Sardar Vallabhbhai Patel
National Police Academy,
Hyderabad

Cyber Crime Investigation Manual

Volume - V

CYBER X

Foreword

Cybercrime is one of the biggest challenges we face today. In the past decade, as technology has grown at an incredible pace, so has our dependence on the internet. While this has improved our lives in countless ways, it has also created new opportunities for criminals. From disrupting critical infrastructure to stealing financial assets and sensitive data, cybercrimes can cause serious harm. What makes it even more alarming is how easy and rewarding these crimes can be, often happening across borders without much cost.

Technology has brought great opportunities but also increased our vulnerability to cyber threats. As cybercrimes grow more frequent and complex, the lack of trained professionals to handle such cases effectively is a major challenge. The shortage of skilled officers leads to delays and unresolved cases, highlighting the need for stronger efforts to build a capable workforce to combat these threats efficiently and on time.

At the Sardar Vallabhbhai Patel National Police Academy (SVPNPA), we've been working hard to bridge this gap. Through our CyberX unit (previously NDCRTC), we've trained over 15,000 officers and staff since 2015. These officers are now better equipped to handle the complexities of cybercrime investigations.

To further support our investigators, the CyberX unit has developed five comprehensive manuals. These manuals are designed to be practical, user-friendly guides to help officers navigate the often-complicated process of cybercrime investigations. They focus on bridging the knowledge and skill gaps, offering clear and actionable insights.

I strongly encourage all investigators to use these manuals to their full advantage. They cover the latest tools and techniques, providing the confidence and clarity needed to take on even the most challenging cases. Together, we can make significant progress in the fight against cybercrime and ensure justice in this ever-changing digital world.

Amit Garg, IPS
Director
Sardar Vallabhbhai Patel
National Police Academy

Contributors:

Mohammed Arif Ali Khan:

Mohammed Arif Ali Khan is working as Chief Forensic Analyst at SVPNPA. He has a decade long experience in capacity building in cyber-crime investigation and digital forensics. He has also worked with the Cyber Crimes Cell, CID Hyderabad and specializes in solving cases related to online harassment, job frauds, fake websites, etc. His interest in Cyber Security was rewarded by companies like Indeed.com, AT&T, Mail.ru for finding security vulnerabilities in their services.

Parmesh Naik:

Parmesh Naik is Senior Forensic Analyst at SVPNPA with over eight years of experience in training law enforcement personnel, specializing in OSINT, Linux forensics, and Malware analysis. His profound understanding of digital forensics is demonstrated through the innovative software tools he has developed, which have become essential in law enforcement investigations.

Shaik Ghousal Mubarak:

Shaik Ghousal Mubarak is working as a Senior Forensic Analyst at SVPNPA. He holds a vast experience of 10 years in the domain of cybercrime investigation.
He previously worked as a cyber-crime consultant at CID Cyber Crimes Hyderabad. He is holding a PG-Diploma in Advance Computing and a B-Tech in Computer Science. His area of interest is Financial Fraud Investigations. Additionally, he is a regular guest speaker at various Police academies, Central Agencies, and other institutions.

Nitin Sharma:

Nitin Sharma is working as the Lead Forensic Analyst at SVPNPA, he imparts training to law enforcement officers and specializes in areas such as Internet Crime Investigation, Cryptocurrency Investigation & Digital Forensics. He holds a PG diploma in Cyber Law & Cyber Forensics from NLSIU Bangalore and an M-Tech in Cyber Security from Gujarat Forensic Sciences University. His extensive experience includes assisting field officers in cases ranging from Internet crimes to Dark Web & Cryptocurrency investigations for agencies like NIA, NCRB, Punjab Police, and others.

Aishwarya Tiwari:

Aishwarya Tiwari is a Forensic Analyst in NDCRTC with four years of specialized experience in training law enforcement agencies and conducting research in cryptocurrency investigation. Aishwarya's expertise is further solidified by a CHFI Certification, a CEH Certification from EC Council, and a Blockchain and Cryptocurrency Diploma from Oxford, London. Aishwarya, continues to make

significant contributions to cyber forensics and security, driven by a steadfast commitment to innovation and excellence in protecting digital assets and mitigating cyber threats.

Priya Ghurde:

Priya Ghurde currently holds the position of 'Cyber Investigation and Forensic Specialist' at the Indian Cyber Crime Coordination Centre (I4C), cryptocurrency-related offenses. Prior to her tenure at I4C, she served as Lead Forensic Analyst at SVPNPA. She has total experience of six years in the field of Cyber Crime Investigation and Cyber Security. She imparts training to law enforcement officers and specializes in areas such as Internet Crime Investigation, Dark web Monitoring & Digital Forensics. She holds B-Tech Degree in Information Technology along with certifications including Cyber Shiksha from Microsoft and CHFI from EC-Council. Her extensive experience includes assisting field officers in cases ranging from Dark Web related investigations to Digital Forensic Investigations for agencies like NIA, NCRB, Punjab Police, and others.

Ashmit Sharma:

Ashmit Sharma, presently serving as Scientist 'B' (Forensic Electronics) at CFSL, DFSS, MHA, GoI (Bhopal) previously as Lead Forensic Analyst at SVPNPA. He is a seasoned professional with expertise in digital forensics. Armed with B-Tech in ECE and an MSc in Forensic Science, Ashmit has honed his skills across various prestigious organizations including RFSL (NR, Dharamshala, HP), CFL (State Crime Branch, Haryana), and CFDML(SFIO). His dedication to continuous learning is evident through his publication of two international papers, focusing on smartphone and WhatsApp vulnerabilities, further establishing his reputation as an avid learner in the field

Mohammed Nazim:

Mohammed Nazim is working as a Forensic Analyst at SVPNPA, equipped with a Computer Science Engineering background and accreditation as an Information Security Management Systems Auditor (ISO 27001). Specializing in CDR/IPDR analysis and fueled by a fervour for Internet Governance, Nazim extends his expertise generously to esteemed institutions such as police academies, NIA, Central Detective Training Institute, and ESCI

Contents

Trending Modus Operandi of Cybercrimes

Acquaintance to Web Server and technology

Investigation of e-mails

Cyber Law and Admissibility of Digital Evidence

Digital crime Scene management

Social media Monitoring and Sentiment Analysis

Tor Based investigation

Investigation of Cryptocurrency

IoT and Cloud Investigation

Metaverse and Techno-Legal challenges in Cyberspace

Trending Modus Operandi of Cyber-crimes

1. Introduction to Cyber Crime

Crime and violence are inherent in our political and social system. With the moving pace of technology, the popularity of internet grows continuously, with not only changing our views of life, but also changing the way crime takes place all over the world. We need a technology that can be used to bring justice to those who are responsible for conducting attacks on computer systems across the globe. Proliferation of Information technology has brought with itself a challenging scenario in society.

It has assumed a very significant position in our life. The unending quest to get better in technology has impregnated various vices in the society. The face of criminal activities has got a new dimension and outlook with the advent of latest technology. For sure, we cannot rule out the contribution of such fascinating technologies in our life.

Today in the world of computers, along with the computers, its users are also increasing very rapidly. Now the time has come in which organizations are strongly dependent on the computers and internet for taking their businesses to the crest.

A large package of information is being sent or received at one click. The large numbers of computers are connected in a cob-web like network, which is necessary for dispatching and receiving information. Along with boom, these computers are also responsible for Cyber Frauds and Cyber.

2. Cyber space

Cyberspace refers to the virtual computer world that is an electronic medium that is used to facilitate online communication. Cyberspace typically involves worldwide computer network made up of many subnetworks that employ communication and data exchange activities.

Cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".[1] The Russian-American Cyber Security Summit, on the other hand, describe cyberspace as "an electronic medium through which information is created, transmitted, received, stored, processed, and deleted. From both definitions we can infer that cyberspace is the combination of the internet and telecommunications technologies that allow for the recording, storage, retrieval and transmission of information.

Cyberspace is the place which availed us online games, chat rooms, and the instant messaging conversations. Cyber space allows users to share information, interact, swap ideas, play games, engage in discussions or social forums, conduct business and create intuitive media, among many other activities.

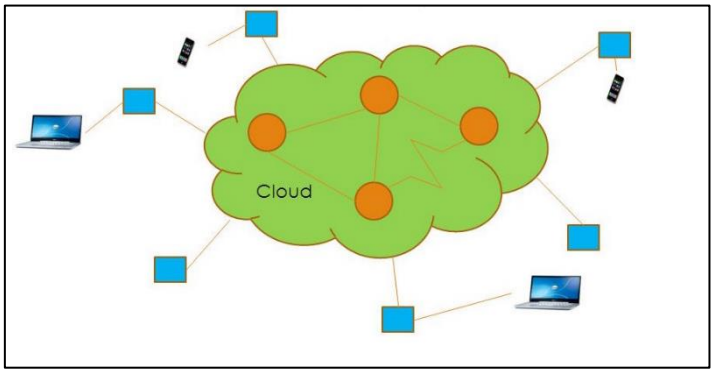


FIGURE 1 CYBER SPACE

[1] Department of Defence Dictionary of Military and Associated Terms, 2010

3. Cyber Crime Definition

Any crime in which a computer is used as a tool or target or both can be called as a cybercrime. But under Indian law "Cybercrime" as such has not been defined under any legislation. Legislation that deals with the offences related to such crimes in India is **Information Technology Act, 2000**, as amended in 2008.

Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. It is very difficult to classify crimes in general into distinct groups as many crimes evolve on a daily basis. A cybercrime includes a wide range of activities, from illegally downloading music files to stealing money from online bank accounts. Cyber criminals are not always financially motivated. Cybercrimes include non-monetary offenses as well. It can include frauds such as job-related frauds, matrimonial frauds; stealing and misusing sensitive personal information (Aadhaar details, credit/debit card details, bank account credentials, etc.); defamation of an individual on social media; distribution of computer viruses etc. Cybercrimes can also lead to physical or sexual abuse.

The proliferation of computer technology has created a new class of threats -"cyber threats"- which societies must confront. These cyber threats can be generically defined as using computer technology to engage in activity that undermines a society's ability to maintain internal or external order.[2]

One common definition describes cyber-crime as any activity in which computers or networks are a tool, a target or a place of criminal activity.[3]

Cyber-crimes can also be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunications networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones."[4]

4. Classification of Cyber Crime

Cyber-crimes were classified by various people differently on the basis of different criterion. For the purpose of understanding the way cyber-crimes are conducted, Cybercrimes can be classified into following categories:

- Crimes targeting computer systems
- Crimes in which computer systems are used as tools/instruments
- Computer as a repository of evidence

i. Crimes Targeting Computer Systems

Crimes where in computer systems are the target and these are committed by a selected group of criminals who are technically expert and requires good knowledge and expertise. Following are the examples of these crimes:

- **Hacking**
  Every act committed with the intention of breaking into a computer and/or network is considered as hacking.

[2] [1]
[3] [14]
[4] [2]

Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.

- **DoS / DDoS**

  Denial-of-service (DoS) attacks overload servers, systems or networks with forged requests in order to overwhelm the target resources and make it difficult or impossible for legitimate users to use them.

  Distributed Denial of Service (DDoS) attack is similar to a DoS attack but the results are prominent. Instead of one computer and one internet connection the DDoS attack utilises many computers and many connections. The computers behind such an attack are often distributed around the whole world and will be part of what is known as a botnet.

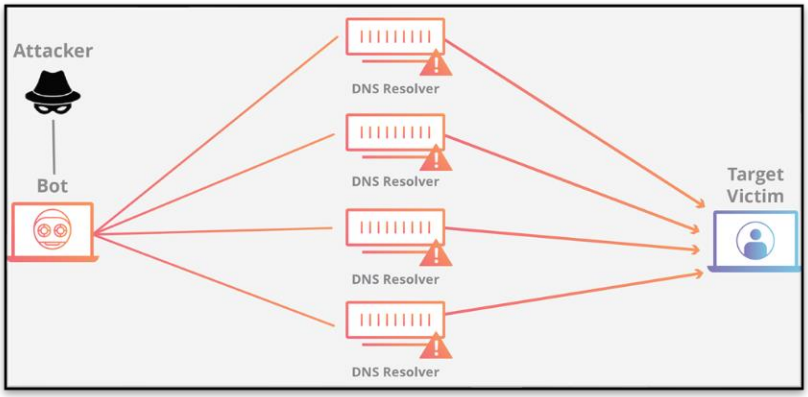


FIGURE 2 : DDOS ATTACK [5]

- **Virus / Malware Spreading**

  Injecting and spreading malicious code in various forms like viruses, worms, trojans, spywares, adware, rootkits etc. These get installed secretly in the victim's computer system and can be used to access and transmit sensitive information about the system, and in some instances, the infected systems can be used as tools to commit other types of cybercrime.

- **Web Defacement**

  Attacker changes the visual appearance of the website by posting some other indecent, hostile and obscene images, messages, videos etc. Sometimes attacker might make the site dysfunctional.

- **Spoofing**

  Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

  Types of Spoofing:

  - ***Email Spoofing***

    Email spoofing occurs when an attacker uses an email message to trick a recipient into thinking it came from a known, trusted source. These emails may include links to

[5] [12]

malicious websites or attachments infected with malware, or they may use social engineering to convince the recipient to freely disclose sensitive information.

- ***Website Spoofing***
  Website spoofing refers to when a website is designed to mimic an existing site known and/or trusted by the user. Attackers use these sites to gain login and other personal information from users.

- ***Caller ID Spoofing***
  With caller ID spoofing, attackers can make it appear as if their phone calls are coming from a specific number—either one that is known and/or trusted to the recipient, or one that indicates a specific geographic location. Attackers can then use social engineering—often posing as someone from a bank or customer support—to convince their targets to, over the phone, provide sensitive information such as passwords, account information, social security numbers, and more

- **Skimming**
  Special electronic devices are inserted in ATM and credit and debit card processing machines to obtain credit and debit card numbers.

FIGURE 3 : SKIMMING [6]

- **Cyber Terrorism**
  Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub national groups or clandestine agents."
  In Information Technology Act (2008), cyber terrorism is defined as, any action with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people like,
  (i) denying or cause the denial of access to any person authorized to access computer resource; or Punishment for dishonestly receiving stolen computer resource or communication device Punishment for identity theft. Punishment for cheating by personation by using computer resource. Punishment for cyber terrorism
  (ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or
  (iii) introducing or causing to introduce any computer contaminant;

[6] [11]

- **Pharming**
  Pharming refers to misdirecting of traffic from one Website to a Website controlled by a criminal hacker by altering the domain name system (e.g., by DNS cache poisoning) or by altering configuration files on a victim's computer.

- **Spamming**
  Spamming means sending multiple copies of unsolicited mails. An e-mail sent to many unwilling recipients in order to sell products or services.

- **Man in the Middle**
  Man-in-the-middle (MitM) attack is a type of attack where the hackers intercept communications between two different parties and redirect the traffic traveling between the two or to just collect the information being shared. MitM attack can help in sniffing login credentials or personal information, sabotage communications and to destroy data.

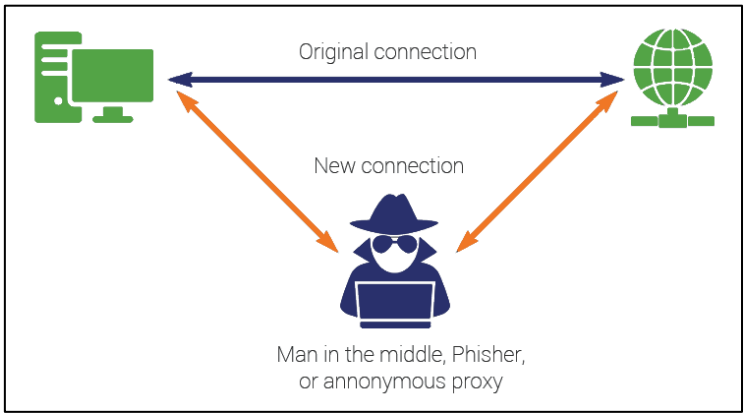


FIGURE 4 : MAN IN THE MIDDLE ATTACK [7]

- **Phishing**
  Phishing attack is conducted using a forged or spoofed e-mail or Web site that imitates or duplicates an official communication or page to trick victims into revealing logon or other confidential information that can be used for penetration, financial fraud or identity theft.

- **Vishing**
  Vishing is a Voice phishing, a form of criminal phone fraud, where fraudster uses social engineering techniques over the telephone system to gain access to private personal and financial information for the purpose of financial reward.

- **Smishing**
  Smishing is a fraudulent practice of sending text messages pretending to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers.

- **Ransomware**
  In this type of attack computer is taken as hostage. Attacker holds the host computer until system owner pays the demanded ransom or money. Ransomware encrypts important files or at times whole system and it becomes inaccessible to user until he fulfils the demand by attacker. CryptoLocker is known to be first of its kind ransomware.

FIGURE 5 : RANSOMWARE ATTACK [8]

- **Email Bombing**
  Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or servers (in case of a company or an email service provider) crashing.

- **Web jacking**
  Web jacking is an act of forcefully taking control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.

- **Rootkit**
  The root account is the most privileged on the system and has administrative level power over system, from having ability to modify the system in any way desired to grant and revoke access permissions to other users on system.

  Hence in simple terms rootkit is nothing but a collection of tools that enabled root access of the computer or network. But the same tools are used by hackers to hide footprints of their intrusion into the system. [9]

ii. Crimes in which computer systems are used as tools/instruments

When the individual is the main target of cyber-crime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited.

These are the crimes which have existed for centuries in offline world. Scams theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases their potential pool of victims and makes them all the harder to trace and apprehend.

The various types of cyber-crimes which can be seen where in computers are used as instruments to commit an offence are:

[8] [9]
[9] [4]

- **Financial Frauds**
  Financial frauds icludes business frauds, investment frauds, mass marketing frauds, offering jobs overseas, Nigerian Frauds, Buiness opportunities etc. where unsuspecting people are lured in trap by the promise of such opportunities and deceived of their money and other valuables.

- **Data Modification**
  In this type of crime attacker gains the access to the system or the database of target and modifies or changes the data. At times authorized users may also commit this crime.

- **Identity Theft**
  Identity of an individual is a collection of unique and stable characteristics associated with the person which distinguishes him/her from others, even two similar looking individuals have a unique identity.
  Identity Theft as a term refers to wrongful use of personal information with an intention of causing legal harm.
  Personal information may include the following but it is not limited to the list mentioned below. It can be Name, Phone Number, Email-ID, Date of birth, Address, Identity card number, Permanent account number, Aadhar card number, Voter ID, Credit/Debit card details, Medicare Number, Passport details, Travel details, etc.

- **Cyber Bullying / Stalking**
  Cyber Stalking/ Cyber bullying is the term is used to refer to the use of the Internet, e-mail, or other electronic communications devices to stalk another person.
  Stalking generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

- **Data Theft**
  Data theft is copying data without permission of the data owner. Attacker may break into the computer system / network and copy classifies and sensitive information.

- **Pornography**
  Posting, publishing and transmitting obscene messages, photographs, videos and text via websites, mails, chatting or blogs over the internet.

- **Intellectual Property Theft**
  Copying knowledge-based assets and capital, trade designs, logos, ideas and innovations, material which is copyrighted is considered as intellectual property theft. Most common crime in this category is source code theft.

- **Cyber Espionage**
  Cyber espionage refers to gaining access to classified, sensitive and intellectual information of a company or an Organization create havoc against the company or the government entity. This information can also be used to influence the political elections and also to topple down the company's profit.

- **Matrimonial Frauds**
  Fraudsters make fake matrimonial account and get in touch with the victim where they promise victim of marriage and try to gain different advantages from victim.

- **App Based Frauds**
  Various apps like OLX, Paytm, GPay, PhonePe etc are used to commit financial frauds. Fraudster contacts victim regarding buying or selling of commodity, and fraudulently transfers money from victim's account to his own account.

- **Salami Attacks**
  These attacks are used for committing financial frauds. The idea here is to make the alteration so insignificant that in a single case it would go completely unnoticed.

- **Data Diddling**
  Data Diddling is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done. The original information to be entered is changed, either by a person typing in the data, a virus that's programmed to change the data, the programmer of the database or application, or anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data.[10]

- **Social Engineering**
  Social engineering involves various malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
  Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry

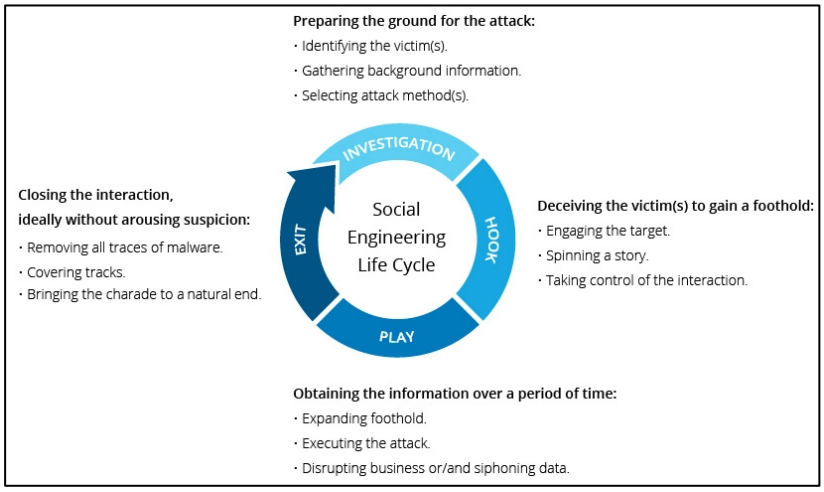


FIGURE 6 : SOCIAL ENGINEERING ATTACK LIFECYCLE

and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.[11]

- **Cyber Squatting**

[10] [13]
[11] [5]

An act of reserving the domain names of someone else's trademark with intent to sell it afterwards to the organization who is the owner of the trademark at a higher price

5. Computer as a Repository of Evidence

The computer/ information stored on the computer plays a non-substantial role in the act of crime, but do contain evidence of the crime.

Important evidence relating to the criminal activity may be found in the computers used by criminals. This may be used as supporting evidences/ documents for investigation of criminal cases registered against them.

The evidence which may be found on a computer system of an accused can be pertaining to, amongst others, any of the following.[12]

- Software piracy
- Gambling details
- Drugs and narcotic substance cases
- Terrorism attack plans and details
- Credit card numbers in fraud cases etc.

6. Malwares and its Types

Malware stands for "Malicious Software". It is designed to gain access and get installed into the computer without the consent of the user. There are various types of malwares, some of the popular ones are:

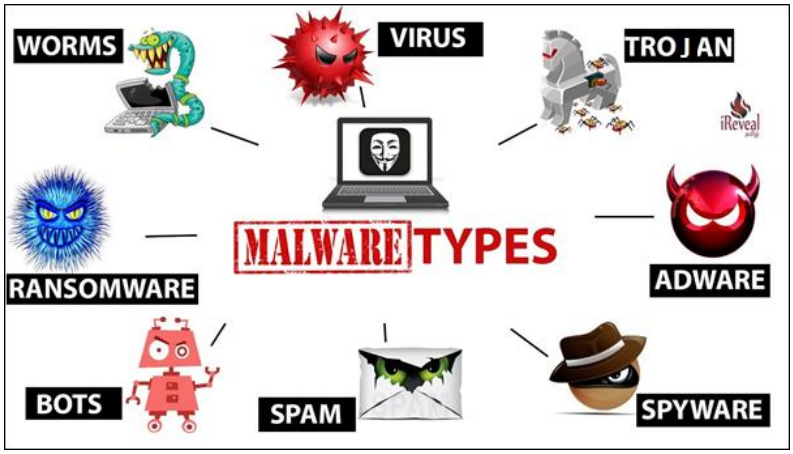


FIGURE 7 : TYPES OF MALWARES[13]

- **Virus**

  A virus is a malicious code written to damage/harm the host computer by deleting or appending a file, occupy memory space of the computer by replicating the copy of the code, slow down the performance of the computer, format the host machine, etc. It can be spread via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc.

[12] [6]

[13] https://techlifezine.com/what-is-malware/

A virus may be present in a computer, but it cannot activate itself without the human intervention. Until and unless the executable file(.exe) is executed, a virus cannot be activated in the host machine. A virus never self-propagates on other systems.

- **Worms**
  They are a class of virus which can propagate themselves. They are different from the virus by the fact that they do not require human intervention to travel over the network and spread from the infected machine to the whole network. Worms can spread either through network, using the loopholes of the Operating System or via email.

- **Trojan Horse**
  Trojan horse is a malicious code that is installed in the host machine by disguising it to be useful software. The user clicks on the link to download the file which is disguised as a useful file or software from legitimate source. It damages the host computer by manipulating the data and creates a backdoor in the host computer so that it could be controlled by a remote computer.

  Compromised system can become a part of botnet(robot-network), a network of computers which are infected by malicious code and controlled by central controller. Trojans neither infect the other computers in the network nor do they replicate.

- **Spyware**
  It is a special type of malware which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine. Mostly it gathers the browsing habits of the user and the send it to the remote server without the knowledge of the owner of the computer. Most of the time they are downloaded in to the host computer while downloading freeware i.e., free application programs from the internet. Spywares may be of various types; It can keep track of the cookies of the host computer, it can act as a keyloggers to sniff the banking passwords and sensitive information, etc.

- **Adware**
  It is a special type of malware which is used for forced advertising. They either redirect the page to some advertising page or pop-up an additional page which promotes some product or event. This adware is financially supported by the organizations whose products are advertised.

Acquaintance to Web Server & Technology

1. Introduction to Servers

A computer programme or apparatus that offers a service to another computer programme and its user, also known as the client, is referred to as a server. The actual computer that a server programme runs on in a data centre is also frequently referred to as a server. It's possible the device serves as a dedicated server or serves other functions.

A server programme responds to requests from client programmes, which may be operating on the same computer or on different machines, in the client/server programming model. Depending on the application, a computer may act as both a client and a server to other programmes requesting services from it.

Working:

A physical machine, a virtual computer, or software that provides server services can all be referred to as servers. Depending on how the word "server" is employed, there are many different ways that a server might operate.

2. Physical and Virtual Servers

A physical server is a machine that runs server software.
A virtual server is a computerized simulation of a physical server. A virtual server has its own operating system and applications, just like a physical server. These are kept apart from any other virtual servers that could be running on the actual server.
A lightweight software component known as a hypervisor must be installed on a physical server in order to create virtual machines. To make the physical server capable of acting as a virtualization host is the hypervisor's responsibility. The virtualization host makes one or more virtual machines accessible to the actual server's hardware resources, including CPU time, memory, storage, and network bandwidth. Administrators can assign particular hardware resources to each virtual server through an administrative console. Because numerous virtual servers can run on a single physical server rather than each workload requiring a separate physical server, this significantly reduces the cost of hardware.

FIGURE 8 SERVERS

i. Server Software

An operating system and an application are the two essential software parts that any server must have. The server application is run on the operating system as a platform. It grants access to the hardware resources underneath and offers the dependency services needed by the application.

The operating system also gives clients a way to communicate with the server application. The server's IP address and fully qualified domain name, for example, are assigned at the operating system level.

- **Desktop Computers Vs. Servers**

Desktop computers and servers have a number of commonalities as well as distinctions. The vast majority of servers are built around X86/X64 CPUs and are capable of running the same software as a

desktop computer. Contrary to the majority of desktop PCs, real servers frequently have several CPU sockets and error-correcting memory. Additionally, in comparison to most desktop PCs, servers often support a far higher memory capacity**.**

Manufacturers of server hardware build servers to handle redundant components since they frequently conduct mission-critical workloads. There are servers that come with redundant network ports and redundant power supply. With the help of these backup parts, a server can keep running even when a crucial component break.

In terms of form factor, server hardware differs from desktop hardware. Modern desktop computers frequently come in the form of towers that can fit under a desk. Even while few companies still sell tower servers, the majority of servers are made to be rack mounted. Depending on how much rack space they take up, these rack mount systems are referred to as having a 1U, 2U, or 4U form factor. For example, a 2U server uses twice as much rack space as a 1U server.

A desktop computer's operating system and a server's operating system are two additional significant differences. A desktop operating system might be able to carry out some server-like tasks, but it is neither intended nor authorized to replace a server operating system. Desktop operating systems like Windows 10 are available.

Hyper-V, Microsoft's virtual machine platform, is a feature of some Windows 10 editions. Although Hyper-V can be run on both Windows 10 and Windows Server, the Hyper-V version that comes with Windows Server is intended for running production virtual servers, whereas the Hyper-V hypervisor in Windows 10 is primarily intended for use in development.

3. Types of Server

- **Web Servers:** An application that serves up requested HTML files or pages is known as a web server. Web browser serves as the client in this scenario.
- **Application Server:** A computer program that creates the business logic for an application software in a distributed network.
- **Proxy Server:** A program that serves as a go-between for a client or user who is requesting a service from another server and an endpoint device such a computer.
- **E-mail Server:** A program that accepts receiving emails from local users (users on the same domain) and remote senders and routes outgoing emails for delivery.
- **Virtual Server:** An application operating on a shared server that is set up such that each user feels as though they have full control over the server.
- **Blade Server:** A server chassis that holds numerous server blades—thin, modular electronic circuit boards. Each blade is a separate server that is frequently devoted to a single application.
- **File Server:** A computer that manages and stores data files centrally so that other computers on the same network can access them.
- **Policy Server:** A security component of a policy-based network that provides authorization services and facilitates tracking and control of files.
- **Database Servers:** A database or databases are hosted on this server. Database queries are executed by client programs to read data from or publish data to the server-hosted database.
- **Print Server:** One or more network-attached printers, or print devices as some server providers refer to them, are accessible to users through this server. The print jobs that users submit are placed in a queue on the print server. Depending on the job type or the person who submitted the print job, certain print servers can prioritise the jobs in the print queue.

4. RAID Configuration

Using RAID technology, data storage can be made more efficient and/or reliable. The acronym refers for either Redundant Array of Independent Drives or, more formally and less frequently, Redundant Array of Inexpensive Disks. A RAID system has two or more parallel-operating discs. These can be

hard drives, but an increasing number of people are using SSD technology instead (Solid State Drives). There are various RAID levels, each of which is best suited for a certain circumstance.

An independent controller card (a hardware RAID controller) may house the software necessary to carry out RAID functionality and manage the discs, or it may just be a driver. Some Windows versions, including Windows Server 2012 and Mac OS X, include software RAID capabilities. Hardware RAID controllers are more expensive than pure software RAID controllers, but they also perform better, especially with RAID 5 and 6.

RAID-systems can be used with a number of interfaces, including SATA, SCSI, IDE, or FC (fiber channel.) There are systems that use SATA disks internally, but that have a FireWire or SCSI-interface for the host system.

i. RAID Level 0- Stripping

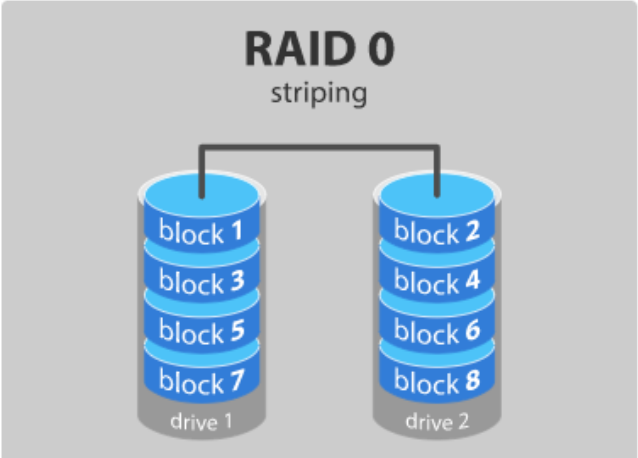


FIGURE 9: RAID 0

In a RAID 0 system, data is divided into blocks and written across all of the array's devices. This provides better I/O speed by employing many drives (at least 2) concurrently. Using numerous controllers, ideally one per disc, can improve this speed even more.

Advantages:

- Great performance is provided by RAID 0 for both read and write operations. The overhead of parity controls does not exist.
- There is no overhead because all storage space is being used.
- The technology is simple to use.

Disadvantages:

- Failure-tolerant RAID 0 is not. All of the data in the RAID 0 array is lost if one drive fails. Mission-critical systems shouldn't use it.

ii. RAID Level 1-Mirroring

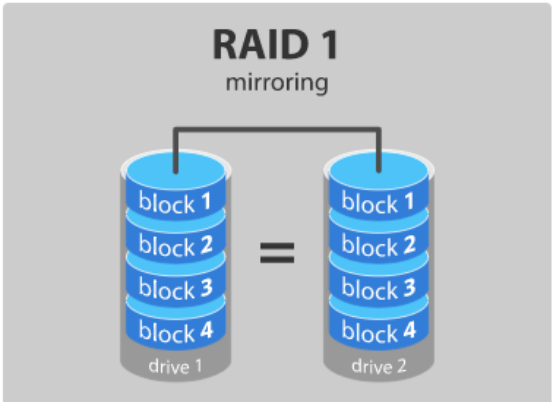


FIGURE 10: RAID 1

Data are stored twice by writing them to both the data drive (or set of data drives) and a mirror drive (or set of drives). In the event of a drive failure, the controller continues to operate and retrieve data using either the data drive or the mirror drive. For a RAID 1 array, you require at least two discs.

Advantages:

- RAID 1 provides fast read and write speeds that are on par with a single disc.
- Data only has to be moved to the new drive in the event that a drive fails rather than being rebuilt.
- It is quite easy to use RAID 1 technology.

Disadvantages:

- The key drawback is that since all data is written twice, the effective storage capacity is just half of the overall drive capacity.
- A hot swap of a failing drive is not always possible with software RAID 1 solutions. Therefore, replacing the faulty drive requires shutting down the computer to which it is linked. This could not be appropriate for servers that are being accessed concurrently by multiple users. These systems frequently employ hardware controllers that enable hot swapping.

iii. RAID Level 5 – Striping with parity

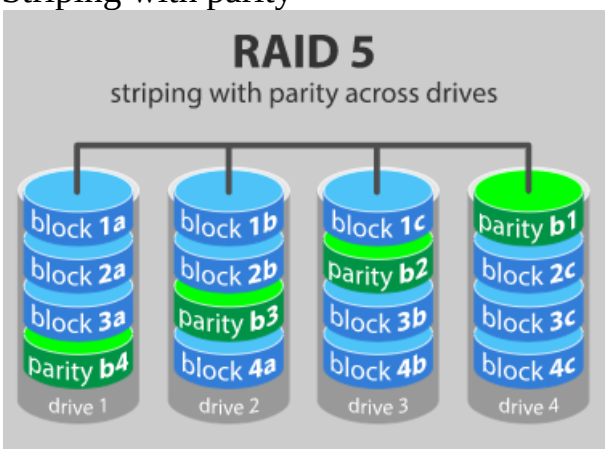


FIGURE 11: RAID 5

The most popular secure RAID level is RAID 5. At least three drives are needed, however up to sixteen can be used. Data blocks are striped across the drives and on one drive a parity checksum of all the block data is written. The parity data are distributed over all drives rather than being written to a single fixed disc. If one of the other data blocks' data is no longer available, the computer can recalculate it using the parity data. In other words, a RAID 5 array may survive a single disc failure without losing

data or the ability to access data. Although software can be used to implement RAID 5, a hardware controller is advised.

Advantages:

- Write data transactions take a little longer than read data operations to complete (due to the parity that has to be calculated).
- Even when the failed drive is being replaced and the storage controller rebuilds the data on the replacement drive, if a drive fails, you may still access all of your data.

Disadvantages:

- Drive failures have an effect on throughput, although this is still acceptable.
- This technology is sophisticated. Depending on the load on the array and the speed of the controller, rebuilding the data when a 4TB disc fails and needs to be replaced could take a day or more. During that time, if another disc fails, the data are permanently gone.

iv. RAID Level 6 – Stripping with double parity

Similar to RAID 5, but RAID 6 writes the parity data to two discs. That means it needs at least 4 drives and is capable of handling 2 drives failing at once. Of course, there are extremely little odds that two drives will fail simultaneously. It takes hours or even more than a day to rebuild the swapped drive in a RAID 5 system, however, if a drive dies and is replaced by a new drive. During that time, if another drive fails, you still lose all of your data. The RAID array will even survive that second failure with RAID 6.

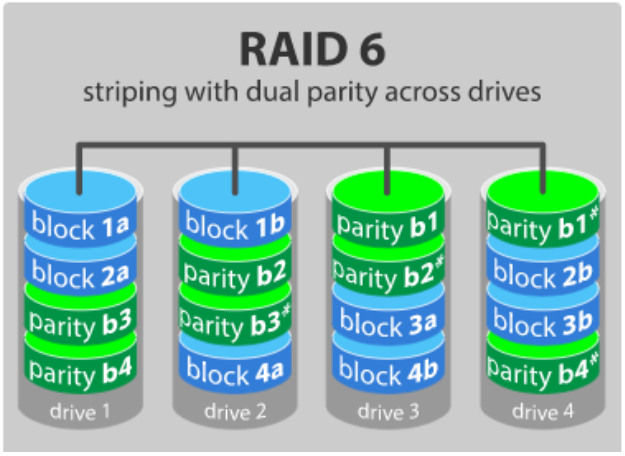


FIGURE 12: RAID 6

- **Advantages:**
  - Read data operations occur very quickly, just like with RAID 5.
  - If two drives fail, you still have access to all data, even while the failed drives are being replaced. So, RAID 6 is more secure than RAID 5.
- **Disadvantages:**
  - Due to the additional parity data that must be calculated, write data transactions take longer than RAID 5 transactions. One report I read showed a 20% decrease in writing performance.
  - Throughput is impacted by drive failure; however, this is still acceptable.
  - This technology is sophisticated. It can take a while to rebuild an array once a drive fails.

