Unit VI Understanding Computer Forensics

Content

- Introduction and Historical Background of Cyber forensics
- Digital Forensics Science, The Need for Computer Forensics
- 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
- Tools and equipment requirements for forensics
- Computer Forensics and Steganography
- Relevance of the OSI 7 Layer Model to Computer Forensics
- Forensics and Social Networking Sites
- Challenges in Computer Forensics
- Special Tools and Techniques
- Forensics Auditing
- Antiforensics

INTRODUCTION

- The purpose of this chapter is to address the other side of crime, that is, use of forensic techniques in the investigation of cybercrimes.
- "Cyber forensics" is a very large domain and addressing it in a single chapter is indeed a challenge.
- Complex technical aspects involved in digital forensics/computer forensics are not possible to cover in a single chapter.
- Therefore, this chapter is aimed at only providing a broad understanding about cyber forensics.
- Cyber forensics plays a key role in investigation of cybercrime. "Evidence" in the case of "cyber offenses" is extremely important from legal perspective.
- There are legal aspects involved in the investigation as well as handling of the digital forensics evidence.
- Only the technically trained and experienced experts should be involved in the forensics activities.

INTRODUCTION

- Computer forensics is primarily concerned with the systematic "identification," "acquisition," "preservation" and "analysis" of digital evidence, typically after an unauthorized access to computer or unauthorized use of computer has taken place;
- While the main focus of "computer security" is the prevention of unauthorized access to computer systems as well as maintaining "confidentiality," "integrity" and "availability" of computer systems.

Historical Background of Cyber forensics

- 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. Law enforcement and the military continue to identify and train more and more of their personnel in the response to crimes involving technology.
- 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.

Historical Background of Cyber forensics

- There are two categories of computer crime: one is the criminal activity that involves using a computer to commit a crime, and the other is a criminal activity that has a computer as a target.
- Forensics means a “characteristic of evidence” that satisfies its suitability for admission as fact and its ability to persuade based upon proof.
- The goal of digital forensics is to determine the “evidential value” of crime scene and related evidence.
- The Florida Computer Crimes Act was the first computer crime law to address computer fraud and intrusion.
- It was enacted in Florida in 1978. “Forensics evidence” is important in the investigation of cybercrimes.

Digital Forensics Science

- Digital forensics is the application of analysis techniques to the reliable and unbiased collection, analysis, interpretation and presentation of digital evidence.
- 1. Computer forensics
- It is the lawful and ethical seizure, acquisition, analysis, reporting and safeguarding of data and metadata derived from digital devices which may contain information that is notable and perhaps of evidentiary value to the trier of fact in managerial, administrative, civil and criminal investigations.
- In other words, it is the collection of techniques and tools used to find evidence in a computer.

Digital Forensics Science

- 2. Digital forensics
- It 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 sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.
- It is difficult to provide a precise definition of “digital evidence” because the evidence is recovered from devices that are not traditionally considered to be computers.

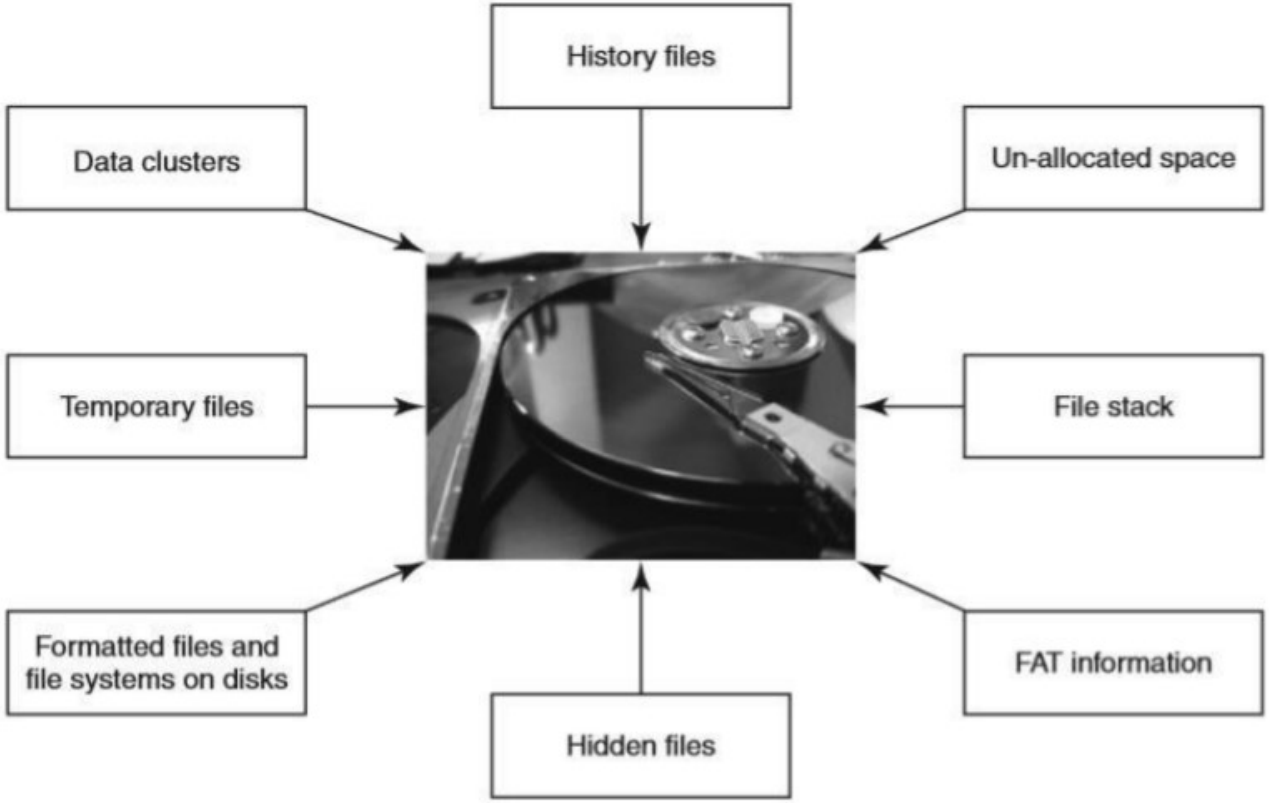
Digital Forensics Science

- Some researchers prefer to expand the definition by including the "collection" and "examination" of all forms of digital data, including the data found in cell phones, PDAs, iPods and other electronic devices.
- 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.

Digital Forensics Science

- 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

Digital Forensics Science



Data seen using forensics tools. FAT means file allocation table.

Digital Forensics Science

- Using digital forensics techniques, one can:
- 1. Corroborate and clarify evidence otherwise discovered.
- 2. Generate investigative leads for follow-up and verification in other ways.
- 3. Provide help to verify an intrusion hypothesis.
- 4. Eliminate incorrect assumptions.

Box 7.1 COFEE Time

- Computer Online Forensic Evidence Extractor (COFEE) is a tool kit, developed by Microsoft, to help computer forensic investigators extract evidence from a Windows computer.
- Installed on a USB flash drive or other external disk drive, it acts as an automated forensic tool during a live analysis.
- Microsoft provides COFEE devices and online technical support free to law enforcement agencies.
- COFEE was developed by Anthony Fung, a former Hong Kong police officer who now works as a senior investigator on Microsoft's Internet Safety Enforcement Team.
- Fung conceived the device following discussions he had at a 2006 law enforcement technology conference sponsored by Microsoft. The device is used by more than 2,000 officers in at least 15 countries.

Box 7.1 COFEE Time

- A case cited by Microsoft in April 2008 credits COFEE as being crucial in a New Zealand investigation into the trafficking of child pornography, producing evidence that led to an arrest.
- In April 2009 Microsoft and Interpol signed an agreement under which INTERPOL would serve as principal international distributor of COFEE.
- University College Dublin's Center for Cyber Crime Investigations in conjunction with Interpol develops programs for training forensic experts in using COFEE.
- The National White Collar Crime Center has been licensed by Microsoft to be the sole US domestic distributor of COFEE.
- First COFEE is configured in advance with an investigator selecting the data they wish to export, this is then saved to a USB device for plugging into the target computer.

Box 7.1 COFEE Time

- A further interface generates reports from the collected data. Estimates cited by Microsoft state jobs that previously took 3–4 hours can be done with COFEE in as little as 20 minutes.
- COFEE includes tools for password decryption, Internet history recovery and other data extraction.
- It also recovers data stored in volatile memory which could be lost if the computer were shut down.
- COFEE consists of three major components the GUI interface for the investigator, the command-line application to be executed on the target machine, and the individual tools which are managed by COFEE and the command-line application.
- It can execute 150 commands on target machine. COFEE was given to law enforcement agencies by Microsoft until it was leaked by Wikileaks in 2009. But nonetheless it is still a handy forensic tool.

Box 7.2 Differences between Forensics Policy and Security Policy

- Number of people believe both of them to be the same, which is not true.
- Security policy is a statement that clearly specifies allowed and disallowed elements with respect to security.
- Forensic policy is a statement that clearly states which assets are forensically important. It also specifies the data needed for investigation into breach of those assets.
- Violation of security policy leads to insecure information systems with vulnerabilities arising due to consequences of insider misuse.
- Violation of forensic policy means lack of evidence which results in the loss of ability of an organization to prove guilty the people who are involved in cybercrime incidence.
- The goal of both policies are different. Goal of forensic policy deal with assets, data and possible storage issues.
- They capture digital evidence and hence integrity of data is preserved.

Box 7.2 Differences between Forensics Policy and Security Policy

- They capture enough data to ensure that prosecution is possible. Forensic policy goals specify the events that must be handled and data that must be preserved.
- Example: Goal is to capture data from network intrusions for possible prosecution.
  - The forensic policy states that all events identified as intrusions have their associated data captured and preserved.
  - Enforcement mechanisms: routine preservation of IDS (Intrusion Detection System), firewall, router and web server logs for some configurable length of time.

The Need for Computer Forensics

- The convergence of Information and Communications Technology (ICT) advances and the pervasive use of computers worldwide together have brought about many advantages to mankind.
- At the same time, this tremendously high technical capacity of modern computers/computing devices provides avenues for misuse as well as opportunities for committing crime.
- The users, businessmen, and organizations have to live with a constant threat from hackers who are very advanced now.
- Looking for digital forensic evidence is like looking for a needle in a haystack.

The Need for Computer Forensics

- 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.

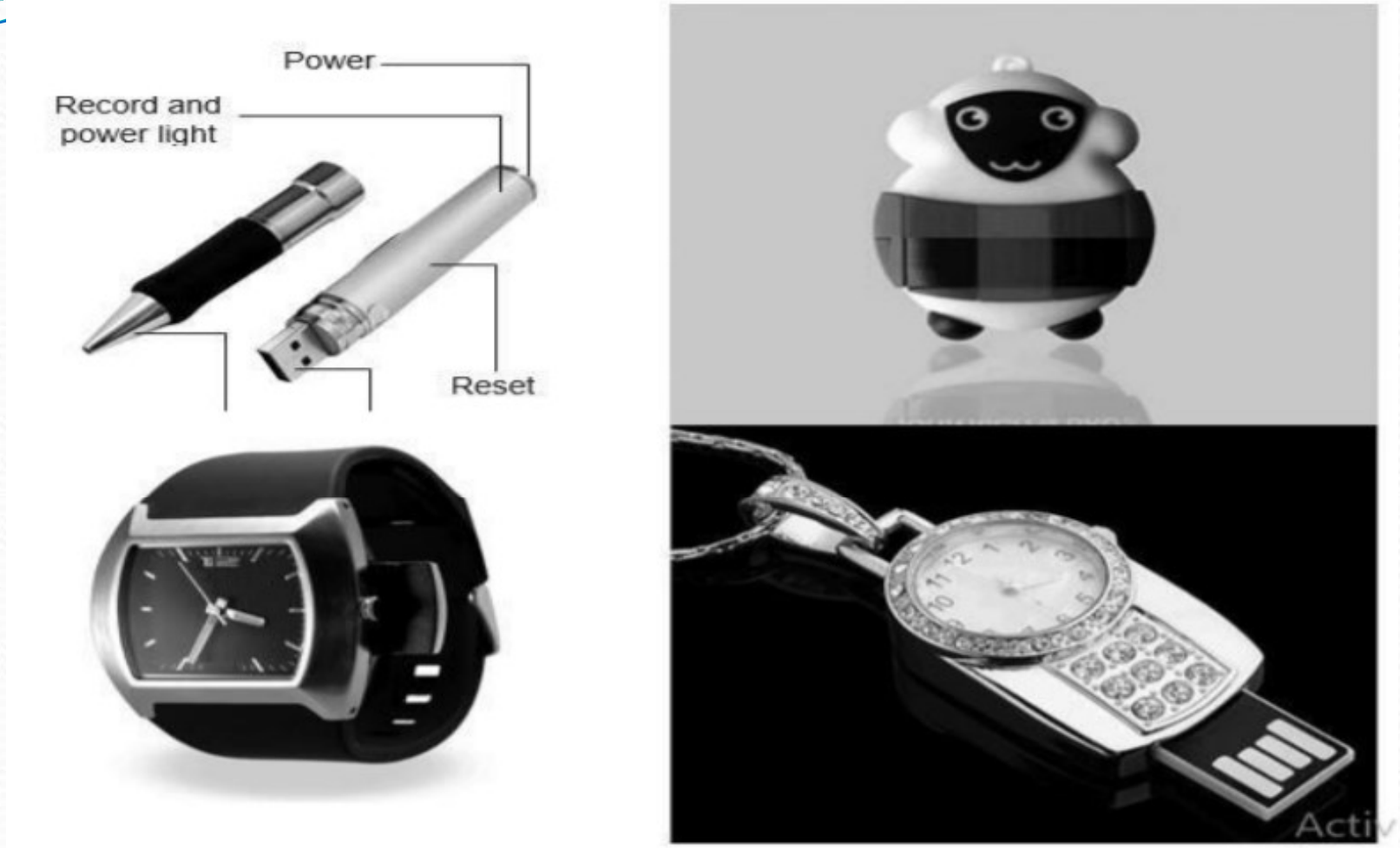


Fig: Hidden and miniaturized storage media.

