

The following are the broad-level elements of the report

1. Identity of the reporting agency
2. Case identifier or submission number
3. Case investigator
4. Identity of the submitter
5. Date of receipt
6. Date of report
7. Descriptive list of items submitted for examination, including serial number, make and model
8. Identity and signature of the examiner
9. Brief description of steps taken during examination, such as string searches, graphics image searches and recovering erased files
10. Results/conclusions.

Testifying

*This phase involves presentation and cross-examination of expert witnesses.

*Depending on the country and legal frameworks in which a cybercrime case is registered, certain standards may apply with regard to the issues of expert witnesses.

*sufficient fact or data

*reliable principle and methods

*witness should be reliable for the case

Phase	*Activities/Processes*	*Outputs*
Evidence Preparation and Identification	• Monitoring authorization and management support, and obtain authorization to do the investigation. • Ensuring that operations and infrastructure are able to support an investigation. • Providing a mechanism for the incident to be detected and confirmed. • Creating an awareness so that the investigation is needed (identify the need for an investigation). • Planning for getting the information needed from both inside and outside the investigating organization. • Identifying the strategy, policies and previous investigations. • Informing the subject of an investigation or other concerned parties that the investigation is taking place.	Plan Authorization Warrant Notification Confirmation
Collection and Recording, Preserving and Transportation	• Determine what a particular piece of digital evidence is, and identifying possible sources of data. • Determine where the evidence is physically located. • Translating the media into data. • Ensuring integrity and authenticity of the digital evidence, for example, write protection, hashes, etc. • Packaging, transporting and storing the digital evidence. • Preventing people from using the digital device or allowing other electromagnetic devices to be used within an affected radius. • Recording the physical scene. • Duplicating digital evidence using standardized and accepted procedures. • Ensuring the validity and integrity of evidence for later use.	Crime type Potential Evidence Sources Media Devices Event

Phase	*Activities/Processes*	*Outputs*
Examination/ Investigation and Analysis, Interpretation and Attribution	• Determining how the data is produced, when and by whom. • Determine and validating the techniques to find and interpret significant data. • Extracting hidden data, discovering the hidden data and matching the pattern. • Recognizing obvious pieces of digital evidence and assessing the skill level of suspect. • Transform the data into a more manageable size and form for analysis. • Confirming or refuting allegations of suspicious activity. • Identifying and locating potential evidence, possibly within unconventional locations. • Constructing detailed documentation for analysis and drawing conclusions based on evidence found. • Determining significant based on evidence found. • Testing and rejecting theories based on the digital evidence. • Organizing the analysis results from the collected physical and digital evidence. • Eliminating duplication of analysis. • Build a timeline. • Constructing a hypothesis of what occurred, and comparing the extracted data with the target. • Documenting the findings and all steps taken.	Log files, file Events log Data Information

Presentation and reporting	• Preparing and presenting the information resulting from the analysis phase. • Determine the issues relevance of the information, its reliability and who can testify to it. • Interpreting the statistical from analysis phase. • Clarifying the evidence and documenting the findings. • Summarizing and providing explanation of conclusions. • Presenting the physical and digital evidence to a court or corporate management. • Attempting to confirm each piece of evidence and each event in the chain either along with each other, or independent of one evidence and/or other events. • Proving the validity of the hypothesis and defend it against criticism and challenge. • Communicating relevant findings to a variety of audiences (management, technical personnel, law enforcement).	Evidence, Report
Disseminating the case	• Ensuring physical and digital property is returned to proper owner. • Determining how and what criminal evidence must be removed. • Reviewing the investigation to identify areas of improvement. • Disseminating the information from the investigation. • Closing out the investigation and preserving knowledge gained.	Evidence Explanation New policies and investigation Procedures Evidence disposed Investigation closed