Investigation of e-mails

1. E-mail Architecture

Electronic mail is a mode of digital communication among worldwide users using computer-based application. It is based on client server architecture.

i. E-Mail Client

An e-mail client is a program that allows a user to access and manages his e-mails. An e-mail client –

- Display all messages in user's inbox.
- Helps User to select and read the message.
- Helps to create mail and add attachment.
- Helps to download the attachment.

Web browser-based e-mail services like Yahoo mail, Gmail etc. are also known as webmail.

Examples of E-Mail Clients

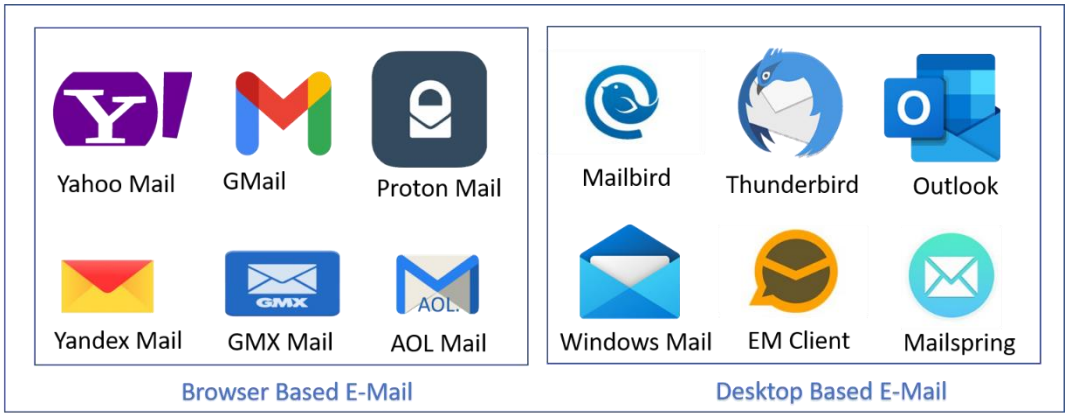


FIGURE 13 : E-MAIL CLIENTS

Note : An E–mail client will be storing all the mails along with the attachments, contacts and the IP address through which user has accessed the mail. Under section 91 CrPC, law enforcement agencies can request for the information from any e-mail service provider.

ii. E-Mail Server

An E-Mail server is a computer that performs the action of sending and receiving the e-mails over a network using a set of communication protocols meant for e-mail communication.

- An E-Mail server connects to and serves several E-Mail Clients.
- It has a number of E-Mail accounts.

- When a user presses the send button on his E-Mail client, the client connects to E-Mail server and passes the message and related information to the server.

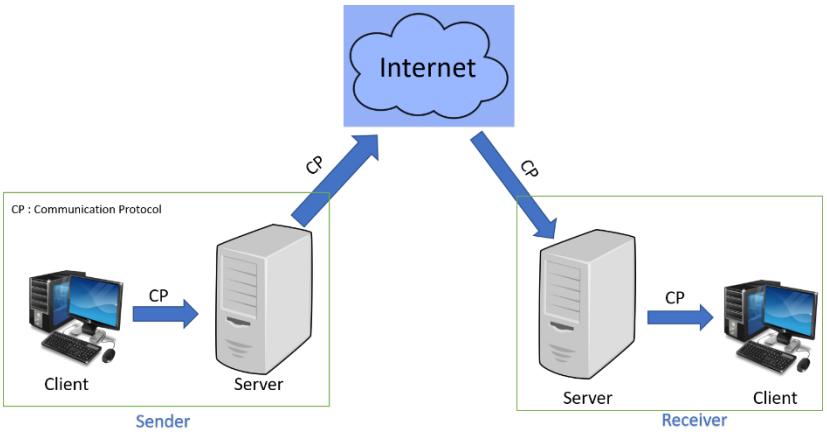


FIGURE 14 : WORKING OF E-MAIL SERVER

2. Communication Protocols used in E-Mail

E-mail uses SMTP (Simple Mail Transfer Protocol) for sending the messages and POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) to retrieve a message from mail server.

Protocol	Description
SMTP (Simple Mail Transfer Protocol)	E-mail is sent using this protocol
POP (Post Office Protocol)	POP downloads the entire email into the local computer and deletes the data on the server once it is downloaded.
IMAP (Internet Message Access Protocol)	With IMAP, the emails will be present in the server and not get downloaded to the user's mail box.

3. E-Mail Address

An email address distinguishes an email box to which email messages are conveyed. For every user the e-mail address is unique in the virtual world. The example of an e-mail address is as follows –

ndcrtc @ svpnpa . gov.in

Here the term 'ndcrtc' represents the user, group or department of a company. The sign '@' is a divider in the e-mail address which is mandatory in all e-mail addresses. svpnpa.gov.in is the domain name and gov.in is the top-level domain in the above example.

Note : The length of username cannot be more than 64 characters and length of domain name cannot be greater than 254 characters.

Tip: For G-mail the dot('.') in between username is not considered for example for Gmail ndcrtc@gmail.com and ndc.rtc@gmail.com or nd.cr.tc@gmail.com all are same email address, but for some other mail services (for example Yahoo mail) dot ('.') in between username can be considered.

i. Flow of E-Mail over Internet

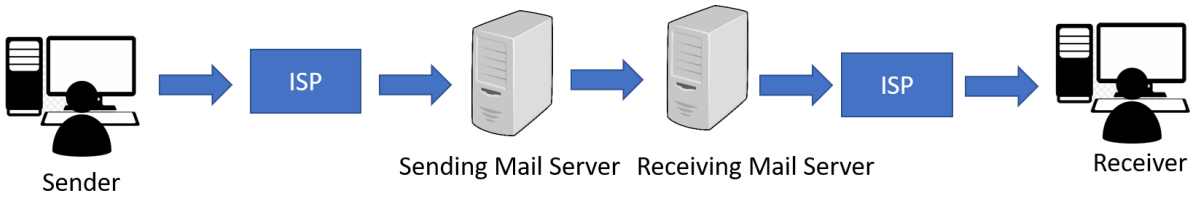


FIGURE 15 : FLOW OF E-MAIL OVER INTERNET

4. E-Mail Related Crimes

i. Phishing

Phishing is a sort of online trick where lawbreakers send an email that gives off an impression of being from a genuine organization and request that you give touchy data. This is typically done by including a connection that will seem to take you to the organization's site to fill in your data – yet the site is a shrewd phony and the data you give goes directly to the law breakers behind the trick.

Phishing Techniques

- **E-Mail Phishing** : Attacker will send a phishing email to the receiver which will look like a genuine e-mail from company and will contain a phishing website link. Now he will create usually try to push users into action to click on that link and fill the details by creating some source of urgency. The information filled by the user on phishing page will go to the attacker.

- **Spear Phishing :** Spear phishing focuses on a particular individual or endeavour, rather than arbitrary application clients. It's a more inside and out adaptation of phishing that requires exceptional information about an association, including its capacity structure.

ii. Spoofing

Email spoofing is the formation of email messages with a fraud sender address. The center email conventions don't have any system for confirmation, making it normal for spam and phishing messages to utilize such ridiculing to misdirect or even trick the beneficiary about the origin of the message.
Spoofed email has become a piece of the day-by-day messages that are conveyed to an individual's inbox. Spam has become a beneficial venture for enthusiastic advertisers and is a state of dispute for the individuals who get it. In any case, mock email has gotten something beyond an annoyance; it is a practical security risk to singular home clients, associations, and organizations. Aggressor's use satirizes email messages to proliferate infections, Trojans, and worms. Criminals use them for phishing plans that endeavour to blackmail cash and data from clueless clients.
Because of the absence of validation in SMTP (Simple Mail Transfer Protocol), aggressors and spammers can without much of a stretch jumble their tracks and make it hard to follow the beginning of their email.

iii. Spamming

spamming can be characterized as the flooding of the Internet with spontaneous or misleading messages. For the most part, spam is utilized for business promoting, regularly for pyramid schemes or for selling questionable items. However, not generally. The most common form of spamming is email spamming.

Types of Spamming

- **E-Mail Spamming**: This is the act of sending spontaneous email messages to an unpredictable arrangement of beneficiaries. It is among the soonest types of web-based spamming and it is evaluated that email spam as of now makes up 80 to 85 percent of all messages on the planet. While this bad habit is illicit in certain wards, it is far less controlled in others.
- **Social Network Spamming:** Social networks, for example, Twitter and Facebook are not safe to spam messages either. There have been various instances of record hacks and sending of bogus demands and connections under the pretence of the record holder's subtleties.
- **Mobile Phone Spamming:** This type of spamming is aimed at the content informing administration of a cell phone and it is very disturbing and may in certain business sectors cause the client to be charged for each instant message got.

5. Components of E-Mail

Before starting analysis of e-mails, it is required to know that an E–mail Consists of three components, namely –

- E–mail Envelope – E–mail is enclosed in a digital envelop analogous to envelope of a hardcopy letter. The E-Mail envelope is only can be read by mail server.
- E–mail Header – Contains the Control and Meta Information of the E – mail. For e.g. originator's E–mail address, recipient's E–mail address, E–mail date/time, information of intermediate E–mail servers (if any) etc.
- E–mail Body – Contains E–mail Text/attachments (in HTML (Hyper Text Mark-up Language) and encoded in MIME (Multipurpose Internet Mail Extensions)).

E-Mail header is the most important part of an E–mail for the purpose of Investigation. It includes information stamped by intermediate E–mail Servers and all the other metadata related to time stamps, details of sender and destination along with the Routing information of an E – mail.

Important e-mail header parameters are -

- Date: The date the message was originated/written.
- Message-ID: Unique Identity of the message generated at sender's mail server.
- To: The main intended recipient(s).
- Cc: Secondary (Carbon Copy) recipients.
- Content-Type: The nature of the message body or section (e.g. text/html, text/plain, multipart/mixed etc.)
- Received: Trace of Mail servers in the path of e-mail through which the message has passed.

6. Viewing Header in Different Web Mails

i. G-Mail

To view the e-mail header of an e-mail using Gmail services,

a) Log into your Gmail Account.
b) Open the E–mail whose headers you want to view.
c) Click the down arrow adjacent to the Reply link in the upper-right corner of the message.
d) Click Show Original.

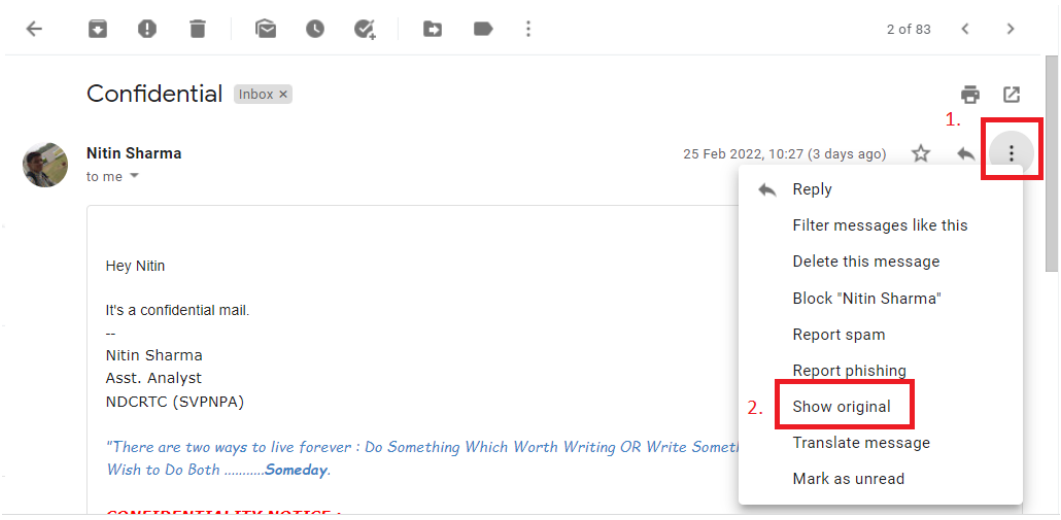


FIGURE 16 : STEPS TO VIEW HEADER IN GMAIL

ii. Yahoo Mail

To view the e-mail header of an e-mail using Yahoo services,

a) Log into your Yahoo mail Account.
b) Open the E–mail whose headers you want to view.
c) Click on the More (gear) icon above the message pan and click on 'View Raw Message'.

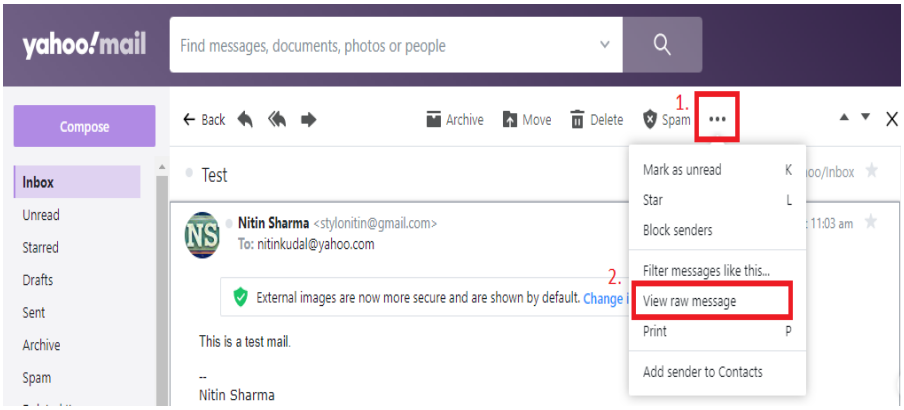


FIGURE 17 : VIEWING HEADER IN YAHOO MAIL

7. Investigation Related to E-Mail

i. Collection of E-Mail as Evidence

- Collect the screenshot of Contents of E-Mail.
- Download the Header of E-Mail or Copy/Paste it to a text file.
- Calculate the hash values of screenshots collected using any hash calculation tool with MD-5 & SHA-1 algorithm.
- Take a 65B certificate for admissibility of the evidence collected.

ii. Analysis of E-Mail Header

E-Mail header contains the metadata of an e-mail which can be analyzed to identify the sender of the e-mail. The 'Received' field in e-mail header contains the information about the path of the e-mail & relative time stamps which can be used to trace back to the sender of e-mail.

The upper most 'Received' field in header indicates the mail server of the receiver, and the last 'Received' field tells information about the sender of the mail. To Analyse the complete path of the e-mail the header should be analyzed using bottom to top approach.

Note: Most of the e-mail service provider do not provide information about the sender of the mail in the header due to privacy restrictions so the last 'Received' field in the header informs about the mail server of the sender. Timestamps in E-Mail

FIGURE 18 : E-MAIL HEADER ANALYSIS

An e-mail header also contains the time stamp for every 'Received' header field which may or may not be in same time zone (depends on the locality of the mail server in the path), by comparing these timestamps one can easily identify the traces of modification in the e-mail.

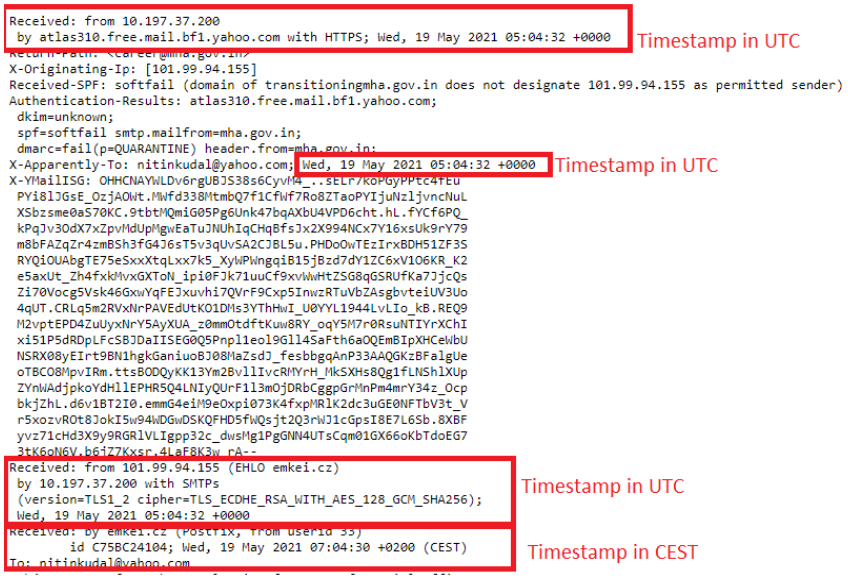


FIGURE 19 : TIMESTAMPS IN E-MAIL HEADER

iii. Conversion among Different Time Zones

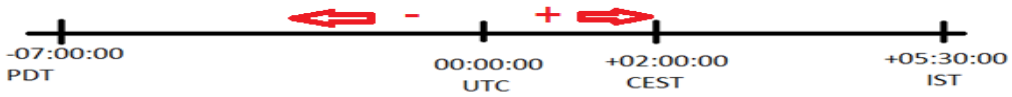


FIGURE 20 : CONVERSION AMONG TIME ZONES

iv. Identification of Spoofed E-Mail

To identify whether an email is spoofed check the header field 'Received-SPF' if the value in this field is anything other than 'Pass' then the email might be spoofed. To clarify the domain name in the header field 'Message-ID' should be matched with the domain in sender's mail if both are mismatched that means e-mail is spoofed.

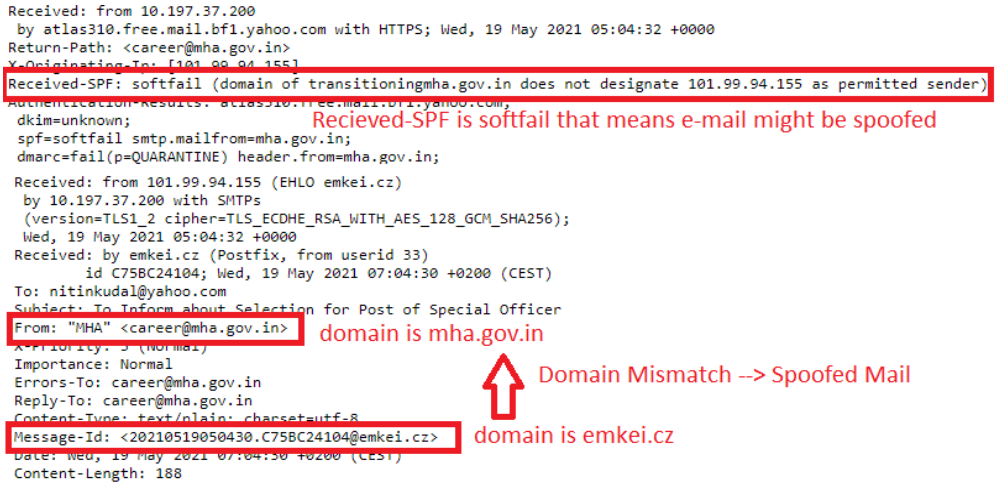


FIGURE 20 : IDENTIFICATION OF SPOOFED E-MAIL

v. Identification of Sender of E-Mail

The details about the sender of the e-mail can be obtained by providing a notice u/s 91 CrPC to the service provider of the e-mail. The format of the notice is shown below –

OFFICE OF THE
SUPERINTENDENT OF POLICE,
CYBER CRIMES, CID,
AP, HYDERABAD.

Date 10-07-2019

Cr.No

Notice U/s.91 Cr.P.C.

It is to inform you that a case is being conducted by this agency wherein the accessing IP Log details of the following Gmail ID is very much required for the purpose of investigation.

@gmail.com

Therefore it is requested to furnish the **Registration & Log details** (including IP Address, Date & Time) of the above Gmail ID **since creation to till date** for the purpose of investigation.

Early action would be highly appreciated.

SUPERINTENDENT OF POLICE,
CYBER CRIME PS, CID,
HYDERABAD.

To
Google Inc.,
Mountain View,
CA, USA.

FIGURE 21 : NOTICE TO GMAIL U/S 91CRPC

The reply from E-Mail Service provider (Google for G-Mail in this case) will be as follows –

############## * Google Confidential and Proprietary * ###############

GOOGLE SUBSCRIBER INFORMATION

Name:[redacted]

e-Mail:[redacted]@gmail.com

Status: Enabled

Services: Android, Emerald Sea Invite, Es Mobile, Gauss, Gmail, Google AdSense, Google Calendar, Google Dashboard, Google Docs, Google Drive, Google Groups, Google Mobile, Google Reader, Google Services, Google Talk, Google Voice, Google Wallet, Google+, Has Google Profile, Has Plusone. Lso Provider, Multilogin. Picasa Web Albums, Pp 2012, Transliteration, Web History, YouTube,

Secondary e-Mail: [redacted]@gmail.com

Created on: 2007/11/28-13:13:36-UTC

IP: 203.199.183.30, on 2007/11/28-13:13:36-UTC

Language Code: en

SMS: 880[redacted]8 [IN]

Nickname: [redacted]

| Time | IP Address | Type |

21 consecutive Login events from IP 49.204.13.181 occurred during past 24 hours prior to the following event.

| 2014/03/20-22:01:46-UTC | 49.204.13.181 | Login |

FIGURE 22 : LOGS FROM GOOGLE

It can be found from the above logs that the most recent activity of this suspect was from IP address 49.204.13.181. Now we need to find the ISP of the obtained IP address.

vi. Identification of ISP of IP Address

To identify the ISP of the IP address the 'Whois Lookup' of the IP address needs to be done. There are multiple websites to perform 'Whois Lookup'.

Open any of the website from the search results and enter the IP Address, one good website to perform 'Whois lookup' is www.whois.domaintools.com.

FIGURE 23 : PERFORMING IP LOOKUP

The result of the above search is as follows –

IP Information for 49.204.13.181

– Quick Stats

IP Location	India Nellore Beam Telecom Pvt Ltd
ASN	AS131269 BEAMTELE-AS-AP ACTFIBERNET Pvt Ltd, IN (registered Dec 14, 2009)
Resolve Host	broadband.actcorp.in
Whois Server	whois.apnic.net
IP Address	49.204.13.181

```
inetnum:        49.204.0.1 - 49.204.255.254
netname:        ACTFIBERNET-Tarnaka
descr:          Beam Telecom Pvt Ltd
country:        IN
geoloc:         28.613939 77.209021
admin-c:        AB208-AP
tech-c:         AB208-AP
abuse-c:        AB999-AP
status:         ALLOCATED NON-PORTABLE
mnt-by:         MAINT-IN-BEAMTELECOM
mnt-irt:        IRT-BEAMTELE-IN
last-modified:  2021-01-15T11:15:21Z
source:         APNIC

irt:            IRT-BEAMTELE-IN
```

FIGURE 24 : IP REGISTRATION DETAILS OF OBTAINED IP

From the above result, it is clear that the IP Address provided by G-Mail is a broadband IP address and the ISP is Beam Telecom Pvt Ltd.

vii. Collection of End-user Details of the IP Address

To Identify the End user of the above IP, IO should write a notice u/s 92 CrPC to the ISP (In this case Beam Telecom Pvt. Ltd.) to obtain the end user details.

Note: In case of IP belongs to a mobile service provider the ISP will provide IP Data Record.

The sample notice u/s 92 CrPC to the ISP is as follows –

To: Beam-Nodal
Subject: Re: CID - Cyber Crime PS - Request for End-User details of IP Addresses - Reg ([redacted])

Sir,

It is requested to furnish the end user details of the following IP Address for the purpose of investigation.

Date	Time (IST)	IP Address
17-12-2015	18:32:50	49.204.13.181

Early action will be highly appreciated.

Superintendent of Police,
Cyber Crimes, CID,
Hyderabad
040-23316750
"THE CYBER SPACE, SAFE TO USE UNSAFE TO MISUSE"

FIGURE 25 : NOTICE U/S92 CRPC TO OBTAIN IP LOG DETAILS

In the response of above notice the Nodal Officer of ISP will provide the end user details which is as follows –
The end user particulars consist of the address of the person who was using the internet at that specific point of time. The investigator can now locate the address and reach the originator of that e-mail.

8. Alternative Way to Find IP Address from E-Mail (IP Logger)

IP Loggers are simple and handy web-services for IP-address logging and collecting statistics for your blog, forum or website. These are basically used by web services for traffic determination and regional traffic distribution along with the traffic timing and other factors that can be determined by those.
For Law Enforcement Agencies, getting IP logs from service providers is still a time taking task. This is where the beauty of the IP Loggers comes in to the picture. The suspect with unknown IP Address can be send an enticing message along with the redirection link to an IP logger and the Public IP address of the suspect will be captured by the IP Logger along with time stamp. This Public IP Address can be used to further track the suspect and his/her activities for surveillance.
Here, one of the IP loggers called Grabify is shown below –

- Visit to www.grabify.link
- Copy the URL on which you want to redirect the suspect

TO,

Superintendent of Police,
Cyber Crimes, CID,
Hyderabad.

Dear Sir ,

Please find the details given below . IP Address is dynamic

Username	IP Address	MAC Address	Start Time	End Time	Contact
sh[redacted]3@gmail.com	49.204.13.181	74:44:01:99:86:0b	17-12-2015 12:56	17-12-2015 22:32	Mr. [redacted]
					[redacted] NAGAR, YOUSUFGUDA CHECKPOST,
					S[redacted]NGR-204.101 ([redacted] NAGAR)
					HYDERABAD, India - 500045
					Mob : 98[redacted]43

Regards,
Ajay Banda, Asst. Manager - Compliance
Mobile: +91 9542445244
BEAM TELECOM PVT. LTD. (An ACT Group Company)
8-2-610/A, Road No - 10 Banjara Hills, Hyderabad, Andhra Pradesh, INDIA - 500 034
www.beamfiber.com

FIGURE 26 : REPLY FROM ISP WITH END USER DETAILS

- Paste the URL in the blank space of grabify and click on 'Create URL'.

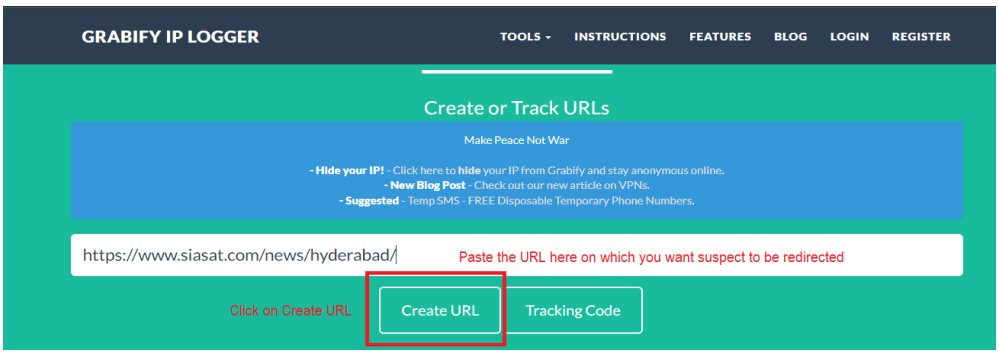


FIGURE 27 : CREATING TRACKING URL

- A new URL has been created which can be shared with suspect via message/e-mail.

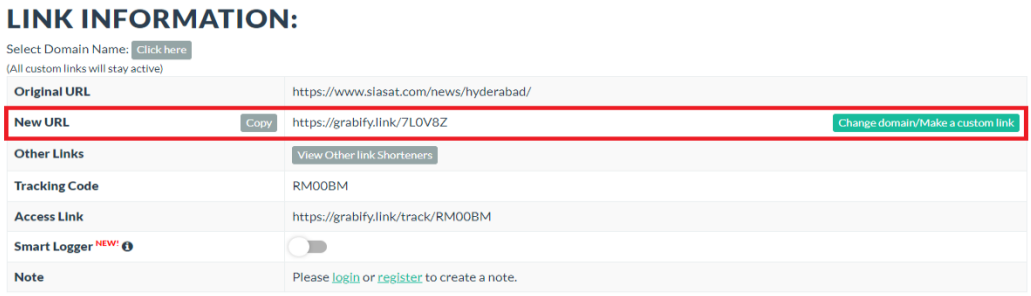


FIGURE 28 : TRACKING LINK

- Tracking link generated by grabify is https://grabify.link/7L0V8Z.
- The Access code for the above link is 'RM00BM' which can be used to access the link in future.

Once the tracking URL is generated, every time someone clicks on the URL a log containing the IP address and other information will be generated.Send the link to the suspect via message/email and wait for click. Once he clicked the IP of suspect can be

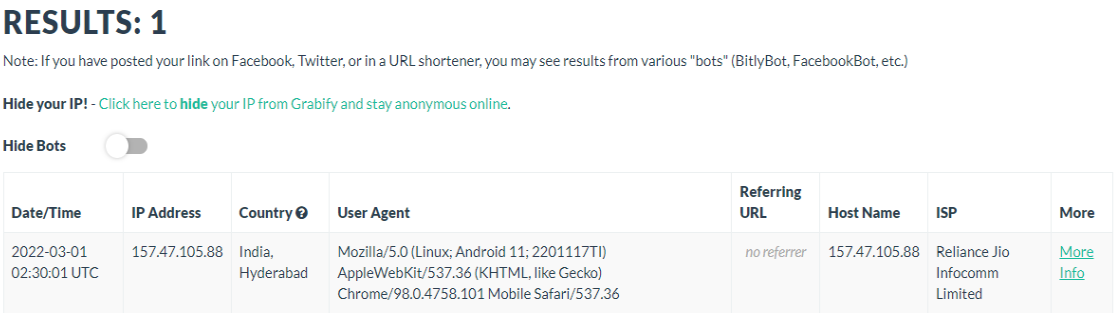


FIGURE 29 : IP LOGS OF SUSPECT

Cyber Law and Admissibility of Digital Evidence

1. Introduction to Information Technology Act 2000

India is one of the earliest nations to bring about a comprehensive law for e-commerce. The Information Technology ACT 2000 as amended in 2008 along with the rules, notification and related amendments to IPC, CrPC, Indian Evidence Act and other relevant special and local laws forms the cyber law frame works in India.

IT Act 2008 was enacted essentially to give legal recognition to electronic documents, securing and authentication of electronic records, e-commerce and promote e- governance. It was enacted following the UN resolution of 1997 which adopted the model law on electronic commerce adopted by UN Commission on International Trade Law and recommends all States to enact and revise their laws giving favourable consideration to the said model act.

Exponential growth of technology gave new ways and means to cybercrimes. To counter this growing cyber threat in 2008, the act was amended. Wide ranging crimes were incorporated in this amendment of the act with the provision of financial penalties as well as punishment varying from a three-year jail term to life sentence. This amendment came into force on 29th October, 2009. Broadly IT Act Amendment 2008 has covered following aspects.

The IT Act 2000 as amended in 2008 contains 13 chapters with 90 sections, 2 schedules. The description below gives a brief description of contents of 13 chapters in the Act.

- **Chapter 1** mentions the title jurisdiction and the application of Information Technology Act, and it has the definitions of various terms that are found in the act.
- **Chapter 2** deals with authentication of electronic records through the process of digital signatures and electronic signatures.
- **Chapter 3** Provides legal recognition to electronic records, electronic signatures, and their use for promoting electronic governance.
- **Chapter 4** discusses the aspects of attributing the electronic records, acknowledging of receipts and time and place of dispatch and receipt of electronic records for all legal purposes.
- **Chapter 5** has three sections, dealing with securing electronic records and electronic signatures.
- **Chapter 6** deals with regulations on persons who have licensed to issue digital signature certificates called certifying authorities. It has provisions specifying appointment functions of Control of certifying authorities, ways of recognizing foreign certifying authorities, powers and procedures to grant, reject, renew, suspend, and revoke licenses to certifying authorities and to investigate into controversies arising out of them.
- **Chapter 7** deals with the procedures to be followed by certifying authorities to issues electronics signatures certificates and procedures to suspend and revoke the signature certificates.
- **Chapter 8** mentions the duties of subscribers to digital signatures certificates while using them.
- **Chapter 9** deals with penalties, compensation, and adjudication process for damages to computer systems. This chapter deals with the civil liabilities on the remedies existing there to.
- **Chapter 10** deals with the establishment of Cyber Appellate Tribunals, it's composition, appointment, duties and various aspects related to functioning of its office.
- **Chapter 11** of this act deals with the cyber-crimes in detail. We're going to discuss this in very much detail in coming time.
- **Chapter 12** provides for some exemptions, the intermediaries would be having, in terms of their liabilities. These intermediaries are those who provide services such as telecom services,

Internet services, hosting of websites, search engines, online payment or market or auction sites, cybercafes, etc.

- **Chapter 12A** was inserted during the amendment in 2008 where in the section 79A was inserted which provide for notifying examiner of electronic evidence who provides expert opinion on electronic form of evidence before any court or authority.
- **Chapter 13** is a miscellaneous chapter which provides for power of investigation officer for protection.

2. Scope and Jurisdiction

As per sections 1, 2 of the IT Act, the act shall extend to whole of India, including Jammu and Kashmir for both the offences and contraventions under this act. And section 75 provides for the extra territorial jurisdiction of the act. Any offence or contravention committed outside India by any person of any nationality is covered under this act provided, it involves a computer or a computer system or a computer network that is located in India.

With regard to subject matters, section 1, 4 states that documents and transactions present in the 1st schedule of the act does not come under this act. The act shall not apply to the documents provided in 1st schedule as shown below:

- The negotiable instrument,
- The power of attorney,
- A trust,
- A will, and
- Any contract for the sale of convenience of immovable property or any interest in any such property under various Acts.

The government also retained the option of adding any other class of documents or transactions to this list through a gazette notification.

With respect to the civil contraventions under this act, there is an exclusive jurisdiction up to 5 crores for the office of adjudicating officer to try the cases in which the claim amount or the damage amount is less than 5 crores. In every state, the IT secretary is appointed as the adjudicating officer for looking into these cases as of.

As per section 61 of the act, the matters that are allocated or kept in the jurisdiction of adjudicating officer and **Cyber Appellate Tribunal** are exclusively kept in their purview and no court shall have any kind of jurisdiction for accepting any suit or performing any proceedings are giving an injunction against such acts. As we have discussed, the adjudicating officer can look into the issues for damage up to 5cores and beyond 5 cores, it is the civil court that has jurisdiction for trying the cases. If the claim is more than 5 cores, then the concern jurisdictional civil court has the power to take the matter and try the case and appeal to the judgments of the civil court lies to the district court and then to the concern high court.

3. Definitions in IT Act 2000

The Act clearly defines the following terms:

a. Access
b. Addressee
c. Adjudicating officer
d. Affixing digital signature
m. Cyber Appellate Tribunal
n. Data
o. Digital signature
p. Digital signature certificate

e. Asymmetric crypto system
f. Certifying authority
g. Computer
h. Computer network
i. Computer system
j. Computer resource
k. Communication device
l. Controller
q. Electronic form
r. Electronic record
s. Information
t. Intermediary
u. Key pair
v. Private key
w. Public key
x. Secure system

4. Offences and Penalties[14]

Section	Offence	Nature of Offence	Penalty	
			Fine Up to	Imprisonment Up to
43	Penalty and compensation for damage to computer, computer system, etc.	Compoundable		
	a) Unauthorised Access b) Unauthorised Downloading, Copying or Extraction c) Computer Virus, Worm or Contaminant d) Damaging a Computer e) Disruption of Computer f) Denial of Services g) Facilitating Unauthorised Access h) Tampering or Manipulating a System i) Destruction, Deletion or Alteration j) Source Code Theft			
43 (A)	Compensation for failure to protect data (by a Corporate body)		5 Crores	
65	Tampering with Computer Source Documents	Cognizable & Bailable	2 Lakhs	3 Years
66	Computer Related Offences	Cognizable & Bailable	5 Lakhs	3 Years
66 (A)	Sending Offensive Messages	Discontinued by Hon'ble Supreme Court in the case of Shreya Singhal vs Union of India on March 24, 2015		
66 (B)	Dishonestly Receiving Stolen System	Cognizable & Bailable	1 Lakh	3 Years
66 (C)	Identity Theft	Cognizable & Bailable	1 Lakh	3 Years
66 (D)	Cheating By Personation	Cognizable & Bailable	1 Lakh	3 Years
66 (E)	Violation of Privacy	Cognizable & Bailable	2 Lakh	3 Years

66 (F)	Cyber Terrorism	Cognizable & Non-Bailable		Life Imprisonment
67	Transmitting Obscene Electronic Material	Cognizable Bailable in case of First Conviction then Non-Bailable	First Conviction 5 Lakh then 10 Lakh	First Conviction 3 Years then 5 Years
67 (A)	Electronic Material with Sexually Explicit act	Cognizable & Non-Bailable	10 Lakh	First Conviction 5 Years then 7 Years
67 (B)	Child Pornography	Cognizable & Non-Bailable	10 Lakh	First Conviction 5 Years then 7 Years
67 (C)	Failure in Preserving Or Retention of Information by Intermediaries	Cognizable & Bailable		3 Years
68 (2)	Deliberate Failure to comply with the order/direction of controller	Non-cognizable & Bailable	1 Lakh	2 Years
69 (4)	Punishment for Failure by intermediary to assist in providing secure access/decrypting information stored to govt. notified agency	Cognizable & Non-Bailable		7 Years
69 (A)	Punishment for failure by the intermediary to comply with the order of the notified agency to block public access to information	Cognizable & Non-Bailable		7 Years
69 (B)	Deliberate failure by the intermediary to provide the notified agency with the technical assistance or online access to the computer resource	Non-cognizable & Bailable		3 Years
70	Unauthorized access to protected system directly or indirectly affects the facility of Critical Information Infrastructure	Cognizable & Non-Bailable		10 Years
71	Punishment for misrepresentation of information to CCA to obtain any e-signature	Non-cognizable & Bailable	1 Lakh	2 Years
72	Punishment for Breach of Confidentiality and Privacy	Non-cognizable & Bailable	1 Lakh	2 Years
72 (A)	Punishment for Disclosure of information in breach of lawful contract	Cognizable & Bailable	5 Lakhs	3 Years
73 (2)	Punishment for publishing false E-Signature Certificate	Non-cognizable & Bailable	1 Lakh	2 Years

Under IT Act section 79, Intermediaries are exempted from there liabilities in certain cases which are as follows -

Section 79	**Exemption from liability of intermediaries in certain cases**
(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third-party information, data, or communication link hosted by him. (corrected vide ITAA 2008)	

The provisions of sub-section (1) shall apply if-
(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or
(b) the intermediary does not-
(i) initiate the transmission,
(ii) select the receiver of the transmission, and
(iii) select or modify the information contained in the transmission
(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf (Inserted Vide ITAA 2008)
(3) The provisions of sub-section (1) shall not apply if-
(a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act (ITAA 2008)
(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner

5. Sections to Power of Police Officials to Act Upon Cyber-Crime & Other Provisions

Section	Description
69 (A)	Power to issue directions for blocking for public access of any information through any computer resource
69 (B)	Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security
70	Protected Systems (Amended Vide ITAA-2008)
70 (B)	Indian Computer Emergency Response Team to serve as national agency for incident response
78	Power to investigate offences
79	Central Government to notify Examiner of Electronic Evidence
80	Power of Police Officer and Other Officers to Enter, Search, etc

6. Intermediary Guidelines rules 2021

The Ministry of Electronics and IT has prepared the Information Technology [Intermediaries Guidelines Rules 2021 in order

(1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person.