Box 7.3 Digital Forensic Investigation and E-Discovery

- Digital evidence plays a crucial role in the threat management life cycle, from incident response to high-stakes corporate litigation.
- Evidence can include computer hard drives, portable storage, portable music players and and others.
- All forms of evidences are verified and duplicated prior to investigation to ensure the integrity of the evidence for litigation purposes.
- Key evidences are more found on enterprise productivity server, network logs or proprietary databases than on users system or file server.
- Users are becoming more sophisticated and so their efforts to circumvent security policy or encrypt, delete or destroy digital evidence.
- So more advanced support is required by forensic experts for acquisition, management and analysis of digital evidence.
- Typical computer forensic services are:
- Data culling and targeting, discovery process, production of evidence, expert affidavit support, criminal testimony, cell phone forensics, PDA forensics, etc.

Box 7.3 Digital Forensic Investigation and E-Discovery

- Specific client requests for forensic evidence extracting solution support includes:
- Index of files on hard drives, Index of recovered files
- MS Office/user generated document extraction
- Unique E mail address extraction, Log extraction
- Storage and forensic image for 1 year
- Keywords search
- Chain of custody
- Mail indexing
- Deleted data recovery, office document recovery
- Conversion to PDF
- Instant messaging history recovery
- Internet activity history, Password recovery
- Format for forensic extracts (DVD, CD, HDD, other)
- Network acquisition

Box 7.3 Digital Forensic Investigation and E-Discovery

- The primary focus of standard e-discovery is the collection of active data and metadata from multiple hard drives and other storage media.
- Litigation can be supported by active data (information readily available to the user, such as e-mail, electronic calendars, word processing files, and databases), or by metadata (that which tells us about the document's author, time of creation, source, and history).
- Data collected in e-discovery can be limited; for deeper recovery, computer forensics is often used.
- The goal of computer forensics is to conduct an autopsy of a computer hard drive – searching hidden folders and unallocated disk space to identify the who, what, where, when, and why from a computer.
- A significant amount of evidence is not readily accessible on a computer; when this occurs, a computer forensic examination is necessary.

Box 7.4 Chain of Custody Example

- In criminal and civil law, the term "chain of custody" refers to the order in which items of evidence have been handled during the investigation of a case.
- Proving that an item has been properly handled through an unbroken chain of custody is required for it to be legally considered as evidence in court.
- While often unnoticed outside the courthouse, proper chain of custody has been a crucial factor in high-profile cases, such as the 1994 murder trial of former professional football star O.J. Simpson.
- In practice, a chain of custody is a chronological paper trail documenting when, how, and by whom individual items of physical or electronic evidence—such as cell phone logs—were collected, handled, analyzed, or otherwise controlled during an investigation.
- Under the law, an item will not be accepted as evidence during the trial—will not be seen by the jury—unless the chain of custody is an unbroken and properly documented trail without gaps or discrepancies.

Box 7.4 Chain of Custody Example

- Example:
- In the O.J. Simpson trial, for example, Simpson's defense showed that crime scene blood samples had been in the possession of multiple investigating officers for various lengths of time without being properly recorded on the Chain of Custody Form.
- This omission enabled the defense to create doubt in the minds of the jurors that blood evidence linking Simpson to the crime could have been planted or contaminated in order to frame him.
- From the time it is collected until it appears in court, an item of evidence must always be in the physical custody of an identifiable, legally-authorized person.
- Thus, a chain of custody in a criminal cased might be:

Box 7.4 Chain of Custody Example

- Example:

1. A police officer collects a gun at the crime scene and places it in a sealed container.
2. The police officer gives the gun to a police forensics technician.
3. The forensics technician removes the gun from the container, collects fingerprints and other evidence present on the weapon, and places the gun along with the evidence collected from it back into the sealed container.
4. The forensics technician gives the gun and related evidence to a police evidence technician.
5. The evidence technician stores the gun and related evidence in a secure place and records everyone who accesses the evidence during the investigation until final disposition of the case.

- Items of evidence are typically moved in and out of storage and handled by different people. All changes in the possession, handling, and analysis of items of evidence must be recorded on a Chain of Custody Form.

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

Cyber forensics and Digital Evidence

- Understanding the uniqueness of digital evidence is important in digital forensic investigation and in maintaining the chain of custody.
- Computer forensic experts know the techniques to retrieve the data from the files listed in standard directory search, hidden files, deleted files, deleted E-mail and passwords, login IDs, encrypted files, hidden partitions, etc.
- Computer systems have:
  - File system
  - Random access memory
  - Physical storage media (including slack are and unallocated space)
  - User created file
  - Computer created file
  - Computer networks

Box 7.5 The Father of Forensic Science : the Sherlock Holmes of France

- Dr. Edmond Locard (13 December 1877 – 4 May 1966) was a French criminologist, the pioneer in forensic science who became known as the "Sherlock Holmes of France".
- He formulated the basic principle of forensic science: "Every contact leaves a trace". This became known as Locard's exchange principle.
  - Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibres from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. **Only human failure to find it, study and understand it, can diminish its value.**
  - In other words, whenever two human beings come into contact, something from one is exchanged to the other, that is, dust, skin cells, hair, etc.

Box 7.5 The Father of Forensic Science : the Sherlock Holmes of France

- Locard studied medicine and law at Lyon, France, eventually becoming the assistant of Alexandre Lacassagne, a criminologist and professor. He held this post until 1910, when he began the foundation of his criminal laboratory.
- In 1910, Locard succeeded in persuading the Police Department of Lyon to give him two attic rooms and two assistants, to start what became the first police laboratory.
- He produced a monumental, seven-volume work, Traité de Criminalistique. He continued with his research until his death in 1966.
- In November 2012, he is nominated to the French Forensic Science Hall of Fame of the Association Québécoise de Criminalistique

Cyber forensics and Digital Evidence

- The Rules of Evidence
- This is a very important discussion, especially, for those who are students of legal courses. It was mentioned in that the Indian IT Act amended the Indian Evidence Act.
- According to the "Indian Evidence Act 1872," "Evidence" means and includes:
- 1. All statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, are called oral evidence.
- 2. All documents that are produced for the inspection of the court are called documentary evidence.
- Paper evidence, the process is clear and intuitively obvious. Digital evidence by its very nature is invisible to the eye. Therefore, the evidence must be developed using tools other than the human eye.

Cyber forensics and Digital Evidence

- 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: We must place the evidence in the correct context to read its meaning.
- This may require looking at the evidence as machine language, for example, American Standard Code for Information Interchange (ASCII).

Cyber forensics and Digital Evidence

- Following are 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.
- 3. keep detailed notes with dates and times. Generate an automatic transmit, if possible. Notes and prints should be signed and dated.

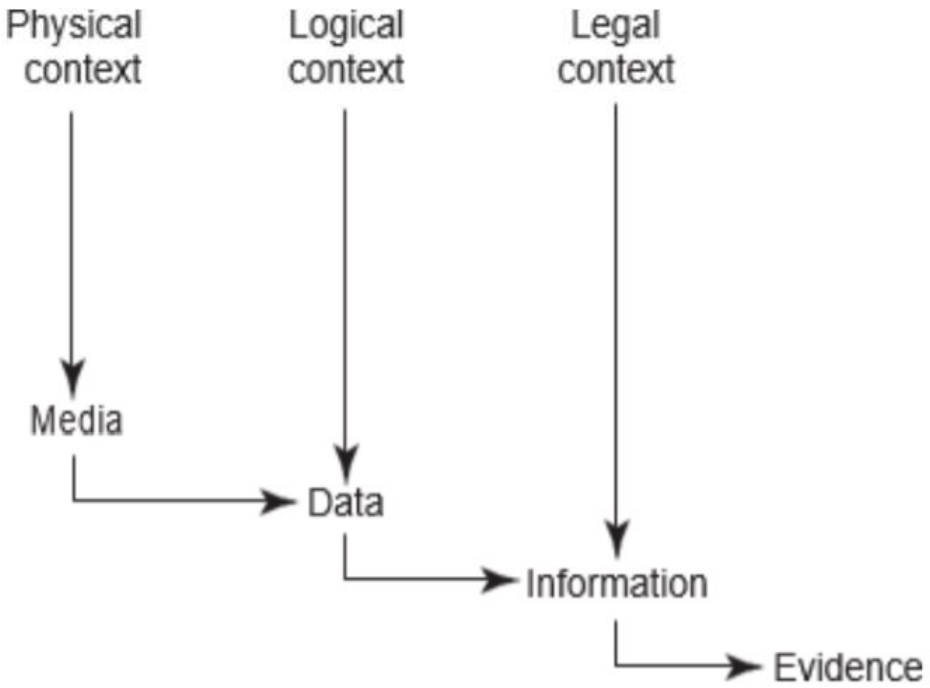


Fig: Path of the digital evidence.

Cyber forensics and Digital Evidence

- 4. Note the difference between the system clock and Coordinated Universal Time (UTC). Also note if UTC or local time is used.
- 5. Be prepared to testify outlining all actions you took and at what times.
- 6. Minimize changes to the data, including content changes and file access time as well.
- 7. Remove external avenues for change.
- 8. Do collection first, and then analysis.
- 9. The procedure should be implementable, in order to test it as per the incident report policy. Also automate it if possible, for the sake of speed and accuracy.
- 10. If there are many devices, allocate the work among the team members.
- 11. Proceed from volatile to the less volatile.
- 12. Make bit-level copy of the systems media. (for analysis purpose and to keep original intact.)

Box 7.6 Electronic Messages and the Indian Evidence Act

- Section 88 of the Indian Evidence Act 1872 is about presumption of as to telegraphic messages. It states that:
- "*Presumption as to telegraphic messages.—The Court may presume that a message, forwarded from a telegraph office to the person to whom such message purports to be addressed, corresponds with a message delivered for transmission at the office from which the message purports to be sent; but the Court shall not make any presumption as to the person by whom such message was delivered for transmission.*"
- As per section 66A of Indian IT Act, "*any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,*" shall be punishable with imprisonment for a term which may extend to three years and with fine.
- In terms of the amended Indian IT Act 2000, that is, the ITA 2008, its interesting to know how court shows when it comes to evidences based on E mails

Box 7.6 Electronic Messages and the Indian Evidence Act

- According to the section 88A of the Indian Evidence Act, "*The Court **may presume** that an electronic message, forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court **shall not make any presumption** as to the person by whom such message was sent.*"
- "May presume."-Whenever it is provided by this Act that the Court may presume a fact, it may either regard such fact as proved, unless and until it is disproved, or may call for proof of it.
- "Shall presume."-Whenever it is directed by this Act that the Court shall presume a fact, it shall regard such fact as proved, unless and until it is disproved.
- "Conclusive proof."-When one fact is declared by this Act to be conclusive proof of another, the Court shall, on proof of the one fact, regard the other as proved, and shall not allow evidence to be given for the purpose of disproving it.

Forensics Analysis of E-Mail

- It was mentioned in chapter 2, how criminals can use 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 it helps establish the authenticity of an E-Mail when suspected.
- Owing to the rising pressure from regulatory agencies and due to possible litigations in global businesses, the organizations are obliged to electronically store information to support discovery and discloser requests.
- An email system is the hardware and software that control the flow of E-mail having two important components: Email server and Email gateway.
- An email consists of two parts: the header and the body.
- The header part is very crucial in forensic analysis as it provides the entire path of the email's journey from its origin to the destination.