Chain of custody

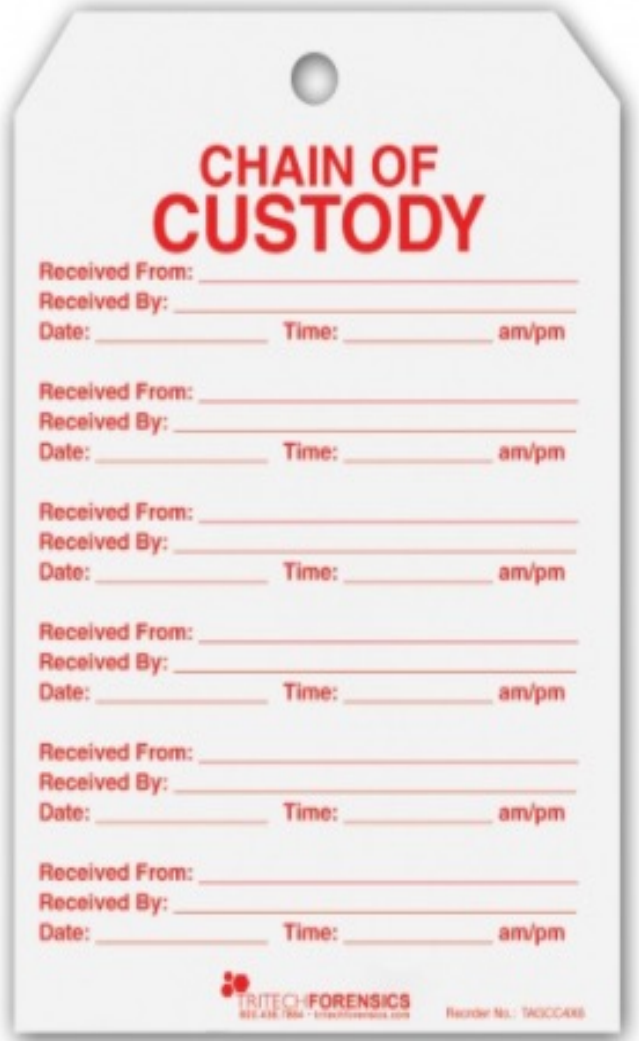
*chain of custody is the central concept in cyberforensic/digial forensics investigation.

*It is the ability to trace and safe guard the sample through all steps from collection, analysis, to final report of the result

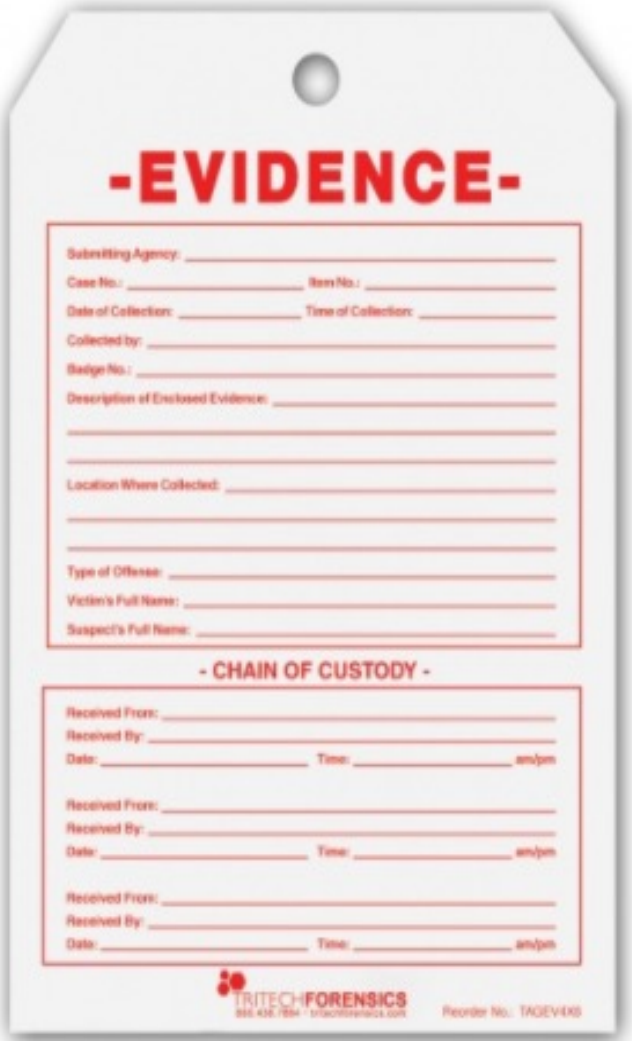
*Chain of custody indicates the collection, sequence of control, transfer and analysis.