(2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that
(a) belongs to another person and to which the user does not have any right to;
(b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically

objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever; (c) harm minors in any way; (d) infringes any patent, trademark, copyright or other proprietary rights; (e) violates any law for the time being in force; (f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature; (g) impersonate another person; (h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource; (i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation
(3) The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2): provided that the following actions by an intermediary shall not amount to hosing, publishing, editing or storing of any such information as specified in sub-rule: (2) (a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource; (b) removal of access to any information, data or communication link by an intermediary after such information, data or communication link comes to the actual knowledge of a person authorised by the intermediary pursuant to any order or direction as per the provisions of the Act;
(4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty-six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes,
(5) The Intermediary shall inform its users that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the Intermediary has the right to immediately terminate the access or usage lights of the users to the computer resource of Intermediary and remove noncompliant information.
(6) The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.

(7) When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing staling clearly the purpose of seeking such information or any such assistance.
(8) The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable security practices and procedures and sensitive personal Information) Rules, 2021.
(9) The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.
(10) The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to "perform thereby circumventing any law for the time being in force: provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.
(11) The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule 3 can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint.

7. Presentation & Admissibility of electronic Evidence in Court of Law

Digital evidence or electronic form of evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence, it is vital that the determination of its relevance, veracity and authenticity be ascertained by the court and to establish if the fact is hearsay or a copy is preferred to the original.

The electronic form of evidence can be found in e-mails, digital photographs, ATM transaction logs, word processing, documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories databases, Contents of computer memory, Computer backups, Computer printouts, Global Positioning System tracks, Logs from a hotel's electronic door locks, Digital video or audio files. Digital Evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive and more readily available.

After the promulgation of IT Act, the definition of 'evidence' in **Indian Evidence Act** has been amended to include electronic records. The definition of 'documentary evidence' has been amended to include all documents, including electronic records produced for inspection by the court. Section 3 of the Evidence Act, 1872 defines evidence as under: "Evidence" - 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; such statements are called oral evidence; 2) all documents including electronic records produced for the inspection of the court. Such documents are called documentary evidence.

The term 'electronic records' has been given the same meaning as that assigned to it under the IT Act. IT Act provides for "data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated microfiche". The definition of 'admission' (Section 17 of the Evidence Act) has been changed to include a statement in oral, documentary or electronic form which suggests an inference to any fact at issue or of relevance. New Section 22-A has been inserted into Evidence Act, to provide for the relevancy of oral evidence regarding the contents of electronic records. It provides that oral admissions regarding the contents of electronic records are not relevant unless the genuineness of the electronic records produced is in question.

New sections 65-A and 65-B are introduced to the Evidence Act, under the Second Schedule to the IT Act. Section 65-A provides that the contents of electronic records may be proved in accordance with the provisions of Section 65-B. Section 65-B provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic, is deemed to be a document and is admissible in evidence without further proof of the original's production, provided that the conditions set out in Section 65-B are satisfied. The conditions specified in Section 65-B (2) are:

1. Firstly, the computer output containing the information should have been produced by the computer during the period over which the computer was used regularly to store or process information for the purpose of any activities regularly carried on over that period by the person having lawful control over the use of the computer.
2. The second requirement is that it must be shown that during the said period the information of the kind contained in electronic record or of the kind from which the information contained is derived was 'regularly fed into the computer in the ordinary course of the said activity'.
3. A third requirement is that during the material part of the said period, the computer was operating properly and that even if it was not operating properly for some time that break did not affect either the record or the accuracy of its contents.
4. The fourth requirement is that the information contained in the record should be a reproduction or derived from the information fed into the computer in the ordinary course of the said activity.

Under Section 65-B (4) the certificate which identifies the electronic record containing the statement and describes the manner in which it was produced giving the particulars of the device involved in the production of that record and deals with the conditions mentioned in Section 65-B (2) and is signed by a person occupying a responsible official position in relation to the operation of the relevant device 'shall be evidence of any matter stated in the certificate'.

8. Electronic evidence -case laws

- **Amitabh Bagchi Vs. Ena Bagchi (AIR 2005 Cal 11)** [Sections 65-A and 65-B of Evidence Act, 1872 were analyzed.] The court held that the physical presence of person in Court may not be required for purpose of adducing evidence and the same can be done through medium like video conferencing. Sections 65-A and 65-B provide provisions for evidences relating to electronic records and admissibility of electronic records, and that definition of electronic records includes video conferencing.

- **State of Maharashtra vs. Dr Praful B Desai (AIR 2003 SC 2053)** [The question involved whether a witness can be examined by means of a video conference.] The Supreme Court observed that video conferencing is an advancement of science and technology which permits seeing, hearing and talking with someone who is not physically present with the same facility and ease as if they were physically present. The legal requirement for the presence of the witness does not mean actual physical presence. The court allowed the examination of a witness through video conferencing and concluded that there is no reason why the examination of a witness by video conferencing should not be an essential part of electronic evidence.
- **BODALA MURALI KRISHNA VS. SMT. BODALA PRATHIMA (2007 (2) ALD 72)** The court held that, "…the amendments carried to the Evidence Act by introduction of Sections 65-A and 65-B are in relation to the electronic record. Sections 67-A and 73-A were introduced as regards proof and verification of digital signatures. As regards presumption to be drawn about such records, Sections 85-A, 85-B, 85-C, 88-A and 90-A were added. These provisions are referred only to demonstrate that the emphasis, at present, is to recognize the electronic records and digital signatures, as admissible pieces of evidence."
- **DHARAMBIR Vs. CENTRAL BUREAU OF INVESTIGATION (148 (2008) DLT 289).** The court arrived at the conclusion that when Section 65-B talks of an electronic record produced by a computer referred to as the computer output) it would also include a hard disc in which information was stored or was earlier stored or continues to be stored. It distinguished as there being two levels of an electronic record. One is the hard disc which once used itself becomes an electronic record in relation to the information regarding the changes the hard disc has been subject to and which information is retrievable from the hard disc by using a software program. The other level of electronic record is the active accessible information recorded in the hard disc in the form of a text file, or sound file or a video file etc. Such information that is accessible can be converted or copied as such to another magnetic or electronic device like a CD, pen drive etc. Even a blank hard disc which contains no information but was once used for recording information can also be copied by producing a cloned had or a mirror image.
- **STATE (NCT OF DELHI) Vs. NAVJOT SANDHU (AIR 2005 SC 3820)** There was an appeal against conviction following the attack on Parliament on December 13 2001. This case dealt with the proof and admissibility of mobile telephone call records. While considering the appeal against the accused for attacking Parliament, a submission was made on behalf of the accused that no reliance could be placed on the mobile telephone call records, because the prosecution had failed to produce the relevant certificate under Section 65-B (4) of the Evidence Act. The Supreme Court concluded that a cross-examination of the competent witness acquainted with the functioning of the computer during the relevant time and the manner in which the printouts of the call records were taken was sufficient to prove the call records.
- **JAGJIT SINGH Vs. STATE OF HARYANA ((2006) 11 SCC 1)** The speaker of the Legislative Assembly of the State of Haryana disqualified a member for defection. When hearing the matter, the Supreme Court considered the digital evidence in the form of interview transcripts from the Zee News television channel, the Aaj Tak television channel and the Haryana News of Punjab Today television channel. The court determined that the electronic evidence placed on record was admissible and upheld the reliance placed by the speaker on the recorded interview when reaching the conclusion that the voices recorded on the CD were those of the persons taking action. The Supreme Court found no infirmity in the speaker's reliance on the digital evidence and the conclusions reached by him. The comments in this case indicate a

trend emerging in Indian courts: judges are beginning to recognize and appreciate the importance of digital evidence in legal proceedings.

- **ANVAR P.V. VERSUS, P.K. BASHEER AND OTHERS,** in CIVIL APPEAL NO. 4226 OF 2012 decided on Sept., 18, 2014, That Computer Output is not admissible without Compliance of 65B, EA overrules the judgment laid down in the State (NCT of Delhi) v. Navjot Sandhu alias Afzal Guru [(2005) 11 SCC 600 by the two judge Bench of the Supreme Court. The court specifically observed that the Judgment of Navjot Sandhu supra, to the extent, the statement of the law on admissibility of electronic evidence pertaining to electronic record of this court, does not lay down correct position and is required to be overruled. This judgment has put to rest the controversies arising from the various conflicting judgments and thereby provided a guideline regarding the practices being followed in the various High Courts and the Trial Court as to the admissibility of the Electronic Evidences. The legal interpretation by the court of the following Sections 22A, 45A, 59, 65A & 65B of the Evidence Act has confirmed that the stored data in CD/DVD/Pen Drive is not admissible without a certificate u/s 65 B(4) of Evidence Act and further clarified that in absence of such a certificate, the oral evidence to prove existence of such electronic evidence and the expert view under section 45A Evidence Act cannot be availed to prove authenticity thereof.

In the Judgment, the Hon'ble Supreme Court has held that Section 65B of the Evidence Act being a 'not obstante clause' would override the general law on secondary evidence under Section 63 and 65 of the Evidence Act. The section 63 and section 65 of the Evidence Act have no application to the secondary evidence of the electronic evidence and same shall be wholly governed by the Section 65A and 65B of the Evidence Act.

The only alternative to prove the electronic record/evidence is by producing the original electronic media as Primary Evidence to the court or it's copy by way secondary evidence u/s 65A/65B of Evidence Act. Thus, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible. In the present case, the court observed that:

"The appellant admittedly has not produced any certificate in terms of Section 65B in respect of the CDs, Exhibits-P4, P8, P9, P10, P12, P13, P15, P20 and P22. Therefore, the same cannot be admitted in evidence. Thus, the whole case set up regarding the corrupt practice using songs, announcements and speeches fall to the ground."

This judgment will have severe implications in all the cases where the prosecution relies heavily on the electronic data specially those cases where the audio-video recordings are produced in the form of CD/DVD before the court. The anticorruption cases are generally based on a lot of electronic / digital evidence and the CD/DVD forwarded to the courts are without a certificate and shall therefore not be admissible as evidence u/s 65B Evidence Act, which makes it mandatory to produce a certificate u/s 65 B(4). The failure to provide the certificate u/s 65 B (4). further occludes the judicial process as the expert view in that matter cannot be availed of till the preceding condition is fulfilled. It has been specified in the judgment that Genuineness, Veracity or Reliability of the evidence is looked into by the court subsequently only after the relevance and admissibility is fulfilled. The requirement to ensure the source and authenticity, pertaining to electronic records is because it is more vulnerable to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to mockery of justice.

The original recording in Digital Voice Recorders/mobile phones need to be preserved as they may get destroyed, in such a case the issuance of certificate under section 65B (4) of the Evidence Act cannot be given. Therefore, such CD/DVD is inadmissible and cannot be exhibited as evidence, the oral testimony or expert opinion is also barred and the recording/data in the CD/DVD's do not serve any purpose for the conviction.

Digital Crime Scene Management

1. SOP for Handling Scene of Crime

Standard Operating Procedure covers process to be followed for the onsite retrieval, securing, transport and handling of digital evidence, as well as its analysis and presentation.

Further it contains procedure for the live acquisition of data onsite, while the identified computer systems are turned on/running, as accessing them later on might be prevented by passwords or encryption. Finally, it covers procedure for the copying of data from a computer system or data storage media (like hard drive and pendrives) in cases where backup copies are required or where the physical collection of a computer system is not possible.

A forensic analysis of a computer system or storage device requires not only the approval of a respective authority but also the need observation by technical experts and well-defined steps to ensure the integrity of the collected evidences to ensure their admissibility in the Court of Law.

Following are the Steps to be followed at the scene of crime:

- Securing the Scene of Crime
- Videography and photography of Scene of Crime
- Interrogating Suspects / Witnesses
- Identification and seizure of digital evidences
- Imaging
- Hashing
- Packing, Labeling, Transporting and Storage of Digital Evidences
- Documenting Seizure Memo
- Maintaining of Chain of Custody

i. Securing the Scene of Crime

The most significant part of evidence collection and safeguarding is protecting the crime scene. This is to keep the appropriate proof uncontaminated until it is very well recorded and gathered. The fruitful arraignment of a case can depends on the condition of the physical proof at the time it is gathered. The assurance of the scene starts with the appearance of the primary cop at the scene and finishes when the scene is discharged from police guardianship.

- At crime scene, every bit of evidence counts so limit contact with the scene to avoid contamination.
- Do not allow anyone to go near the area except authorized officials.
- Upon arriving, if there was a surveillance camera, make sure to disconnect it before doing anything; you can also cover it if you cannot stop it instantly.
- Limit access and movement on the crime scene.
- Secure the scene by moving bystanders to a designated area. After securing the crime scene and preventing unauthorized access,
- The IO must follow general principles for the correct acquisition of digital devices holding the digital evidence.

ii. Videography and Photograph of the Scene of Crime

IO should videograph/ photograph whole crime scene and should also draw the network architecture sketches in ‘as is where is’ condition of the crime scene.

It is important to take a Close shot of the MONITOR, in such a way that the System Date and Time has to be visible and the Running Processes on the screen has to be visible. Take a Long shot and close shot of the Scene of Crime from various angles.

Take a photograph of front panel and back panel of the system so that it can be easily identified the connectivity of the devices like Keyboard, Mouse, Monitor, Network Cable and any external devices connected to the system

iii. Interrogating the Suspect / Witnesses

After identifying the scene of crime, IO should secure it and take note of every individual physically present at the scene of crime and their role at the time of securing the scene of crime.

- Isolate the person immediately who is working on the computer if any, and interrogate him/her without allowing him/her touching the Computer.
- People who were at the crime scene should be questioned about the following:
  a) What they saw, and furthermore where and how
  b) The names of all people present at the crime scene, also their phone numbers, e-mail addresses, and roles/jobs in the target organization
  c) Their work account usernames and passwords
  d) Social profiles and IM chat screen names for all employee of interest
  e) Identity of any administrator/site manager who can identify devices and custodians at the crime scene
  f) The number, types, and models of devices involved in incident
  g) The type of digital data (e.g., e-mail, databases, images, documents, etc.) expected to be involved in the incident
  h) The type of operating system involved in the incident
  i) Whether any of the digital data owned by target organization is stored outside its premises (e.g., cloud storage, remote locations etc.)
  j) Identity of any contractors who have remote access ability to target the organization's network
  k) Whether data access restriction is in place
  l) Any suspicious about who may have conducted the attack (e.g., a disgruntled ex-employee).

After returning to the lab and analyzing the primary information collected, more questions can be prepared to ask the possible suspects/witnesses. Gather information as provided in the questionnaire(s) above, on all the security systems including encryption policies, off site data storage, data center and disaster recovery policies of the organization or back up plans etc.

Recognize the complainant/owner(s) of the various devices and get the access details, usernames and service provider's details. IO ought to guarantee that these people are accessible alongside the search and seizure group for getting access to different password protected / secured data.

iv. Identifying and Seizure of Evidences

In this phase, the physical evidence (digital device) will be seized and transferred safely to the forensic lab. This evidence can be any computing device type such as laptop, tablet, mobile phone, external hard drive, USB flash drive, wearable device (e.g., digital watch), or even a desktop PC. Remember, you need to have a permission from the proper authority (e.g., court warrant) to seize the suspect's machine. Upon arriving to the crime scene, the suspect digital device should be examined by a well-trained technician to ensure the digital evidence is acquired/ preserved in a forensically sound manner.

➢ What is Digital Evidence?

According to Section 79A of Information Technology (Amendment) Act, 2008 a digital or electronic evidence is "any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones or digital fax machines."

In following sections, we will see how different digital devices are seized at scene of crime.

➢ **Desktop Computer**

Procedure to seize Computer when found in Power ON condition

Step 1	Isolating the accused working on the computer if any and his/her Interrogation without allowing him/her to touch the computer.
Step 2	Visible inspection of Scene of Crime in front of technically qualified independent witnesses without touching anything.
Step 3	Photography of the Scene of Crime (SoC) • Close shot of the MONITOR. • Long shot and close shot of the SoC from various angles showing all the devices connected with the computer. • Long and close shot of the system from different angles identifying all externally connected devices to the system
Step 4	Collection of fingers print if required.
Step 5	Search for any kind of external memory devices like Pen Drive, Hard Disk, etc.
Step 6	Collection of RAM dump and system information, encrypted files if any by the IO/ Cyber Forensic Expert.
Step 7	Pull the power cable from electricity switchboard and then remove the power cable from SMPS (Switch Mode Power Supply) from the back of CPU Cabinet.
Step 8	Make sure that the computer system is completely turned off and then detach the devices connected externally like Keyboard, Mouse, Monitor, Printer / scanner etc. (if connected) from the back of CPU Cabinet.
Step 9	Remove the CPU Cabinet Cover by removing the screws on the back of the case and by sliding the cover back and by lifting it off. Use the screw-driver as per the type of screw is required to do the task.
Step 10	Take a photograph of the inside view showing all peripherals connectivity on Motherboard like Hard Disk, RAM, NIC, BIOS etc.
Step 11	Take a photograph of the Hard Disk showing: • Unique Sr.No. of the Hard Disk • Connector Ports • Jumper Position • Logic Board ..etc.
Step 12	Calculate the Hash Value of the Seized Hard Disk and Other devices collected (If Possible)
Step 13	Take an Image of Seized Media (Hard Disk / Pendrive/ SD Card ...etc) via Write Blocker and create at least 2 image copies (duplicate) using Forensic Imaging Tool. Note: The Original evidence has to be sent to the Forensic Lab along with seizure list and questionnaire with permission of the court as per regular procedure, first image

	has to be kept with IO for analysis, second image to be handed over to the accused party if requested.
Step 14	Preparation of seizure list mentioning all details like Unique S.No. of External Drives, Hard Disk and Hash value of the Hard Disk and other external memory devices.
Step 15	Dispatch the Seized Media as mentioned in step 13.

Procedure to seize Computer when found in Power OFF Condition

Step 1	Follow the Steps from 2 to 5 as mentioned in previous section "System Power on Condition"
Step 2	Remove the power cable from electricity switchboard and then remove the power cable from SMPS (Switch Mode Power Supply) from the back of CPU Cabinet.
Step 3	Detach the devices connected externally like Keyboard, Mouse, Monitor, Printer / scanner etc. (if connected) from the back of CPU Cabinet.
Step 4	Follow the Steps from 9 to 15 as mentioned in previous section "System Power on Condition".

- **Laptop**

Procedure to seize Laptop when found in OFF condition:

Step 1	Take a Photograph of entire crime scene with short shot and long shot in such a way that all the cables (Network Cable / Power Cable/ Modem Cable) and devices connected to it, and all the documents or files placed around the laptop and if any external storage devices like CD/DVD / Pendrive / SD Card/ Hard drive / Floppy Drive are available should be visible.
Step 2	Uniquely label all the cables and devices connected to the laptop as well as the connection they occupied.
Step 3	Remove the power supply and battery from the laptop.
Step 4	Remove the back cover of Laptop and take a photograph of internal cable and device connectivity of the motherboard.
Step 5	Remove the Hard Disk from the Laptop, and take a photograph of Hard Disk where Hard Disk Serial Number, Make, Model, Capacity and any user-applied markings or identifiers should be visible.
Step 6	Fill the Search and Seizure memo and Document all the activities done and the details of the cables and devices collected at the Scene of Crime.
Step 7	Secure all the cables, batteries, devices in an Anti-Static Package.
Step 8	Use bubble wrap after Anti-Static Packaging in order to avoid physical damage.

Step 9	Finally, pack the entire collected evidence in an envelope or Carton Box and label the details.
Step 10	Transport the evidence securely to Forensic Science Laboratory for Analysis.

Note: At the scene of crime, look out carefully for pieces of paper with possible passwords, handwritten notes, any printed material like hardware or software manuals, text or graphic material that may reveal information relevant to the investigation. These forms of evidence also should be documented and preserved in compliance with departmental policies.

If the IO is carrying Forensic Investigation Laptop along with all the tools pre-installed in it, he / she has to connect the Hard Disk of a Laptop and other storage devices to Forensic Investigation Laptop via Write Blocker to take a Hash Value and to take image of the evidence collected. Note down the collected Hash Values in Seizure and in the documentation prepared by IO.

Procedure to seize Laptop when found in ON Condition:

Step 1	If the Laptop is in Power ON condition and if it is not locked, then we have to follow the same procedure which we have followed in seizing of a Desktop computer.
Step 2	Follow the Steps from 1 to 6 as mentioned in Desktop in On Condition and then pull the power plug from Laptop and as well as from the switch board and then remove the battery from backside of laptop. [The hibernation file present in the laptop will preserve the current state of a system by recording memory and open files before shutting off the system.]
Step 3	Follow the steps from 4 to 10 as mentioned in seizing of a Laptop when it is in OFF condition.

Note: Remove the battery from backside of laptop or other portable device to preserve swap files, temporary data files, and other information that might be altered or deleted during a graceful shutdown. Unfortunately, a sudden loss of power can cause some Operating Systems to corrupt data, such as open files.

Laptop Hard drives may require special interface adapters to connect to forensic workstation. Some laptop hard drive/motherboard combinations may have security devices that do not allow them to be accessed outside of the laptop computer. Image these computers using a cable acquisition procedure or by booting the laptop using a forensic operating system environment.

- **Network Devices**
  - **Overview of Network Forensics**

Network Forensics is a process of collecting and analyzing raw network data and tracking network traffic systematically to ascertain how an attack was carried out or how an event occurred on a network. Because network attacks are on the rise, the focus is more on this field and there is an increasing demand for skilled technicians.

When intruders break into a network, they leave a trail behind. Being able to spot variations in network traffic can help in tracking intrusions. So, knowing network's typical traffic patterns is important. For example, the primary ISP of SVP National Police Academy has peak hours of use between 9:30 AM to 6:30 PM, as it is the standard working hours at SVP National Police Academy. If a usage spike occurred during the night, the network administrator on duty would recognize it as an unusual activity and could take steps to investigate it.

The use of in-built Firewall logs, System logs, and other logs will generally point to an Entry Time, Place, and IP address that can be used to determine how the event was propagated through the network and what steps can be taken to minimize any future event, by providing solid data on the event. A large

part of network forensics is being able to monitor the network traffic in order to isolate the number of servers that need to be taken down for the traditional forensics process.

- **The Importance of DHCP Logs**

If the network for which you are performing network forensics if uses Dynamic Host Configuration Protocol (DHCP), then it is vitally important that the organization records and preserves the DHCP logs for the period of time being examined. Without the DHCP logs, an IT-savvy attorney can challenge the link between the Internet Protocol (IP) address and the computer and, ultimately, to the user of that computer. If DHCP logs are not available, you will need to find other ways to establish the link between a computer and an IP address. If you have access to the suspect's computer or the computer of interest, you may find logged records of the IP address in the security event log and the firewall log. Although it is still part of the network, you might be able to query the DHCP server or perform ipconfig/ all on the suspect's computer.

The DHCP log entry also provides you a way to physically locate the computer within the network. These logs describe which device issued the IP address to a computer with a specific Mac address. The switch logs can divulge which switch port was used. The switch port connects by cable to your cable infrastructure. Following this cable leads to a specific data jack in a specific building and room. If network or facilities team has maintained a good database of these associations, then we can find the physical location of the suspected computer. Otherwise, you have to physically locate the suspected computer by going room to room and checking the identifiers on each data jack. If the jacks aren't labeled, pull on wires and follow the cable, which may or may not be possible with walls and floors in place.

- **Hub**

A hub, also called a network hub, is a common connection point for devices in a network.
Hubs are devices commonly used to connect segments of a LAN. The hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets. (Reference http://www.webopedia.com/TERM/H/hub.html)
Note: Hubs do not contain any logs. IO should take photographs of the device along with indicating model number of the device and also note all MAC addresses of the physical ports of the device.

- **Switches**

Switch is a device that filters and forward packets between LAN segments. Event logs generated by the device will be available.

- **Routers**

A router is a hardware device, and is designed to receive, and forward incoming packages to another network. It is normally used in large organizations.

- **Wireless Routers**

Wireless Routers are used to provide network for mobile, laptop etc. It creates a network of WiFi devices and provide them internet or intranetworking facility.

- **Modem**

Modem is a device used to convert telephone signals into digital signals. Generally used for houses to provide internet connection.
Note: All these devices have at least one MAC address for basic inter communication. Devices such as routers and switches having more than one MAC address.

- **NIC Card**

A network interface controller (NIC, also known as a network interface card, network adapter, LAN adapter or physical network interface and by similar terms) is a computer hardware component that connects a computer to a computer network.

- **Packet Capturing Devices**

These types of devices can be placed anywhere in the network, if these types of devices are placed inside the network, then IO can ask network administrator to provide PCAP(Packet Capture) files. After taking these files HASH values also must be generated.

Device	Network logs	MAC Addresses	Volatile Information
Hub	No	Yes	Yes
Switch	Yes	Yes	Yes
Router	Yes	Yes	Yes
Wireless Router	No	Yes	Yes
Modem	No	Yes	Yes

Procedure to Seize Network Devices:

Step 1	Identify the network device (Hub, Switch, Router Bridge etc), it can be checked using internet search of model number of the device.
Step 2	Take Photographs of – Device indicating brand and model number. – Connected cables with serial number.
Step 3	– If the device found in Switched off state: Collect MAC addresses of all ports, and seize the device with proper chain of custody. – If the device found in switched ON state: Intimate Network Administrator to collect volatile information from these devices like ARP cache table, MAC addresses etc.
Step 3	If any volatile information is collected from net admin collect HASH value of the given file.

Note: Do not try to operate the device without proper knowledge.

Crime Scene Scenarios of (MODEM/WiFi Routers):

Generally, Modems are used for home environment or small organizations.

Step1	Take Photographs of MODEM indicating its manufacturer and model along with serial numbers
Step 2	IF the MODEM is ON, then browse into the MODEM through any of the computer devices which are connected to the MODEM. The password for the same should be available with the Network Administrator. Note down various details which are available in the MODEM. Such as, – MAC addresses connected with the MODEM

	– Logs of websites – The static IP assigned to the router
Step 3	IF the MODEM is switched off, then seize the Modem with proper chain of custody

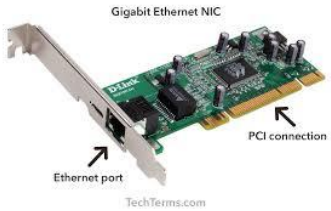
- **Order of Volatility**

It is the responsibility of IO to decide the order in which the digital evidence will be gathered. They should start with the most volatile and go to the least volatile evidence. The following order is suggested by many digital forensic processes, beginning with the most volatile:

1. CPU, registers, and system cache.
2. Routing table, ARP cache, process table, and kernel statistics.
3. RAM memory.
4. Temporary file systems.
5. Swap space or virtual memory (named "pagefile" in Windows OS). This is a file on the hard drive that extends the amount of RAM available to a computer.
6. Hard drive and/or other removable media storage.
7. Remote logging and monitoring data.
8. Physical configuration, network topology.
9. Backup data and printouts.

a. List of digital evidence, that can be present at scene of crime:

Sr. No	Device		Evidence Contingency
1	A Desktop Computer Cabinet (CPU)		Device contains components which stores all the files and folders including deleted files.
2	Display Monitor(CRT/LCD/TFT etc), Screens of Mobile Phones		All the graphics and files displayed on open screen
3	Smart Cards, Dongles and Biometric Scanners etc		Identification and authentication information of the card and user.

4	Answering Machines		Stored call logs and messages along with details such as deleted messages, caller identification information, last number called, memos
5	Digital Cameras		Images, Videos, Removable Cartridges & Time Stamps
6	Smart Phones, Personal Digital Assistants		Address books, Appointment calendars, e-mails, Phone book etc.
7	Hard Drives		All stored files
8	LAN Cards / NIC Cards		MAC address
9	Modems, Routers, Hubs, Switches		Information related to IP address
10	Servers		Last Logins, Pages accessed, mails exchanged, content downloaded etc.

11	Network Cables and Connectors		Network cables are used to trace back to their respective computers. Connectors help in identifying the type of devices that are connected to the computer.
12	Pagers		Address information, phone book, Text messages
13	Printers		Number of prints last printed, usage logs, Time & date information. Can be examined for fingerprints.
14	Removable Storage Media and Devices		All stored files.
15	Telephones		Stored names and Messages(Voice / Text), memos, passwords, phone numbers, recorded calls.
16	Copiers		May store documents (electronic / physical), usage logs, time and date stamp

17	CD and DVD Drives		Stored files
18	Credit Card Skimmers		Track of magnetic stripe contain Cardholder's information: Expiry Date User's address Credit card number User name
19	Digital Watches		Phone numbers, Address book, appointment calendar, e-mails etc
20	Facsimile Machines		Send / receive logs, film cartridge, some documents
21	Global Positioning Systems (GPS)		Travel logs, Home location, Previous destinations, way point coordinates, way point name etc.
22	Keyboard and Mouse		Fingerprints

TABLE 1 DIGITAL EVIDENCES

v. Imaging – Forensic Copy of Digital Storage Media

Unlike normal case scenarios the digital evidence can be easily contaminated. Which means the evidence may get changed intentionally or unintentionally very easily and the decontamination is impossible. So, the Investigating officer should take proper precautionary measures in order to preserve

the integrity of the evidence. One of the main principles of Cyber Forensics is “Never Work on Originals”. So, the best practice followed in Cyber Forensics is to make “Forensic Copy” of the storage media obtained from scene of crime.

vi. Packing, Labelling, Transporting and Storage of Digital Evidences

After documenting and labeling all devices and cables, you are ready to package and transfer them to lab.Start the packing procedure by putting a tape over the power switch, so the device won't power on unintentionally while in travel, and afterward put the digital device in antistatic bag. At last, put the collected device(s) in an appropriate evidence bag, seal it using tape, and record your name and date/time on it.

While shipping the electronic evidence, make a point to put them safely in the back seat of the vehicle and secure them to avoid exposure to physical shock and vibration. The atmosphere in the transportation vehicle ought to be dry, cool, and away from magnetic sources (e.g., speaker magnets, radio transmitters) and dust. Try not to expose evidence bag to high temperature or moisture since it may damage digital evidence inside it.

vii. Documenting Seizure Memo

Seizure memo is one of the most significant components of the forensic procedure. It is fundamental that the means taken for collection of evidence ought to be exact and repeatable with similar outcomes each time it is performed. For this to occur, an appropriate documentation of the procedure utilized for collection should be kept up for each gadget that is collected.

The seizure memo form must contain the following details about evidence:

1. Contents of the bag.
2. Names of investigators who:
    a. Seized the evidence.
    b. Photographed evidence and crime scene.
    c. Created the crime scene sketch diagram.
    d. Packaged the evidence in the bag.
3. Location where evidence was found and seized.
4. Suspect information and criminal record if applicable.
5. Date and time of seizure.
6. Passwords of seized devices (if available).
7. Any additional notes.

viii. Maintaining of Chain of Custody

Chain of custody refers to the documentation that shows the individuals who have been depended with the proof. These individuals would have held onto the equipment, individuals who are accountable for moving the proof from scene of crime to scientific lab, individuals responsible for examining proof, etc

When the proof is gathered and each time it is moved, it ought to be recorded and nobody else other than the individual depended with the display will approach the proof.

Important Points Regarding Chain of Custody:

1. Inspect the storage medium in person.

2. Use appropriate physical security and data encryption.
3. Store multiple copies at different locations.
4. Protect digital magnetic media from external electric and magnetic field.
5. Protect optical media from scratches.
6. Make record of all people with physical or electronic access to the data.
7. Always accompany evidence with their chain-of-custody forms.

2. Live Data Acquisition of the System

Live Forensics is a methodology for extracting forensically sound evidence from "live" system. According to traditional forensics procedure, power plug is pulled to switch off the system when the system is in the running mode. But in live forensics, before pulling the cord we collect information such as details in memory, running process, network connection etc. In Live Forensic volatile data that may be lost by a power down is collected from a running system. Live forensics considers the value of the data that may be lost by powering down a system and collects it while the system is still running. The other objective of live forensics is to minimize impacts to the integrity of data while collecting evidence from the suspect system.

i. The goal of live forensics

The goal of live forensics is to extract and preserve the volatile data on a system while, to the extent possible, otherwise preserving the state of the system. When powering down a computer system, the volatile information is lost which may contain lot of fruitful information of the case. So, Live Forensics has become an important part of digital forensic investigations. This information will not be available for further analysis, although it may contain valuable clues regarding the incident, and there is sometimes no other way to obtain it other than collecting it on the running system.

Case scenario: A fake Facebook ID is created in the name of a girl. Obscene images of the same girl have been uploaded in that fake account. Girl approached police station and complained about the same. The case has been registered and investigation started. Investigating officer has found the place from which images have been uploaded. A Team of investigation has reached the crime scene. The accused has been captured with two computers which are in ON and unlocked condition.

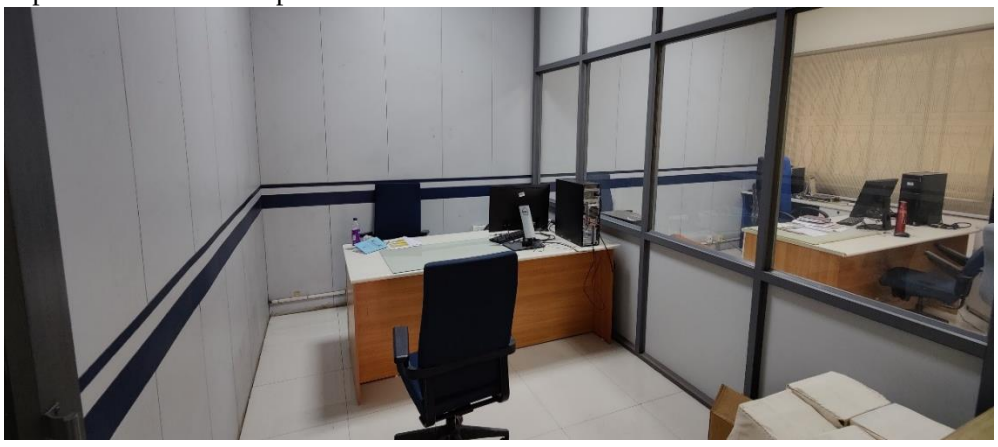


FIGURE 30: CRIME SCENE WITH TWO DESKTOP COMPUTERS (ON AND UNLOCK CONDITION)

ii. How should IO handle the computers found in the crime scene?

Whatever the data collected from running system is called live acquisition. Volatile data is temporary data which will be deleted if the computer is switched off. Volatile can be acquired during live acquisition only. Non-volatile data such as hard drive data may be collected even in OFF condition of

the system. In Live acquisition, the most significant issue is volatility. IOs should take care of the volatile data as first priority.