E-mail Header Example

Return-Path: <bogdan@fx.ro>
Received: from srv01.advenzia.com (root@localhost)
by emailaddressmanager.com (8.11.6/8.11.6) with ESMTP id i2OApwQ14083
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 10:51:58 GMT
X-ClientAddr: 193.231.208.29
Received: **from** corporate.fx.ro (corporate.fx.ro [193.231.208.29])
by srv01.advenzia.com (8.11.6/8.11.6) with ESMTP id i2OApvs14078
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 10:51:57 GMT
Received: from mail.fx.ro (mail3.fx.ro [193.231.208.3])
by corporate.fx.ro (8.12.11/8.12.7) with ESMTP id i2OAtxBr025924
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 12:55:59 +0200
Received: from localhost.localdomain (corporate2.fx.ro [193.231.208.28])
by mail.fx.ro (8.12.11/8.12.3) with ESMTP id i2OAtoQe006624
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 12:55:50 +0200
Date: Wed, 24 Mar 2004 12:55:50 +0200
Message-Id: <200403241055.i2OAtoQe006624@mail.fx.ro>
Content-Disposition: inline
Content-Transfer-Encoding: binary
MIME-Version: 1.0
To: support@emailaddressmanager.com
Subject: How to read email headers
From: bogdan@fx.ro
Reply-To: bogdan@fx.ro
Content-Type: text/plain; charset=us-ascii
X-Originating-Ip: [80.97.5.101]
X-Mailer: FX Webmail webmail.fx.ro
X-RAVMilter-Version: 8.4.3(snapshot 20030212) (mail)
Status:

Forensics Analysis of E-Mail

- 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.
- Header information varies with email service provider, Email applications and system configurations.
- As we saw, the header part contains the information that is needed for email routing, subject line and time stamps whereas the body part the actual message or data of the email.
- The header and body are separated by a blank line.
- The header contains several mandatory and optional fields, trace information and heading fields (with field having a name and a value).

Forensics Analysis of E-Mail

- As you may have already noticed, there are three paragraphs starting with the Received tag: each of them was added to the email header by email servers, as the email travelled from the sender to the receiver.
- Since our goal is to see who sent it, we only care about the last one (the blue lines).
- By reading the Received From tag, we can notice that the email was sent via corporate2.fx.ro, which is the ISP domain of the sender, using the IP 193.231.208.28.
- The email was sent using SMTP ("with ESMTP id") from the mail server called mail.fx.ro.
- Looking further into the message, you will see the tag called X-Originating-IP: this tag normally gives the real IP address of the sender.
- The X-Mailer tag says what email client was used to send the email (on our case, the email was sent using FX Webmail).

Box 7.7 Precautions for using E-mail as an Evidence

- Ensure use of emails is subject to agreed procedures enforced and supported by high level management.
- Train users about acceptable use of email and about their rights and obligations expected of them.
- Implement access control mechanisms for attributed usage with a person, a terminal, a date and a time.
- Ensure computer systems are kept safe and secure.
- Retention and deletion of email should be organization defined and not user-defined.
- Implement a solution that archives and stores emails centrally. The archive must support all file formats and also retain metadata.
- The archive should classify the emails at the time of entry to it by preventing duplicate entries as well.
- Make sure the archiving platform facilitates the exporting of evidence as files as a part of e discovery process.

Box 7.7 Precautions for using E-mail as an Evidence

- Implement an archiving solution that allows full search and retrieval of along with the metadata.
- Enable logging of all the events acting on the archive. The logs should be retained as part of the archive, for auditing and verification purposes.
- Provide contingency for continuity of both archiving and discovery in the event of an outage.
- Ensure the archiving platform supports the marking-up of files so that privileged materials can be withheld and/or redacted during E-discovery.

Forensics Analysis of E-Mail

- The internet service provider plays an important role in email forensics.
- ISP provides internet access to businesses, organizations, schools, colleges, and individuals. E.g. MTNL, BSNL, Reliance Jio, Vodafone Idea, Airtel, Hathway, GTPL Broadband, Excitel, You Broadband etc.
- The ISP can provide name, address and contact number of the subscriber of the internet service, type of IP address and any other information which is required.

Forensics Analysis of E-Mail

Table 1.30: Internet Subscriber Base and Market Share of top 10 Service Providers

S.No	ISP	No. of Subscribers	Share (%)
1	Reliance Jio Infocomm Ltd	355926487	51.76
2	Bharti Airtel Ltd.	154880425	22.52
3	Vodafone Idea Limited	140342199	20.41
4	Bharat Sanchar Nigam Ltd.	28216649	4.10
5	Atria Convergence Technologies Pvt. Ltd.	1479233	0.22
6	Mahanagar Telephone Nigam Ltd.	1164440	0.17
7	Hathway Cable & Datacom Pvt. Ltd.	861946	0.13
8	You Broadband India Pvt. Ltd.	773597	0.11
9	GTPL Broadband Pvt. Ltd.	301750	0.04
10	Excitel Broadband Private Limited	294000	0.04
	Total of Top 10 ISPs	**684240726**	**99.51**
	Others	3382700	0.49
	Grand Total	**687623426**	**100**

Forensics Analysis of E-Mail

- Here is the starting part of the header of a **junk email (spam)**, which includes information about the transfer of the email between the sender and the receiver:

```
Return-Path: <ydcddlhanqz@yahoo.com>
Received: from mail.fx.ro (mail4.fx.ro [193.231.208.4])
        by fx.ro (8.12.7/8.12.7) with ESMTP id i2OAVxGs024789;
        Wed, 24 Mar 2004 12:31:59 +0200 (EET)
Received: from mailv.fx.ro (localhost.localdomain [127.0.0.1])
        by mail.fx.ro (8.12.11/8.12.3) with ESMTP id i2OAVxaA004610;
        Wed, 24 Mar 2004 12:31:59 +0200
Received: (from root@localhost)
        by mailv.fx.ro (8.12.11/8.12.3/Submit) id i2OAVxh1004609;
        Wed, 24 Mar 2004 12:31:59 +0200
Received: from 206.85.220.156 by 217.225.143.240;
```

- Let's analyze the red highlighted lines:
- Return-path: the header tells that if you reply to this email message, the reply will be sent to ydcdd...@yahoo.com. Would you use such an email address for real?
- Received tags: as on web blogs, read them from the bottom to top. The header says the email was originally sent from 206.85... and it was sent to 217.225... (which is the name/IP of the first mail server that got involved into transporting this message).

Forensics Analysis of E-Mail

- Then suddenly, the next Received tag says the message was received from root@localhost, by mailv.fx.ro.
- You can also notice that so far, the Received tags do not contain any information about how the email was transmitted (the "with" tag is missing: this tag tells the protocol used to send the email).
- Going deeper with the analysis, you can use an IP tracing tool, like Visual Route, in order to see to whom the IP belongs to.
- As in most of the spamming cases, the starting IP (206.85...) is unreachable, which means that the spammer could have routed the real IP or he could have used a dynamic IP (a normal case for dial-up users).
- However, by tracing 217.225..., you will get to the ISP used by the spammer, a German provider.
- The ISP has nothing to do with the spam itself, but it was simply used by the spammer to connect to the Internet.

Digital Forensics Life Cycle

- As per FBI's (Federal Bureau of Investigation) view, digital evidence is present in nearly every crime scene.
- That is why law enforcement must know how to recognize, seize, transport and store original digital evidence to preserve it for forensics examination.
- Cardinal rules to remember are that the evidence:
- 1. Is admissible.
- 2. Is authentic.
- 3. Is complete.
- 4. Is reliable.
- 5. Is understandable and believable.
- Let us now understand what is involved in the digital forensics process.

Box 7.8 Forensic Experts : What they do?

- Computer forensic experts acquire and examine potential evidence during an investigation, including data that's been deleted, encrypted, or damaged.
- Any steps taken during this process are documented, and methodologies are used to prevent the evidence from being altered, corrupted, or destroyed.
- While serving as an expert for the defense, the forensic expert should remain impartial and perform many of the same functions as that of the prosecution.
- Forensic experts may also be used in civil litigations. Because information dealing with a case may be stored on computers or other devices, computer forensic experts may be used to search for data such as e-mail, text messages, chat logs, Web site history, calendar files, spreadsheets, documents, images, and other files on a machine.

Box 7.8 Forensic Experts : What they do?

- Because the data acquired through computer forensics includes documents, spreadsheets, and other files that contain information outside the computer expert's scope of knowledge, additional experts will be used to explain what has been found.
- In such situations, the investigation and ensuing criminal or civil litigations will often use other experts that are suited to the evidence.
- A forensic expert team brings the following benefits:
- 1. Technical Expertise
- 2. Forensic Methodology
- 3. Experience and Efficiency
- The *Chain of Custody* concept is also very important in digital forensics.

Box 7.9 Case Briefing

- In case briefing, consider the following:
- 1. Ensure you know both, your client's and the adverse party's position, and have seen all relevant paperwork.
- 2. Try not to project bias in the case description; the intent should be to consider the case objectively, and provide you with the good news and the bad news(bad news early can be a good news later)
- 3. Be upfront in discussing any limitations or restrictions on the forensic investigation, including budgetary constraints, time deadlines, cooperation levels to be expected from the adverse party, required travel, onsite or after-hours forensics imaging requirements, etc.

Box 7.9 Case Briefing

- Case briefing is a long-used method of studying law. Its purpose is to have students identify the rules of law found in court cases and analyze how courts apply these rules of law to the facts of a case in an objective and rational manner.
- Case briefing hones analytic skills and heightens understanding of the role of courts in defining, interpreting, and applying law.
- Several basic components of a brief are present in almost all brief styles. If your brief style includes the following elements, you should do well:
  - Facts
  - Issue or issues
  - Holding, including the rule of law
  - Rationale

Digital Forensics Life Cycle

- The Digital Forensics Process
- The digital forensics process needs to be understood in the legal context starting from preparation of the evidence to testifying.
- Digital forensics evidence consists of exhibits, each consisting of a sequence of bits, presented by witnesses in a legal matter to help jurors establish the facts of the case and support or refute legal theories of the case.
- 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. Broadly speaking, the forensics life cycle involves the following phases:

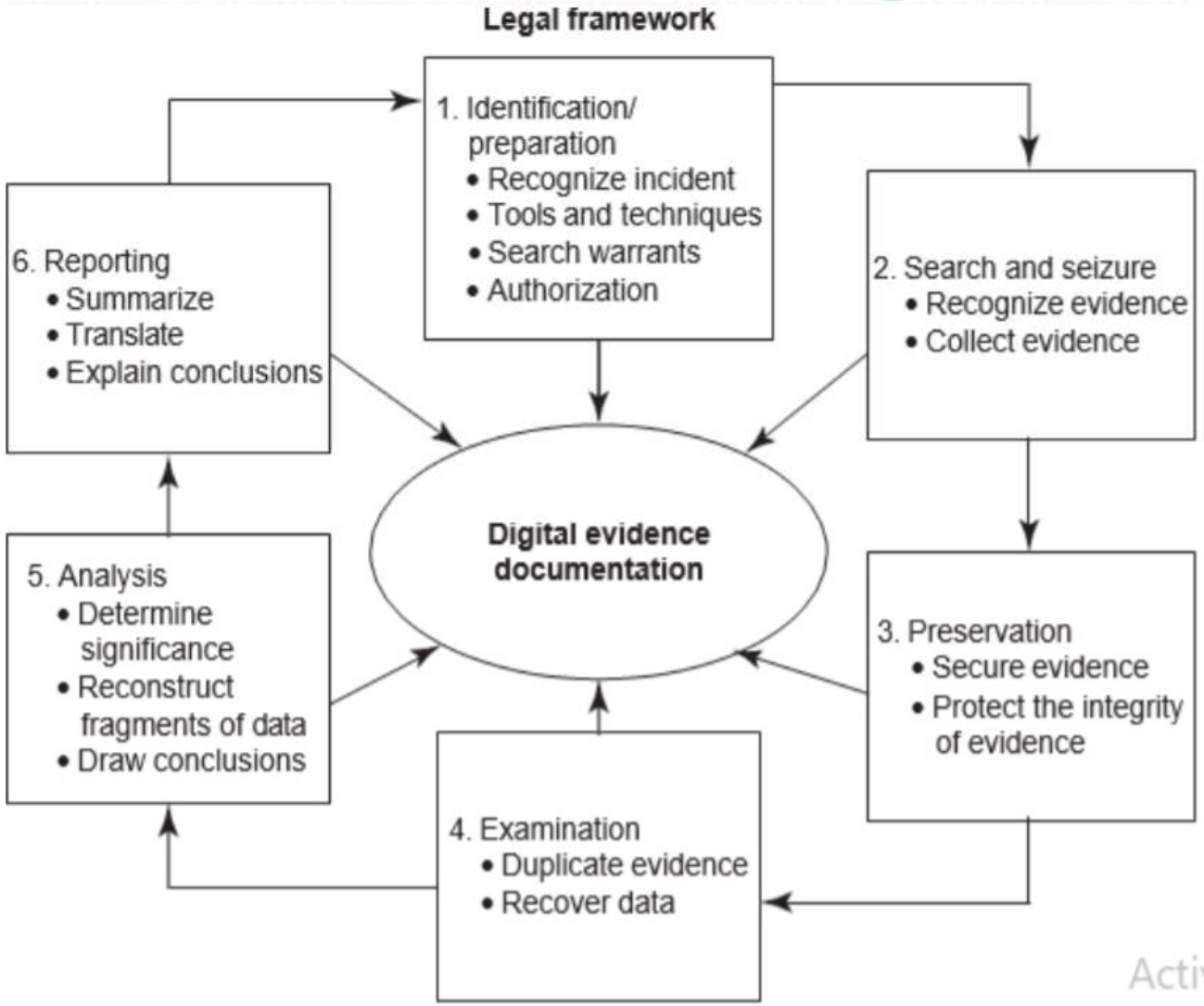


Fig: Process model for understanding a seizure and handling of forensics evidence legal

Digital Forensics Life Cycle

- The Phases in Computer Forensics/Digital Forensics
- 1. Preparation and identification
- 2. Collection and recording
- 3. Storing and transporting
- 4. Examination/investigation
- 5. Analysis, interpretation and attribution
- 6. Reporting and
- 7. Testifying.
- To mention very briefly, the process involves the following activities:

Digital Forensics Life Cycle

- The process involves following activities:
- 1. Prepare: Case briefings engagement terms, 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, testimony.