*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.

*It demonstrates trust to the courts and to the client that the evidence has not tampered.


CHAIN OF
CUSTODY
Received From:
Received By:
Date: Time: am/pm
Received From:
Received By:
Date: Time: am/pm
Received From:
Received By:
Date: Time: am/pm
Received From:
Received By:
Date: Time: am/pm
Received From:
Received By:
Date: Time: am/pm
Received From:
Received By:
Date: Time: am/pm
TRITECH FORENSICS


-EVIDENCE-
Submitting Agency:
Case No.:
Item No.:
Date of Collection:
Time of Collection:
Collected by:
Badge No.:
Description of Enclosed Evidence:
Location Where Collected:
Type of Offense:
Victim's Full Name:
Suspect's Full Name:
TRITECH FORENSICS


-EVIDENCE-
Submitting Agency:
Case No.: Item No.:
Date of Collection: Time of Collection:
Collected by:
Badge No.:
Description of Enclosed Evidence:
Location Where Collected:
Type of Offense:
Victim's Full Name:
Suspect's Full Name:
- CHAIN OF CUSTODY -
Received From:
Received By:
Date: Time: am/pm
Received From:
Received By:
Date: Time: am/pm
Received From:
Received By:
Date: Time: am/pm
TRITECH FORENSICS

The Chain of Custody Form

What is the evidence?: For example- digital information includes the filename, 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?

Where was it stored?

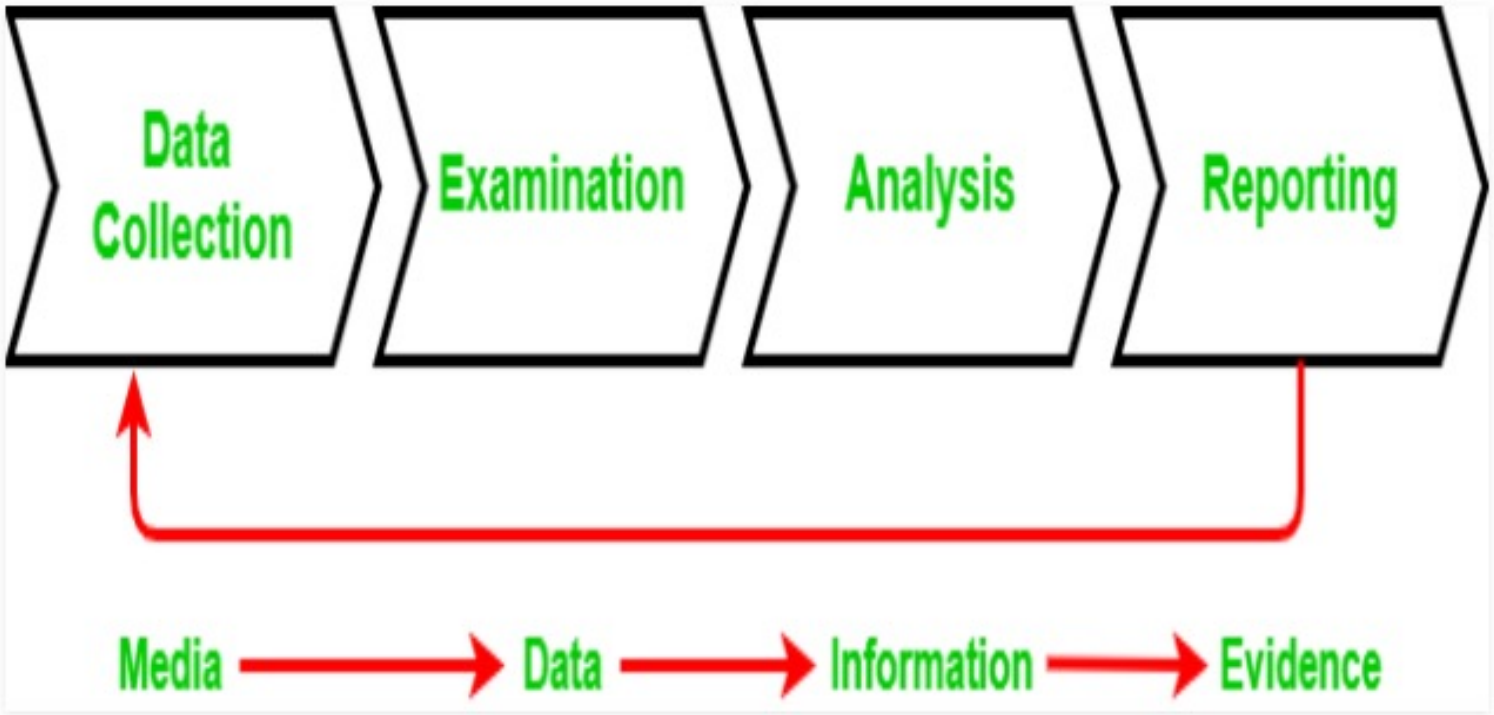
How you transported it?: For example- in a sealed static-free bag, or in a secure storage container.