Based on the nature of volatility the following order of the contents should be collected,

1. Network Information such local routing tables, address resolution protocol cache, current state etc.,
2. RAM Dump including page file and swap file
3. Current running processes
4. Temporary files
5. Static data such as physical configuration of the system

Network information is changing so frequently. It is lifespan is 10 nanoseconds. The address resolution protocol (ARP) cache list of IP addresses mapped to their physical addresses such as MAC addresses. This can be seen by using "arp -a" command through command prompt of windows Operating system. Similarly, "route print" command gives the routing table present in the memory.

Practically, RAM dump gives the most of the data required for analysis. When acquiring RAM dump, page file and swap files also must be acquired. FTK imager is the tool which can be used acquire the RAM dump. Currently opened files, running processes and other information is available in RAM dump.

iii. Information to be focused during the analysis of memory contents:

- System time
- Logged-on user(s)
- Open files
- Network information
- Network connections
- Process information
- Process to port mapping
- Process memory
- Network Status
- Clipboard contents
- Service/ driver information
- Command history
- Mapped drives
- Shares

iv. Information found in RAM:

- Cryptographic keys
- Processes running
- Executed console commands
- Clipboard contents
- Network information
- Decrypted contents
- Registry hives
- Text files and images
- Deleted files
- Web browsing logs
- Open/active registry keys
- Internet account passwords (e.g., e-mail, social media, and cloud storage)

Windows registry gives the static information and configuration of the system. Registry is a local database created at the time of installation of the operating system. This database is in the form of hives. Registry can be acquired by using FTK imager. Regripper, F-Rat etc., are the tools available for registry analysis.

v. Pagefile.sys

Forensic examiners should not ignore the importance of virtual memory, as this file can hold important information shifted from RAM. For example, fragments of decrypted files can still reside there, and encryption keys or passwords (or a fragment of it) can also be found here. The pagefile.sys is a hidden system file, it resides by default at %SystemDrive%\pagefile.sys; however, a user can change its default location.

Nowadays capacity of the physical memory is increasing with the continual advance of computing power (for example, it is common these days to buy a laptop with 16 GB of RAM memory). This effectively limits the need to swap any files to the virtual memory, which results in low expectations of computer forensic investigators when investigating pagefile.sys.

vi. Swapfil.sys

Swap file is used to store the idle and other non-active objects transferred from the RAM, whenever a user tries to access an idle process again, its information will be shifted to the RAM. In modern Windows versions (like 8 and 10) we can see that both Pagefile and Swapfile exist together on a system drive; we can consider that these two files form together what is known now as virtual memory in Windows OS. Swapfile has a fixed size in modern Windows versions (8, 10), which is 256 MB.

Also, RAM dump contains various programs running such as loaded drivers, dynamic link libraries, handles, and callbacks. If any malware attacking system its foot prints will be found on RAM itself irrespective of its capabilities such as obfuscation, encrypted etc., The kernel space which consists most of the information of current running processes including malware will be fetched by using this memory forensics. Volatility is the better tool for analysing kernel space and other behaviours.

For every investigator, it is required to identify the information where it is located in the RAM. They should be able to identify the exact location various data such IP addresses are stored in user space. This can be done with various forensics tools.

The following is the standard operating procedure of volatile memory acquisition.

- ✓ Date and time of the system must be recorded at the first instance
- ✓ Date and time for every time when a forensic tool or command is used must be recorded.
- ✓ Document all the collected material and activities carried out.
- ✓ Don’t shutdown/restart a computer until all the required volatile data is collected. Rather hibernate option may be used based on certain situations.
- ✓ Photographs of the running system at the crime scene must be taken and documented
- ✓ All the logs of collection activities must be maintained.
- ✓ Don’t run administrative utilities and diagnostic utilities during live acquisition.
- ✓ Save the collected data to any removable storage media and follow seizure procedures.

After collecting all the information, documentation and seizure procedures should be followed before they are shifted for analysis. Chain of custody documents of the total process, devices, and data must be maintained.

In the above case scenario, Since the computers are found in running state and unlocked condition, the above procedures are to be followed to acquire the live and volatile data. The uploaded images could be found from the computer, and Fake Facebook ID and login details also may be found from RAM dump analysis. The enough content to prove the crime in the court of law can be acquired from the scene.

3. Creating Disk Image and Image Analysis

When a hard disk or pendrive is to be processed in a crime a scene, first and foremost step is to prevent the additional writings into disks. Write access should be blocked by using write blockers. The second step is to calculate the Hash value of original disk. MD5 and SHA-1 and SHA-256 are widely available algorithms for calculating hash values. These hash values will be used to comparison to ensure the integrity of the data in sub sequent phases of the processing of the devices.

When extracting data from hard disk or pendrive, it is inevitable to create an image of the disks and drives to avoid any loss of integrity in original disks. Creating an image does not equal to copy and paste of the data. It is bit-to-bit copy, including folders, files, slack space and unallocated space unaltered file into new disk known as imaged disk. It copies right from first bit to last bit on the disk to imaged disk. It is exact copy of the original disk. Copying may consume time but it is mandatory to image a disk before sending original disk for analysis. The imaged disk may contain any hidden files, recently deleted but not overwritten files and also any files left over in free and slack space. Imaged disks and processing them will leads to find paths and evidence in the investigation. Back up of the data is not considered as image of the disk. It is not exact copy of the physical disk. Forensic images of the disks can be created with the help of specialized forensics software. FTK imager is one tool will be used for creating an image of the disk.

i. Process of imaging a disk

Step 1: Goto file menu in the FTK imager window and select Create disk image. It is shown in the figure.

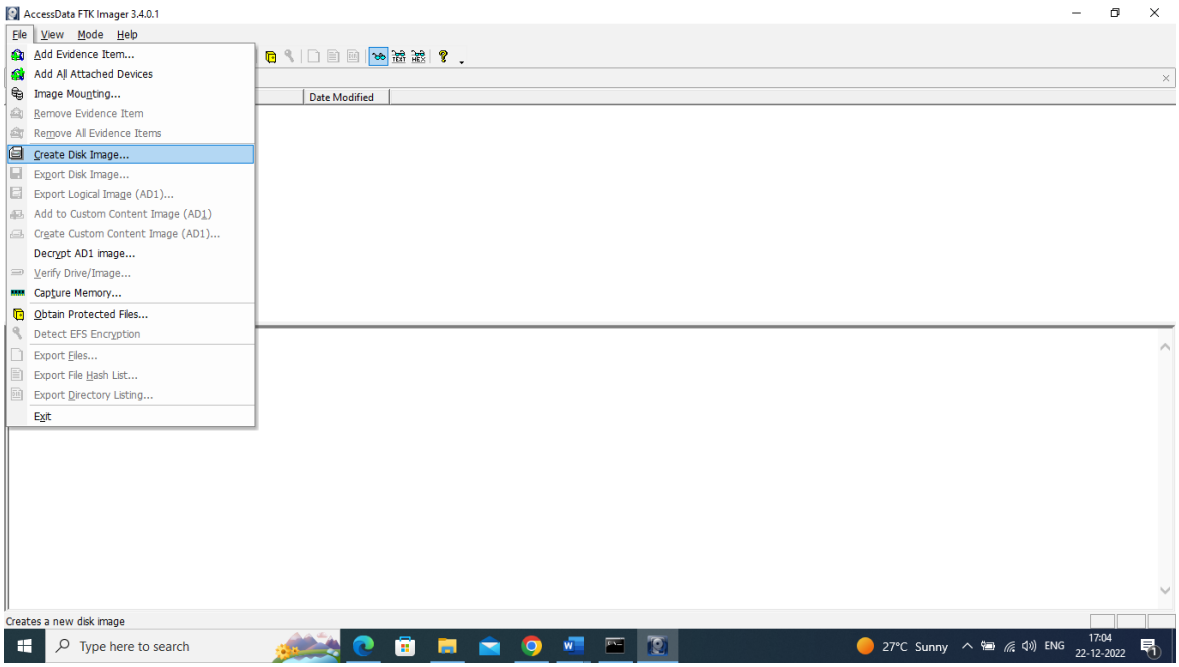


FIGURE 31: CREATING AN IMAGE OF DISK USING FTK IMAGER

Step 2: After clicking on create disk image in the previous step, the following window is arrived. In this select physical drive and click on next

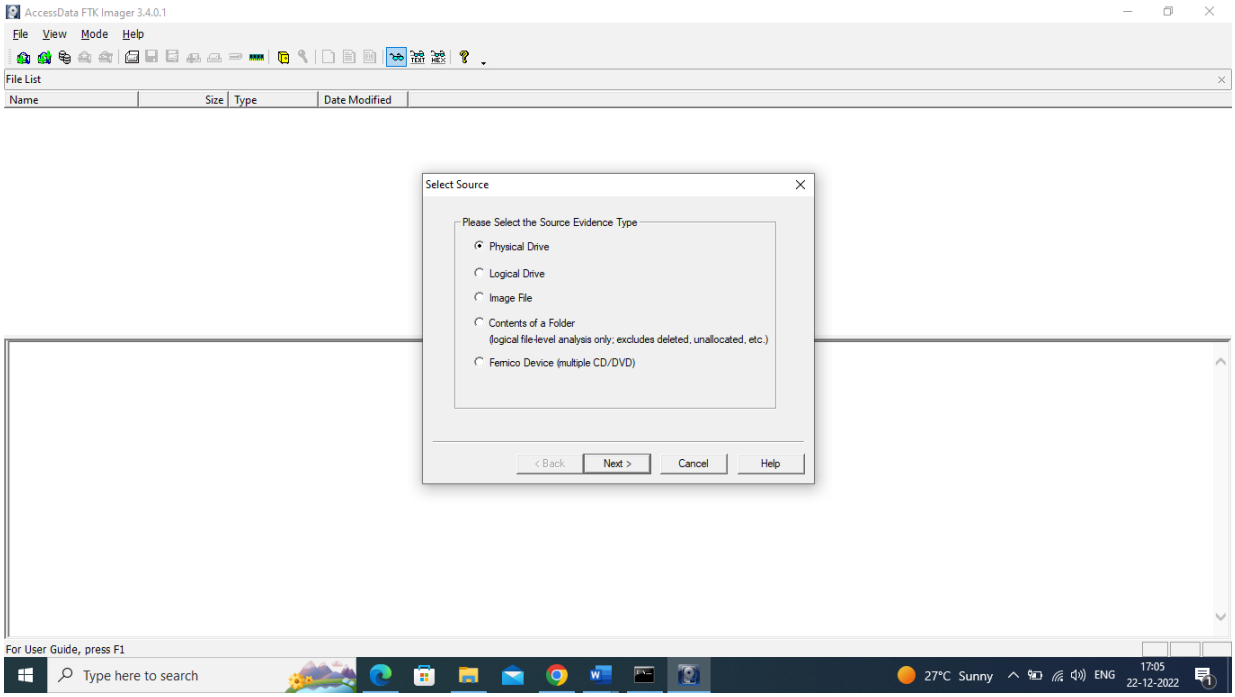


FIGURE 32: SELECT PHYSICAL DRIVE

Step 3: In this step you have to select image type. E01 is selected for this case. It is shown in the following figure. And click on next.

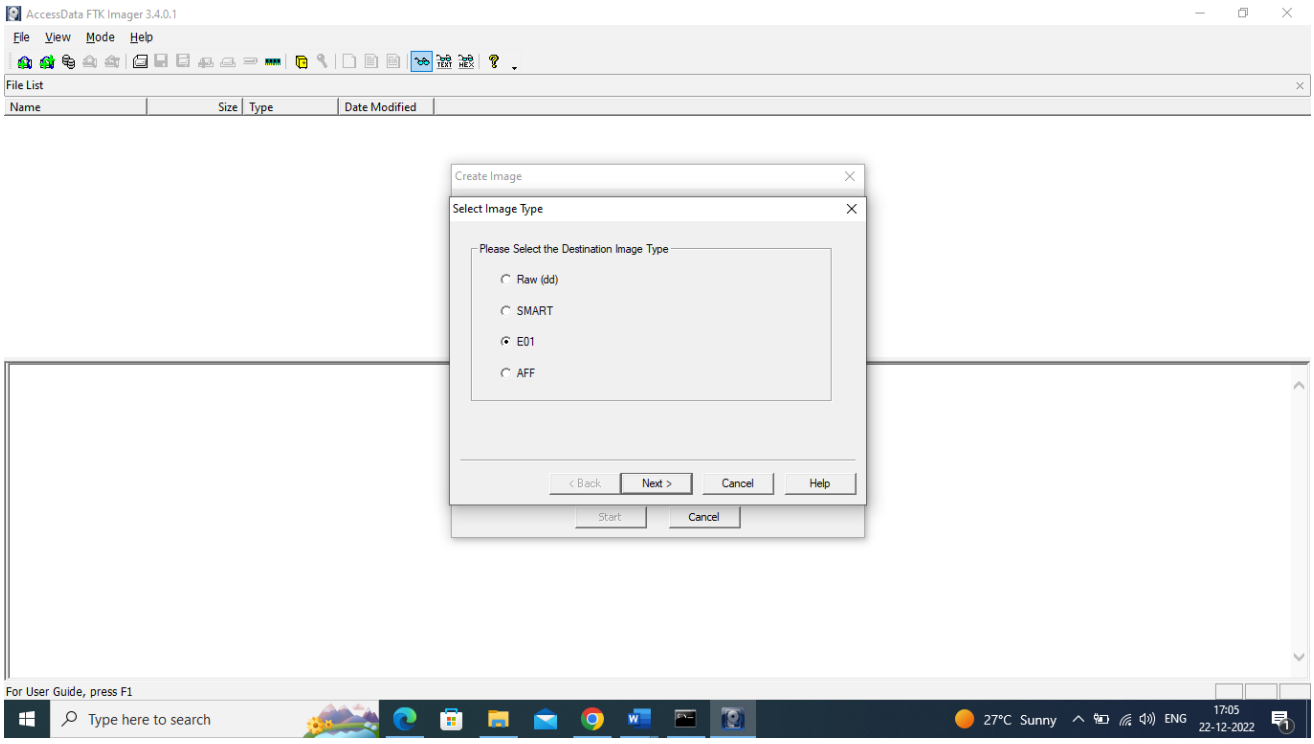


FIGURE 33: SELECT IMAGE TYPE AS E01

Step 4: As shown in the following figure, source is already selected as physical drive, but destination is to be selected. It is recommended to select the destination by clicking on add option which will become the imaged disk and click on start button below

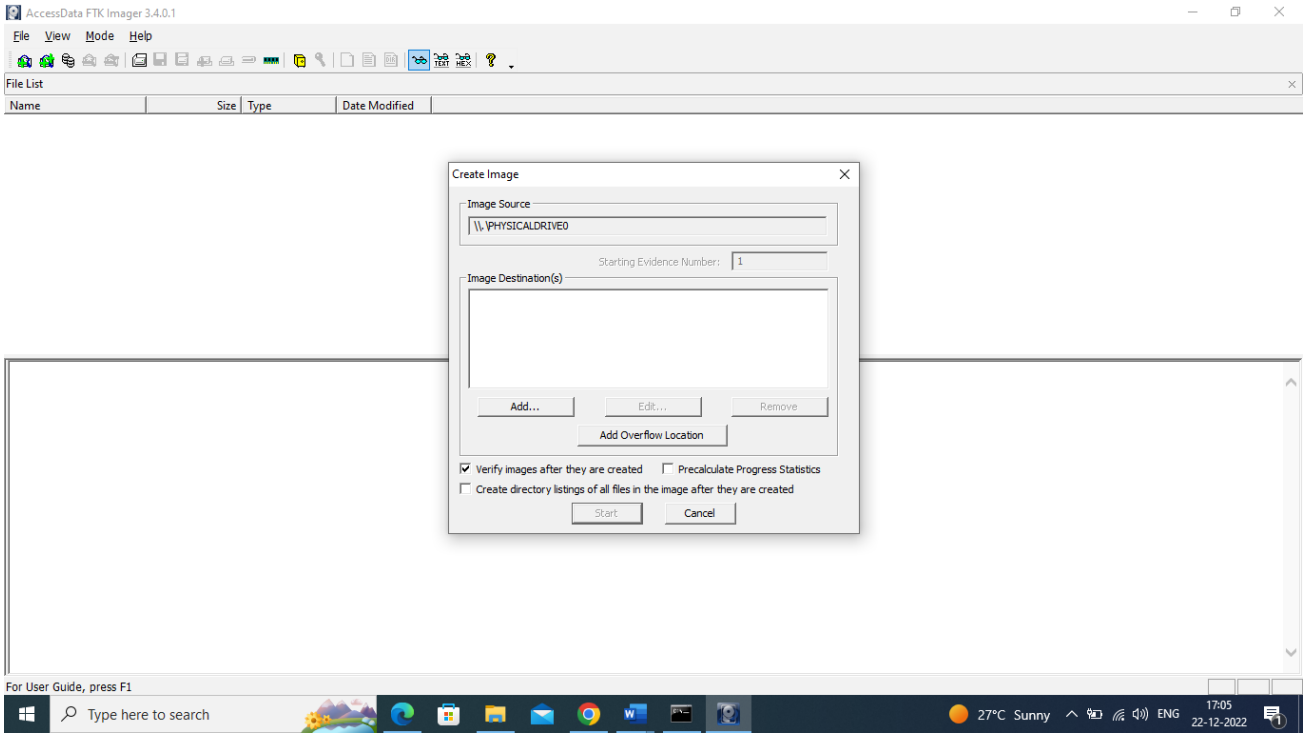


FIGURE 34: SELECTING IMAGE DESTINATION AND START

Image will be created in the destination location. That is known as imaged disk. Imaged disk may be sent for analysis by following the procedures and protocols.

After imaging the disk, those disks, may be sent for analysis. Autopsy is the tool used for disk analysis.

ii. Image Analysis using Autopsy

Autopsy is a digital forensics platform and graphical interface to “The Sleuth Kit” and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card. Autopsy advantages

1. Free

2. Open Source

3. Better results

Autopsy is built into the SANS Investigative Forensic Toolkit Workstation (SIFT Workstation) that you can download fromforensics.sans.org. Autopsy is available from http://www.sleuthkit.org/autopsy. a) Start using Autopsy

Step1: Create a new case using autopsy.

FIGURE 35: AUTOPSY

There will be three options
1. Create New Case: To create new case.
2. Open Recent Case: To open recent case which is recently analysed.
3. Open Existing Case: To open Existing/ Old.
Here "Create New Case" is selected.

Step 2: Enter the Case Details
After clicking "Create New Case", you will see a window which ask about the case name and base directory where you want to save case related files and information. After filling information click "Next".

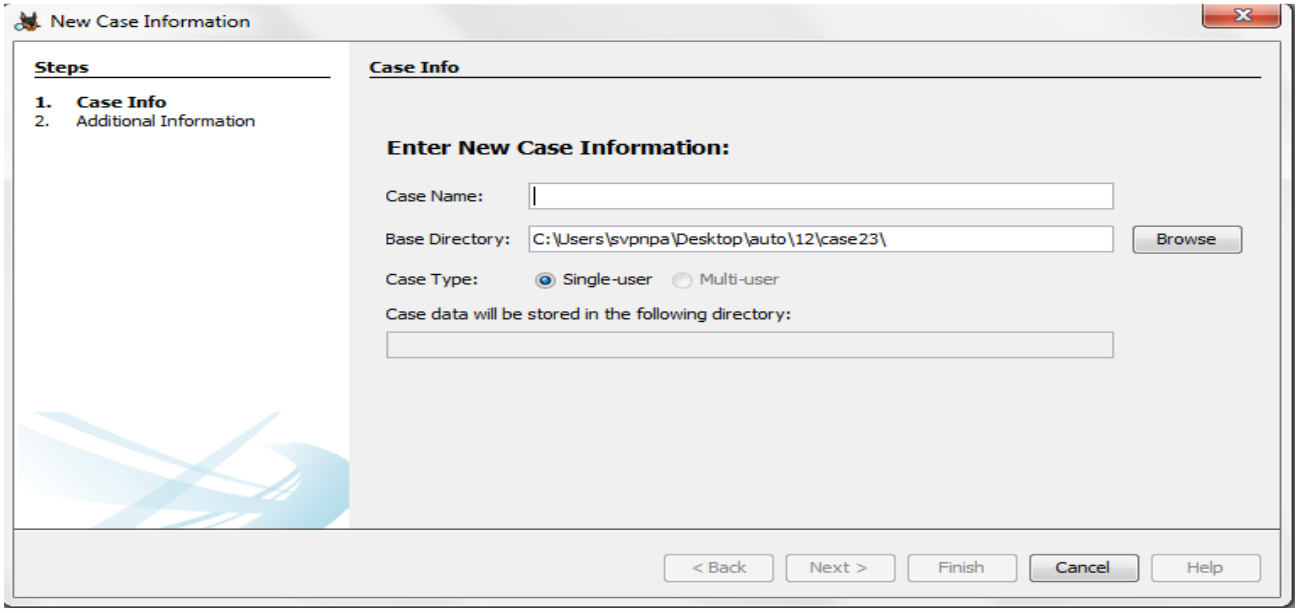


FIGURE 36: NEW CASE

Step 3: Enter the Case Number and Examiner Name
Next window is for case number and examiner name, put unique case number and examiner name and click "Finish".

and click "Finish".

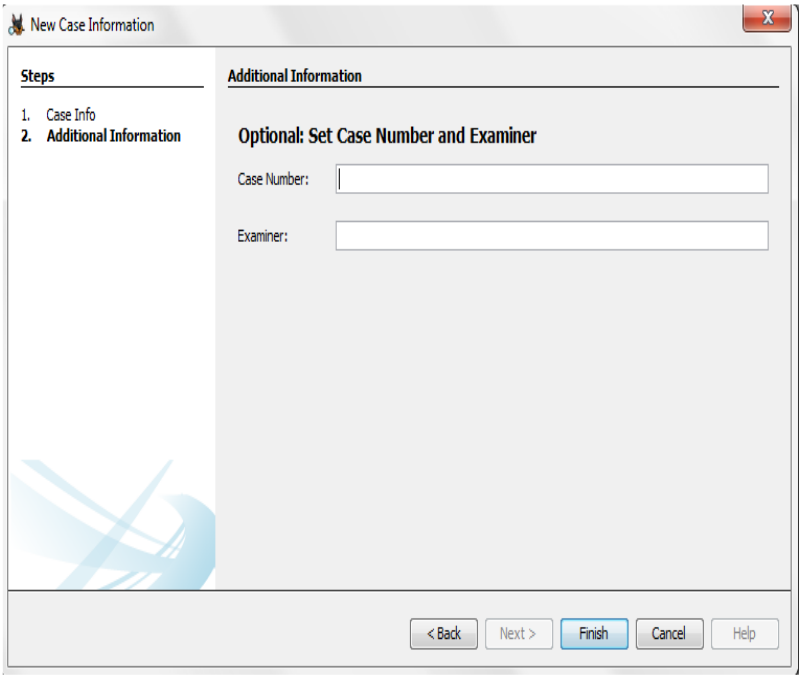


FIGURE 37: CASE INFO

Step 4: Add evidence item.
You can add a data source in several ways:

- After you create a case, it automatically prompts you to add a data source.
- There is a toolbar item to add a Data Source when a case is open.
- The "Case", "Add Data Source" menu item when a case is open.

The data source must remain accessible for the duration of the analysis because the case contains a reference to the data source. It does not copy the data source into the case folder.
Regardless of the type of data source, there are some common steps in the process:
1. You will be prompted to specify the data source to add.

2. Autopsy will perform a basic examination of the data source and populate an embedded database with an entry for each file in the data source. No content is analyzed in the process, only the files are enumerated.

3. While it is examining the data source, you will be prompted with a list of ingest modules to enable.

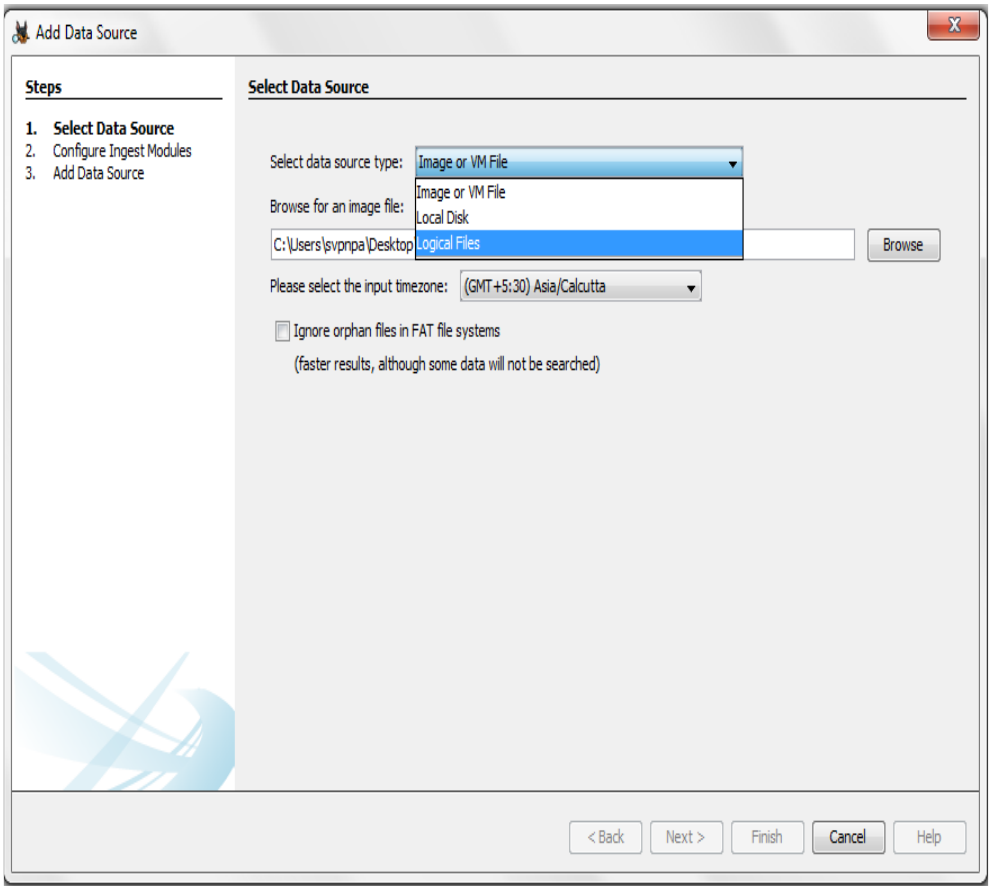


FIGURE 38: DATA SOURCE

To add a new data source at beginning, follow this:
Select file location by clicking browse.
Now select the Time Zone, it will be the same as evidence item. If evidence seized from a machine which follow GMT+5:30 time zone, then we also select the same.
Last option is to check a box, which will ignore orphan files. Orphan file are default DLL file in windows system. After all set click "Next"

Step 5: Configuring Ingest Modules
You will be presented with an interface to configure ether ingest modules. From here, you can choose to enable or disable each module and some modules will have further configuration settings.

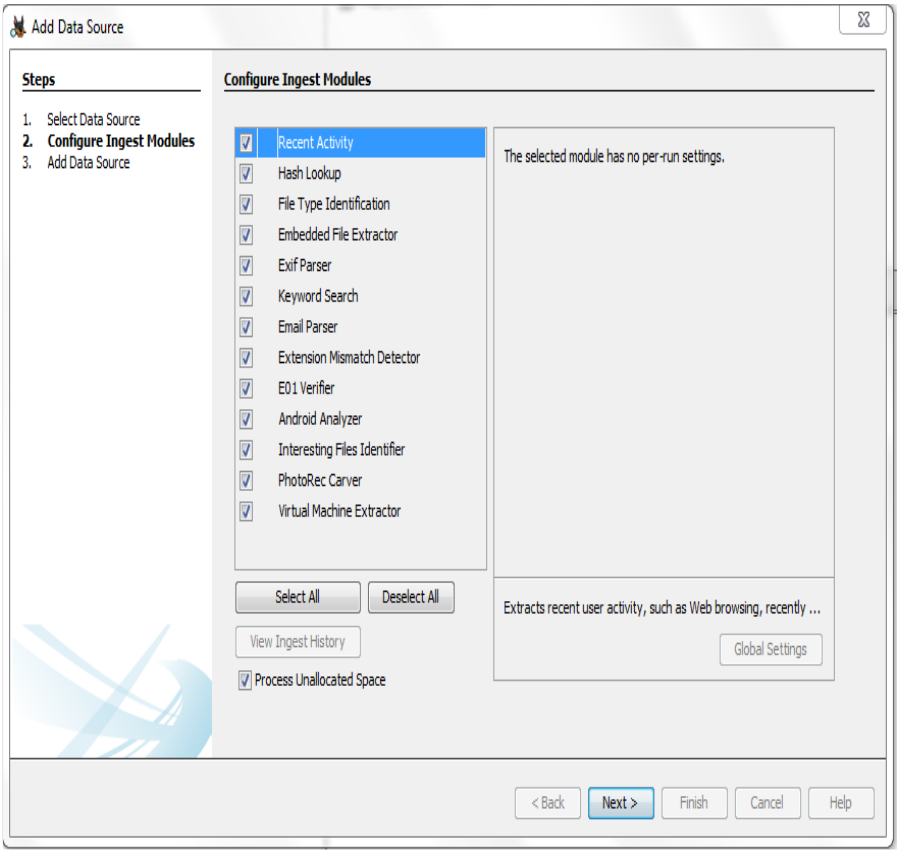


FIGURE 39: INGEST MODELS

There are two places to configure ingest modules. When you select the module name, you may have some "runtime" options to configure in the panel to the right. These are generally settings that you may want to change from image to image.

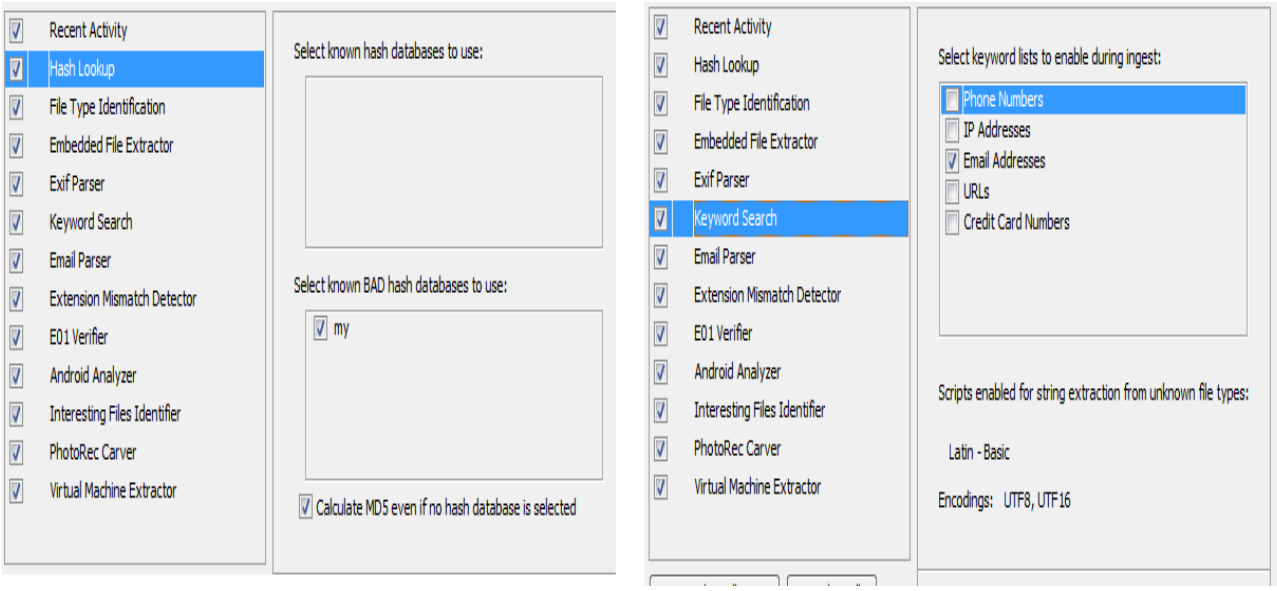


FIGURE 40: RUNTIME OPTIONS

There may also be an "Advanced" button that is enabled in the lower corner. Pressing this button allows you to change global settings that are not specific to a single image. This advanced configuration panel can often be found in the "Tools", "Options" menu too.

As an example, the hash lookup module will allow you to enable or disable hash databases in the “run time” options panel, but require you to go to the "Advanced" dialog to add or remove hash databases from the Autopsy configuration.
Autopsy now ask you about to "Finish" the configuration and start the analysis

After clicking "Finish", it will analyze the data source, and the progress bar will be shown at bottom right as shown above.

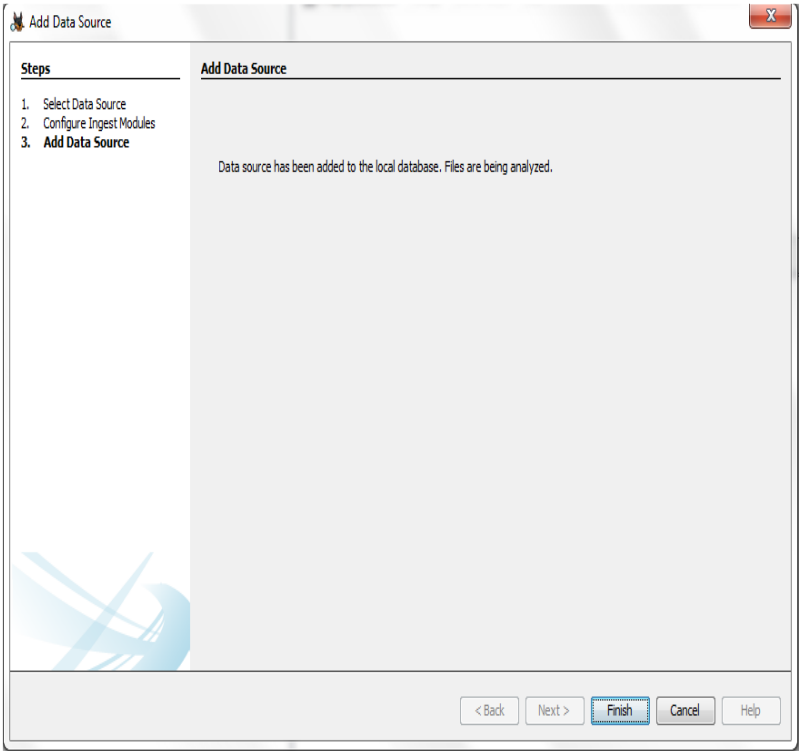


FIGURE 41: CLICK FINISH

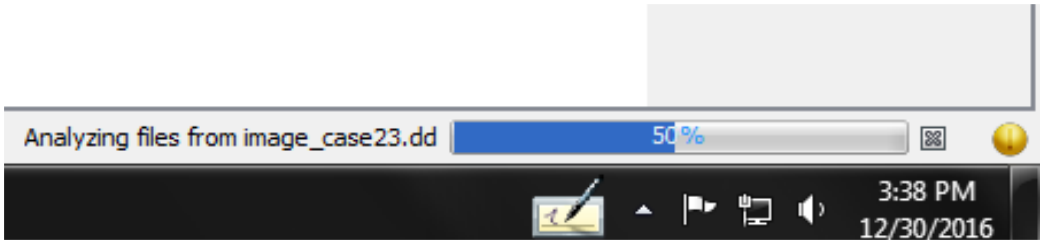


FIGURE 42: ANALYSIS IN PROGRESS

b) Analyse Evidence Source
Recent Activity Module:
The Recent Activity module extracts user activity as saved by web browsers (including web searches), installed programs, and the operating system.
This allows you to see what activity has occurred in the last seven days of usage, what web sites were visited, what the machine did, and what it connected to.

Results show up in the tree under "Extracted Content".

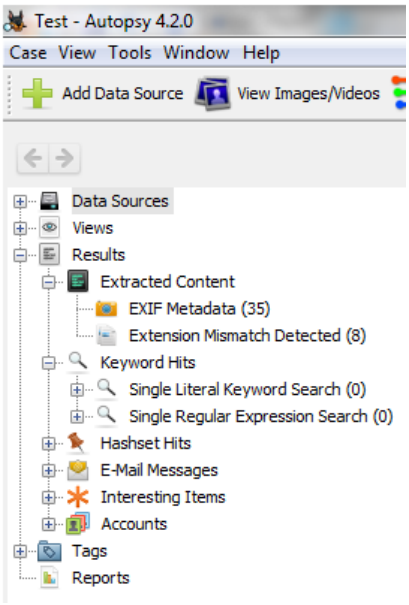


FIGURE 42: EXTRACTED CONTENT

Hexadecimal Analysis:

You can also analyse data using hexadecimal values; just click "Data Sources", hexadecimal value will available at right panel, like given below.