Digital Forensics Life Cycle

- Preparing for the Evidence and Identifying the Evidence
- In order to be processed and applied, evidence must first be identified as evidence.
- It can happen that there is an enormous amount of potential evidence available for a legal matter, and it is also possible that the vast majority of the potential evidence may never get identified.
- Evidence of an activity that caused digital evidence to come into being might be contained in a time stamp associated with different programs on different computers.

Digital Forensics Life Cycle

- <u>Collecting and Recording Digital Evidence</u>
- 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 web pages (which must be preserved as they are subject to change).

Fig: Media that can hold digital evidences.

Digital Forensics Life Cycle

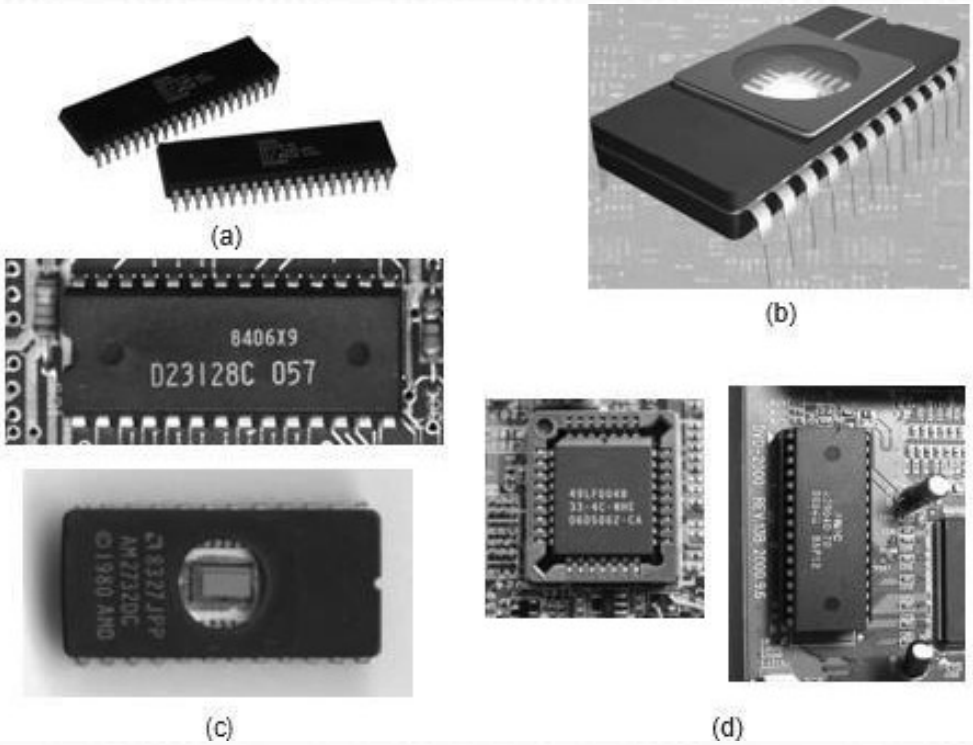
- Collecting and Recording Digital Evidence

Fig: Some more media that can hold digital evidences.

Digital Forensics Life Cycle

- Storing and Transporting Digital Evidence
- The following are specific practices that have been adopted in the handling of 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.

- Fig: Embedded memories inside computer. (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.



Digital Forensics Life Cycle

- Some of the most valuable information obtained in the course of a forensics examination will come from the computer user.
- An interview with the user can yield valuable information about the system configuration, applications, encryption keys and methodology.
- Forensics analysis is much easier when analysts have the user's passphrases to access encrypted files, containers and network servers.
- As a general rule, one should not examine digital information unless one has the legal authority to do so.
- Amateur forensics examiners should keep this in mind before starting any unauthorized investigation.
- For the purpose of digital evidence examination, "imaging of electronic media" (on which the evidence is believed to be residing) becomes necessary.

Digital Forensics Life Cycle

- Examining/Investigating Digital Evidence
- The owner's consent is very important in forensic investigation as without it an owner's content cannot be examined.
- The investigator must ensure that he/she has the legal authority to seize, copy, and examine data.
- Live and Dead analysis: the analysis on live systems is called live analysis.
- The analysis on the data which is at rest, for example data on a hard drive, is called dead analysis.
- They systems have to be shut down out of the fear of digital time bombs which may erase the data on the computer if the system is on.
- For analysis imaging technique is used to create sector wise copy of the data ensuring no change is made to the original.

Digital Forensics Life Cycle

- Analysis, Interpretation and Attribution
- Analysis, interpretation and attribution of evidence are the most difficult aspects encountered by most forensics analysts.
- In the digital forensics arena, there are usually only a finite number of possible event sequences that could have produced evidence.
- Examples of common digital analysis types include:
- 1. Media Analysis: analysis of the data from the storage device. It doesn't consider any partitions or OS specific data structures but a fixed unit based structure like sector.
- 2. Media Management Analysis: analysis of the management system used to organize the data, which includes partitions and may be volume management or redundant array of independent disks (RAID) systems that merge data from multiple storage devices to a single virtual storage device.

Digital Forensics Life Cycle

- 3. File System Analysis: analysis of a partition data inside a partition or disk, to extract the contents of a file and to recover deleted files.
- 4. Application Analysis: analysis of data inside a file, with files having application specific format(user or application created)
- 5. Network Analysis: analysis of data on a communication network. Network packets can be examined using the OSI model to interpret raw data into an application level steam.
- Some most common application types are OS analysis and executable analysis.
- 6. OS Analysis: an application but a special one which runs very first when computer is a started. It analyzes the configuration files and output files to determine what events may have occurred.

Digital Forensics Life Cycle

- 7. Executable Analysis: executables are digital objects that can cause events to occur and they are frequently examined during intrusion investigations to find out what events the executables caused.
- 8. Image Analysis: this analysis is important as many images are contraband. It can find where the picture is taken and who or what is there in the picture.
- Image Analysis can also be used to examine images for evidence of steganography.
- 9. Video Analysis: digital videos can be captured by security cameras or personal cameras, and webcams.
- Video analysis examines the video for the identification of objects in the video and the location where it was shot.

Digital Forensics Life Cycle

- Reporting
- After the analysis report is generated which may be in a written form or an oral testimony or a combination of the two.
- The report results may need be presented to a wide variety of audience including law enforcement officials, technical experts, legal experts, corporate management, etc.
- Presentation of a report is more of an art than a science, but there is a substantial amount of scientific literature on methods of presentation and their impact on those who observe it.
- Reporting is a complex and tricky process as no guidelines are defined for the use of order of information, use of graphics, demonstration, etc.

Digital Forensics Life Cycle

- Reporting
- 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.

Digital Forensics Life Cycle

- 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.
- Only expert witnesses can address issues based on scientific, technical or other specialized knowledge.
- A witness qualified as an expert by knowledge, skill, experience, training or education may testify in the form of an opinion or
- If (a) the testimony is based on sufficient fact data, (b) the testimony is the product of reliable principles and methods, (c) the witness has applied the principles and methods reliably to the facts of the case.

Box 7.10 File Carving – a Powerful Technique for Digital Forensics

- File carving is a process used in computer forensics to extract data from a disk drive or other storage device without the assistance of the file system that originality created the file.
- It is a method that recovers files at unallocated space without any file information and is used to recover data and execute a digital forensic investigation.
- As a forensics technique that recovers files based merely on file structure and content and without any matching file system meta-data, file carving is most often used to recover files from the unallocated space in a drive.
- Unallocated space refers to the area of the drive which no longer holds any file information as indicated by the file system structures like the file table.

Box 7.10 File Carving – a Powerful Technique for Digital Forensics

- File carving is the process of trying to recover files without this metadata. This is done by analyzing the raw data and identifying what it is (text, executable, png, mp3, etc.).
- This can be done in different ways, but the simplest is to look for the signature or "magic numbers" that mark the beginning and/or end of a particular file type.
- For instance, every Java class file has as its first four bytes the hexadecimal value CA FE BA BE. Some files contain footers as well, making it just as simple to identify the ending of the file.
- Most file systems, such as the FAT family and UNIX's Fast File System, work with the concept of clusters of an equal and fixed size.
- For example, a FAT32 file system might be broken into clusters of 4 KiB each. Any file smaller than 4 KiB fits into a single cluster, and there is never more than one file in each cluster.

Box 7.10 File Carving – a Powerful Technique for Digital Forensics

- Files that take up more than 4 KiB are allocated across many clusters.
- These clusters are all contiguous or scattered across two or potentially many more so called fragments, with each fragment containing a number of contiguous clusters storing one part of the file's data.
- Obviously large files are more likely to be fragmented.
- Simson Garfinkel reported fragmentation statistics collected from over 350 disks containing FAT, NTFS and UFS file systems.
- He showed that while fragmentation in a typical disk is low, the fragmentation rate of forensically important files such as email, JPEG and Word documents is relatively high.
- The fragmentation rate of JPEG files was found to be 16%, Word documents had 17% fragmentation, AVI had a 22% fragmentation rate and PST files (Microsoft Outlook) had a 58% fragmentation rate (the fraction of files being fragmented into two or more fragments).

Box 7.10 File Carving – a Powerful Technique for Digital Forensics

- File carving is a highly complex task, but can be performed using free or commercial software and is often performed in conjunction with computer forensics examinations or alongside other recovery efforts (e.g. hardware repair) by data recovery companies.

- Whereas the primary goal of data recovery is to recover the file content, computer forensics examiners are often just as interested in the metadata such as who owned a file, where it was stored, and when it was last modified.
- Thus, while a forensic examiner could use file carving to prove that a file was once stored on a hard drive, he or she might need to seek out other evidence to prove who put it there.

Example of an Image constructed from a segmented file

Table 7.5 | Digital forensics – phase-wise outputs

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

(*Continued*)

Table 7.5 | (Continued)

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

	• Documenting the findings and all steps taken.	
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

Precautions to be taken when collecting Electronic Evidence

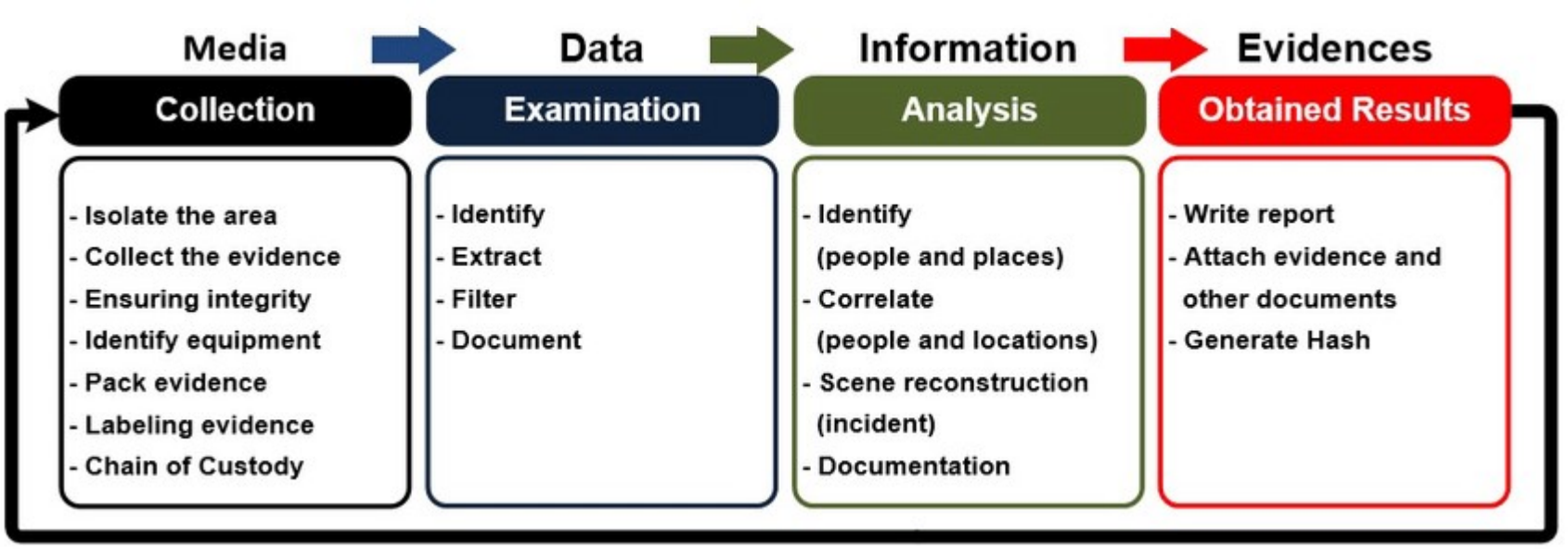
- One of the most important measure is to ensure that the evidence has been successfully collected.
- And that there is a clear chain of custody right from the crime scene to the investigator and ultimately to the court.
- To comply with the need to maintain the integrity of digital evidence, certain rules must be complied with:
- Principle 1: no actions taken by the law enforcement agencies or their agents should change data held on a computer or storage media, which may be relied upon in court.
- Principle 2: in cases where a person finds it necessary to access original data held on a computer or on storage media that person must be competent to do so and be able to give evidence explaining the relevance and implications of his/her actions.