How it was tracked?

How it was stored?: For example- in a secure storage container.

Who has access to the evidence?: This involves developing a check-in/ check-out process.

Stage of the chain of custody



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

Examination: It is important to capture screenshots throughout the process to show the tasks that are completed and the evidence uncovered.

Analysis: . 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.

Network forensics

***Network forensics** is a sub-branch of digital **forensics** relating to the monitoring and analysis of computer **network** traffic

* **Network forensics** can be generally **defined** as a science of discovering and retrieving evidential information in a networked environment about a crime in such a way as to make it admissible in court.

*The purposes of information gathering, legal evidence, or intrusion detection

*Process of collecting and analyzing raw network data and tracking network traffic

* how an attack was carried out *or how an event occurred on a network*

*The **process** of capture, recording, and analysis of **network** packets to determine the source of **network** security attacks is known as **Network Forensics**

* For example, web server logs can be **used** to show when (or if) a suspect accessed information related to criminal activity. Email accounts can often contain useful evidence; but email headers are easily faked and, so, **network forensics** may be **used** to prove the exact origin of incriminating material.

***Network based evidence** is also useful when examining host **evidence** as it provides a second source of event corroboration which is extremely useful in determining the root cause of an incident.

Approaching a Computer Forensics Investigation

- Criminal will always leave a track
- Not easy to find track
- Vast development in the technology
- Evidence collection has to be done correctly
- Depending on the nature of the computer
  - DO NOT CHANGE
- Engagement contract

Typical approach of investigation

1. Secure the subject system (from tampering or unauthorized changes during the investigation);
2. take a copy of hard drive/disk (if applicable and appropriate);
3. identify and recover all files (including deleted files);
4. access/view/copy hidden, protected and temp files;
5. study "special" areas on the drive (e.g., the residue from previously deleted files);
6. investigate the settings and any data from applications and programs used on the system;
7. consider the system as a whole from various perspectives, including its structure and overall contents;
8. consider general factors relating to the user's computer and other activity and habits in the context of the investigation;
9. create detailed and considered report, containing an assessment of the data and information collected.

Typical Elements Addressed in a Forensics Investigation Engagement Contract

- Authorization
- Confidentiality
- Payment
- Consent and acknowledgement
- Limitation and liability

No. 067 /A-6011/14/2011/14/PERS.II SECTION.
Government of India
CENTRAL BUREAU OF INVESTIGATION
(Department of Personnel & Training), New Delhi.

ENGAGEMENT OF PAIRVI OFFICERS ON CONTRACTUAL BASIS IN CBI

Looking for retired and serving Police Officers of the rank of Inspector and above for appointment as Pairvi Oficers on contractual basis initially for a period of 01 year which can be extended upto 03 years at a consolidated remuneration not exceeding Rs.40,000/- per month. The person engaged shall have no right to claim regularization/absorption in the organization after the expiry of period of contract.