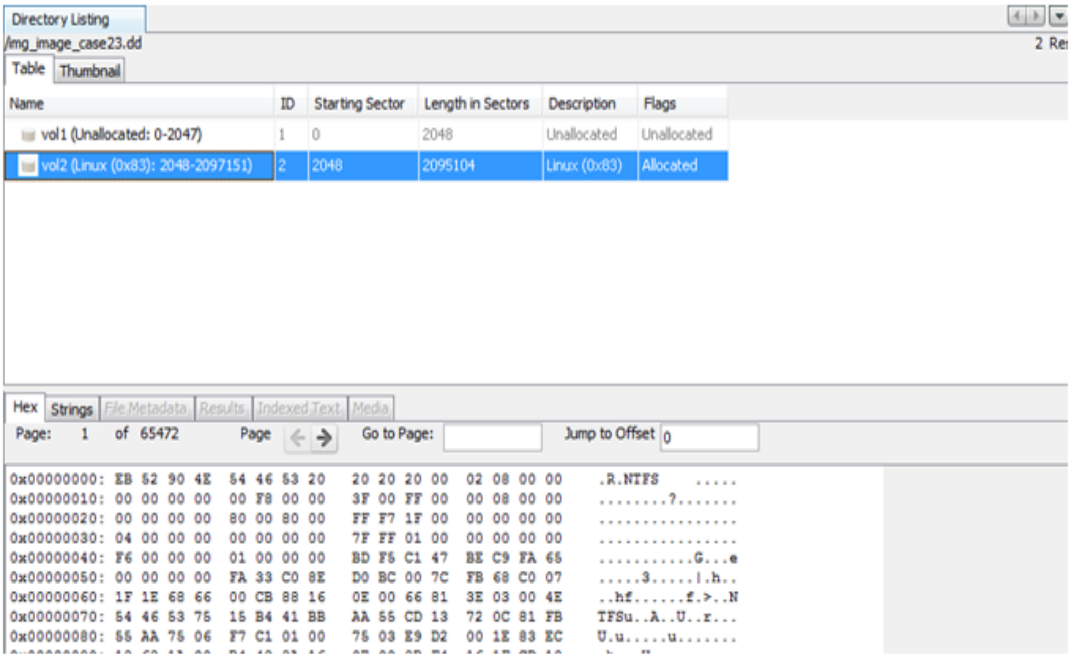


FIGURE 43: HEXADECIMAL ANALYSIS

Keyword Search:

Keyword searches of the file system image can be performed using ASCII strings and grep regular expressions. Searches can be performed on either the full file system image or just the unallocated space. An index file can be created for faster searches. Strings that are frequently searched for can be easily configured into Autopsy for automated searching.

To search keyword, go to tools-->Options and select "Keyword Search" tab. Now add some keyword to search in evidence source. From here you can create new list or you can use existing list to analyse.

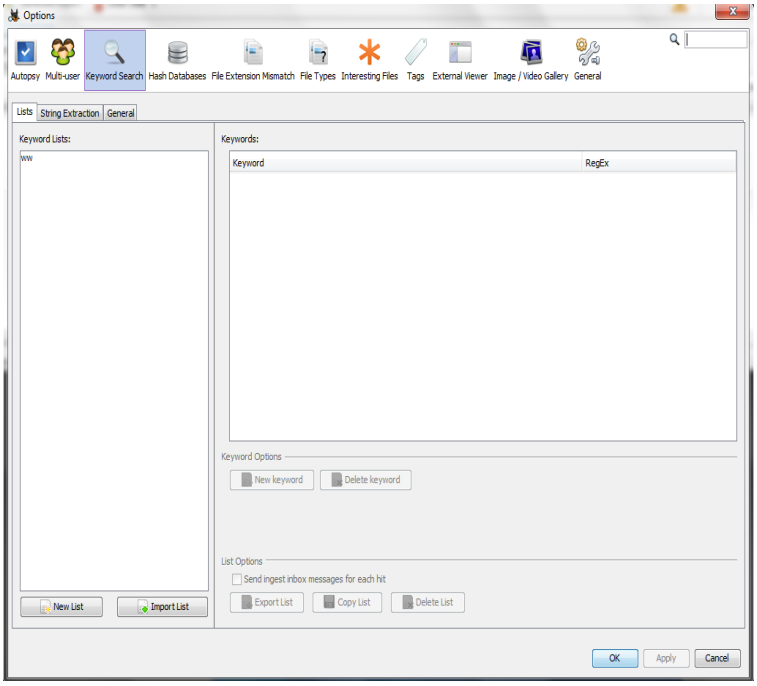


FIGURE 44: KEYWORD SEARCH

Content Viewer:

The Content Viewer lives in the lower right-hand side of the Autopsy main screen and show pictures, video, hex, text, extracted strings, metadata, etc. They are enabled when you select a file in the file list above it.

The Content Viewer is context-aware, meaning it will present different views of the content based on the type of file selected. For example, a .JPG would show up as a picture, a text file would show up as text, and a .bin file would show up as hex output.

The screen shots below show some examples of content viewers in action. First screen shot shows the image, second shows hexadecimal values of that image and third screen shot shows the metadata information of this image.

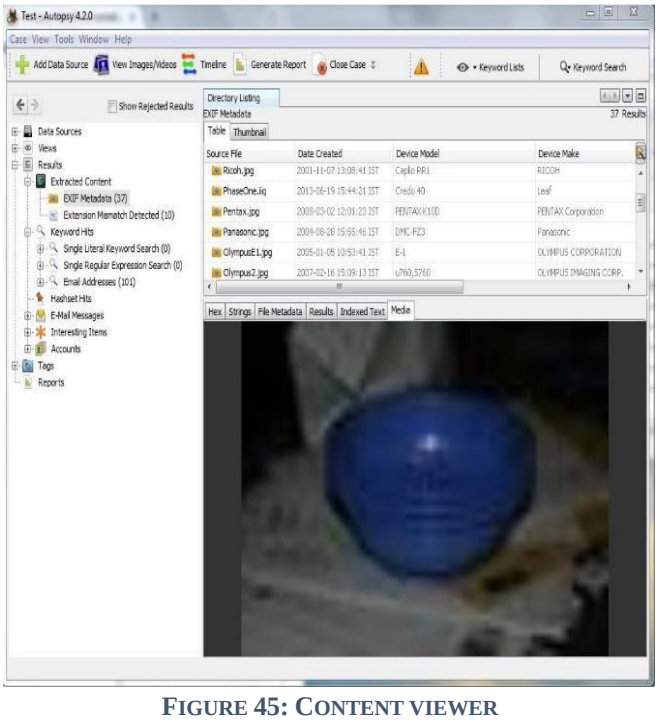


FIGURE 45: CONTENT VIEWER

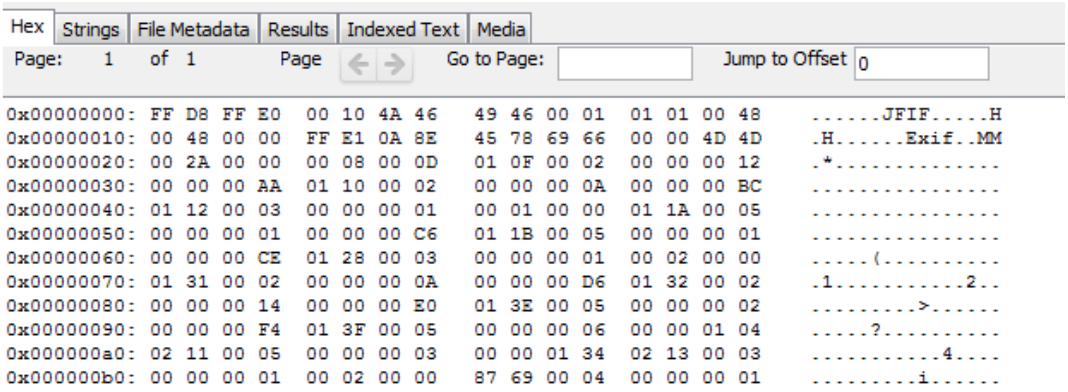


FIGURE 46: HEX VIEWER

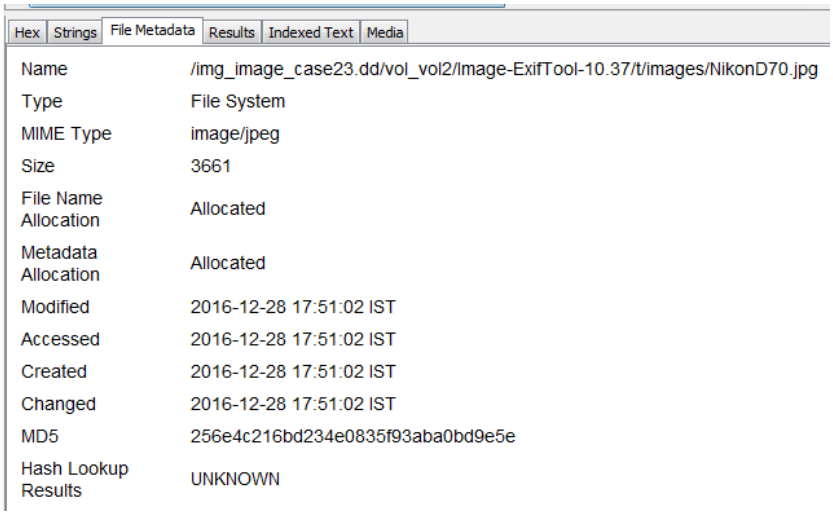


FIGURE 47: FILE METADATA

Email Parser Module:

The Email Parser module identifies Thunderbird MBOX files and PST format files based on file signatures, extracting the e-mails from them, adding the results to the Blackboard. This module skips known files and creates a Black board artifact for each message. It adds email attachments as derived files. This allows the user to identify email-based communications from the system being analyzed. The results of this show up in the "Results", "E-Mail Messages" portion of the tree.

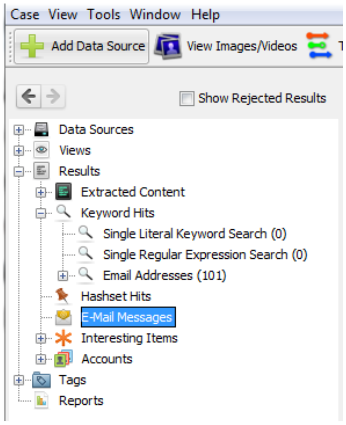


FIGURE 48: E-MAIL MESSAGES

Photo RecCarver Module:

The Photo RecCarver module carves files from unallocated space in the data source and sends the files found through ingest processing chain. This can help viewer discover more information about files that used to be on the device and were subsequently deleted. These are simply extra files that were found in "empty" portions of the device storage. The results of carving show up on the tree under the appropriate data source with the heading
"$CarvedFiles".

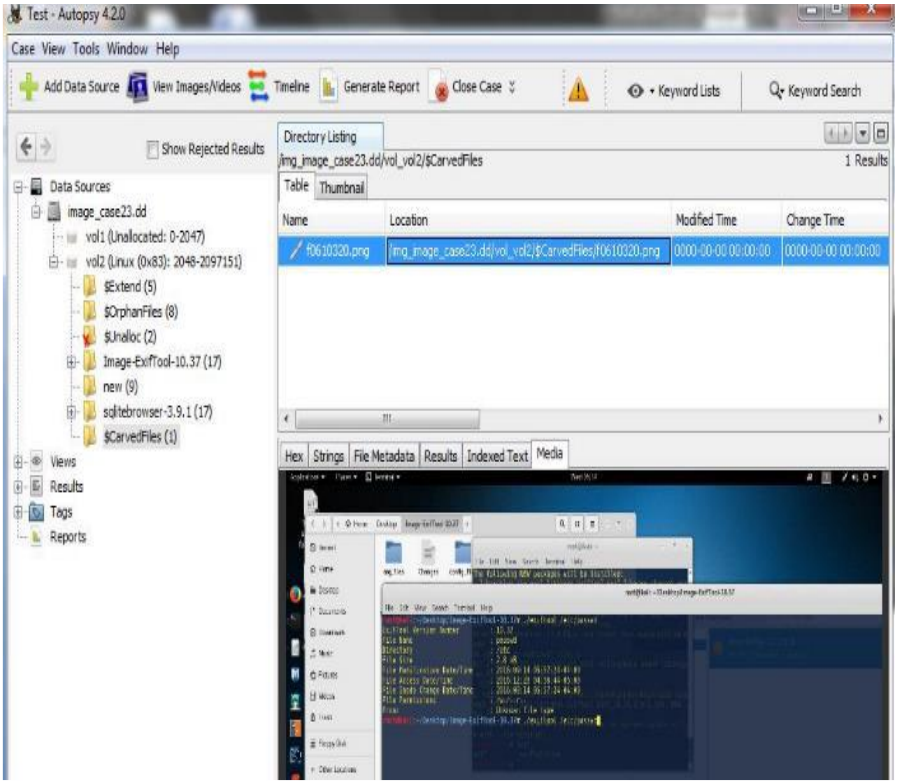


FIGURE 49: RECARVER

Reporting:
To generate the report, we have to create some tag or bookmarks.
1. Tagging
Tagging (or Bookmarking) allows you to create a reference to a file or object and easily find it later. When an interesting item is discovered, the user can tag it by right-clicking the item and selecting one of the tag options.
When you tag a Black board artifact result, you have the choice to either:

- Tag File– use this when the file itself is of interest
- Tag Result–use this when the result is of interest

Which to choose depends upon the context and what you desire in the final report. For example, we are choosing Tag File here.

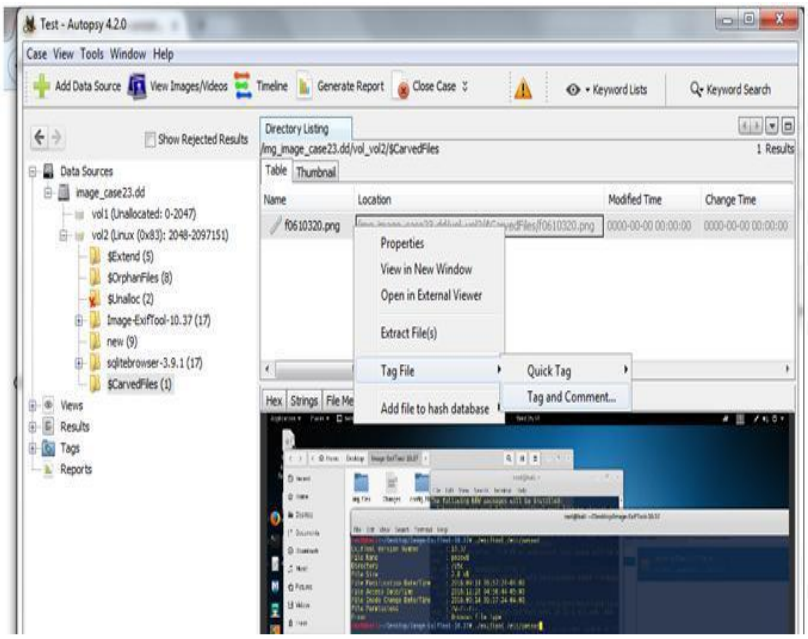


FIGURE 50: TAGGING

Once you have chosen to tag the file or the result, there are two more options:

- • Quick Tag–use this if you just want the tag
- • Tag and Comment–use this if you need to add a comment about this tag.

After clicking Tag and Comment, window will pop-up. Enter Comment and continue.

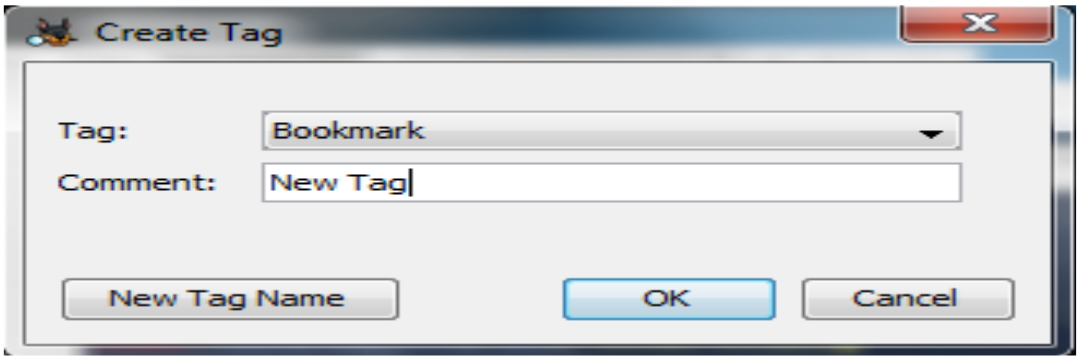


FIGURE 51: ADD TAG

2. Generate Report:
   To create reports, go to "Tools", "Generate Report". You can choose several different types of reports. We will go through the HTML report here.
   Select HTML here and click next.

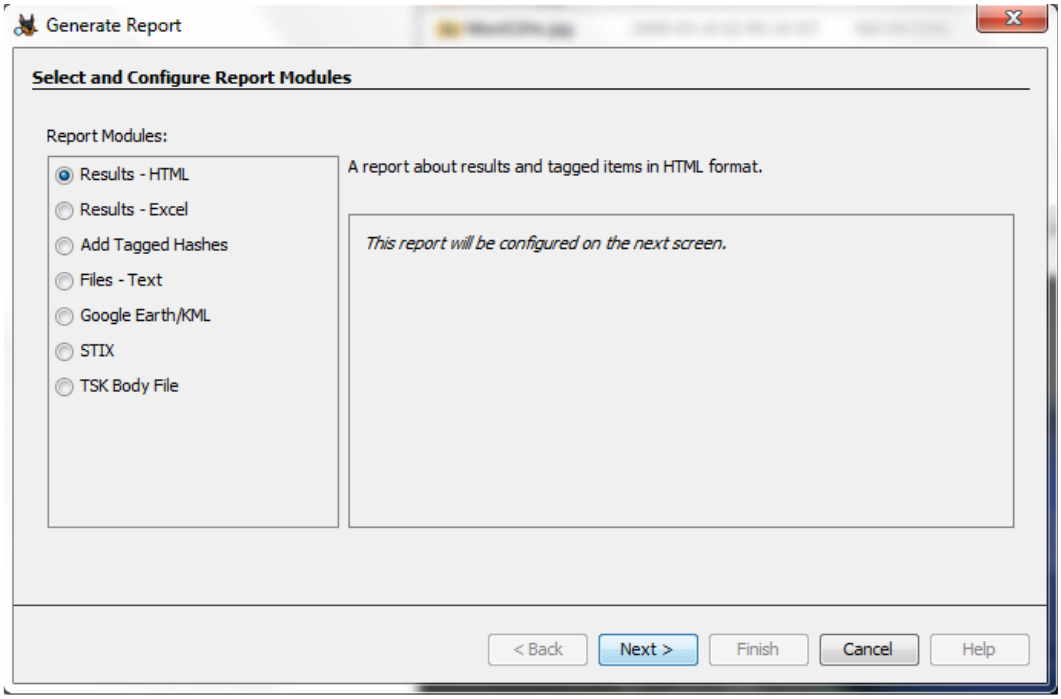


FIGURE 52: REPORT GENERATION

The report will be generated at the given location, you can click on a hyperlink and open it in a browser, and view it. It will show all details related to the case.

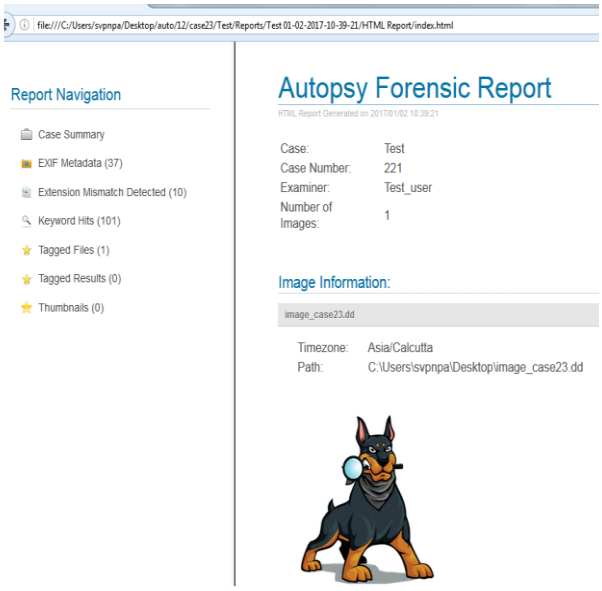


FIGURE 53: FINAL REPORT

4. Guidelines for Documentation and Seizure of Digital Evidence

i. Steps for seizure (With Hard Disk Drive as a sample)

- Collect all the digital evidence: preferably the original if possible/ available or if not the cloned copies and certify them under 65B IEA.
- Separate out the main copy and the working copies.
- Pack all the working copies in a separate box, which would later be used in the PS for analysis/Investigation.

- For the main copies put the white tape on the connecting ports of each Hard Disk Drive along with department's seal. The seal and the tape will ensure that no one has accessed the Hard Disk Drives.
- Seal the main copies by putting them in an anti-static bag then in a bubble bag and then in a storage box and then again wrap the white tape around the storage box so that no-one can open the box without removing the tape, and then place a seal of the department.
- Take signature of witnesses and officer in charge, on the seal.
- If we are seizing a system or any other digital evidence, then it should be wrapped with tape and sealed in such a manner that no-one can start or open the digital evidence without breaking the seal.

ii. Documentation during seizure

If the acquisition process is done on the scene of crime, the seizure process is completed after the acquisition. If the acquisition is not possible on the scene of crime, then the devices are seized and are forwarded to forensic lab for acquisition and analysis.

The Hard Disk Drives which are to be seized may be either the original Hard Disk Drives found at premises, or the cloned copies made by technical persons.

Invariably, the original storage media is seized. Preferably two cloned copies are taken, one cloned copy may be handed over to the victim/witness/owner of the premises being searched upon and the other should be kept with IO as working copy for further investigation/analysis.

In case of seizure, documentation is very important:

- **Physical items**: There are well-established procedures for handling the physical items, such as the computer, the PDA, or the cellular telephone.
- **Data acquisition**:
  - **What types of digital evidence have been collected?** For example, is there hard copy (printed) version of the e-mail/ other digital data? Is there an electronic copy? Does it contain full header information?
  - **Who handled the evidence-** Document the name and job function?
  - **How was the digital evidence collected and stored?**
    - Identify any tools or methods used to collect the digital evidence.
    - Determine who had access to the digital evidence after it was collected (anyone with access to the evidence should be considered part of the chain of custody). Account for all storage of data as well.
  - **When was the evidence collected?** Document the date and time when the evidence was collected.
  - **Where was the evidence when it was collected?**
    - Geographical Details
    - Hardware device details
      - ✓ What kind of machine/device that held the digital evidence?
      - ✓ Who had access to the machine/device?
      - ✓ Who owned the machine/device?
      - ✓ Was a serial number present?
      - ✓ Was the machine/device a shared device?
      - ✓ Was information retrieved from a network?

- ✓ Was information password-protected?
- ✓ Who had access to password-protected information?
- ✓ Offsite (e.g., servers – e- mail or remote – and web pages)

- Document the details of each Hard Disk Drives or digital evidence which must be seized. There may be many attributes which we have to note down such as serial no of device, its capacity, used space by data, operating system used and password (if there any).
- Before seizing any of the digital evidence, their hash value must be calculated using forensic tools. The report generated by these tools has to be attached along with the panchnama.
- Case name, premises, date of seizure, place etc. This kind of information can also be written on each digital evidence for memory purpose.

5. Broad Outline for the Panchnama

1. PS name, Case number etc
2. Calling local resident as Witnesses - their name and details to be recorded and how they have been informed to come as witness.
3. Briefing to the witnesses and informing about the search to be conducted, showing authorization to search etc
4. Showing the tool kit and documenting that they are wiped clean/new. Checksum to be calculated for the blank storage. (Using WinHex)
5. Noting details of team members and the roles.
6. Proceeding to the scene at what time and how. (Presuming that you are already at the scene locality)
7. Reaching the scene. Outer description and time of arrival. The boundaries of the location (N,S, E and W)
8. Production of search warrant/ informing the owner of the place about the search if it is without warrant.
9. Giving personal search before conducting the search and documenting it.
10. Entering the room and taking photographs in all angles, documenting how things are lying. Also, make a sketch of the same.
11. Secure the scene and note the details of the persons present at the scene
12. Isolate the person and keep them away from touching anything.
13. Documenting how the computer was found, and peripherals seen connected to it. The condition of computer and all devices found there. Document and photograph in all angles
14. Perform triage first to identify the evidence
15. Label the cables, devices and other evidence as identified above.
16. Put seal tapes on the unused ports with signature of the IO and witnesses. (to be incorporated based on case requirements)
17. Acquisition of evidence – in sequential order as per triage outcome. Volatile first and non-volatile later if the system is found in ON and unlocked situation.
18. If the disk is being cloned/image is being made, then duly mention the tools used and the way they are connected before.

19. If any settings are being changed (sleep settings, hibernate enabled etc.) then that should be noted with details and reasons thereof in the Panchnama.
20. Note the system time and actual time. Note the processes running in the system and capture the screen as seen in a photograph.
21. Videography saved into a memory card all the process carried out by the IO to acquire data. Document the same with full details.
22. This original memory card would be the video evidence for the Panchnama.
23. Fill the seizure forms with all technical details.
24. Calculate before and after hash values of the evidence as found using two different algorithms and confirm using different tools.
25. Mention all the tools and their versions used, and the detailed processes followed for each step above.
26. Disassemble the device – this to be recorded and noted down.
27. Mention how the packing is done for each item as it is seized.
28. Label the packings with seals, signatures, and appropriate evidence numbers
29. Mention the details in chain of custody form
30. Fill the forwarding note and the questions to be asked
31. Close the Panchnama by mentioning the time of closure and the details of the available light in the place.

Note:

1. If the system is locked: Then the accused is to be questioned to share the password. The IO should be aware of the limitation to use this password given by accused.
2. The 65B to be prepared if the RAM dump or any other data is copied.
3. The 65B is also to be prepared if the WinAudit report is obtained.

Mention the details of how the evidence is packed, stored and being transported to FSL after due approval of court in the Case diary.

Social Media Monitoring and Sentiment Analysis

1. What is social media monitoring?

Social media monitoring is the process of identifying and determining what is being said about a brand, individual or product through different social and online channels.

i. How does social media monitoring work?

Most social media monitoring tools work by continuously crawling and indexing sites, sometimes in real time, such as Twitter. Once all of those sites are indexed, they can then be searched to find mentions, opinions and sentiment on specific products, brands, companies, people, places, etc.

The unstructured data created by millions of users posting and tweeting each day can fuel competitive advantages and help support marketers and other decision makers make more informed, critical decisions. This is possible if you can distill those millions of posts and tweets down into concrete information, and when you are able to understand what the users are actually saying. On social media, users express themselves using their own language: if you want to understand what they are saying, you need to understand all of the ways they communicate: slang, jargon, acronyms, abbreviations and so on.

Using cognitive computing technology, social media monitoring tools can really understand users and what they express on social media, comprehending intent, sentiment, opinion and preferences.

2. Social Media Monitoring for LEA

Social media has become a cesspool of information, a journal of movements, opinions, relationships, and ideologies. This makes Social Media a salient platform for monitoring and analysis of individuals, groups, and events. This information, rather data is of crucial importance to the law enforcement agencies for tracking and monitoring of suspects and criminals.

With almost 462 million people, more than 35% of India's population is online. India has the second-largest number of internet users in the world and it has experienced 30.5 % growth since 2015. The growing users are making it a goldmine of information.

The recent trend of posting live pictures and videos of criminal and disastrous activities has become an instrument of real-time information dispensation of the causalities. This can help the LEA not only in staying updated but also in planning their next course of action.

Social media analytics is a part of OSINT processing, where data collected from publicly available sources are used to create intelligence. Social media, includes all platforms like Facebook, Google, Instagram, LinkedIn, Yelp, Twitter, etc. Twitter hashtags and trending videos are high zones of activity which can be monitored by the Law Enforcement Agencies (LEA) constantly.

i. Predicting Mass agitation

People usually turn to social media to advertise any strike, rally or any other important event that requires public turnover. This becomes an area of interest for the LEA because of the constant possibility of these events taking a violent turn and it’s precautionary to monitor them before they get out of hand.

OSINT, especially social media analytics conveys the Time, Date, Location, People of Interest and other various details which can help to monitor and control the law and order situation. It can help us track public opinions and sentiments across various social media platforms. It can also predict the scope and reach of any propaganda or radical movements.

For example- If LEA learns that there are whispers of mass agitation scheduled to happen on a specific day, they can take considerable steps to control the damage while monitoring it to prevent major casualties or damage.

ii. Suspect Profiling

Once the reckoning of an event is known to the LEA, surveillance follows. It is also known as Social Profiling which is the process of constructing a User's (usually a suspect) profile using their publicly and voluntarily shared social data. In general, profiling refers to the data science process of generating

a person's profile with AI-based algorithms and technology. It helps in understanding the suspect and its behavioural aspects with the 360-degree assessment.

This includes -

- Monitoring the posts, tweets, etc
- Keeping track of the number of people supporting it and against it
- Capturing the degree of sentiments
- Activities of the concerned individual in lieu of provoking or instigating people
- The general consensus regarding the concerned individual or the content shared by them

3. Why business need a social media monitoring strategy

To be successful, any business strategy must incorporate social media. Organizations need to be able to hear the conversations taking place about your company and your brand in order to reach the right people at the best time with the most insightful content. Social media monitoring is exactly what you need to achieve this.

Many companies might think that social media monitoring is just tracking mentions and replying when prompted. Nothing could be more wrong.

Social media monitoring is the use of tools to listen to millions of conversations on the web to determine what is being said about a particular brand, issues, people or producst, and to discover opportunities. It is how we monitor the web world. Social media monitoring can be passive, for example, listening to people to discover what interests them, or it can be active, searching for references to your brand, campaigns or actions.

Social media monitoring is not just about social networks, but it the entire web, including forums, blogs, news sites, communities and anywhere that conversations take place on the web.

iii. How does it affect ecommerce businesses?

Social media listening can impact how you market your ecommerce business. Businesses engaged in social monitoring actively search digital media channels for keywords or phrases directly related to their brands.

Once you have an idea of your company's public perception, you can:

- React in real time with consumers on social platforms
- Determine how certain demographics feel about your brand
- Use positive feedback in marketing, etc.
- Use negative feedback to correct errors in your business
- Build brand credibility and authenticity
- Refine marketing spend by eliminating channels with the lowest or worst engagement levels
- See which social media marketing campaigns are performing the best and the worst
- Calculate return on investment through advanced reporting capabilities

Social media monitoring can give you a glimpse into what's being said about your brand in real time, gathering publicly available data and organizing it in a way that works to your advantage. Social monitoring tools can also help you grow your online awareness for your ecommerce store. You can act

on what's being said about your company and in turn, reconnect with prospective customers using the same social channels.

4. What's the Difference Between Social Monitoring and Listening?

You'll hear people talking about social media listening tools when they mean social media monitoring tools, and vice versa, but technically they are different things. The key distinction lies in how close you are to the action: think zoomed-in vs. zoomed-out.

Social media monitoring means dealing with the day-to-day of managing your social monitoring platform feeds and reacting accordingly. It's liking a comment on Instagram, getting into a conversation on Facebook, or replying to a tweet. It's responding to queries, compliments, and complaints.

Social listening shows you the bigger picture. If you have all those likes, comments and posts gathered into graphs and categories, you'll see patterns at play. You can then make decisions based on your understanding of what your customers or competitors are doing, within the context of industry changes. Most importantly, you can note trends, find new opportunities and pre-empt a social crisis before it happens by listening to the digital world around you and seeking out information. Now, let's take a look at some of the reasons why marketers and PRs at successful companies take both approaches.

5. Manual Social Media Monitoring Vs Media Monitoring Tools

In the fast-paced world of digital, you're better off using an automation tool for a social media search than trying to handle tasks manually.

The latter can quickly become unreliable, so you're likely to miss important conversations. It also wastes time that you could dedicate more usefully to other projects.

If you're interested in seeing how much time a social media monitoring tool could save you.

6. Tools of Social Media Monitoring

Identify and analyzing of online trend–

For monitoring purpose, it is necessary to follow the trend of social media. Trend is nothing but discussion of matters on social media by in majority users.

Below are some trends extracted based on HASHTAG.

Trending #hashtag on twitter

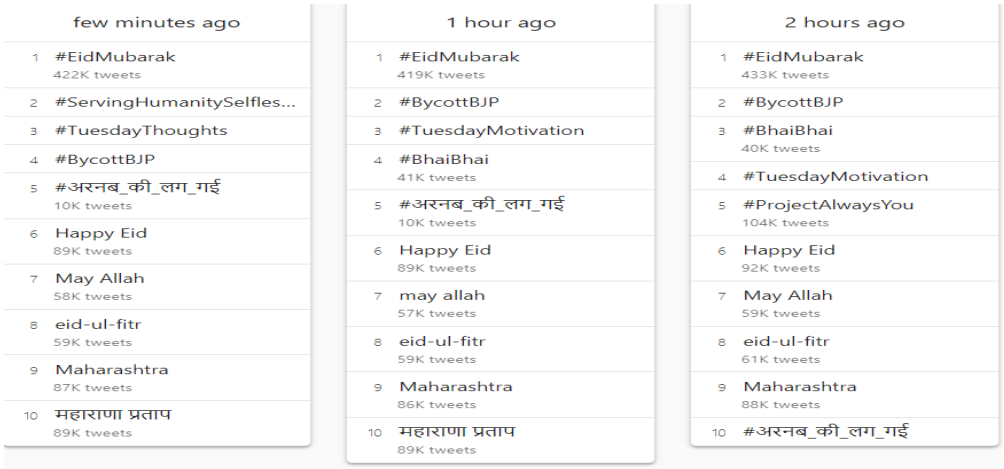


FIGURE 54: HASHTAGS

i. Google Trends

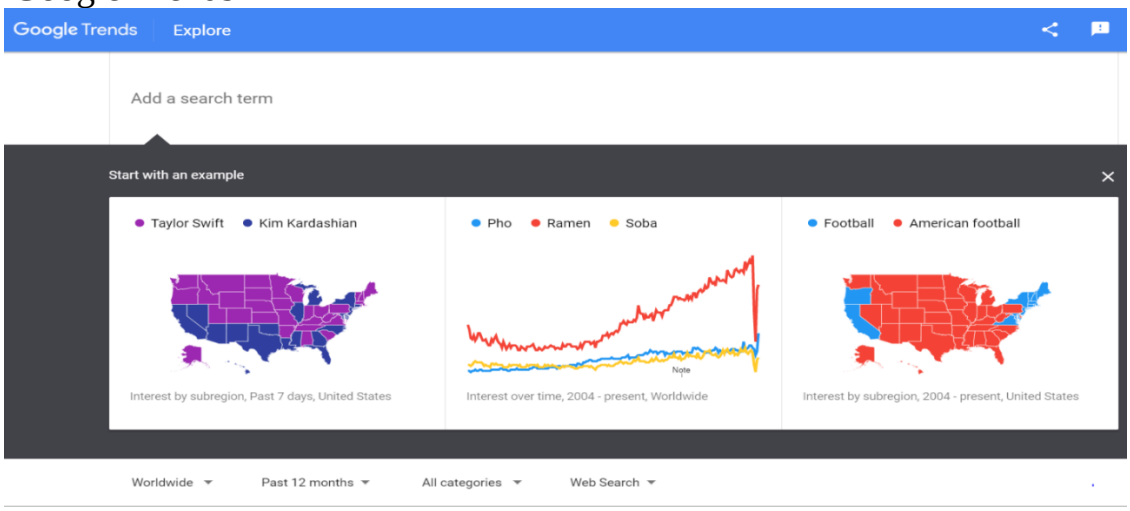


FIGURE 54: GOOGLE TRENDS

ii. X1 Social Discovery

X1 Social Discovery™ is the industry's first integrated solution specifically designed to enable eDiscovery and computer forensics professionals to effectively address social media content. X1 Social Discovery provides a powerful platform to collect, authenticate, search, review and produce electronically stored information (ESI) from popular social media sites, such as Facebook, Twitter, and LinkedIn. Built upon the industry-leading and patented X1 search technology and designed by experienced eDiscovery practitioners, searches are instantaneous and comprehensive. Automated searches are performed across multiple accounts and sources, including linked content, which often constitutes the most relevant aspect of individual social media streams. Unlike archiving and image capture solutions, X1 Social Discovery provides for case-centric litigation workflow from search and collection through production in searchable native format, while preserving critical metadata not possible through image capture, printouts, or raw data archival of RSS feeds.

X1 Social Discovery collects and indexes social streams relevant to a litigation case or investigation and provides for powerful fast-as-you-type search, link expansion, live previews, and instant search of the content behind embedded links. Existing data is collected (including Twitter content often years old) and all new content for identified streams are ingested continuously. Relevant data can be exported directly to the leading attorney review platform Relativity®, or to the most common load file formats. As merely viewing a Facebook or LinkedIn page in a browser can alter important metadata, X1 Social Discovery accesses social media sites in read-only mode to ensure evidence is not altered by the examiner. An MD5 hash is generated for all ingested social media items, metadata is captured and preserved at all times, and integrated logging and reporting is generated to support authentication and chain of custody consistent with best practices. We believe that X1 Social Discovery represents best practices to perform litigation holds for or otherwise capture Social Media content and to search and manage the content in a case-centric manner.

a. Main Features of X1 Social Discovery

Below we've listed the main features of Social Discovery.