Precautions to be taken when collecting Electronic Evidence

- Principle 3: an audit trail or record of all the processes applied to computer based electronic evidence should be created and preserved.
- An independent third party should be able to examine those processes and achieve the same results.
- Principle 4: the person in-charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Chain of Custody Concept

- 1. Chain of custody is the central concept in cyber forensics/digital forensics investigation.
- 2. The purpose of the chain of custody is that the proponent of a piece of evidence must demonstrate that it is what it purports to be.
- 3. The chain of custody is a chronological written record of those individuals who have had custody of the evidence from its initial acquisition until its final disposition.



Network Forensics

- Recall the mention of network forensics. We have already discussed that open networks can be the source of many network-based cyber attacks.
- A situation like this leads to the point that network forensics professionals need to understand how wireless networks work and the fundamentals of related technology.
- Wireless forensics is a discipline included within the computer forensics science, and specifically, within the network forensics field.
- The goal of wireless forensics is to provide the methodology and tools required to collect and analyze (wireless) network traffic that can be presented as valid digital evidence in a court of law.

Approaching a Computer Forensics Investigation

- From the discussion so far, we can appreciate that computer forensics investigation is a detailed science.
- Now, let us understand how a forensics investigation is typically approached and the broad phases involved in the investigation.
- The phases involved are as follows:
- 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;

Approaching a Computer Forensics Investigation

- 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.

Approaching a Computer Forensics Investigation

- Typical Elements Addressed in a Forensics Investigation Engagement Contract
- Typically, the following important elements are addressed before while drawing up a forensics investigation engagement contract
- 1. Authorization: customer will be asked to authorize the forensic laboratory or its agents to conduct an evaluation of the data/media/equipment onsite or offsite and throughout the investigation engagement.
- The customer may require to authorize the forensic lab, their employees, independent contractors, and agents to securely receive and transport all collected evidences to and from and between their premises.
- Customer has to affirm/declare that he/she is the actual owner of all the evidences being used in the investigation or has the legal rights to use them.

Approaching a Computer Forensics Investigation

- 2. Confidentiality: the forensic investigator is supposed to use all the data/equipments involved for the purpose of fulfilling the engagement, and is expected to hold all this in strictest confidence.
- Computer forensic labs cannot share it with other than the people involved in the investigation and has to employ appropriate technical and organizational measures to safeguard any customer information.
- 3. Payment: customer agrees to pay the computer forensic lab all sums authorized from time to time by customer, which includes:
- 1) Computer forensic lab services,
- 2) Travel expenses for onsite work,
- 3) Shipping and insurance expenses if any,
- 4) Media or/and off-the-shelf software used for service management.

Approaching a Computer Forensics Investigation

- 4. Consent and acknowledgement: verbal, written or electronic consent has to be provided by the customer wherever it is applicable.
- 5. Limitation of liability: the computer forensic lab will not consider itself liable for any claims regarding the physical functioning of equipment/media or the condition or existence of the data stored on the media during or after service.
- Neither the lab will be liable for the loss of data or loss of revenues or profits, goodwill or loss of anticipated savings or any consequential loss before or after the services.

Approaching a Computer Forensics Investigation

- 1. Customer's representation: Customer needs to warrant the forensics laboratory that he/she is the owner of, and/or has the right to be in possession of, all equipment/data/media furnished to the laboratory and that collection, possession, processing and transfer of such equipment/data/media are in compliance with data protection laws to which customer is subject to.

- 2. Legal aspects/the law side: Both the parties need to agree that the agreement shall be governed by prevailing law in every particular way including formation and interpretation and shall be deemed to have been made in the country where the contract is signed.

Approaching a Computer Forensics Investigation

- 3. Data protection: The computer forensics laboratory (engaged in the investigation) will hold the information that the customer has given verbally, electronically **or**
- in any submitted form for the purpose of the forensics investigation to be carried out as per contracted services from the forensics laboratory.

- 4. Waiver/breach of contract: The waiver by either party of a breach or default of any of the provisions on this agreement by either party shall not be construed as a waiver of any succeeding breach of the same or other provisions, nor shall any delay or omission on the part of either party to exercise or avail itself of any right, power or privilege that it has, **or**
- may have hereunder operates as a waiver of any breach or default by either party.

Solving a Computer Forensics Case

- These are just some broad illustrative steps and they may vary depending on the specific case in hand.
- 1. Prepare for the forensics examination.
- 2. Talk to key people to find out what you are looking for and what the circumstances surrounding the case are.
- 3. If you are convinced that the case has a sound foundation, start assembling your tools to collect the data in question. Identify the target media.
- 4. Collect the data from the target media. You will be creating an exact duplicate image of the device in question. To do this, you will need to use an imaging software application like the commercial in Case or the open-source Sleuth Kit/Autopsy.

Solving a Computer Forensics Case

- 5. To extract the contents of the computer in question, connect the computer you are investigating to a portable hard drive or other storage media and then boot the computer under investigation according to the directions for the software you are using.
- 6. When collecting evidence, be sure to check E-Mail records as well. Quite often, these messages yield a great deal of information.
- 7. Examine the collected evidence on the image you have created. Document anything that you find and where you found it.
- 8. Analyze the evidence you have collected by manually looking into the storage media and, if the target system has a Windows OS, check the registry.
- 9. Report your findings back to your client. Be sure to provide a clear, concise report; this report may end up as evidence in a court case.

Computer Forensics and Steganography

- Steganography is the art of information hiding.
- The threat raised by steganography is very real. Its use is not easy to detect or intercept, as the information does not need to be broadcast across the Internet.
- The hidden message can reside unsuspectingly on a website, for example, and can be viewed from around the world.
- In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves.
- Invisible ink has been in use for centuries-for fun by children and students and for serious espionage by spies and terrorists.

Computer Forensics and Steganography

- Steganography hides the covert message but not the fact that two parties are communicating with each other.
- The steganography process generally involves placing a hidden message in some transport medium, called the carrier.
- The secret message is embedded in the carrier to form the steganography medium.
- The use of a steganography key may be employed for encryption of the hidden message and/or for randomization in the steganography scheme.

Computer Forensics and Steganography

- Steganography by its very nature, poses a threat to computer forensic analysis as they now must consider a much broader scope of information for analysis and investigation.
- Hence, its considered as one of the antiforensic methods.
- Computer forensic methods are used for removal and subversion of evidence with the intent of mitigating results of computer forensics.
- Other antiforensic techniques are encryption, self-splitting files plus encryption, database rootkits, BIOS rootkits, bypassing the integrity checks, etc.

Computer Forensics and Steganography

- Rootkits
- The term rootkit is used to describe the mechanisms and techniques whereby malware including viruses, Spyware and Trojans attempt to hide their presence from Spyware blockers, antivirus and system management utilities.
- A rootkit is software used by cybercriminals to gain control over a target computer or network.
- Rootkits can sometimes appear as a single piece of software but are often made up of a collection of tools that allow hackers administrator-level control over the target device.

Computer Forensics and Steganography

- Rootkits
- Hackers install rootkits on target machines in a number of ways:

1. The most common is through phishing or another type of social engineering attack. Victims unknowingly download and install malware that hides within other processes running on their machines and give the hackers control of almost all aspects of the operating system.
2. Another way is through exploiting a vulnerability – i.e., a weakness in software or an operating system that has not been updated – and forcing the rootkit onto the computer.
3. Malware can also be bundled with other files, such as infected PDFs, pirated media, or apps obtained from suspicious third-party stores.

Computer Forensics and Steganography

- Rootkits
- Rootkits operate near or within the kernel of the operating system, which gives them the ability to initiate commands to the computer.
- Anything which uses an operating system is a potential target for a rootkit – which, as the Internet of Things expands, may include items like your fridge or thermostat.
- Rootkits can hide keyloggers, which makes it easy for cybercriminals to steal your personal information, such as credit card or online banking details.
- Rootkits can allow hackers to use your computer to launch DDoS attacks or send out spam emails. They can even disable or remove security software.
- Types of Rootkits: Hardware to Firmware, Bootloader, Memory, Application, Kernel mode, Virtual rootkits.
- Tools: Flame, Stuxnet, Necurs, ZeroAccess, etc.

Computer Forensics and Steganography

- Information Hiding
- Concealing the very existence of some kind of information (e.g., a series of data bits, the identity of the communicating party, etc.) for some specific purpose (e.g., to prove ownership, to remain untraceable, etc.)
- Information hiding is a technique of hiding secret using redundant cover data such as images, audio, movies, documents, etc.
- For example, digital video, audio and images are increasingly embedded with imperceptible marks, which may contain hidden signatures or watermarks that help to prevent unauthorized copy.
- It is a performance that inserts secret messages into a cover file, so that the existence of the messages is not apparent.

Computer Forensics and Steganography

- Information Hiding
- Two techniques which are used to hide information are 1) Watermarking, 2) Steganography
- Water marking is the process of embedding information into a digital signal in a way that is difficult to remove, the signal may be audio, pictures, video or text files; its mostly used to demonstrate the intellectual property rights purpose such as adding copy right logo or text (author signature) for multimedia files.
- Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message.
- Since, the main use for steganography is to send secure messages between parties, then it's aim to prevent the message being detected by any other party.

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.
- Step 1: Foot Printing
- Foot printing includes a combination of tools and techniques used to create a full profile of the organization's security posture. These include its domain names, IP addresses and network blocks.