2. The retired officers of the Central/State Police Forces of the rank of Inspector or above with 10 years of experience in Investigation and Prosecution of Criminal Cases in the Court of Law are eligible for appointment to the above mentioned post. The candidates will be on whole time appointment and will have no right to undertake part time private employment during the period of contract.

3. The total vacancies of Pairvi Officers is 22+1*=23. The number of vacancies at each location are given in Annexure-I. The number of vacancies and place of interview are subject to change.

4. The application forms can be downloaded from CBI website (www.cbi.nic.in). The completed application in the prescribed format (Annexure –II) alongwith requisite documents may be sent by Regd./Speed Post on addresses given against each location in Annexure-I. **The last date of receipt of applications11-03-2013.**

5. Incomplete application and application received after last date will be summarily rejected.

*One post of Pairvi Officer (Contract basis) is lying vacant at Kolkata against the strength of 6 Pairvi Oficers (Contract basis).

Sd/-

Dy. Director (Admin.)
CBI/HO/New Delhi

1. Copy to all Head of Zones and Head of Branches
2. CBI website

Solving a computer forensic case

- Prepare for the forensic examination
- Talk to key people
- Circumstance Surrounding the case
- Start assembling the question
- Collect data from the target
- Extract the answer for the question
- Collect the evidence – Email
- Analysis the evidence
- Report your findings

Setting up a Computer Forensics Laboratory: Understanding the Requirements

- Four requirement
  - Physical space
  - Hardware
  - Software
  - Investigation aids - procedure

Forensics Analysis of E-Mail

*Fake mails for various cybercrime offenses.

* There are tools available that help create fake mails

* Forensics analysis of E-Mails is an important aspect of cyber forensics analysis

* Common means of communication.

* E-Mail act as the digital evidence.

* E-mail system include hardware and software

* Two important component :Email- server, Email-gateway

* Email server -Forward , collect, store, deliver

* Email gateway - connection between the email server

* Mail server software - controls flow of email , compose ,send ,read, all action

* Two parts = header and body

* Mail server software is a network server software that controls the flow of

* E-Mail and the mail client software helps each user read, compose, send and delete messages.