- Facebook Capture Scanner
  Our Facebook Capture scanner allows users to login with an account to capture public user profile data or login with user credentials in order to capture credentialed user profile data. The Facebook Capture scanner supports parsing of data from Facebook User profiles, Pages, and Groups.
- Twitter Capture Scanner
  Our new Twitter Capture scanner allows users to login with an account to capture public Twitter data or login with user credentials in order to capture credentialed Twitter data. The

Twitter Capture scanner supports parsing of User Info, Tweets, Linked Content, Messages, and Followers/Followees. The Twitter Capture scanner also has the abiity to index based on Twitter Advanced Search criteria.

- YouTube Examiner - Public Information
  A YouTube Examiner account is able to index public videos from a targeted user or individual public videos.
- Tumblr Credentialed Account
  A Tumblr Credentialed account is able to index blog info, blog posts, and sub blogs of the Credentialed User. Please be aware that comments and private messages or fan mail are not available.
- Tumblr Examiner Account
  A Tumblr Examiner account is able to index public information from targeted users including blog info and blog posts.
- Web Collections
  Web collections give the user the ability to capture single web pages, or crawl an entire website. Additionally, there are options to bulk import data, configure crawls to add or exclude pages or types of files, and include sub domains, images and videos if desired.
- Web Mail Collections
  Social Discovery has the ability to index web mail and configurable IMAP accounts.

b. Key Benefits

- Collections
  Data is collected and indexed from social media streams, linked content and websites through APIs, webmail connectors and direct web navigation. X1 Social Discovery aggregates data from these multiple sources in real time, in a highly scalable and case-centric manner.
- Search
  Perform broad, unified searches across multiple accounts, social media streams and websites from a single interface. Linked content is automatically indexed and searched through the patented X1 fast-as-you-type search from one user interface. Results are aggregated for sorting, tagging and export consistent with standard eDiscovery, or investigative, workflow.
- Authentication
  MD5 hash values of individual items are calculated upon capture and maintained through export. Automated logging and reports are generated. Key metadata unique to social media & web streams are captured through deep integration with APIs provided by the publishers. This metadata is important to establishing chain of custody and also provides key evidence relevant to the substantive case as well as authentication.
- Production
  Maintain data in a searchable native format from collection through production, uniquely providing a complete platform to address social media in the same manner as devices, e-mail and e-documents. Deliver collected email in PST format while maintaining hierarchical structure.

c. Web Capture & Web Crawl

X1 Social Discovery has the ability to conduct single-page web capture and multiple-page web crawl, while adding this data to the overall collection so that it can be can reviewed alongside the rest of the social media content.

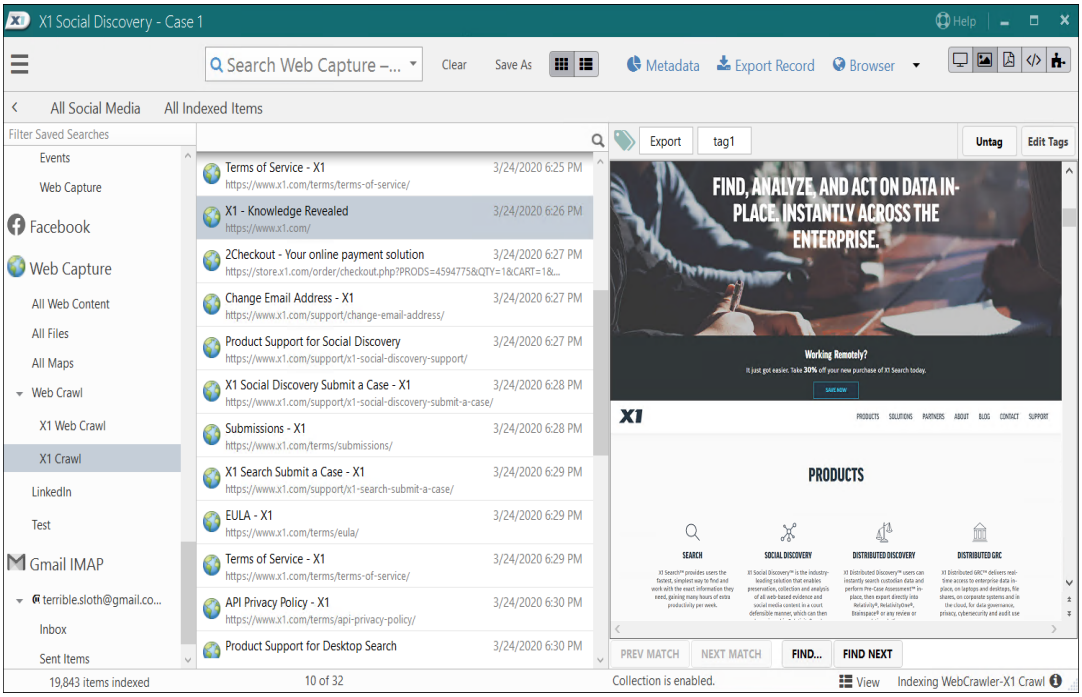


FIGURE 55: WEB CAPTURE & WEB CRAWL

d. Search and Highlight Content

Quickly search against both the metadata fields and the content of the referenced links using the X1 'fast as you type' search and instantly see highlighted matches while filtering your results

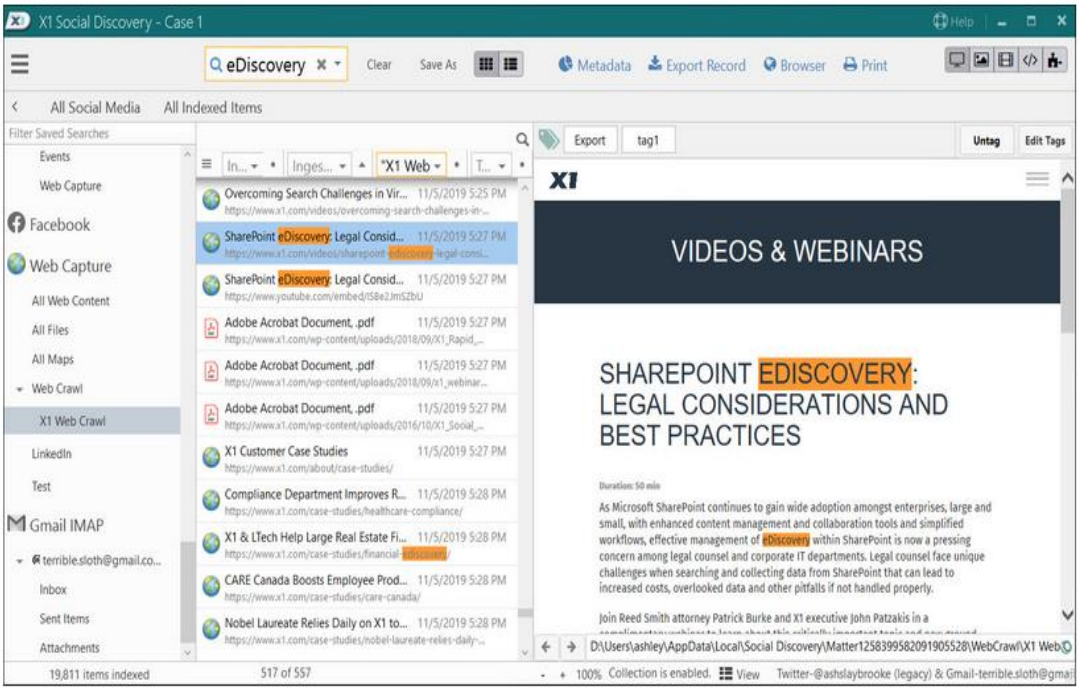


FIGURE 56: SEARCH AND HIGHLIGHT CONTENT

e. YouTube Video Download

X1 Social Discovery can also capture entire YouTube channels and individual videos including the metadata associated with the video

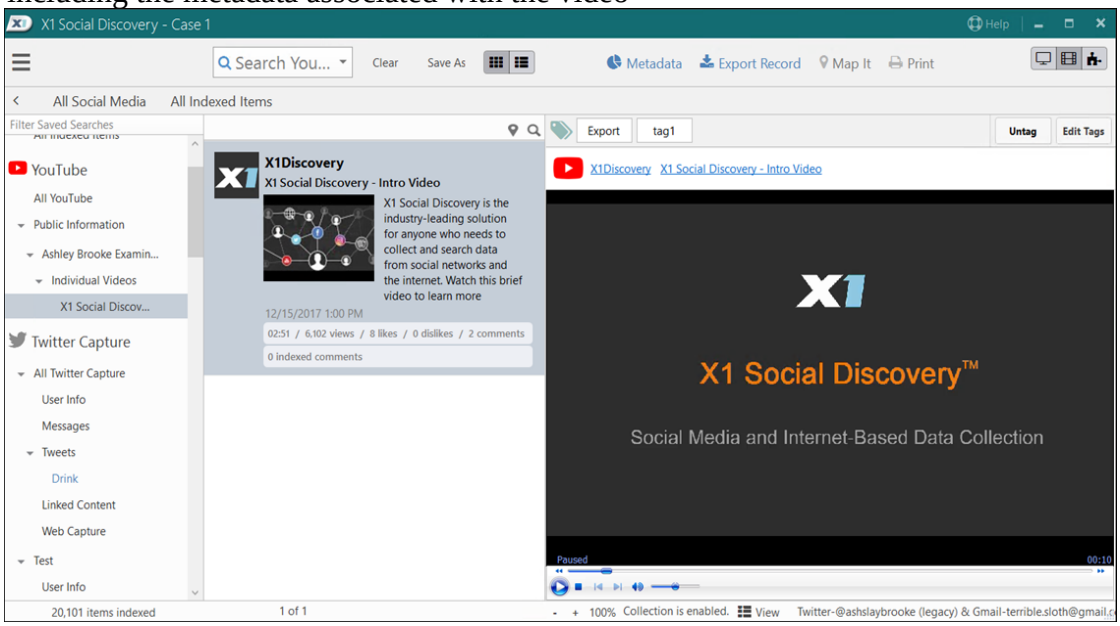


FIGURE 57: YOUTUBE VIDEO DOWNLOAD

f. Webmail Connector – IMAP

X1 Social Discovery's webmail connector indexes any email box which uses IMAP configuration, with pre-set collection options for Gmail, Yahoo, Outlook.com, and AOL

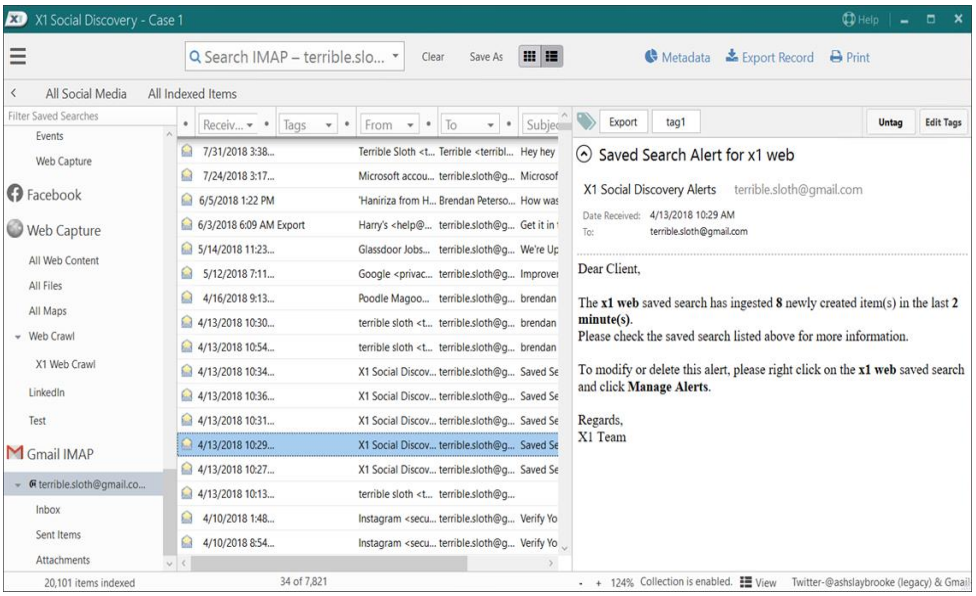


FIGURE 58: WEBMAIL CONNECTOR – IMAP

iii. Social Mention

Real-time social media search and analysis

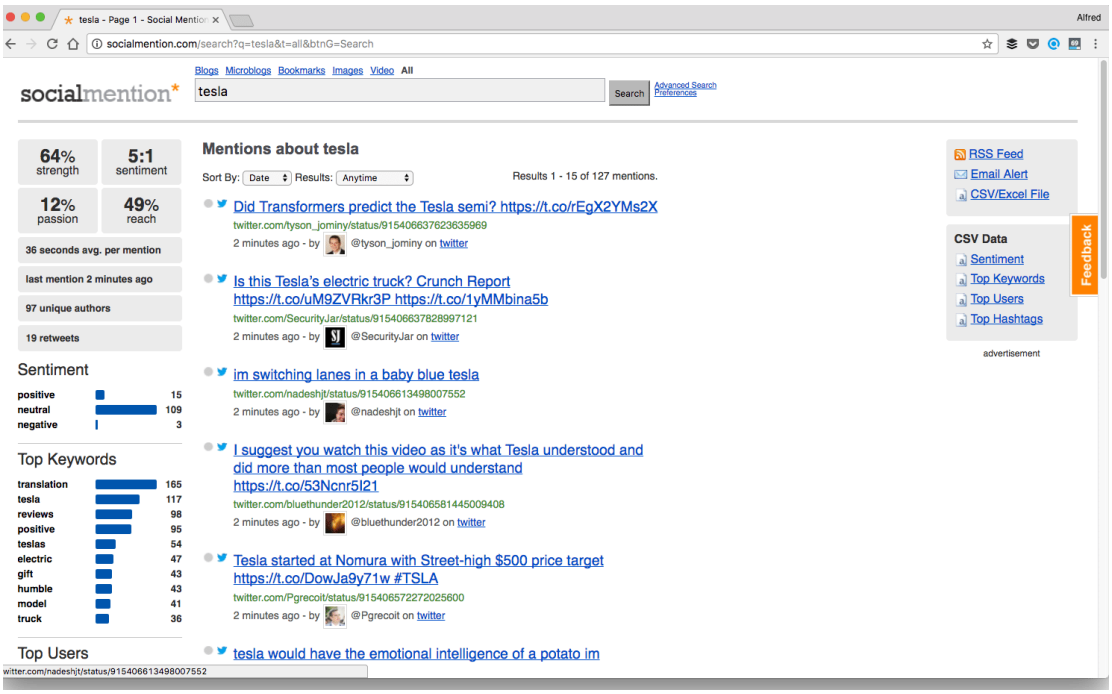


FIGURE 59: SOCIAL MENTION

Not to be confused with Mention above, Social Mention is a free social media search engine for user-generated content across the web. It lets you find and measure what people are saying about your brand and products on places such as Twitter, YouTube, and blogs.

Since an account is not required, I believe Social Mention doesn't save your searches.

Platforms supported: Twitter, Facebook, YouTube, Google, and other websites

iv. Keyhole

Hashtag tracking for Twitter, Instagram, and Facebook

Rather than finding individual mentions of your brand, Keyhole provides trends, insights, and analysis of your preferred hashtags, keywords, or accounts. This makes it better for gathering data and reporting results than replying your social media mentions.

If you want to test out its tools, it offers free hashtag, keyword, and account tracking.

Platforms supported: Twitter and Instagram

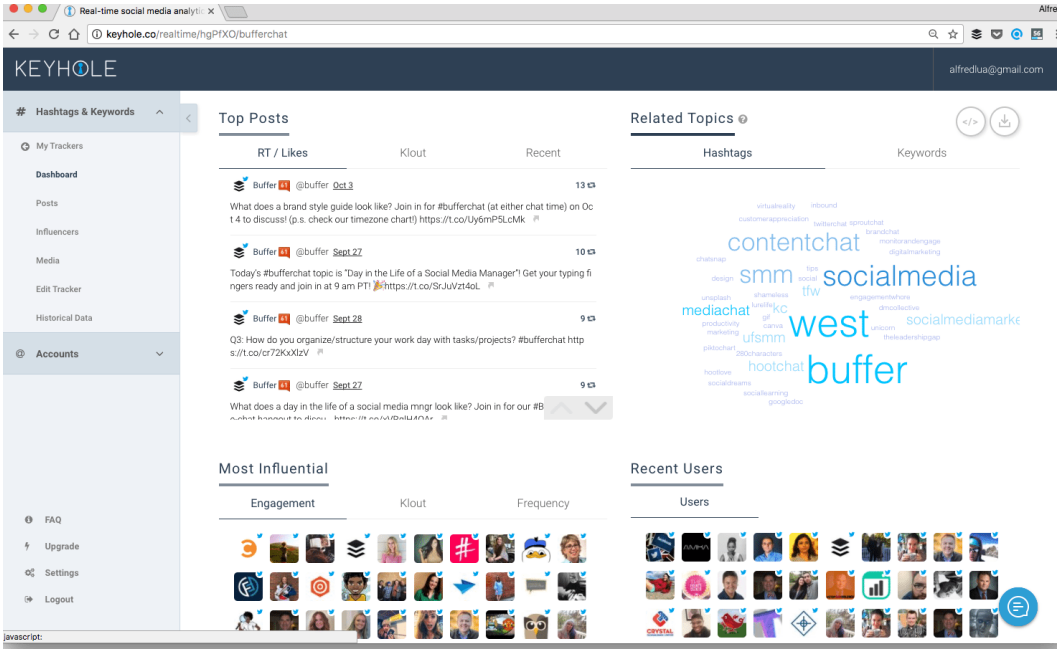


FIGURE 60: KEYHOLE

v. TweetDeck

The most powerful Twitter tool for real-time tracking, organizing, and engagement

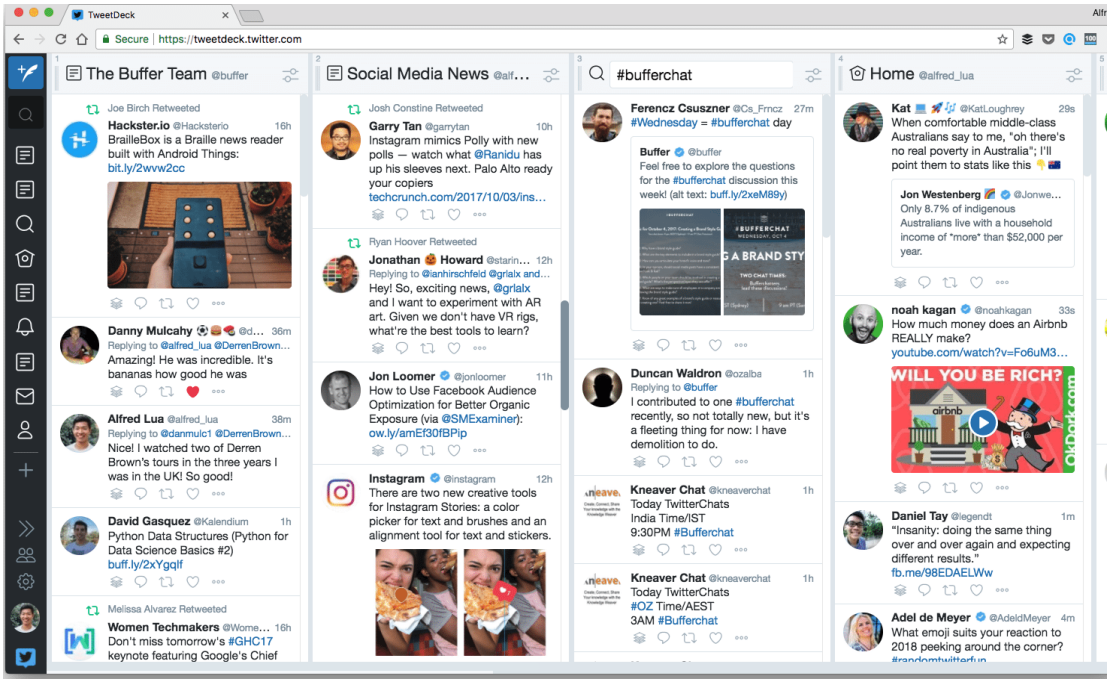


FIGURE 61: TWEETDECK

TweetDeck is the official Twitter management dashboard, where you can manage multiple Twitter accounts and monitor mentions, keywords, Twitter lists, and more in separate columns. And it's free!

Platform supported: Twitter

vi. Hootsuite

Effectively track topics that matter—then respond quickly

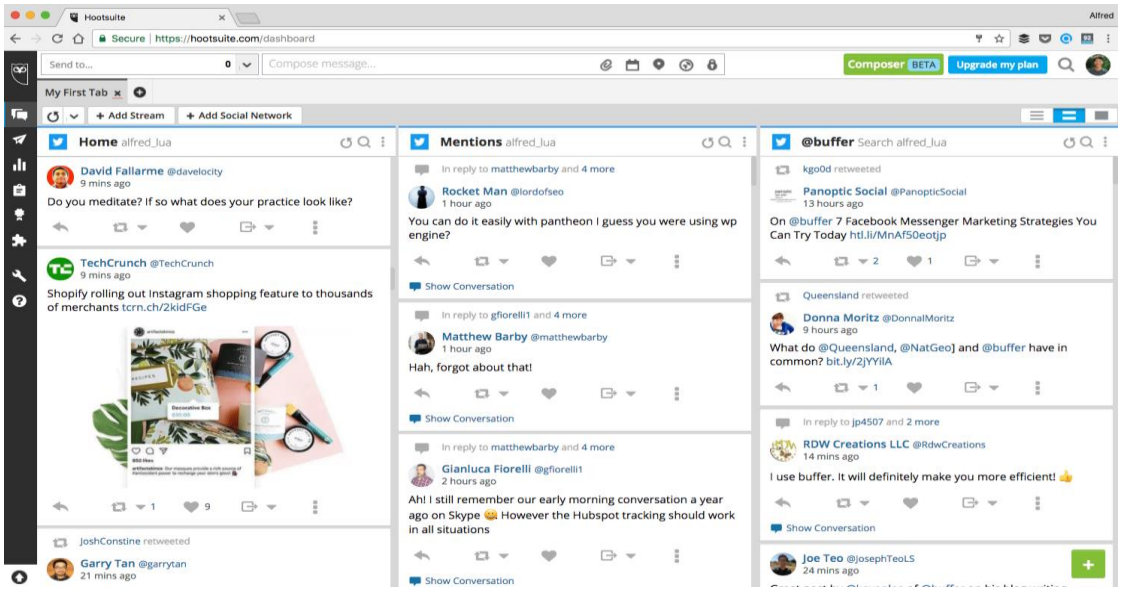


FIGURE 62: HOOTSUITE

Hootsuite's monitoring tool is part of its entire package of social media management tools. If you were to subscribe to one of their plans, you can also enjoy other features such as scheduling and analytics.

With Hootsuite, you can set up unlimited streams of social media content based on your mentions, selected keywords, hashtags, or locations. Furthermore, Hootsuite integrates with more than a hundred apps to help you do more from its dashboard.

Platforms supported: Twitter, Facebook, Instagram, LinkedIn, Google+, blogs, forums, and more

7. Sentiment Analysis

Sentiment analysis is a text analysis method that detects polarity (e.g. a *positive* or *negative* opinion) within text, whether a whole document, paragraph, sentence, or clause.

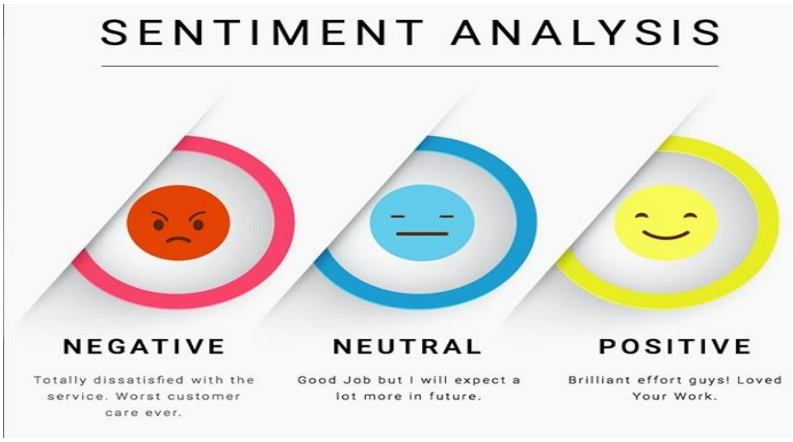


FIGURE 63: SENTIMENT ANALYSIS

sentiment analysis is the process of collecting and analyzing information on how people talk about your brand on social media. Rather than a simple count of mentions or comments, sentiment analysis considers emotions and opinions.

Social media sentiment analysis is sometimes called “opinion mining.” That’s because it’s all about digging into the words and context of social posts to understand the opinions they reveal.
Measuring social sentiment is an important part of any social media monitoring plan.

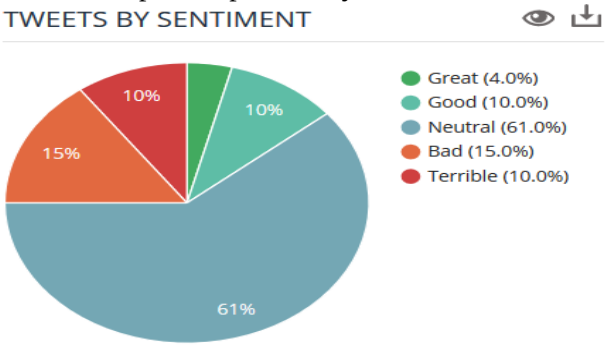


FIGURE 64: TWEETS BY SENTIMENTS

8. Tool for sentiment analyzing

i. Social Bearing

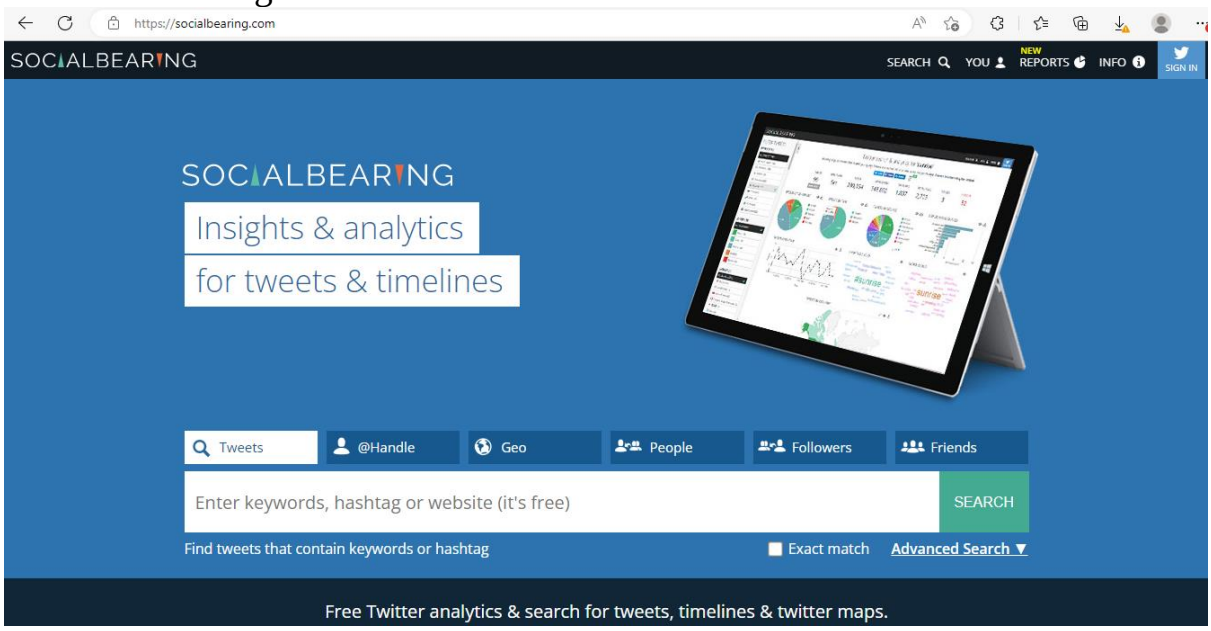


FIGURE 65: SOCIAL BEARING

For example, a sentiment analysis is done on Telangana, and we have got the result below

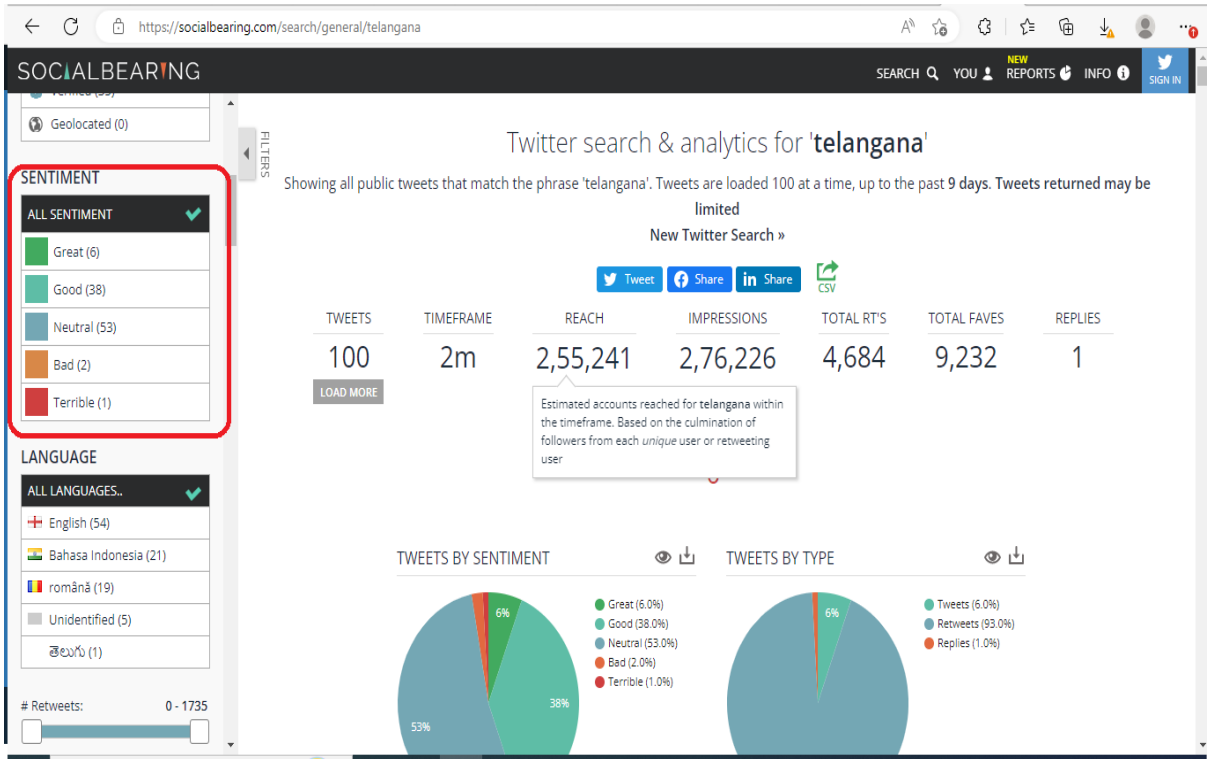


FIGURE 66: SOCIALBEARING -TWITTER ANALYTICS FOR TELENGANA

In the picture below you can see the sentiment analysis is done on Telangana and we have got 6 results as great, 38 as good, 58 as neutral, 2 as bad and 1 as terrible

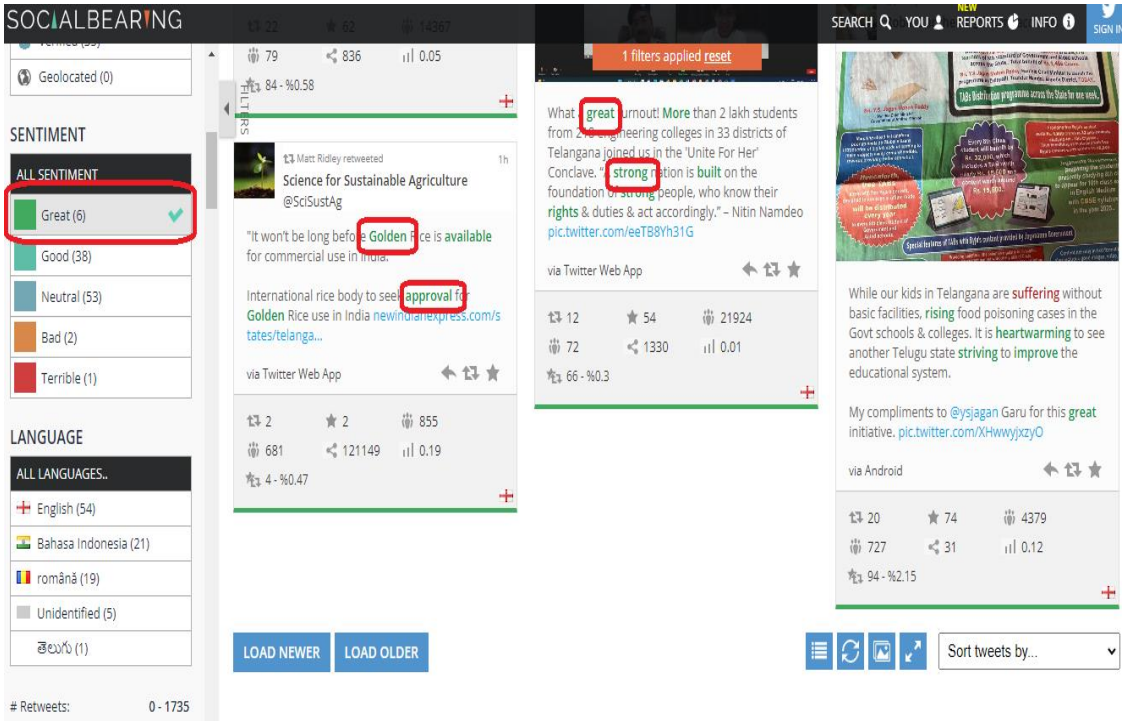


FIGURE 67: SOCIALBEARING -TWITTER ANALYTICS FOR TELENGANA

ii. BOT analysis – Botometer

Bots are operated on **social media networks**, and used to automatically generate messages, advocate ideas, act as a follower of users, and as fake accounts to gain followers themselves.

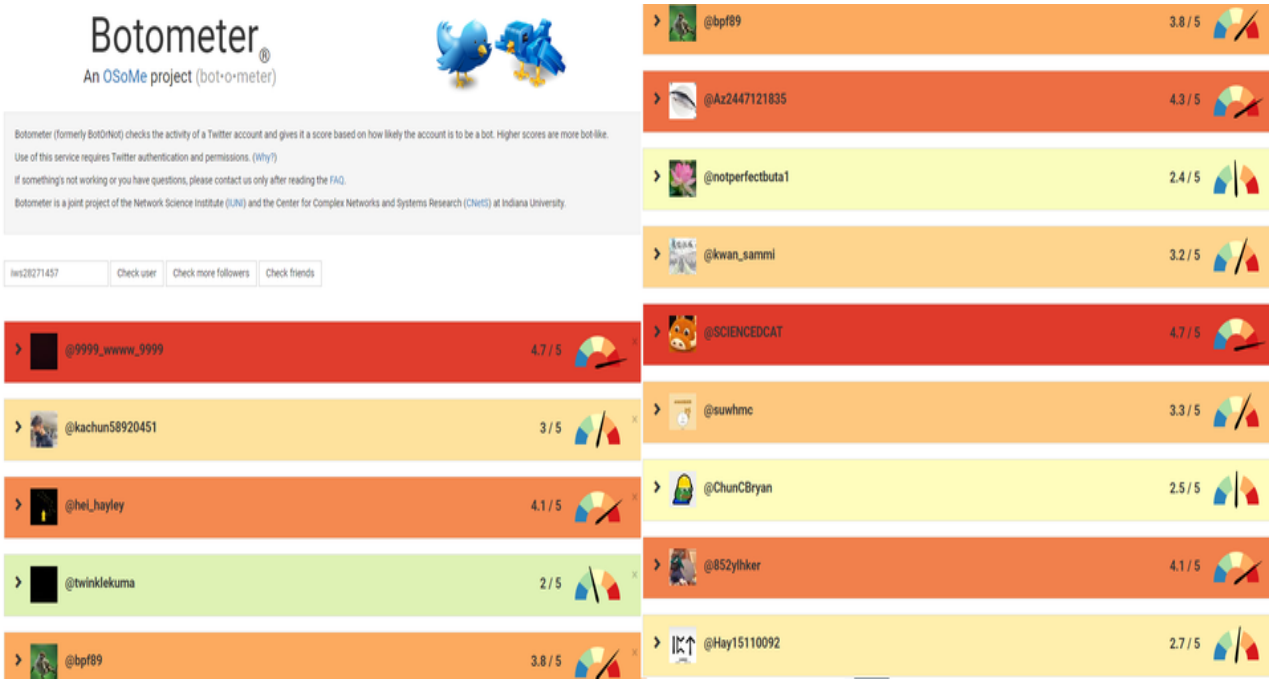


FIGURE 68: BOTOMETER

iii. Advance searching in Search Engines

Contrary to what you might think, advanced search strategies aren't just for **advanced users**. They're for **everyone**, whether you have a lot of experience with searching online or just a little. The only tool you need is **Advanced Search** page(s).

a. Google advance search

You can access it from the results page by clicking **Settings**.