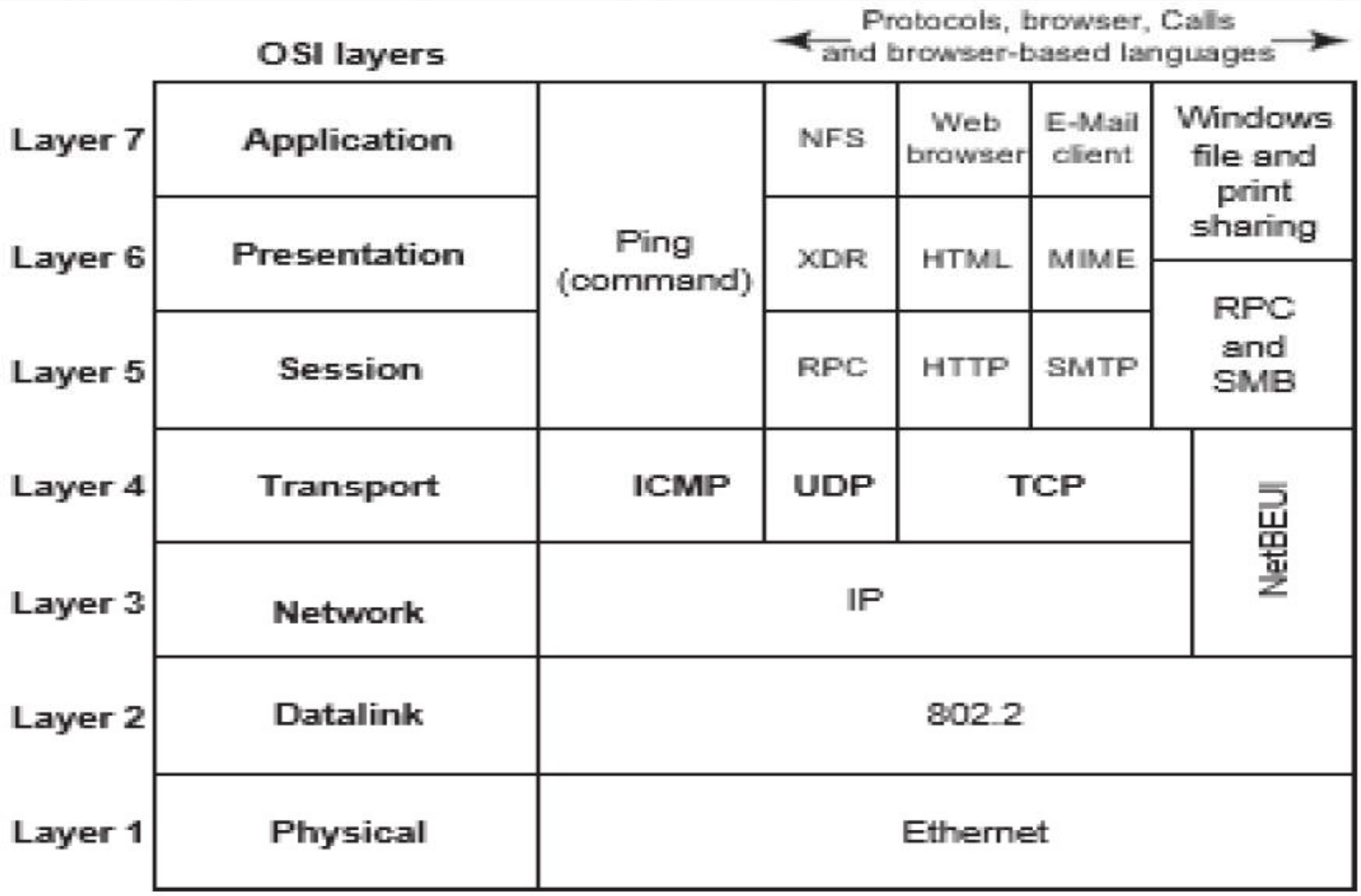


Fig: The OSI 7 Layer Model with Internet Protocols.

Network hackers

Fig: Network hacking steps

Relevance of the OSI 7 Layer Model to Computer Forensics

- Step 2: Scanning and Probing
- The hacker will typically send a ping echo request packet to a series of target IP addresses.
- As a result of this exploratory move by the hacker, the machines assigned to one of these IP address will send out echo response thereby confirming that there is a live machine associated with that address.
- Similarly, a TCP scan sends a TCP synchronization request to a series of ports and to the machines that provide the associated service to respond.

Relevance of the OSI 7 Layer Model to Computer Forensics

- Step 3: Gaining Access
- The hacker's ultimate goal is to gain access to your system so that he/she can perform some malicious action, such as stealing credit card information, downloading confidential files or manipulating critical data.
- Step 4: Privilege
- When a hacker gains access to the system, he will only have the privileges granted to the user or account that is running the process that has been exploited.

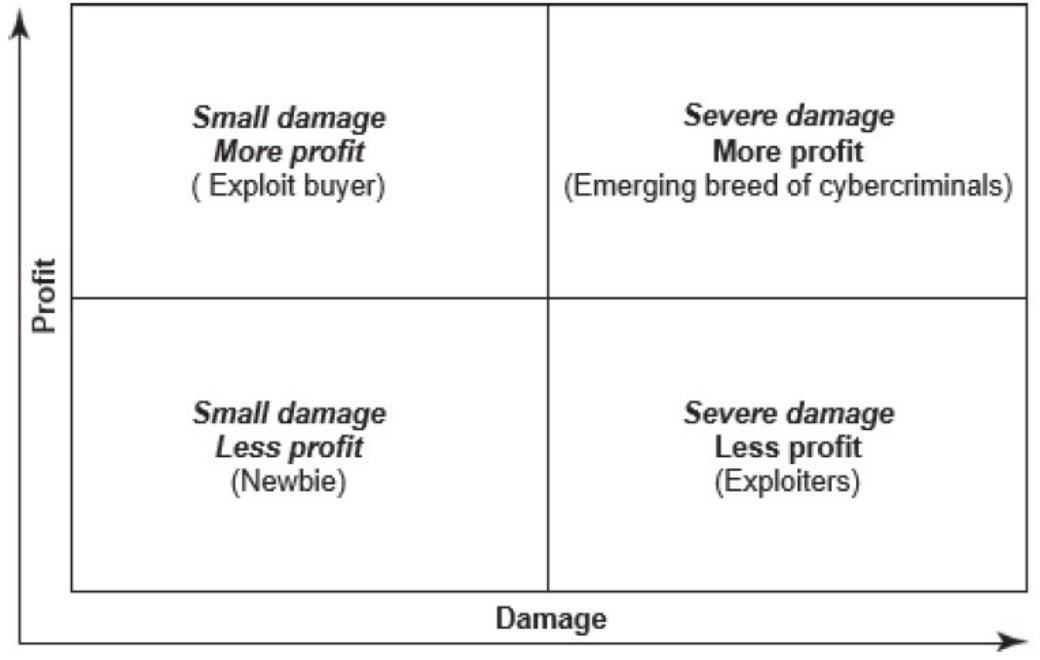


Fig. Hacker categories (profit and damage).

Relevance of the OSI 7 Layer Model to Computer Forensics

- Step 5: Exploit
- Gaining root access gives the hacker full control on the network. Every hacker seems to have his/her own reasons for hacking.
- Some hackers do it for fun or a challenge, some do it for financial gain and others do it to “get even”.
- Step 6: Retracting
- There are many reasons that drive cybercriminals to hacking.
- Step 7: Installing Backdoors
- Finally, most hackers will try creating provisions for entry into the network/hacked system for later use.
- By this, they will do by installing a backdoor to allow them access in the future.

Forensics and Social Networking Sites

- Social Media needs no introduction. It has taken over the world and our lives like an insidious wave. It is a wave that has brought the world closer, yet not without detrimental effects.
- At present, over 3.397 billion users are active on social media who spend 116 minutes per day on an average.
- With abundant personal information available on social media platforms, it is now the hotbed of crimes and malicious activities.
- But, where there's a crime, there's also inspection to bring justice to victims and combat such occurrences in the future.
- Know how investigators extract social media forensics evidence and engage in forensic analysis of social networking applications on mobile devices.

Forensics and Social Networking Sites

- Social Media Statistics
- The social media world is of mammoth size, and it is only increasing by the day! Here are some social media statistics for you.
- Did you know that Facebook adds 500,000 new users to its fraternity every day? This amounts to the creation of 6 new profiles every second!
- There are 1.3 billion accounts on Twitter, with 326 million active users each month!
- LinkedIn contains a user base of 500 million members whereas Snapchat has 187 million active users daily! In fact, 60% of Snapchat users are under the age of 25.
- Pinterest boasts of 200 million active users every month.
- Did you know that YouTube sees around 1,148 billion mobile video views each day?
- When it comes to publishing content, users publish 74.7 million blog posts per month on WordPress alone!

Forensics and Social Networking Sites

- According to oberlo.in survey,
- The latest social media statistics show that there are 3.78 billion social media users worldwide in 2021 – and this number is only going to continue growing over the next few years (Statista, 2020).
- As it stands, that equates to about 48 percent of the current world population.
- One of the reasons for the high usage of social media is that mobile possibilities for users are continually improving, which makes it increasingly simpler to access social media, no matter where you are.
- Most social media networks are also available as mobile apps or have been optimized for mobile browsing, making it easier for users to access their favorite sites while on the go.
- For more info visit: https://www.oberlo.in/blog/social-media-marketing-tatistics#:~:text=The%20latest%20social%20media%20statistics%20show%20that%20there%20are%203.78,of%20the%20current%20world%20population.

Forensics and Social Networking Sites

- Type of Social Networking Platforms
- We all know what social media is. But, what most don't know is that Facebook, Instagram, Twitter, Snapchat and WhatsApp are not the only social media platforms.
- The classification of social media platforms is on the basis of its primary objective of use. Following are the different types of social networking platforms.
- **1. Social Networks** (Use: To associate with people and brands virtually. Examples: Facebook, Twitter, WhatsApp, LinkedIn)
- **2. Media Sharing Networks** (Use: To search for and share photos, videos, live videos, and other forms of media online. Examples: Instagram, Snapchat, YouTube)
- **3. Discussion Forums**(Use: Serves as a platform to search, discuss, and exchange information, news, and opinions. Examples: Reddit, Quora, Digg)
- **4. Bookmarking and Content Curation Networks** (Use: To explore, save, exchange, and discuss new and trending content and media. Examples: Pinterest, Flipboard)

Forensics and Social Networking Sites

- **5. Consumer Review Networks** (Use: To search, review, and share opinions/information about brands, restaurants, products, services, travel destinations, etc. Examples: Yelp, Zomato, TripAdvisor)
- **6. Blogging and Publishing Networks** (Use: To publish, explore, and comment on content online. Examples: WordPress, Tumblr, Medium)
- **7. Sharing Economy Networks** (Use: To find, advertise, share, and trade products and services online. Examples: Airbnb, Uber, Task rabbit)
- **8. Anonymous Social Networks** (Use: To anonymously spy, vent, gossip, and sometimes bully. Examples: Whisper, Ask.fm, After School)

TYPES OF SOCIAL MEDIA PLATFORMS

Social Networks

Media Sharing Networks

Discussion Forums

Content Curation Networks

Consumer Review Networks

Blogging Networks

Sharing Economy Networks

Anonymous Social Networks

INCOGNITO
FORENSIC FOUNDATION

Forensics and Social Networking Sites

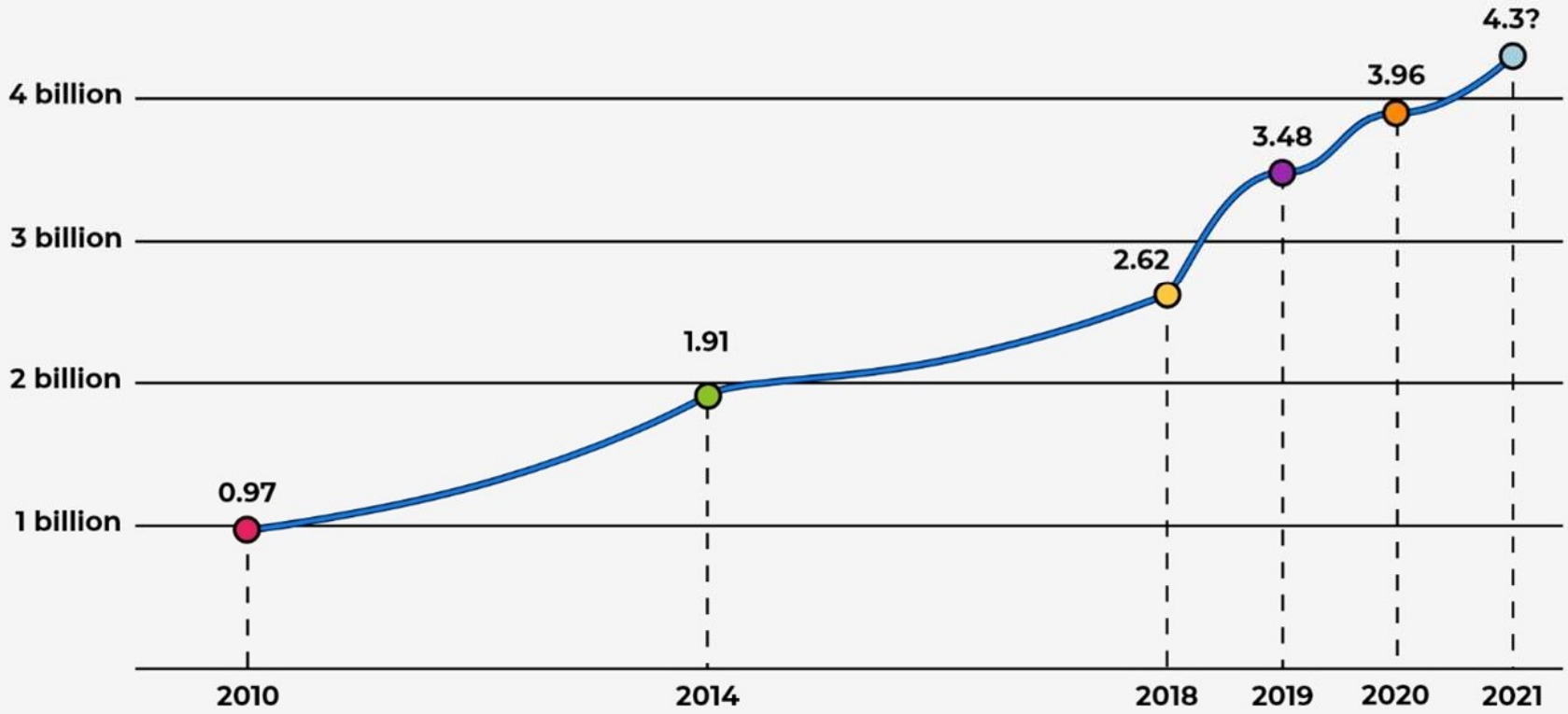
- Social Networking Platforms Offers a Lucrative Platform for Executing Social Media Crimes.
- On the righteous side, one may use social media platforms to socialize and communicate with people but its anonymous and diverse nature is used by miscreants for unethical activities.
- Innocent-looking profiles can often be the masquerade for fraudsters, phishers, child predators, lechers, and other cyber criminals.
- In spite of the stringent policies imposed by social media platforms, there are approximately 270 million fake profiles on Facebook!!!
- Additionally, the abundance of personal information available on social networking platforms renders them a favorite of cyber criminals.
- After the compromise of a profile, a hacker can access, manipulate and misuse its information for various malicious activities.
- Other unscrupulous activities on such platforms include stalking, bullying, defamation, circulation of illegal or pornographic material etc.