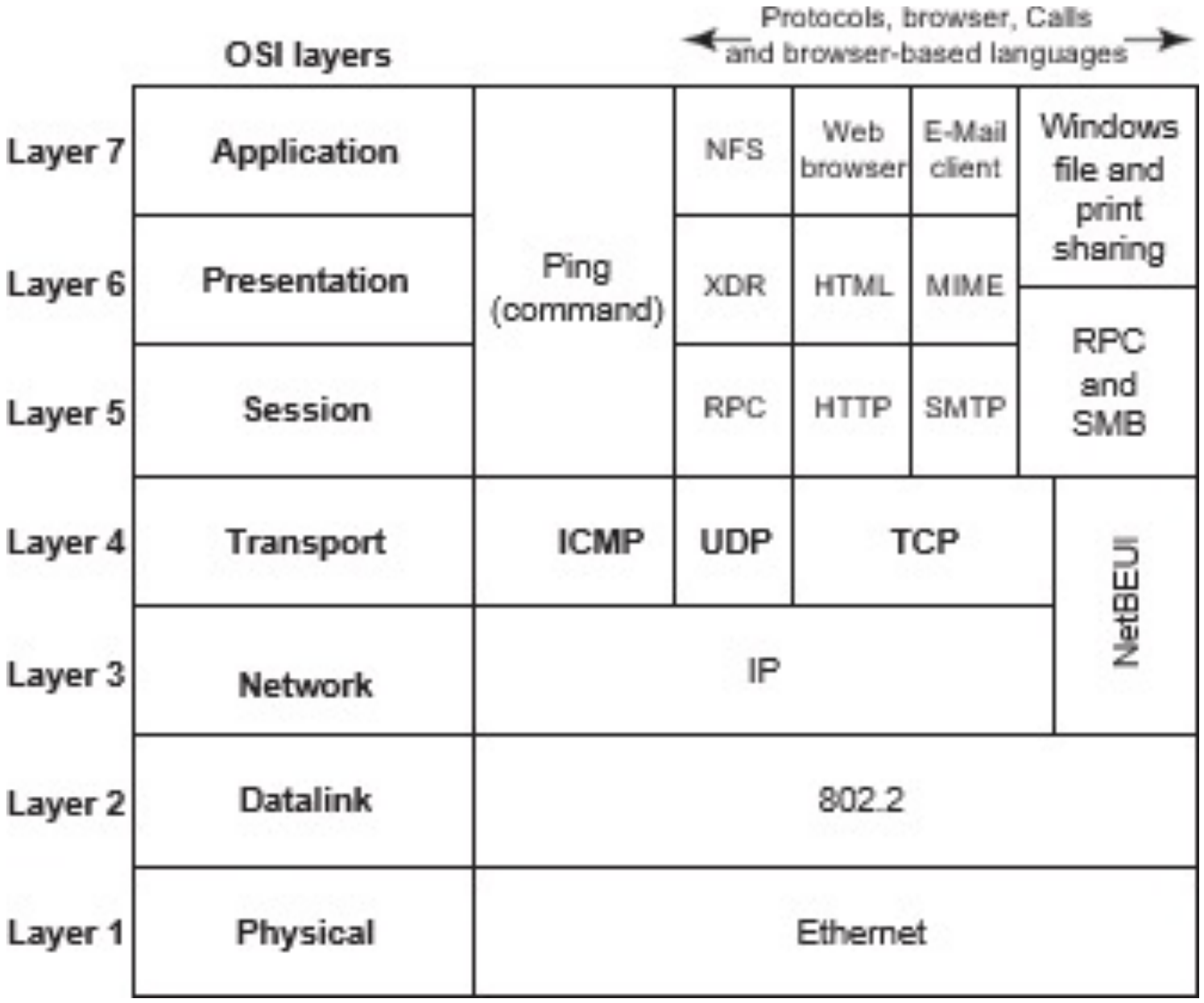
* E-Mail tracing is done by examining the header information contained in E-Mail messages to determine their source.

Message header

1. Return-Path: <secret@hotmail.com>
2. Received: from mailhub-1.net.treas.gov ([10.7.14.10]) by nccmail.usss.treas.gov for <avenit@usss.treas.gov>; Fri, 18 Feb 2000 11:46:07-0500
3. Received: from mx-relay.treas.gov ([199.196.144.6]) bytias4.net.treas.gov via smtpd (for mailhub.net.treas.gov [10.7.8.10]) with SMTP; 18 Feb 2000 16:55:44
4. Received: from hotmail.com (f7.law4.hotmail.com [216.33.149.7]) by mx-relay2.treas.gov for <avenit@usss.treas.gov>; Fri, 18 Feb 2000 11:55:44 – 0500 (EST)
5. Message-ID: <20000218165543.56965.qmail@hotmail.com>
6. Received: from 199.196.144.42 by www.hotmail.com with HTTP; Fri, 18 Feb 2000 08:55:43
7. X-Originating-IP: [199.196.144.42]
8. From: "Secret" <secret@hotmail.com>
9. To: avenit@usss.treas.gov
10. CC: smith@aol.com

Relevance of the OSI 7 Layer Model to Computer Forensics

- The OSI 7 Layer Model is useful from computer forensics perspective because it addresses
- the network protocols and network communication processes. The basic familiarity with the OSI 7
- Layer Model is assumed for the discussion in this section.