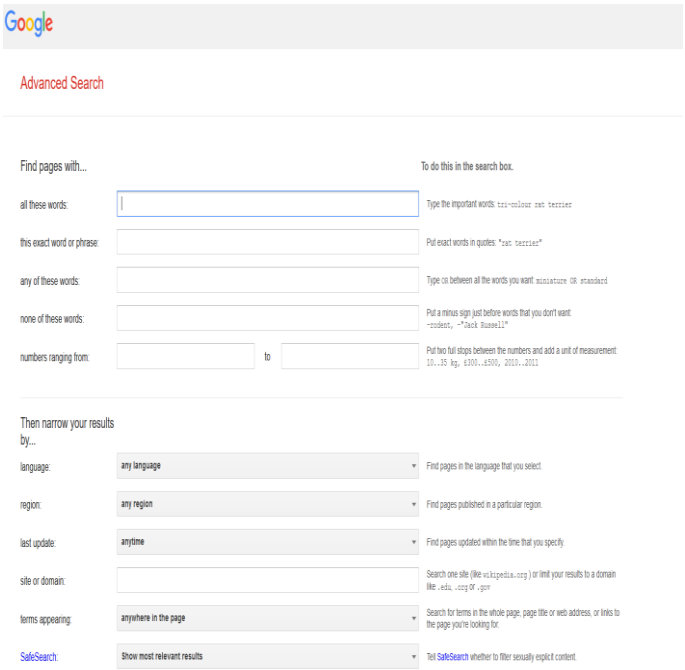


FIGURE 69: GOOGLE ADVANCE SEARCH

b. Twitter advance search

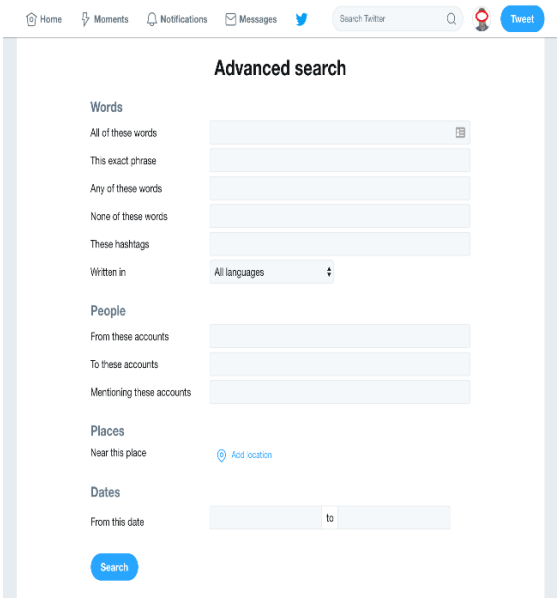


FIGURE 70: TWITTER ADVANCE SEARCH

c. Facebook advance search

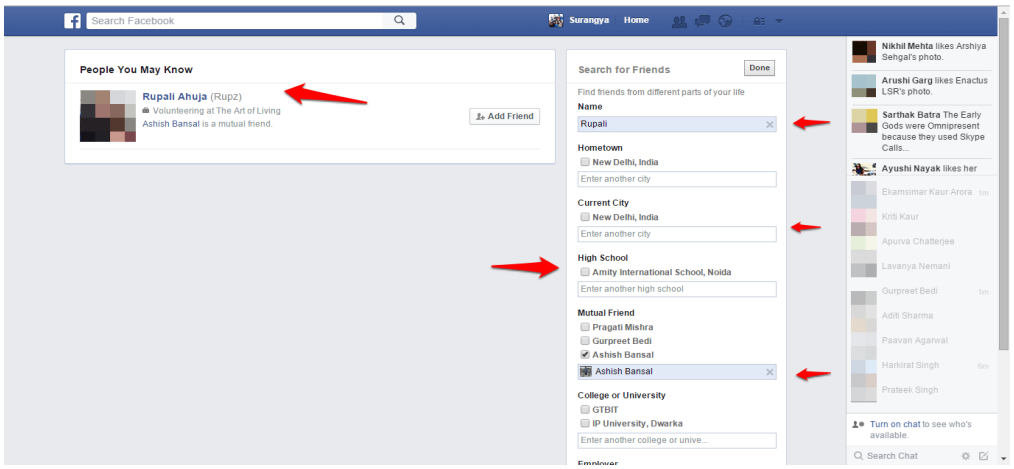


FIGURE 71: FACEBOOK ADVANCE SEARCH

d. YouTube advance search

FIGURE 72: YOUTUBE ADVANCE SEARCH

TOR Based Investigation

1. Dark Web Introduction

Internet is a nothing but huge library of websites which people use for various purposes. We use search engines like Google, Bing, DuckDuckGo for accessing these websites. But not all websites are accessible by these search engines or standard browsers like Edge, Chrome or Firefox. This restriction on accessing websites creates different layers of Internet. The hidden layer which needs special browser and search engine is known as Dark Web.

i. Layers of the Internet

There are basically three layers of Internet depending on how they can be accessed by users.

a. Surface Web

Surface web is that part of the World Wide Web which is easily available to the general public and accessible through standard web search engines. It is section of the internet that is being indexed by search engines.

The websites, webpages and information that user find using web search engine like Google, Yahoo, Bing, etc. only portray that user are exploring just the surface of the web. Search Engines use the crawling technique to index the webpages. Thus, the we generally access only surface web. Only 4% of the online content is available for the general public in the entire ocean of the web

b. Deep Web

Deep web is that content of World Wide Web which is not indexed by standard web search engines. The content of the deep web is behind HTTP forms, and it used for many general purposes such as web mail, online banking, and services for which users has to pay and which is protected by a paywall. Search engines won't provide access to the links that are deep inside the website even if the search is specific. Content of the deep web can be accessed by a direct URL or IP address using normal browsers, but it will require some type of authentication like password or other security measures to get access to its database.

c. Dark Web

The Dark Web is defined as a layer of information and pages that one can only get access to through so-called "overlay networks", which run on top of the normal internet. one need special software to access the Dark Web because a lot of it is encrypted, and most of the dark web pages are hosted anonymously.

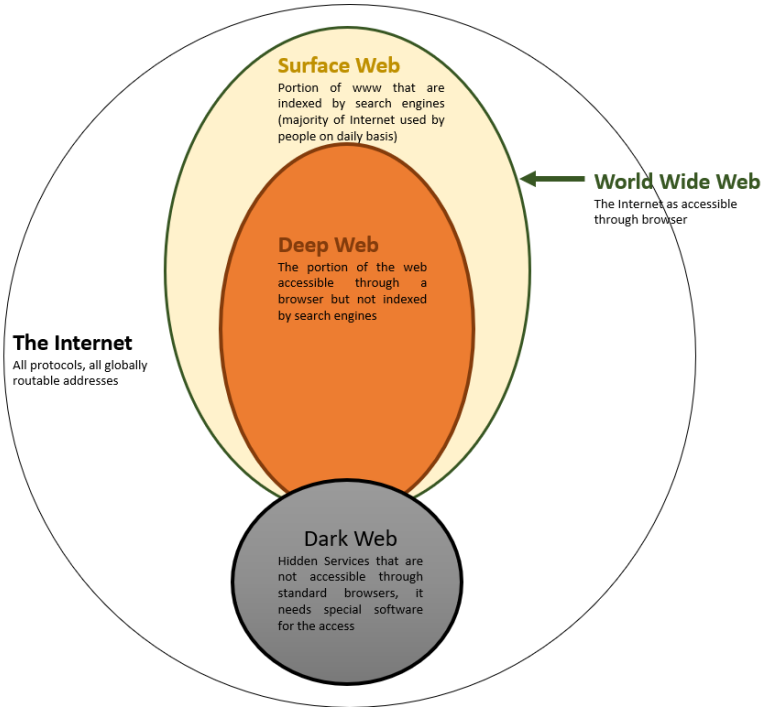


FIGURE 73: LAYERS OF INTERNET

2. Different Darkwebs

i. I2P

The Invisible Internet Project (I2P) is a private network layer that is entirely encrypted. It safeguards both your activities and your location.

I2P shields the user from the server and the server from the user. I2P traffic is entirely internal to the network. I2P traffic does not directly interface with the Internet. It's a layer that sits on top of the web. Between you and your peers, encrypted unidirectional tunnels are used. Nobody can see where the traffic comes from, where it goes, or what it contains. I2P also has a high level of resilience to censorship and pattern recognition. Location blocking is also decreased because the network relies on peers to route data.

The I2P network is run entirely by volunteers. Peers share a portion of their resources, especially bandwidth, with other network members. This eliminates the need for centralised servers to run the network.

ii. Freenet

Freenet is a piece of free software that allows you to share files anonymously, browse and publish "freesites" (web sites available exclusively on Freenet), and discuss on forums without fear of being censored. Freenet is decentralised to make it less vulnerable to attack, and it is highly difficult to identify when used in "darknet" mode, when users only connect with their friends.

Freenet node communications are encrypted and routed through other nodes, making it incredibly difficult to figure out who is seeking information and what it is about.

Users help the network by donating bandwidth and a piece of their hard drive (referred to as the "data store") for file storage. Files are retained or removed automatically according on their popularity, with the least popular being purged to create room for newer or more popular content. Because files are encrypted, the user can't easily see what's in his datastore, and hence can't be held responsible for it. This distributed data storage underpins chat forums, websites, and search functionality.

iii. TOR

Tor (The Onion Router) is an advancement of a program that was originally developed by the US Navy in the mid-1990s. It provides user greater anonymity online by encrypting internet traffic and passing it through a series of nodes.

When a user connects to Tor, his outgoing internet traffic is rerouted through a random series of at least three nodes (called relays) before routed its destination i.e., the website the user wants to visit. User's computer is connected to an entry node, and the traffic passes through is the exit node, after which it reaches its destination. Even incoming traffic is rerouted in the same way.

FIGURE 9 TORPROJECT.ORG

Along with the traffic passing through several nodes, the traffic is also encrypted multiple times. It might lose a level of encryption at each node, but it is never fully decrypted until it leaves the exit node for its destination.

Each node has an identifying IP address, which is encrypted. Only the IP address of final / exit node is visible to the destination website.

Currently Tor network is made up of about 7,000 relays (nodes) and 800 bridges. Bridges are similar to relays, but they are not recorded in the Tor directory. These are typically used by anyone who is unable to access the Tor network by regular means.

- **IP address privacy**
  On Tor network, user activity will never be traceable back to user IP address. Internet Service Provider (ISP) will not be able to view information about the contents of user traffic, including which website user is visiting. ISP would see only a Tor entry node, and the IP address of the Tor exit node.
- **Using Tor**
  The easiest way to use Tor is through the Tor browser. This is a Firefox-based application which can be downloaded and installed on computer. Its versions are available for MacOS, Windows, and Linux. Tor browser enables user to access Clearnet and ". onion" sites through the browser. If the use of the Tor browser is blocked, user may opt for a tor bridge. User first just needs to locate a bridge then configure it with the Tor browser.
- **Anonymity using Tor**
  Since all the traffic arriving at destination will appear to come from a Tor exit node, so will have the IP address of that node assigned to it. Because the traffic has passed through several additional nodes while encrypted, it can't be traced back to user.

It must be noted that using the Tor browser only protects traffic going through that particular connection and would not anonymize other apps on the computer. Also, user's ISP can see that user is using Tor. For improved privacy, user can use a VPN alongside the Tor browser.

- **Tor and the Darknet**
  Clear net websites can be accessed using Tor, but it can also access darknet websites, specifically. onion sites. These are sites which only people using the Tor browser can access, and have. onion as part of their URL. They are also referred to as "Tor hidden services." These websites are not indexed by search engines and can be difficult to find if users don't know where to look. Tor protects the anonymity of the operators of. onion sites, so it would be difficult to find out who is hosting the site. Hence the combination of both operator and user anonymity makes the darknet ideal for criminal activity.
- **Why to use Tor?**
  It is always presumed that Tor is used for illegal activities or to access dark web but it is not true. Tor can simply be used by any privacy-conscious user for day-to-day browsing on Clearnet sites, to help maintain user anonymity and privacy while online.
  There are also some professions where anonymity is necessary for various reasons and using Tor include helps them to achieve it:
  - Journalists
  - Law enforcement officers
  - Activists
  - Whistle blowers
  - Business executives
  - Bloggers
  - Militaries
  - IT professionals

- **Legality of Tor**
  Tor is completely legal, even if it has been or is now restricted in some countries. Though ISPs have been reported to throttle the bandwidth of Tor users and have even contacted customers to tell them to stop using the Tor browser. Users might be questioned by ISPs regarding which websites they are connecting to through Tor.
  Authorities themselves at times become suspicious of Tor users and conduct investigations into their activities on those grounds alone. However, there haven't been any reports of penalties or prosecutions relating to Tor use.

3. Illegitimate Activities on The Dark Web

The Dark Web allows its customers to anonymously reach to its websites utilizing applications like TOR. This way they can escape from monitoring and their identities remain concealed. Notwithstanding the way that online anonymity makes way for customer privacy, it in like manner opens approaches to a lot of criminal activities. Some of these are mentioned below:

1. **Counterfeit Currency:**
   Many counterfeit currency distributors are active on Dark Web, who sells fake currency with a guarantee of surpassing standard ultraviolet light checks successfully.
2. **Forged Documents:**

Several sites on the Dark Web provides fake passports, immigration papers, driving licences and other identity documents for any country in the world. These services allow notorious people to acquire fake citizenship as per their needs. Other forged documents that are readily available include citizenship papers, fake IDs, college diplomas and even diplomatic identity cards.

3. **Drugs:**
   On the Dark Web, you may buy a variety of illicit substances of various types and quality. On Dark Web marketplaces, even illegal medications and pharmaceuticals like Ritalin and Xanax can be found. Silk Road is an example of a Dark Web marketplace which became famous for the wide range of drugs that were sold through it in huge amounts.
4. **Stolen Confidential Information:**
   This involves the purchase and sale of stolen credit card numbers, bank account numbers, and even personal data such as social security numbers. Apart from physical credit or debit cards, bank accounts can also be purchased at different prices in this Dark world.
5. **Hackers:**
   Hackers can easily buy sophisticated malwares and even get paid by interested parties to carry out any kind of online hacking attacks against specific governments, organizations or individuals.
6. **Arms and Ammunitions:**
   Illegal trade of explosives, weapons and firearms is also carried out openly. These services ensure that the specified products are delivered to the customer in special packaging that is easily scanned and security checked.
7. **Human Organ Trafficking:**
   Human organ trafficking is another business which has its roots deeply penetrated in the Dark Web. Organs such as kidneys, liver, heart, and eyeballs are routinely purchased in these underground markets.
8. **Terrorist Activities:**
   From secret communication and propaganda to recruitment and training for terrorist, everything that cannot be openly done on the Visible Web, is carried out through Dark Web.
9. **Child Pornography:**
   The Dark Web has also become famous destination for hosting child abuse videos as well as child pornography.

The list of illicit activities carried out using Dark Web is endless. Criminals thrive in this secret world because procedures to trace their footprints are complex and tracking them is much more difficult. The adoption of Bitcoin and other cryptocurrencies as a means of payment is a crucial element driving the proliferation of Dark Web-based crimes.

4. Gathering information about TOR nodes/ relays:

- To ensure whether given IP address belongs to TOR network, the IP addresses can be searched on TOR directory if IP is present in list means it is part of TOR network. link for tor directory is:

  https://www.dan.me.uk/torlist/
- To verify if given IP address was used as Tor Relay Node on Specific Date:

  https://metrics.torproject.org/exonerator.html
- To gather information about TOR nodes:

https://torstatus.rueckgr.at/

- To find repository of TOR Relays in India:
  https://metrics.torproject.org/rs.html

5. Crawling websites of Tor

The technique of indexing data on online sites using a software or automated script is known as web crawling. Web crawlers, spiders, spider bots, and crawler are all names for automated scripts or programmes that crawl the website. Web crawlers save pages to be processed by a search engine, which indexes the pages so that users may find information more quickly. A crawler's job is to figure out what's on each page. This allows users to quickly access any information on one or more pages.

On the dark web, website URLs are generally made up of a randomized string of letters and digits, followed by the ". onion" subdomain. Standard browsers such as Chrome and Safari are unable to resolve these websites, which need the use of the TOR browser.

Crawling Tor website will index links to websites, email addresses, crypto currency addresses present on the websites also it will gather information about server where website might be hosted.

Some tools are enlisted below which can be used to crawl ". onion" websites:

- OnionScan
- OnionOff
- Onion-nmap
- TorBot
- TorCrawl
- Onion Ingestor

6. Evidences related to TOR in windows system

i. RAMDUMP:

RAMDUMP is nothing but copy of the volatile memory of the system taken during live acquisition of the system. When it comes to investigation related to darkweb majority of the evidences can be found in RAM, hence taking RAMDUMP will help course of investigation in multiple ways.

Following evidences can be expected to find in RAMDUMP:

- URL of the websites visited by the user
- Emails addresses on which user communicated
- All recent activities along with recently composed mails, personally identifiable details, file names that are attached with mail etc.
- Crypto currency addresses
- Passwords of some accounts which user might have accessed recently

ii. TOR browser

When user install TOR browser it creates folder with name "Tor Browser" in the location which user has selected for installation. This folder contains multiple sub folders using which we can gather some evidences.

Bookmarks of the TOR browser can be extracted from "places.sqlite" file which is present in the folder" Profile.default". Path of this folder is:

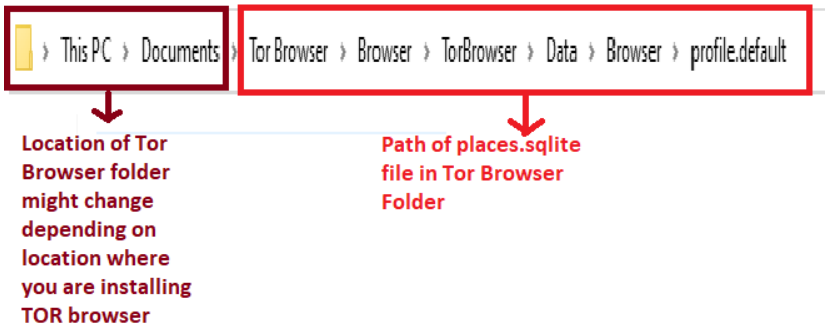


FIGURE 74: PATH FOR PLACES.SQLITE FILE

Date & Time of last use of TOR can be found in "state" file which is present in following location:

FIGURE 75: PATH TO "STATE" FILE

State file should be opened using notepad to see the timestamp:

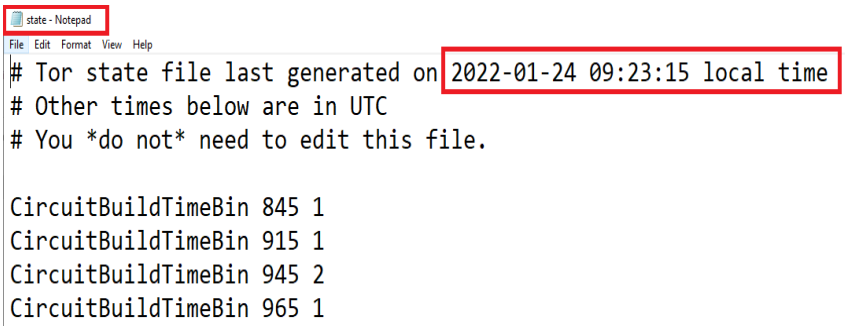


FIGURE 76: STATE FILE IN NOTEPAD

If user has configured any restricted Entry or Exit node then that information can be gathered from "torrc" file present at following location:

FIGURE 77: PATH TO "TORRC" FILE

Open "torrc" file using notepad:

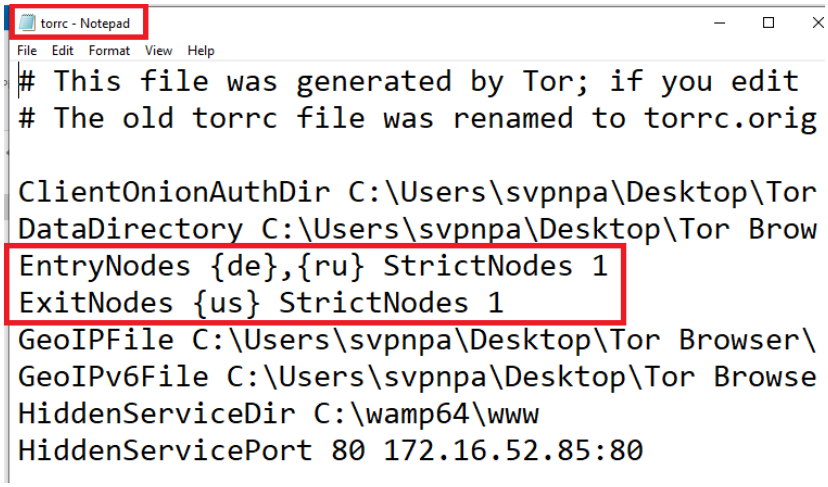


FIGURE 78: TORRC FILE IN NOTEPAD

7. Taking archive of Tor Websites:

Tor websites are very unstable in nature they might go down at any point of time considering the security reasons. Hence in this situation if investigation related to some website is ongoing and that website goes down it might create hindrance for further investigation. To avoid this circumstances IO can take archive of the TOR website so that even if the website goes down in future, he can refer to the offline copy of the website to continue with investigation. There are few tools which can be sued for the same purpose.

i. archive.today:

You can just open "archive.today" website on any browser. Paste the url of the ".onion" site of which you want to take archive. And add ".pet" extension after ".onion" and click on save.

FIGURE 10 ARCHIVE.TODAY

ii. Hunchly

It is the paid tool which can keep record of all your investigation activities on darkweb once you enable capture of the browser which you are using for investigation.

Dashboard of Hunchly tool:

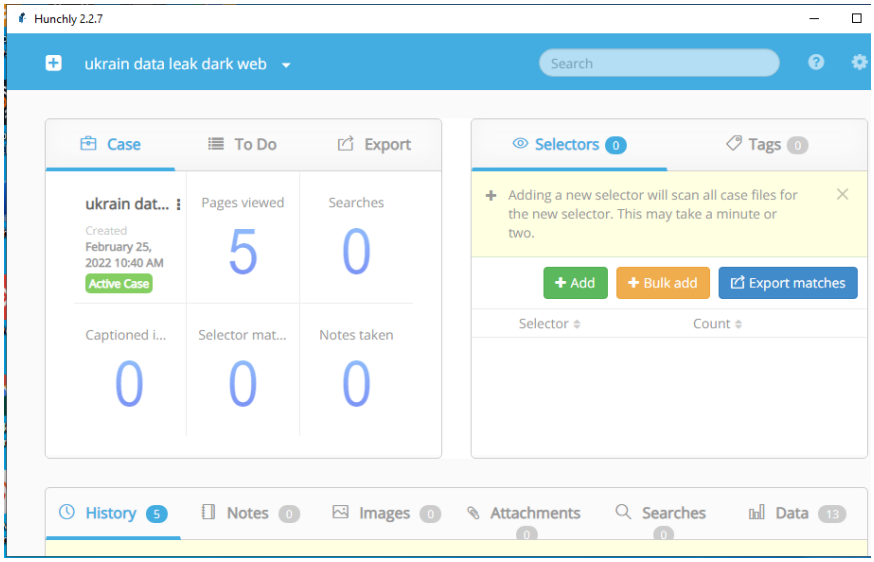


FIGURE 80: HUNCHLY

I. Configuring Entry/Exit Nodes:

To configure entry/exit nodes, first open 'torrc' file from the Tor Browser folder, Path for the same is as follows:

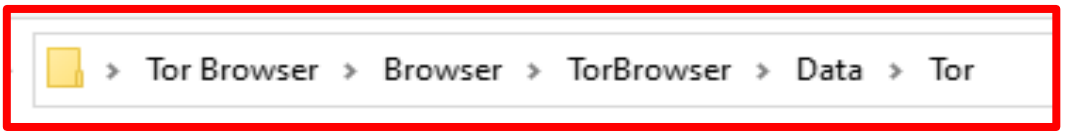


FIGURE 81: PATH TO TORRC FILE

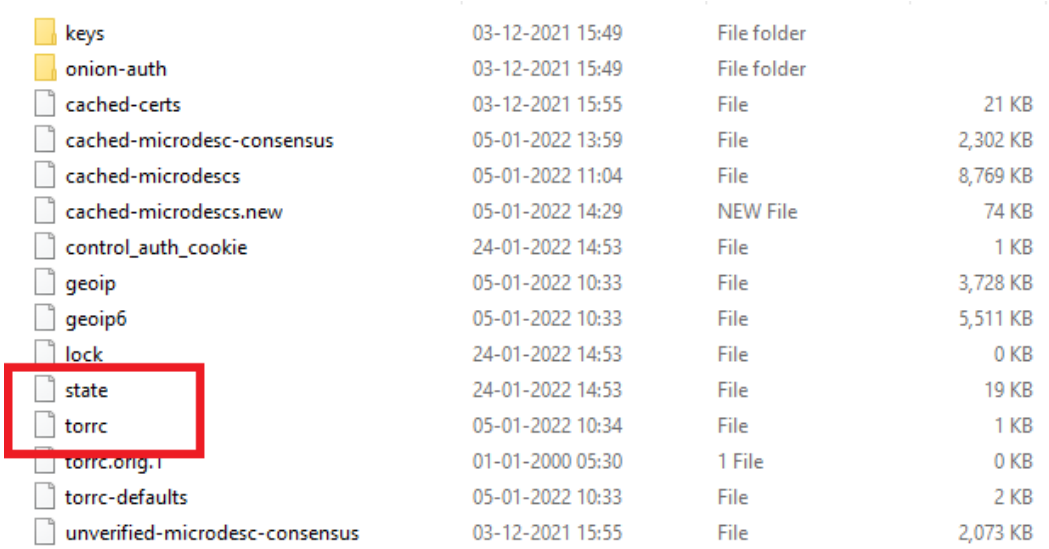


FIGURE 82: TORRC FILE

Add the following lines in **torrc** file of Tor Browser:

- To use entry nodes only from specific country

  EntryNodes {in} StrictNodes 1

  EntryNodes {in},{au},{us} StrictNodes 1

- To use exit nodes only from specific country

ExitNodes {in} StrictNodes 1

ExitNodes {in},{au},{us} StrictNodes 1

- If you do NOT want to use nodes from specific country

ExcludeEntryNodes {cn},{pk} StrictNodes 1

ExcludeExitNodes {us},{cn},{pk} StrictNodes 1

ExcludeNodes {cn},{pk} StrictNodes 1

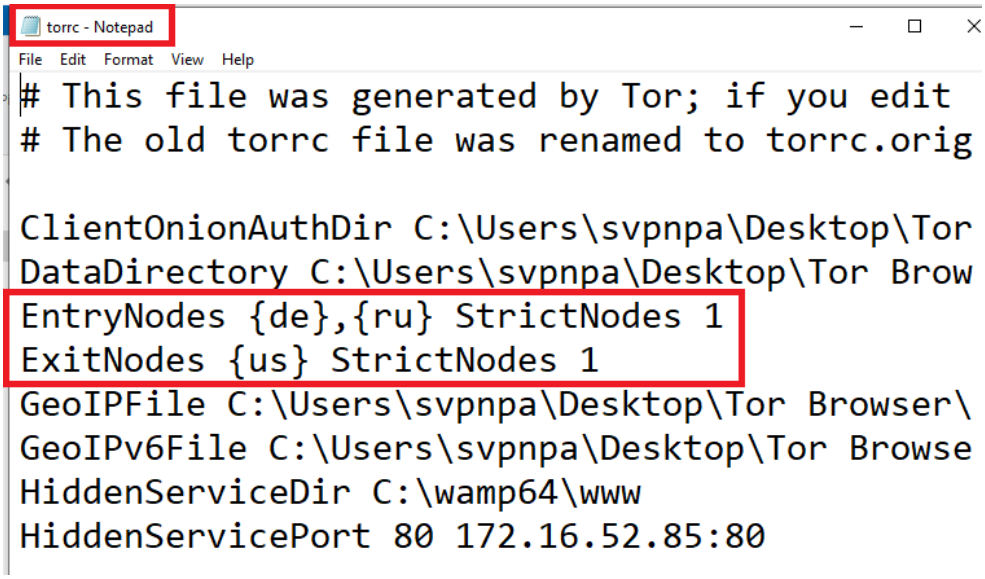


FIGURE 83: TOR NODE CUSTOMIZATION

Investigation of Cryptocurrency

1. Basic understanding of Crypto Currency

The idea of 'cryptocurrencies' started its advent from 1998 itself. The first known attempt for creating a digital cryptocurrency was B-Money and Bit Gold, but both never came into reality.

Cryptocurrencies are the digital or virtual currencies working on the cryptographic principles. It doesn't have any physical existence or they are not tangible. They only exist as a set of programming codes. Yet they are capable of providing high security and usability than many existing currencies.

Cryptocurrency works on blockchain technology; we have already seen how blockchain works. In the case of cryptocurrency, the ledger keeps the track of cryptocurrency that is generated and transacted across the network. Every individual in a particular blockchain will have a unique account Id/address. The cryptocurrency is always associated with this account (Currency is Debited and Credited to this account).

People can manage their account through the application called wallets. Through the wallets, anyone can make the transaction to anyone on the network (both the sender and receiver must have an account). The transactions are verified by nodes and added to the blockchain ledger. So, the immutable and encrypted ledger of blockchain is the backbone of cryptocurrency.

All features of blockchain are also applicable to cryptocurrency; the encryption mechanism, peer to peer network, and no central authority/central server to control. Each cryptocurrency will work on a blockchain protocol. One of the most famous cryptocurrencies is bitcoin which works on the bitcoin blockchain. And ether is another fast-growing cryptocurrency which runs on Ethereum protocol. While comparing with the traditional currencies, the cryptocurrencies provide highly anonymous nature for participants. The only visible identity of a user will be his account ID, rest everything will be encrypted. The participants will not have any idea about the real identity of a user.

2. Evolution of Cryptocurrency

Digital currencies have always been an active area of research for many decades. Early proposals to create digital cash go as far back as the early 1980s.

- In **1982**, **David Chaum**, a computer scientist, and cryptographer proposed a scheme that used blind signatures to build untraceable digital currency. This research was published in a research paper, Blind **Signatures for Untraceable Payments**.
  In this scheme, a bank would issue digital money by signing a blind and random serial number presented to it by the user. The user could then use the digital token signed by the bank as currency. The limitation of this scheme was that the bank had to keep track of all used serial numbers. This was a central system by design and required to be trusted by the users.
- Later on, in **1988**, **David Chaum and others** proposed a refined version named **e-cash** that not only used a blinded signature, but also some private identification data to craft a message that was then sent to the bank.
  This scheme allowed the detection of double spending but did not prevent it. If the same token was used at two different locations, then the identity of the double spender would be revealed. e-cash could only represent a fixed amount of money.
- **Adam Back,** a cryptographer and now CEO of Blockstream, who is involved in blockchain development, introduced **hashcash** in **1997**. It was originally proposed to control email spam. The idea behind hashcash was to solve a computational puzzle that was easy to verify but comparatively difficult to compute. The idea was that for a single user and a single email, the extra computational effort was negligible, but someone sending a large number of spam emails would be discouraged as the time and resources required to run the spam campaign would increase substantially.
- In **1998**, **B-money** was proposed by **Wei Dai,** a computer engineer who used to work for Microsoft, introduced the idea of using Proof of Work (PoW) to create money. The term Proof of Work emerged and got popular later with Bitcoin, but in Wei Dai's B-money an idea of creating money was introduced by providing a solution to a previously unsolved computational problem. This concept is similar to PoW, where money is created by broadcasting a solution to a previously unsolved computational problem.
  A major weakness in the given system was that an adversary with higher computational power could generate unsolicited money without allowing the network to adjust to an appropriate difficulty

level. The system did not have detailed account on the consensus mechanism between nodes and several security issues such as Sybil attacks were not addressed.

- In contemporary time with Wei Dai, **Nick Szabo**, a computer scientist introduced the concept of **BitGold**, which was also based on the PoW mechanism but had the same problems as B-money with the exception that the network difficulty level was adjustable.
- **Tomas Sander and Amnon Ta-Shma** from the International Computer Science Institute (ICSI), Berkley introduced an **e-cash scheme** under a research paper named **Auditable, Anonymous Electronic Cash** in 1999. It was first time used in Merkle trees to represent coins and Zero-Knowledge Proofs (ZKPs) to prove the possession of coins.
  This scheme required a central bank to keep record of all used serial numbers. This scheme allowed users to be fully anonymous. This was a theoretical design which was not practical to implement due to inefficient proof mechanisms.
- **Reusable Proof of Work (RPoW)** was introduced in **2004** by **Hal Finney**, a computer scientist, developer and first person to receive Bitcoin from Satoshi Nakamoto. It used the hashcash scheme by Adam Back as a proof of computational resources spent to create the money. This was also a central system that kept a central database to keep track of all used PoW tokens. This was an online system that used remote attestation made possible by a trusted computing platform (TPM hardware).
  All the above-mentioned schemes were intelligently designed but were weak from one aspect or another. Specifically, all the schemes which rely on a central server required to be trusted by the users.
- In **2008**, **Bitcoin** was introduced through a paper called, Bitcoin: A Peer-to-Peer Electronic Cash System. It was written by **Satoshi Nakamoto**, which is believed to be a anonymous name, hence the true identity of Bitcoin inventor is unknown and subject of much speculation.

The first key idea introduced in the paper was of a purely peer-to-peer electronic cash that does need an intermediary bank to transfer payments between peers.

Bitcoin is built on decades of cryptographic research such as the research in Merkle trees, hash functions, public key cryptography, and digital signatures. Moreover, ideas such as BitGold, B-money, hashcash, and cryptographic time stamping provided the foundations for bitcoin invention. All these technologies are cleverly combined in Bitcoin to create the world's first decentralized currency.

The key issue that has been addressed in Bitcoin is an elegant solution to the Byzantine Generals' Problem along with a practical solution of the double spend problem.

The below figure shows analysis of the selected cryptocurrencies is based on the information available to the public via the internet.

Name	Symbol		Market Cap[122]	Supply limit[123]
Bitcoin		BTC	$124.969.093.161	21 million
Ethereum		ETH	$57.462.517.858	TBD[124]
Ripple		XRP	$23.790.387.789	100 billion
Bitcoin Cash		BCH	$17.159.025.225	21 million
Litecoin		LTC	$6.704.709.572	84 million
Stellar		XLM	$5.128.373.973	100 billion
Cardano		ADA	$5.034.129.651	45 billion
IOTA		MIOTA	$4.038.240.572	2,779,530,283,277,761
NEO		NEO	$3.386.383.000	100 million
Monero		XMR	$2.626.586.260	18,4 million
Dash		DASH	$2.592.894.544	17.74 – 18.92 million[125]

FIGURE 84: SOME CRYPTOCURRENCIES

3. Types of Wallets

The wallet is a software application which is used to store private or public keys and Bitcoin address. It performs multiple functions, such as receiving and sending bitcoins. Nowadays, software usually offers both functionalities: Bitcoin client and wallet. On the disk, the Bitcoin core client wallets are stored as the Berkeley DB file.

Private keys are generated by randomly choosing a 256-bit number by wallet software. Private keys are used by wallets to sign the outgoing transactions. Wallets do not store any coins, and there is no concept of wallets storing balance or coins for a user. In fact, in the Bitcoin network, coins do not exist; instead, only transaction information is stored on the blockchain which are then used to calculate the number of bitcoins.

There are different types of wallets that can be used to store private keys. As a software program, they also provide some functions to the users to manage and carry out transactions on the Bitcoin network.

- **Non-deterministic wallets**

It contain randomly generated private keys and are also called *just a bunch of key wallets*. The Bitcoin core client generates some keys when first started and generates keys as and when required.

- **Deterministic wallets**

Here keys are derived out of a seed value via hash functions. This seed number is generated randomly and is commonly represented by human-readable mnemonic code words.

- **Hierarchical Deterministic wallets**

Hierarchical Deterministic (HD) wallets store keys in a tree structure derived from a seed. The seed generates the parent key (master key), which is used to generate child keys and, subsequently, grandchild keys. Key generation in HD wallets does not generate keys directly; instead, it produces some information (private key generation information) that can be used to generate a sequence of private keys. The complete hierarchy of private keys in an HD wallet is easily recoverable if the master private key is known.

- **Brain wallets**

The master private key can also be derived from the hash of passwords that are memorized. The key idea is that this passphrase is used to derive the private key and if used in HD wallets, this can result in a full HD wallet that is derived from a single memorized password. This is known as a brain wallet.

- **Paper wallets**

A paper-based wallet with the required key material printed on it. It requires physical security to be stored.

- **Hardware wallets**

Hardware wallet suggests the use of tamper-resistant device to store keys. It is the most secure way of storing any amount of cryptocurrency. There have been no verifiable incidents of money being stolen from a hardware wallet. Unlike paper wallets, which must be imported to software at some point, hardware wallets can be used securely and interactively. Moreover, they are immune to computer viruses, the funds stored cannot be transferred out of the device in plaintext, and in most instances, their software is open source.