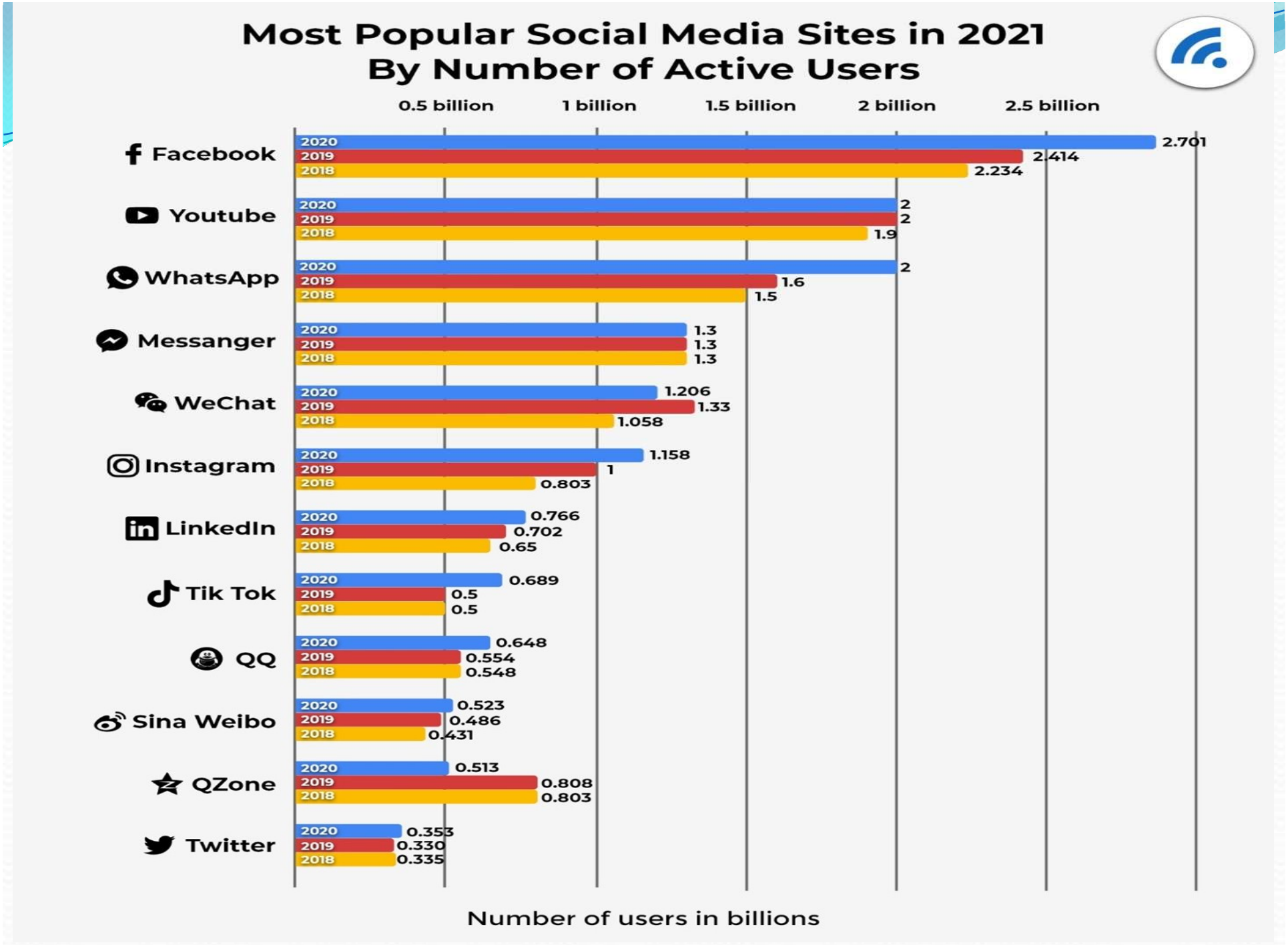
Following are some types of social media crimes.

Forensics and Social Networking Sites

- Social Media Forensics or Social Network Forensics
- Precisely known as social media forensics or social network forensics, it focuses on retrieval of electronic evidence from social networking activities.
- Such evidence often plays a crucial role in the conviction or acquittal of a suspect.
- Social media forensics involves the application of cyber investigation and digital analysis techniques for:
  - Collecting information from social networking platforms such as Facebook, Twitter, LinkedIn etc.
  - Storing,
  - Analyzing, and
  - Preserving the information for fighting a case in the court of law
- Social Media Forensics is basically about locating the source of electronic evidence. This is accompanied by collecting it in an unhampered way while complying with all laws.

Number of Social Media Users Around the World in 2021




Most Popular Social Media Sites in 2021
By Number of Active Users
0.5 billion
1 billion
1.5 billion
2 billion
2.5 billion
Facebook
2020 2.701
2019 2.414
2018 2.234
Youtube
2020 2
2019 2
2018 1.9
WhatsApp
2020 2
2019 1.6
2018 1.5
Messanger
2020 1.3
2019 1.3
2018 1.3
WeChat
2020 1.206
2019 1.33
2018 1.058
Instagram
2020 1.158
2019 1
2018 0.803
LinkedIn
2020 0.766
2019 0.702
2018 0.65
Tik Tok
2020 0.689
2019 0.5
2018 0.5
QQ
2020 0.648
2019 0.554
2018 0.548
Sina Weibo
2020 0.523
2019 0.486
2018 0.431
QZone
2020 0.513
2019 0.808
2018 0.803
Twitter
2020 0.353
2019 0.330
2018 0.335
Number of users in billions

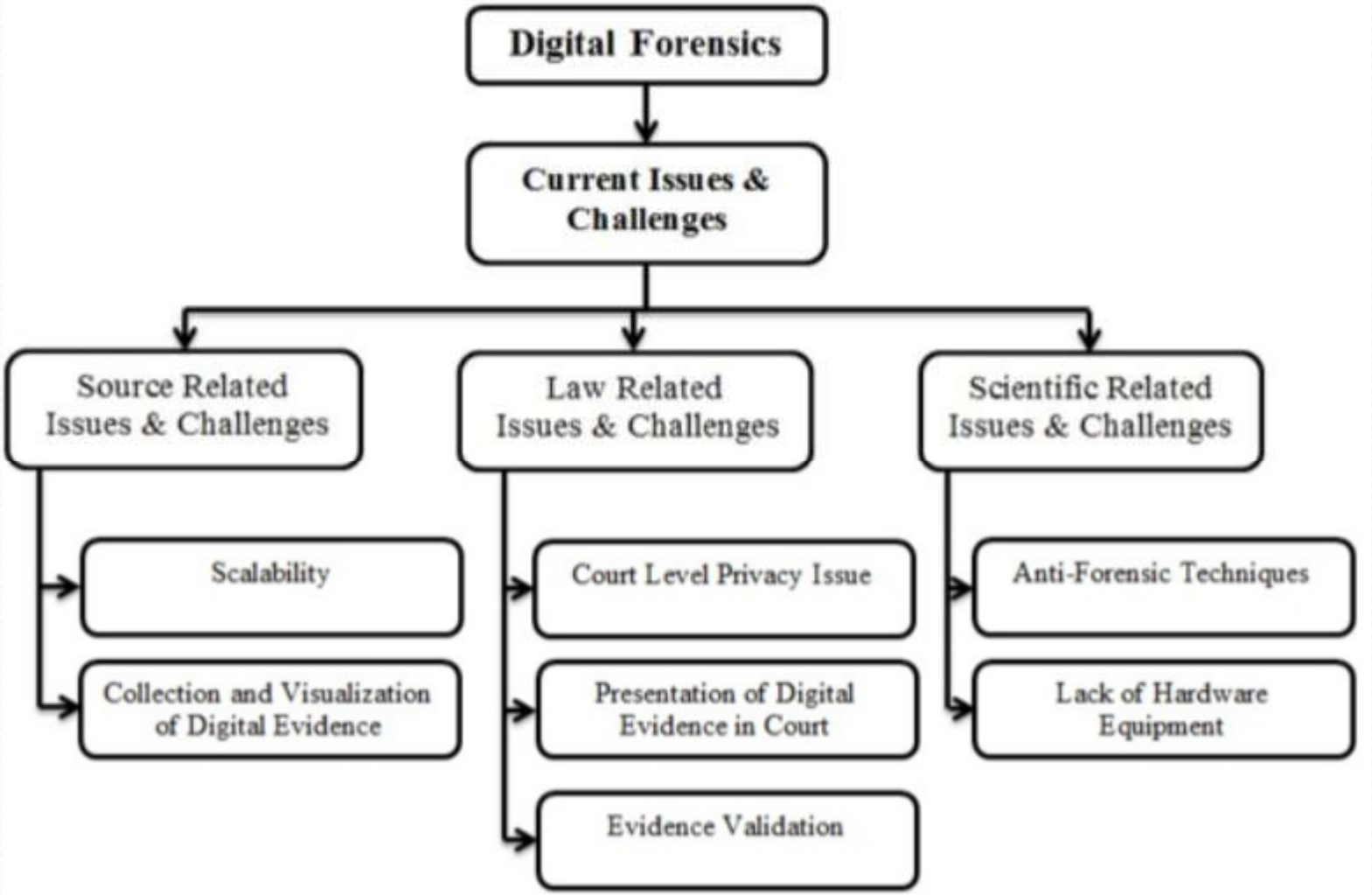
Challenges in Computer Forensics

- A survey by India Times in early 2019 stated that "58% of data breach victims are the persons or organizations who have a small type of business at very low or medium-level" (C.R. Srinivasan, 2019).
- Moreover, with the voluminous increase in the use of mobile devices, tabs, laptops, etc., the implementation of cyber-attacks is very easy for the attackers. Hence, the examination and analysis of cyber-attacks and security exploits have become imperative.
- (1) (PDF) Current Challenges of Digital Forensics in Cyber Security. Available from: https://www.researchgate.net/publication/338756056_Current_Challenges_of_Digital_Forensics_in_Cyber_Security [accessed Jun 07 2021].

Challenges in Computer Forensics

- In the present scenario, cyber crimes have inundated the cyber world creating several challenges for cybersecurity experts.
- Since a lack of awareness among the end-users creates a path for attackers to exploit them or their organizations, digital forensic has gained enormous significance in the investigation process of an incident related to cybercrime.
- But this has also created lots of issues and challenges for the experts and examiners, some related to technology or advancement, some related to standards and rules and some related to the basic functionality of investigation.
- The main issues and challenges of digital forensics can be classified mainly in three major parts –
- I. Source Related Issues & Challenges
- II. Law Related Issues & Challenges
- III. Scientific Issues & Challenges

Challenges in Computer Forensics



Tree Structure of the Issues and Challenges of Digital Forensic

Challenges in Computer Forensics

- Source Related Issues & Challenges
- These types of challenges and issues come in digital forensics because of the problem of functional issues, related to the basic environment or plan of action that is taken by the experts and examiners to investigate the incident.
- *Scalability*
- This is a crucial problem and a burning area of digital forensics.
- Scalability is related to the volume issue of digital investigation.
- In the volume issue, the examiners talk about the quantity of the metadata or sensitive information found on the crime scene.
- Sometimes, it is a very composite work for an examiner or expert to collect and use the collected data to find the desired information.

Challenges in Computer Forensics

- Source Related Issues & Challenges
- Some researchers have found the main problems of this issue to be:
  - The volume and complexity of a victim's data or system are increasing rapidly.
  - According to digital harm or data growth, the experts will neither update themselves nor adopt new technology very often.
  - The proportion of cybercrime incidents is much high as compared to examiners that are present in the industry nowadays.
- So, this creates a misbalanced situation. Hence, it requires an in-depth investigation for every expert or examiner.
- To mitigate this type of issue and challenge, we need to create a structured time-stamped forensic examination process that aligns with the current scenario of Cybercrime and investigation.