OSI layers
Protocols, browser, Calls and browser-based languages
Layer 7
Application
Layer 6
Presentation
Layer 5
Session
Layer 4
Transport
Layer 3
Network
Layer 2
Datalink
Layer 1
Physical
Ping (command)
NFS
Web browser
E-Mail client
Windows file and print sharing
XDR
HTML
MIME
RPC and SMB
RPC
HTTP
SMTP
ICMP
UDP
TCP
NetBEUI
IP
802.2
Ethernet

Network hackers

Foot printing Step 1

Scanning and probing Step 2

Gaining access Step 3

Privilege escalation Step 4

Exploiting Step 5

Retracting Step 6

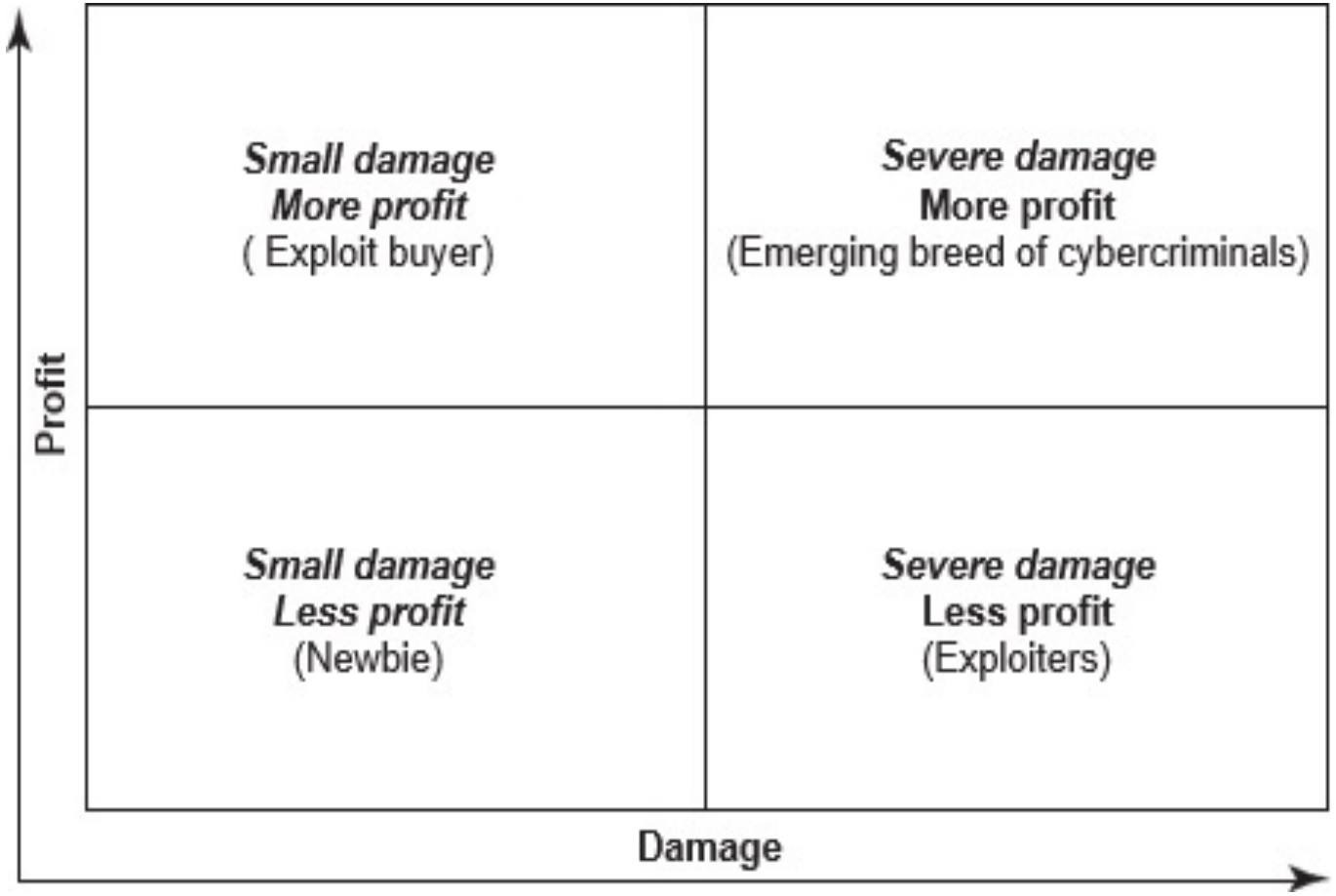
Installing backdoors Step 7

Step 1: foot printing

- Create a full profile of the organization's security posture.
- These include its domain names, ip addresses and network blocks.
- Ip, domain- scan ,ping sweeps= nmap