Challenges in Computer Forensics

- Source Related Issues & Challenges
- *Collection and Visualization of Digital Evidence*
- The examiners focus on the time that is taken to collect and visualize the evidence in a readable manner in front of the affected parties and jurisdictions.
- Because of the scientific issues like data encryption, steganography, data hiding, defragmentation and, etc., the examiners take more time than normal.
- This creates a massive issue and sometimes the retrieval of data is too critical and complex.
- This also leads to the risk of corrupted data. So all these technical issues make the collection and visualization of sensitive data a time taking process because of which further non-technical investigation also gets delayed.
- The researcher Roussev (2016) has suggested that "*A good solution of the issue is to make an embedded help team for a forensic examiner in the large investigation*".

Challenges in Computer Forensics

- Law-Related Issues and Challenges
- Different countries have different laws and some countries don't even have a law or established standards for cyber and forensic examinations.
- So, there are several ambiguities and issues related to digital forensics and cybersecurity laws.
- For instance, if an examiner finds that the incident has been done by a system that is located in a foreign country and that country does not have any cyber law, then the examiner can't do anything and this creates an enormous challenge for the experts and examiners.
- There are many other law-related issues. Some of the major issues are mentioned below:
  - Court Level Privacy Issue
  - Presentation of Digital Evidence In Court
  - Evidence Validation

Challenges in Computer Forensics

- Law-Related Issues and Challenges
- *Court Level Privacy Issue*
- 60% of the individual users and 77% of the enterprises (medium, small & big) produce private confidential information and data in their daily uses and it may be risky for them if this information or data gets disclosed publicly or to attackers.
- In most cases, experts need to disclose the private data or information related to an organization and a person to found the real truth and in such cases it is very difficult to maintain privacy.
- *Presentation of Digital Evidence In Court*
- The presentation of evidence in the courtroom is very difficult in a readable form.
- And sometimes the opposition party questions the format of sensitive data in which the data is represented in the front of the court and common in many cases opposition questions on the validation of tools that are used in the collection and analysis phase of Forensic investigation.

Challenges in Computer Forensics

- Law-Related Issues and Challenges
- *Evidence Validation*
- Evidence validation is the heart of digital forensic and plays a crucial role in resolving any kind of digital or cybercrime.
- There are many cases in court in which the opposition lawyer challenges the tool used in the examination of evidence and it creates a major issue in digital forensics because every tool has its pros & cons.
- So it's difficult for an examiner to find which tool is perfect for which task. Many countries have their legal valid tool list after this issue but these tools also have vulnerabilities.
- There is no 100% perfect tool for any task and this issue continues to be a dilemma in digital forensics.

Challenges in Computer Forensics

- Scientific Issues and Challenges
- Scientific or technical issues are very critical in today's era because the use of technology is present in both a good and bad way.
- Like examiners and investigators use the computers and technologies in a good manner to examine the evidence and crime scene, some persons use the technology and computer in a nugatory manner to do some illegal, unauthorized activity and to be anonymous.
- This type of use of technology and computers scientifically create an issue and this is both the most dangerous and most effective issue in today's era.
- There are mainly two types of challenges: Anti-forensics techniques like Data encryption, data hiding in storage space, steganography, attack against cyber forensic tools, etc.

Challenges in Computer Forensics

- Lack of Hardware Equipment
- This is a very important issue in digital forensics because there is a major lack of hardware equipment in the forensic investigation process.
- Sometimes the case is not too big to afford or use high embedded hardware. There are also some fields of digital forensics for which the hardware has not been manufactured yet.
- Hardware plays a vital role in the digital forensic investigation because, with the help of hardware, the examiner works properly without any delay in time.
- And in the phase where an examiner collects the evidence, the hardware can play a master role because with the help of hardware and examiner's doesn't need a large team to get the result.
- The lengthy-time duration that an examiner takes in the collection phase also gets reduced.

Special Tools and Techniques

- So far we have seen various forensic tools. Like File carving and COFEE in this chapter only. Most forensic tools have following principles:
- Creating forensic quality or sector-by-sector images of media
- Locating deleted/old partitions
- Ascertaining date/time stamp information
- Obtaining data from slack space
- Recovering or undeleting file and directories, carving or recovering data based on files headers/footers
- Performing keyword searches
- Recovering internet history information.

Special Tools and Techniques

- Visit the following link for latest data recovery tools:
- https://techtalk.gfi.com/the-top-23-free-data-recovery-tools/
- Partition recovery tools
- https://www.handyrecovery.com/best-partition-recovery-software/
- File carving tools
- https://linuxhint.com/file_carving_tools_linux/
- Best open source digital forensic tools
- https://hıdfs.com/the-best-open-source-digital-forensic-tools/

Forensics Auditing (or Forensics Accounting)

- A forensic audit is an analysis and review of the financial records of a company or person to extract facts, which can be used in a court of law.
- Forensic auditing is a specialty in the accounting industry, and most major accounting firms have a department forensic auditing.
- Forensic audits include the experience in accounting and auditing practices as well as expert knowledge of forensic audit's legal framework.
- Forensic audits cover a large spectrum of investigative activities. There may be a forensic audit to prosecute a party for fraud, embezzlement or other financial crimes.
- The auditor may be called in during the process of a forensic audit to serve as an expert witness during trial proceedings.
- Forensic audits could also include situations that do not involve financial fraud, such as bankruptcy filing disputes, closures of businesses, and divorces.

Forensics Auditing (or Forensics Accounting)

- <u>What Necessitates a Forensic Audit?</u>
- Forensic audit investigations may expose, or confirm, various kinds of illegal activities.
- Normally, instead of a normal audit, a forensic audit is used if there is a possibility that the evidence gathered would be used in court.
- The forensic audit process is similar to a traditional financial audit — planning, gathering evidence, and writing a report — with the additional step of a possible appearance in court.
- The lawyers on both sides offer evidence that the crime is either discovered or disproved, which decides the harm sustained. They explain their conclusions to the defendant should the case go to trial before the judge.
- Several reasons for having forensic audits are
- Corruption or Fraud (Conflicts of interest, Extortion)
- Asset Misappropriation
- Financial Statement Fraud

Forensics Auditing (or Forensics Accounting)

- How Forensic Audit works?
- The process of a forensic audit is similar to a regular financial audit—planning, collecting evidence, writing a report—with the additional step of a potential court appearance.
- The attorneys for both sides offer evidence that either uncovers or disproves the fraud and determines the damages suffered.
- They present their findings to the client, and the court should the case go to trial.
- **1. Planning the Investigation**
- During the planning stage, the forensic auditor and team will plan their investigation to achieve objectives, such as
  - Identifying what fraud, if any, is being carried out
  - Determining the period during which the fraud occurred
  - Discovering how the fraud was concealed
  - Naming the perpetrators of the fraud
  - Quantifying the loss suffered as a result of the fraud
  - Gathering relevant evidence that is admissible in court
  - Suggesting measures to prevent such frauds from occurring in the future

Forensics Auditing (or Forensics Accounting)

- **2. Collecting Evidence**
- The evidence collected should be adequate(and are not damaged/altered) to prove the fraudster's identity (s) in court, reveal the fraud scheme's details, and document the financial loss suffered and the parties affected by the fraud.
- A logical flow of evidence will help the court in understanding the fraud and the evidence presented.
- **3. Reporting**
- A forensic audit requires a written report about the fraud to be presented to the client to proceed to file a legal case if they so desire.
- At a minimum, the report should include:
  - The findings of the investigation
  - A summary of the evidence collected
  - An explanation of how the fraud was perpetrated
  - Suggestions for preventing similar frauds in the future—such as improving internal controls

Forensics Auditing (or Forensics Accounting)

- **4. Court Proceedings**
- The forensic auditor must be present during court proceedings to explain the evidence collected and how the team identified the suspect(s).
- They should simplify any complex accounting issues and explain the case in a layperson's language so that people who have no understanding of legal or accounting terms can understand the fraud clearly.

Forensics Auditing (or Forensics Accounting)

Sr. No.	Particulars	Audit (Professional Skepticism)	Forensic Audit (Investigative mentality)
1	Objectives	Express an opinion as to 'True & Fair presentation.	Whether fraud has taken place.
2	Techniques	Substantive & Compliance. Sample based.	Investigative, substantive and in depth checking.
3	Period	Normally for a particular accounting period.	As agreed.
4	Verification of stock, estimation realizable value of assets, provisions, liability etc.	Relies on the Management certificate / Management Representation.	Independent verification of suspected / selected items where misappropriation is suspected.
5	Off balance sheet items (like contracts etc.)	Used to vouch the arithmetic accuracy & compliance with procedures.	Regulatory & propriety of these transactions / contracts are examined.
6	Adverse findings if any	Negative opinion or qualified opinion expressed with / without quantification.	Legal determination of fraud impact and identification of perpetrators depending on scope.

Antiforensics

- Anti-forensics is an approach used by cybercriminals to challenge evidence gathering and analysis processes.
- The primary purpose of anti-forensic techniques is to make it hard or even impossible for a cyber forensic investigator to conduct a digital investigation.
- “Anti-forensics” (AF) is a growing collection of tools and techniques that frustrate forensic tools, investigations and investigators.
- Liu and Brown identify four primary goals for anti-forensics:
  - Avoiding detection that some kind of event has taken place.
  - Disrupting the collection of information.
  - Increasing the time that an examiner needs to spend on a case.
  - Casting doubt on a forensic report or testimony (Liu and Brown, 2006).

Antiforensic

- Other goals might include:
  - Forcing the forensic tool to reveal its presence.
  - Subverting the forensic tool (e.g., using the forensic tool itself to attack the organization in which it is running).
  - Mounting a direct attack against the forensic examiner (e.g., discovering and disconnecting the examiner's network, or bombing the building in which the examiner is working).
  - Leaving no evidence that an anti-forensic tool has been run.
- (1) (PDF) Anti-forensics: Techniques, detection and countermeasures. Available from: https://www.researchgate.net/publication/228339244_Anti-forensics_Techniques_detection_and_countermeasures [accessed Jun 08 2021].

Antiforensic

- Approaching the problem of anti-forensic techniques
- The right solution is to build a healthy community of digital forensic investigators.
- The experience of skilled professionals will help others to stay one step ahead of obfuscation, steganography, encryption, tunneling, and other anti-forensic measures.
- The community should share their discoveries so that others won't fall for the same mistake.
- Other than that, maintaining a continuous educational environment will be a wise move.

Antiforensic

- Fascinating Anti-Forensic Techniques to Cover Digital Footprints
- **1. Encryption**
- Under encryption, the data is converted into an unreadable format ("encrypted data" or "ciphertext") using a pair of keys.
- The encrypted data can be deciphered only by using the paired-up key. This is one of the traditional methods to protect data.
- Under modern cryptography methods, Data Encryption Standard (DES), Advanced Encryption Standard (AES), are a few of the popular techniques. They use symmetric as well as asymmetric encryption.
- *Difference between symmetric and asymmetric algorithms?*
- Symmetric algorithms use a single key to encrypt and decrypt data, while asymmetric algorithms use two separate keys for both the processes.

Antiforensic

- Fascinating Anti-Forensic Techniques to Cover Digital Footprints
- **2. Steganography**
- Steganography allows messages and even huge files to be hidden in pictures, text, audio, and video files.
- It is challenging to identify a steganography-attack, but repetitive patterns can reveal the secret message to the investigator. With that, the professionals can also use advanced tools to spot hidden data.
- **3. Tunneling**
- This method uses encapsulation to allow private communications to be exchanged over a public network.
- The data packets will flow from public networks, thus generating no suspicion. One of the common ways is to use a Virtual Private Network (VPN), which encrypts the data for security reasons.
- To eliminate such attacks, organizations must continuously monitor their encrypted network connections.

Antiforensic

- Fascinating Anti-Forensic Techniques to Cover Digital Footprints
- **4. Onion Routing**
- The process of sending messages which are encrypted in layers, denoting layers of an onion, is referred to as onion routing.
- The data packet goes through several networking nodes where every layer of encryption gets peeled off. With the stripping of the final layer, the message gets closer to reach its destination.
- The message remains anonymous to the entire message delivery chain except the nodes placed after the source and before the destination.
- One of the best practices to fight against onion routing is to use reverse routing. This elimination process is time-consuming but can be used to defeat onion routing.

Antiforensic

- Fascinating Anti-Forensic Techniques to Cover Digital Footprints
- **5. Obfuscation**
- A technique that makes a message difficult to understand because of its ambiguous language is known as obfuscation.
- This method uses jargon and ingroup phrases to communicate. It could be intentional and unintentional.
- The primary objective is to reduce the risk of exposure. It can be done by altering the signature or fingerprint of malicious code.
- Deobfuscation is the same as countering onion routing. Removing layers exposes clean and readable code.
- **6. Spoofing**
- The act of disguising communication to gain access to unauthorized systems or data.
- Spoofing can be performed through emails, phone calls, and websites.
- Two most common ways of spoofing are IP spoofing and MAC spoofing.