Step 2: scanning and probing

- Hacker send a ping echo request packet to a series of target IP addresses.
- Confirming that there is a live machine associated with that address.
- TCP scan sends a TCP synchronization request to a series of ports and to the machines that provide the associated service to respond.
- Nmap- device type and os details, weakness of the system


Small damage
More profit
(Exploit buyer)
Severe damage
More profit
(Emerging breed of cybercriminals)
Small damage
Less profit
(Newbie)
Severe damage
Less profit
(Exploiters)
Profit
Damage

Step 3: Gaining Access

- The hacker's ultimate goal is to gain access to your system
- can perform some malicious action, such as stealing credit card information, downloading confidential files or manipulating critical data.
- Security weakness of individual machine

Step 4: Privilege

- privileges granted to the user or account that is running the process that has been exploited.
- Root user – super power

Step 5: Exploit

- Every hacker seems to have own reasons for hacking. Some hackers do it for fun or a challenge, some do it for financial gain
- others do it to "get even".

Step 6: Retracting

- Don’t want to caught and sent to jail
- Hackers take some time to change the log
- Try to mislead the forensic investigation

Step 7: Installing Backdoors

- most hackers will try creating provisions for entry into the network/hacked system
- backdoor to allow them access

Computer forensic and steganography

- Steganography is art of hiding
- Technology – immoral purpose
- Goal of **steganography** is to insert a message into a carrier signal so that it cannot be detected by unintended recipients.
- **Steganalysis** attempts to discover hidden signals in suspected carriers or at the least detect which media contain hidden signals.
- Difference between crytography and stegaography .
- Some times it called as antiforensic method

Other method act as antiforensic method

- Encryption
- Self splitting file encryption
- Database rootkit
- BIOS rootkits
- Bypassing integrity checkers

Rootkits

- A rootkit is malicious software that is extremely difficult to spot and, therefore, very difficult to remove.
- One of the most famous and dangerous rootkits in history was stuxnet.
- Designed to infect a target pc and allow an attacker to install a set of tools that grant him persistent remote access to the computer.
- Spy on your computer.
- often bury themselves deep into the operating system

- Three main function:
  - Maintain root access to the system
  - Hide the presence of the attacker
  - Attack against other system

  Primary function - access via communication , protocols

  Second function - misrepresent the function and confuse the systen

  Third function – meet the attacker objective ,gather the packet traces on local network ,vulnerability scans ,launch automated attacks
  - super user access to a computer

Binary Rootkits

- Take administrative utilities and modify them to hide specific connection
- No limitation in the changes – root ,admin,user
- Hide inside until compromise (settlement)
- Create confusing and unsuspecting directory name
- Ignore the common files and temp files

Information hiding

- Digital age – hidden In many ways
- Stenography - invisible to casual observer
- Two reason for hiding
  - Trying to protect the confidential data
  - Interesting in hiding

  Three common approach
  - least sign bit
  - masking
  - algorithms

Challenges in Computer Forensics

- Investigation of cybercrimes is not a easy task.
- Looking for forensic evidence difficult
- **Challenges:**
- Most of the exsiting tools and methods allows anyone to alter any attributes associated with digital data.
- How to collect the specific, probative and case-related info from very large groups of files; Approaches like: link analysis and visualization.
- Need techniques for lead discovery, for “patterns” - text & data mining; intelligent info retrieval;

Network forensics Challenges

- N/w spans multiple time-zones and multiple jurisdictions.
- This makes it necessary to use absolutely trusted timestamps(to ensure the authentication and integrity of timestamps for each piece of network evidence) and ensuring the all jurisdictions collaborate.
- N/w data are available in both offline and real-time mode.
- Data involves many different protocols and the amount of data could potentially be very large due to increasing n/w bandwidth.
- Protocols involves multiple layer of signals.
- There need to be a paradigm shift for network forensics techniques to analyse the rate and size of captured data.