FIGURE 85: HARDWARE WALLET

Name	Price	Features
Ledger Nano S	58 €	Screen; two buttons that you need to press simultaneously to confirm a transaction, which prevents hackers from hacking into it and confirming payments; PIN code; box ships with an anti-tampering seal
TREZOR	$99	Screen; two buttons; wallet can be backed up with up to 24 words + passphrase; PIN code
KeepKey	$99	Screen; digital screen and metal body; PIN code; number randomization; can be backed with up to 24 words; recovery can be done with

- **Online wallets**

Online wallets are stored entirely online and are provided as a service usually via the cloud. They provide a web interface to the users to manage their wallets and perform various functions such as making and receiving payments.

Service	Features
Coinbase	One-stop solution, an exchange integrated with a wallet
Lumi Wallet	Free, easy, client-side interface to generate one wallet that supports BTC, ETH and plenty of ERC20 tokens
Circle	Users can store, send, receive and buy Bitcoins
Blockchain	One of the most popular web-based wallets
Strongcoin	Offers a hybrid wallet, which lets you encrypt your private address keys before sending them to its servers
Xapo	A simple Bitcoin wallet, with the added security of a cold-storage vault

- **Mobile Wallets**

Mobile wallets are applications installed on mobile devices. They can provide various methods to make payments, most significantly the ability to use smartphone cameras to scan QR codes quickly and make payments. Mobile wallets are available for the Android platform and iOS, for example, Blockchain, breadwallet, Copay, and Jaxx.

Name	Operating System	Features
FreeWallet	iOS, Android	Cold storage, withdraw from and to any cryptocurrency
Edge	iOS, Android	Zero-knowledge, single sign-on, one-touch 2 factor authentication
Atomic Wallet	iOS, Android	Very user-friendly, 500+ assets, instant exchange, buy crypto option, custody-free app.

Lumi Wallet	iOS, Android	Secure and easy crypto wallet & exchange for mobile
Blockchain Wallet	iOS, Android	Hierarchical deterministic, enable to browse Bitcoin merchants in your area, open source software
Copay	iOS, Android, Windows Mobile	Can have multiple users, so the group approves each transaction to send money, open source software
Jaxx	iOS, Android	Cold storage, no verification required
Mycelium	iOS, Android	Cold storage, hierarchical deterministic, open source softwar

- **Desktop Wallets**

Desktop wallets are downloaded and installed onto your computer, storing your private keys on your hard drive. By definition, they are more secure than online and mobile wallets, as they don't rely on third parties for their data and are harder to steal. They are still connected to the internet, which makes them inherently less secure. However, desktop wallets are a great solution for those who trade small amounts of Bitcoin from their computers.

There is a variety of different options of desktop wallets that cater to different needs. Some focus on security, some on anonymity and so on.

Name	Operating system	Features
Electrum	MacOS, Windows, Linux	One of the most popular, robust, effective and secure desktop wallets; open source; allows you to replace a transaction fee on an already broadcasted transaction, which speeds up the confirmation process; address tagging; encryption
Exodus	MacOS, Windows, Linux	Very user-friendly and easy to understand, reliable wallet
Atomic Wallet	MacOS, Windows, Linux	Atomic is available for Mac OS, Windows and Linux, 500+ assets, keys are encrypted on your device, instant exchange, buy crypto option, custody-free app, 24/7 help center.

Bitcoin Core	MacOS, Windows, Linux	Full node wallet, you need to download the entire blockchain to use it. It allows you to independently verify transactions and not rely on anyone else in the system
Copay	MacOS, Windows, Linux	Multisignature wallet; mobile and desktop; open source
Armory	MacOS, Windows, Linux, Ubuntu, RaspberriPi	Prioritizes safety and security; features a variety of encryption and cold-storage opti

4. Bitcoin

Bitcoin is the first application of blockchain technology. Bitcoin has begun a revolution with the introduction of the very first completely decentralized digital currency, and the one that has proven to be extremely secure and stable from a network and protocol perspective. As a currency bitcoin is quite unstable and highly volatile, although valuable.

Bitcoin can be defined in various ways; it's a protocol, a digital currency, and a platform. It is a combination of peer-to-peer network, protocols, software that facilitates the creation and usage of the digital currency named bitcoin. Nodes in this peer-to-peer network talk to each other using the Bitcoin protocol.

Since its introduction in 2008 by Satoshi Nakamoto, Bitcoin has gained massive popularity, and at present it is currently the most successful digital currency in the world with billions of dollars invested in it. Its popularity is also evident from the high number of users and investors, increasing bitcoin price, everyday news related to Bitcoin, and the number of start-ups and companies that are offering bitcoin-based online exchanges, and it's now also traded as Bitcoin Futures on Chicago Mercantile Exchange (CME).

The name of the Bitcoin inventor Satoshi Nakamoto is believed to be anonymous, as the true identity of Bitcoin inventor is unknown. It is built on tremendous research in the field of cryptography, digital cash, and distributed computing.

i. Bitcoin Transaction Using a Blockchain Wallet

For demonstration we are using Blockchain wallet for mobile devices.

1. To initiate transaction sender needs the address of beneficiary, which can be obtained from payment request sent from a user, via any appropriate communication mechanism. The sender can also initiate a transfer to send money to another user. In any case, the address of beneficiary is required. Here we begin with creating request

FIGURE 86: TRANSACTION REQUEST

2. The sender either enters the receiver's address or scans the QR code that has the Bitcoin address, amount and optional description encoded in it.

FIGURE 87: RECEIVERS QR CODE

3. In the wallet of the sender, this transaction is constructed by following some rules and broadcasted to the Bitcoin network. From a user's point of view, once the QR code is decoded the transaction will appear similar to what is shown in the following screenshot. (How the transaction is created, digitally signed, broadcasted, validated and added to the block is explained in following sections.)

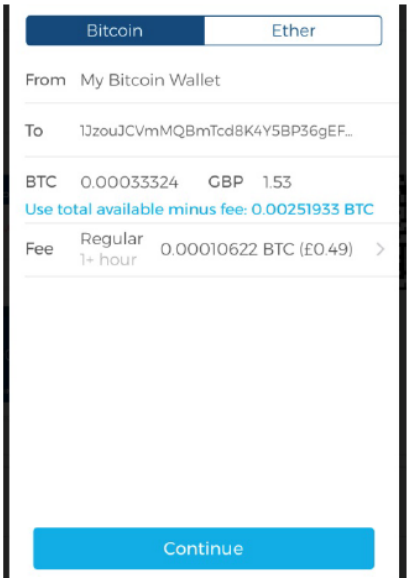


FIGURE 88: TRANSACTION INITIATION

Fee is calculated based on the size of the transaction and a fee rate is a value that depends on the volume of the transaction in the network. This is represented in Satoshis/byte. Fee in Bitcoin network ensures that your transaction will be included by miners in the block.

4. Once the transaction is sent it will appear as shown here in the Blockchain wallet software:

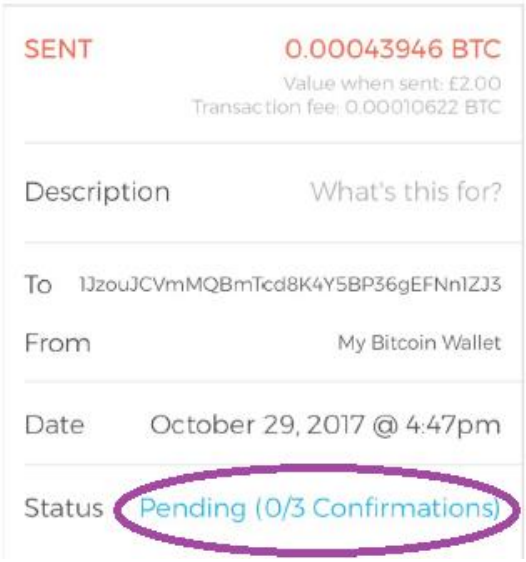


FIGURE 89: TRANSACTION INITIATED BUT CONFIRMATION PENDING

After the transaction has been constructed, signed and sent out to the Bitcoin network. This transaction will be picked up by miners to be verified and included in the block.
In the preceding screenshot, confirmation is pending for this transaction. These confirmations will start to appear as soon as the transaction is verified, included in the block, and mined.

5. The following screenshot visually shows how the transaction flowed on the network from origin (sender) to receivers on the right-hand side.

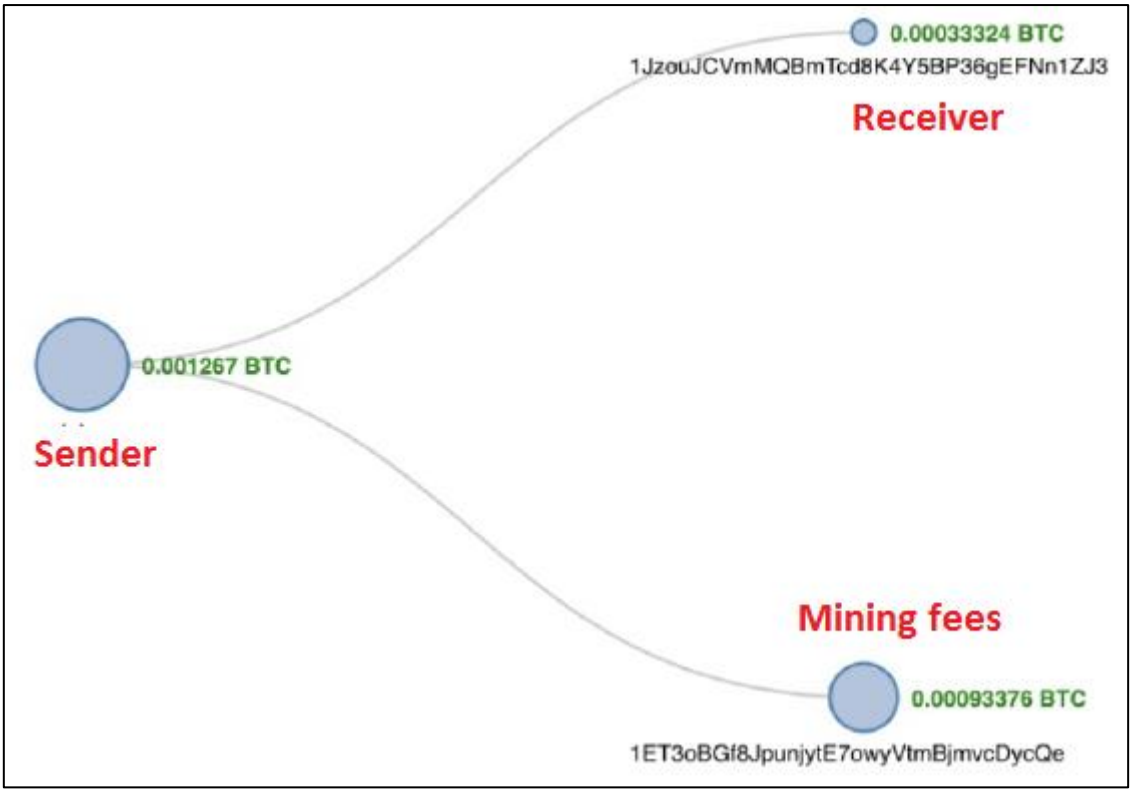


FIGURE 90: TRANSACTION FLOW

Here a payment of 0.001267 BTC (approximately 11 USD) is originated from the sender's address and been paid to receiver's address (starting with 1Jz). The fee of 0.00010622 (approximately 95 cents) is also deducted from the transaction as mining fee.

6. A summary view of various attributes of the transaction:

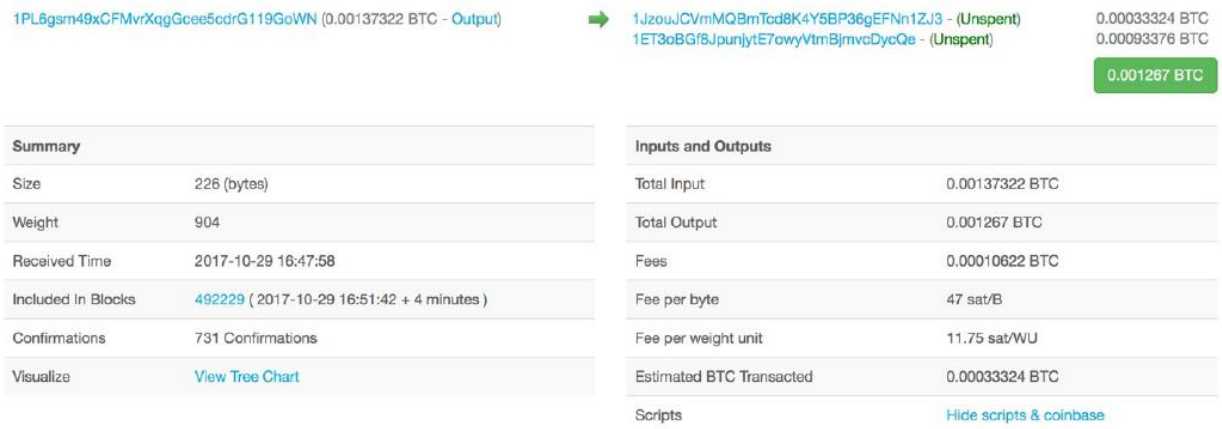


FIGURE 91: ATTRIBUTES OF TRANSACTION

There numbers of fields involved in transaction that contain various values are listed here with their purpose and explanation:

- **Size:** This is the size of the transaction in bytes.
- **Weight:** This is the new metric given for block and transaction size since the introduction of **Segregated**
- **Witness** (**SegWit**) version of Bitcoin.
- **Received Time:** This is the time when the transaction is received.

- **Included In Blocks:** This shows the block number on the blockchain in which the transaction is included.
- **Confirmations:** This is the number of confirmations by miners for this transaction.
- **Total Input:** This is the number of total inputs in the transaction.
- **Total Output:** This is the number of total outputs in the transaction.
- **Fees:** This is the total fees charged.
- **Fee per byte:** This field represents the total fee divided by the number of bytes in a transaction. For example, 10 Satoshis per byte.
- **Fee per weight unit:** For legacy transaction it is calculated using *total number of bytes * 4*. For SegWit
- transactions it is calculated by combining SegWit marker, flag, and witness field as one weight unit and each byte of other fields as four weight units.

The bitcoin currency, being digital has various denominations which are shown in the following table. A sender or receiver can request any amount. The smallest bitcoin denomination is the Satoshi. The bitcoin currency units are described as follows:

DENOMINATION	ABBREVIATION	FAMILIAR NAME	VALUE IN BTC
Satoshi	SAT	Satoshi	0.00000001 BTC
Microbit	µBTC (uBTC)	Microbitcoin or Bit	0.000001 BTC
Millibit	mBTC	Millibitcoin	0.001 BTC
Centibit	cBTC	Centibitcoin	0.01 BTC
Decibit	dBTC	Decibitcoin	0.1 BTC
Bitcoin	BTC	Bitcoin	1 BTC
DecaBit	daBTC	Decabitcoin	10 BTC
Hectobit	hBTC	Hectobitcoin	100 BTC
Kilobit	kBTC	Kilobitcoin	1000 BTC
Megabit	MBTC	Megabitcoin	1000000 BTC

FIGURE 92: BITCOIN DENOMINATION

ii. Key Elements of Bitcoin

- Digital keys

Elliptic Curve Cryptography (**ECC**) is used to generate public and private key pairs in the Bitcoin network.

Private keys are needed to be kept safe and it normally resides only on the owner's side. Private keys are used to digitally sign the transactions proving the ownership of the bitcoins.

Private keys are usually encoded in **Wallet Import Format** (**WIF**) form in order to make them easier to copy and use. It is a way to represent the full size private key in a different format. WIF can be converted into a private key and vice versa.
An example of a private key:
"A3ED7EC8A03667180D01FB4251A546C2B9F2FE33507C68B7D9D4E1FA5714195201"
Private key converted into WIF format looks like this:
"L2iN7umV7kbr6LuCmgM27rBnptGbDVc8g4ZBm6EbgTPQXnj1RCZP"

Public keys exist on the blockchain and all network members have access to it. Public keys are derived from private keys due to their special mathematical relationship with the private keys. Once a transaction signed with the private key is broadcasted on the Bitcoin network, public keys are used by the nodes to verify that the transaction has indeed been signed with the corresponding private key. This process of verification proves the ownership of the bitcoin.

- Addresses

A bitcoin address is created by taking the corresponding public key of a private key and hashing it twice, first with the SHA-256 algorithm and then with RIPEMD-160. The resultant 160-bit hash is then prefixed with a version number and finally encoded with a Base58Check encoding scheme. The bitcoin addresses are 26-35 characters long and begin with digit 1 or 3. Currently, there are two types of addresses, the commonly used P2PKH and another P2SH type, starting with number 1 and 3, respectively.

A typical bitcoin address looks like a string shown below:
"1ANAguGG8bikEv2fYsTBnRUmx7QUcK58wt"

- Transactions

Transactions are the core functions of the bitcoin ecosystem. Transactions can be as simple as just sending some bitcoins to a bitcoin address, or it can be complex depending on the requirements. Each transaction is composed of at least one input and output. Inputs can be thought of as coins being spent that have been created in a previous transaction and outputs as coins being created. If a transaction is minting new coins, then there is no input and therefore no signature is needed. If a transaction is to send coins to some other user (a bitcoin address), then it needs to be signed by the sender with their private key and a reference is also required to the previous transaction in order to show the origin of the coins. Coins are, in fact, unspent transaction outputs represented in Satoshis.
Transactions are not encrypted and are publicly visible in the blockchain. Blocks are made up of transactions and these can be viewed using any online blockchain explorer.

- Blockchain

Blockchain is a distributed ledger of a timestamped, ordered, and immutable list of all transactions on the Bitcoin network. Each block is identified by a hash in the chain and is linked to its previous block by referencing the previous block's hash.

- Mining

Mining is a process by which new blocks are added to the blockchain. Blocks contain transactions that are validated via the mining process by mining nodes on the Bitcoin network. Blocks, once mined and verified are added to the blockchain which keeps the blockchain growing. This process is resource-intensive due to the requirements of PoW where miners compete in order to find a number which is less than the difficulty target of the network. This difficulty in finding the correct value (also called sometimes the mathematical puzzle) is there to ensure that the required resources have been spent by miners before a new proposed block can be accepted.
New coins are minted by the miners by solving the PoW problem, also known as partial hash inversion problem. This process consumes a high amount of resources including computing power and electricity. This process also secures the system against frauds and double spending attacks while adding more virtual currency to the Bitcoin ecosystem.

Once a node connects to the bitcoin network, there are several tasks that a bitcoin miner performs:

- **Synching up with the network**: Once a new node joins the bitcoin network, it downloads the blockchain by requesting historical blocks from other nodes. This is mentioned here in the context of the bitcoin miner; however, this not necessarily a task only for a miner.
- **Transaction validation**: Transactions broadcasted on the network are validated by full nodes by verifying and validating signatures and outputs.
- **Block validation**: Miners and full nodes can start validating blocks received by them by evaluating them against certain rules. This includes the verification of each transaction in the block along with verification of the nonce value.
- **Create a new block**: Miners propose a new block by combining transactions broadcasted on the network after validating them.
- **Perform Proof of Work**: This task is the core of the mining process and this is where miners find a valid block by solving a computational puzzle. The block header contains a 32-bit nonce field and miners are required to repeatedly vary the nonce until the resultant hash is less than a predetermined target.
- **Fetch reward**: Once a node solves the hash puzzle (PoW), it immediately broadcasts the results, and other nodes verify it and accept the block. There is a slight chance that the newly minted block will not be accepted by other miners on the network due to a clash with another block found at roughly the same time, but once accepted, the miner is rewarded with 12.5 bitcoins and any associated transaction fees.

- The Bitcoin networks

The Bitcoin network is a peer-to-peer network where nodes exchange transactions and blocks. There are different types of nodes on the network. There are two main types of nodes, **full nodes** and **SPV nodes**.

Full nodes are implementations of Bitcoin core clients performing the wallet, miner, full blockchain storage, and network routing functions. However, it is not necessary to perform all these functions. Simple Payment Verification (SPV) nodes or lightweight clients perform only wallet and network routing functionality.

- Wallets (client software)

The wallet is a software application which is used to store private or public keys and Bitcoin address. It performs multiple functions, such as receiving and sending bitcoins. Nowadays, software usually offers both functionalities: Bitcoin client and wallet. On the disk, the Bitcoin core client wallets are stored as the Berkeley DB file.

Private keys are generated by randomly choosing a 256-bit number by wallet software. Private keys are used by wallets to sign the outgoing transactions. Wallets do not store any coins, and there is no concept of wallets storing balance or coins for a user. In fact, in the Bitcoin network, coins do not exist; instead, only transaction information is stored on the blockchain which are then used to calculate the number of bitcoins.

5. Ethereum

Vitalik Buterin conceptualized Ethereum in November, **2013.** The core idea proposed was the development of a Turing-complete language that allows the implemntation of arbitrary programs (smart contracts) for blockchain and decentralized applications. This concept is in contrast to Bitcoin, where the scripting language is limited in nature and allows necessary operations only.

The core idea in Ethereum blockchain is, executing transactions incrementally from a genesis state is into a final state. The final transformation is then accepted as the absolute undisputed version of the state. In the following diagram, the Ethereum state transition function is shown, where a transaction execution has resulted in a state transition:

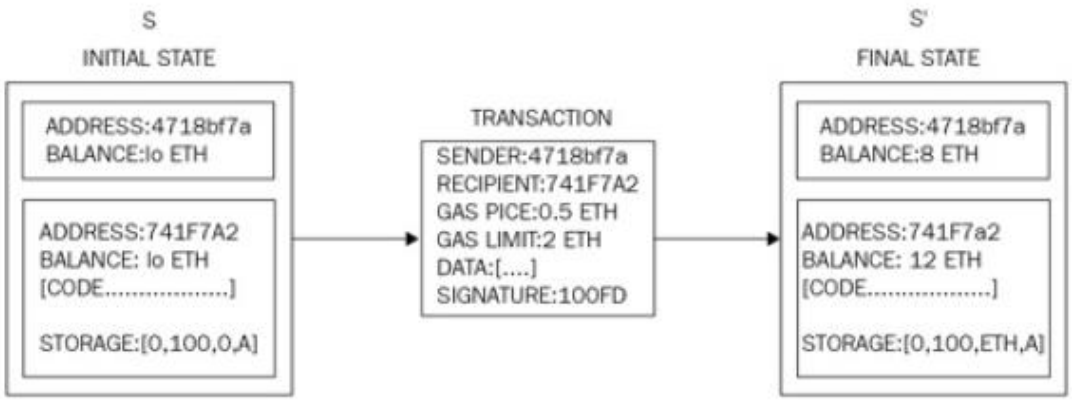


FIGURE 93: ETHEREUM STATE TRANSITION FUNCTION

i. The Ethereum network

The Ethereum network is a peer-to-peer network where nodes participate in order to maintain the blockchain and contribute to the consensus mechanism. Networks can be divided into three types, based on requirements and usage. These types are described in the following subsections.

- **Mainnet**

Mainnet is the current live network of Ethereum. The current version of mainnet is Byzantium (Metropolis) and its chain ID is 1. Chain ID is used to identify the network.

- **Testnet**

Testnet is also called Ropsten and is the widely used network for the Ethereum blockchain. This test blockchain is used to test smart contracts and DApps before being deployed to the production live blockchain. Moreover, being a test network, it allows experimentation and research. The main testnet is called Ropsten which contains all features of other smaller and special purpose testnets that were created for specific releases.

Other testnets include Kovan and Rinkeby which were developed for testing Byzantium releases. The changes that were implemented on these smaller testnets also been implemented on Ropsten. Now the Ropsten test network contains all properties of Kovan and Rinkeby.

- **Private net**

This is the private network that can be created by generating a new genesis block. This is usually the case in private blockchain distributed ledger networks, where a private group of entities start their blockchain and use it as a permissioned blockchain.

The following table shows the list of Ethereum network with their network IDs. These network IDs are used to identify the network by Ethereum clients.

Network name	Network ID / Chain ID
Ethereum mainnet	1
Morden	2
Ropsten	3
Rinkeby	4
Kovan	42
Ethereum Classic mainnet	61

FIGURE 94: ETHEREUM NETWORK IDS

ii. Components of the Ethereum Blockchain

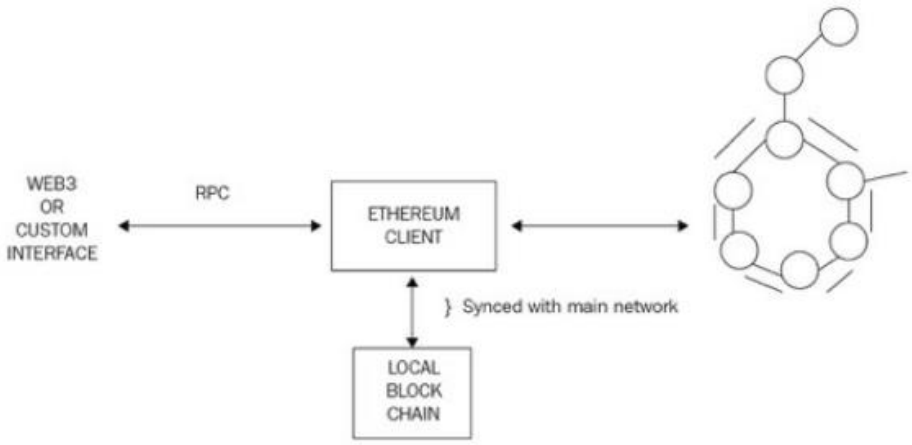


FIGURE 95: ETHEREUM ARCHITECTURE

The Ethereum blockchain stack consists of various components.

- Ethereum blockchain running on the peer-to-peer **Ethereum network.**
- **Ethereum client** (usually Geth) that runs on the nodes and connects to the peer-to-peer Ethereum network from where blockchain is downloaded and stored locally. It provides various functions, such as mining and account management. The local copy of the blockchain is synchronized regularly with the network.
- **web3.js library** that allows interaction with the Geth client via the Remote Procedure Call (RPC) interface.
- **Keys and addresses**
  Keys and addresses are used in Ethereum blockchain to represent ownership and transfer of Ether. Keys are used in pairs of private and public type. The private key is generated randomly and is kept secret whereas a public key is derived from the private key. Addresses are derived from the public keys which are a 20-bytes code used to identify accounts.
  The process of key generation and address derivation is described here:

1. A private key is randomly chosen (256 bits positive integer) under the rules defined by elliptic curve secp256k1 specification (in the range [1, secp256k1n − 1]).
2. The public key is then derived from this private key using ECDSA recovery function. We will discuss this later in the next section, Accounts in the context of digital signatures.
3. An address is derived from the public key which is the right most 160 bits of the Keccak hash of the public key.

- **Accounts**

Accounts are one of the main building blocks of the Ethereum blockchain. Ethereum is a transaction driven state mechanism, the state is created or updated as a result of the interaction between accounts and transaction execution. Operations performed between and on the accounts, represent state transitions.

Two kinds of accounts exist in Ethereum:

Externally Owned Accounts (EOAs)

- EOAs are similar to accounts that are controlled by a private key in Bitcoin.
- EOAs has ether balance
- They are capable of sending transactions
- They have no associated code
- They are controlled by private keys
- Accounts contain a key-value store
- They are associated with a human user

Contract Accounts (CAs)

- CAs are the accounts that have code associated with them along with the private key.
- CAs have Ether balance.
- They have associated code that is kept in memory/storage on the blockchain.
- They can get triggered and execute code in response to a transaction or a message from other contracts. It is worth noting that due to the Turing-completeness property of the Ethereum blockchain, the code within contract accounts can be of any level of complexity. The code is executed by Ethereum Virtual Machine (EVM) by each mining node on the Ethereum network.
- CAs can maintain their permanent state and can call other contracts.
- They are not intrinsically associated with any user or actor on the blockchain.
- CAs contain a key-value store.

- **Transactions and messages**

A transaction in Ethereum is a digitally signed data packet using a private key that contains the instructions, upon completion of which, either result in a message call or contract creation. Transactions can be divided into two types based on the output they produce:

Message call transactions: This transaction just produce a message call that is used to pass messages from one contract account to another.

Contract creation transactions: These transactions result in the creation of a new contract account. This means that when this transaction is executed successfully, it creates an account with the associated code.

- **Ether cryptocurrency/tokens**

As an incentive to the miners, Ethereum rewards its own native currency called Ether (ETH), as an incentive to the miners.

There are two Ethereum blockchains:

1. Ethereum Classic, and its currency is represented by ETC

2. ETH it is a the hard-forked version, which continues to grow and on which active development is being carried out.

Ether is minted by miners as currency rewards for their computational effort spend to secure the network by verifying and with validation transactions and blocks. Ether is used within the Ethereum blockchain to pay for the execution of contracts on the EVM. Ether is used to purchase gas as crypto fuel, which is required to perform computation on the Ethereum blockchain.

- **The EVM**

EVM is a simple stack-based execution machine that runs bytecode instructions to transform the system state from one state to another. The word size of the virtual machine is set to 256-bit. The stack size is limited to 1024 elements and is based on the Last In, First Out (LIFO) queue.

EVM is a Turing-complete machine but is limited by the amount of gas that is required to run any instruction. This means that infinite loops that can result in denial of service attacks are not possible due to gas requirements.

EVM also supports exception handling, in case exceptions occur, such as not having enough gas or invalid instructions, in which case the machine would immediately halt and return the error to the executing agent.

EVM is an entirely isolated and sandboxed runtime environment. The code that runs on the EVM does not have access to any external resources, such as a network or filesystem. This results in increased security, deterministic execution and allows untrusted code (anyone can run code) to be run on Ethereum blockchain.

- **Smart contracts**

A smart contract is a secure and unstoppable computer program representing an agreement that is automatically executable and enforceable.

A smart contract is nothing but a computer program that is written in a language that a computer or target machine can understand. It comprehends agreements between parties in the form of business logic. Smart contracts are automatically executed when certain conditions are met. They are enforceable, which means all contractual terms are executed as defined and expected, even in the presence of adversaries.

6. Components in Cryptocurrency system

i. Cryptocurrency user

A cryptocurrency user is a natural person or legal entity who obtains coins to use them for various purposes like

(i) to purchase real or virtual goods or services
(ii) to make P2P payments, or
(iii) to hold them for investment purposes

Cryptocurrency users can obtain coin through multiple ways:

- User can simply buy his coins on a cryptocurrency exchange using fiat money or another cryptocurrency;
- User can buy his coins directly from another cryptocurrency user (i.e. through a trading platform, referred to as a "P2P exchange");
- If a cryptocurrency is based on a PoW consensus mechanism, user can mine a new coin (i.e. participate in the validation of transactions by solving of a "cryptographic puzzle" and be rewarded a new coin);
- In some cases user can obtain his coins directly from the coin offeror, either as part of a free initial offering of coins or in the framework of a crowd sale set-up by the coin offeror (e.g. a large bulk of ether (cf. Ethereum) was sold in a crowdsale to cover certain development costs);
- If user sells goods or services in exchange for cryptocurrency, he can also receive coins as a payment for those goods or services;
- In case of a "hard fork" of a coin's blockchain, user will automatically obtain an amount of the newly created coin;
- User can receive coins as a gift or donation from another cryptocurrency user

ii. Cryptocurrency Miners

"Miners" are important entity of cryptocurrency since they participate in validating transactions on the blockchain by solving a "cryptographic puzzle". The process of mining relates to cryptocurrencies that are based on a PoW consensus mechanism. A miner supports the network by harnessing computing power to validate transactions and is rewarded with newly mined coins. Miners can be cryptocurrency

users, or, more commonly, parties who have made a new business out of mining coins to sell them for fiat currency (such as US Dollar or Euro).

iii. Cryptocurrency Exchanges

Cryptocurrency exchanges are entities that facilitate exchange services to cryptocurrency users, usually against payment of a certain fee (i.e. a commission). They allow cryptocurrency users to sell their coins for fiat currency or buy new coins with fiat currency. They generally function both as a bourse and as a form of exchange office. Examples of well-known cryptocurrency exchanges are: Bitfinex, HitBTC, Kraken and Coinbase GDAX. Some exchanges are pure cryptocurrency exchanges, which means that they only accept payments in other cryptocurrencies, usually Bitcoin (for example Binance), whereas others also accept payments in fiat currencies such as US dollar or Euro (for example Coinbase).
Moreover, many cryptocurrency exchanges only allow their users to buy a particular selection of coins. Many cryptocurrency exchanges (i.e. both regular and pure cryptocurrency exchanges) operate as custodian wallet providers (for example Bitfinex). In general cryptocurrency exchanges offer their users a wide array of payment options, such as wire transfers, PayPal transfers, credit cards and other coins. Some cryptocurrency exchanges also provide statistics on the cryptocurrency market (like trading volumes and volatility of the coins traded) and offer conversion services to merchants who accept payments in cryptocurrencies.

iv. Wallet Providers

Wallet providers are those entities that provide cryptocurrency users digital wallets or e-wallets which are used for holding, storing and transferring coins. A wallet holds a cryptocurrency user's cryptographic keys. A wallet provider simply translates a cryptocurrency user's transaction history into human readable format, which looks much like a regular bank account transaction detail.
There are several types of wallet providers:

- **Hardware wallet providers** that provide cryptocurrency users with specific hardware solutions to privately store their cryptographic keys (e.g. Ledger Wallet;
- **Software wallet providers** that provide cryptocurrency users with software applications which allow them to access the network, send and receive coins and locally save their cryptographic keys (e.g. Jaxx);
- **Custodian wallet providers** that take (online) custody of a cryptocurrency user's cryptographic keys (e.g. Coinbase).

v. Coin Inventotrs

Coin inventors are individuals or organizations who have developed the technical foundations of a cryptocurrency and set the initial rules for its use. In some cases, their identity is known (e.g. Ripple, Litecoin, Cardano), but more often they remain unidentified (eg. Bitcoin, Monero). Some remain involved in maintaining and improving the cryptocurrency's code and underlying algorithm, while others simply disappear (e.g. Bitcoin).

vi. Coin offerors

Coin offerors are individuals or organizations that offer coins to cryptocurrency users upon the coin's initial release, either against payment (i.e. through a crowdsale) or at no charge (i.e. in the framework of a specific (sign-up) program (e.g. Stellar)), normally to fund the coin's further development or boost its initial popularity. The coins issued by coin offerors offer to cryptocurrency users are created or pre-mined prior to the coin's official release / the coin's inception. Coins that are distributed this way are either partially pre-mined or pre-created (i.e. cryptocurrency users can still generate more coins after the release), or are fully pre-mined or pre-created. In the latter case the coin offeror usually retains a large portion of the coins (e.g. this is the case with Stellar). It is important to note that not all coins have an identifiable coin offeror, nor are all coins pre-mined or is its full supply pre-created. A coin offeror can be the same person as the coin inventor, or another individual or organization.

7. Challenges in Cryptocurrency

Cryptocurrencies despite of its huge advantages and multiple future perspective, is not free from financial problems and security concerns. The main problems and impacts of cryptocurrency can include:

i. Security threats:

Hackers and malicious users if successful in breaking cryptocurrency system, they can create as much as they want from virtual currency. This will lead to the ability to create fake virtual currency or steal virtual currency by just seating in front of computer. For example, selling in-game virtual items and virtual currency is against World of Warcraft (WoW) game policies. Therefore, many users log into WoW gold selling websites to buy virtual gold in order to pay for virtual items that they need. Many of WoW gold selling websites are not reliable and they are vulnerable to hacking and many users are complaining about paying real money for nothing or for fake virtual currency

ii. Collapse concerns in cryptocurrency systems:

Unlimited issuing of cryptocurrency in the variety crypto communities will lead to economic problems since its issuing is not based on the demand and supply. It is possible for some providers such as Second Life to issue unlimited Linden Dollars and increase their virtual items prices in order to gain more real revenues. On the other hand, it will suffer from inflation and economic issues leading to collapse in the cryptocurrency system.

iii. Impact on real economy:

Since some crypto currency systems are connected with real world monetary systems, they may affect the demands and supply facilities of main stream economy. For example, enabling users to purchase virtual and real goods and services with cryptocurrency in some platforms may reduce the demands on fiat money. Users will no longer depend on fiat money for their purchase. On the other hand, some platforms enable users to exchange their virtual currency with real currency and this will increase the demands on fiat currency. This fluctuation will affect on the main stream economy.

iv. Gold farming risks:

Gold farmers are players who play in social games such as World of Warcraft in order to gain gold, which is virtual currency of the game, and then sell it for real money. The targeted buyers are the players who do not have enough time to play and compete for gaining virtual currency. In fact, huge cash flow is generated from gold farming process and it is not controlled and regulated. This will increase fraud and financial risks where virtual currency is exchanged with real money in unreliable environment.

v. Money laundering:

Money laundering is one risk that is very likely to rise with the use of cryptocurrency especially with platforms that enable users to exchange cryptocurrency with fiat money.

vi. Unknown identity risks:

Since most of the cryptocurrencies keep identity of user anonymous, financial transactions cannot be monitored very well. There is no way to recognize the source of creating or cashing out the virtual currencies. This leads to inability to track the transactions in case of money laundering suspicion. Moreover, unknown identity will enable criminals to get paid with virtual currency for their crimes.

vii. Black market for cryptocurrency:

The increasing popularity of virtual currency in online environment has led to a thriving black market for trading virtual currency with real money. By observing several social games' forums, some fraud cases have been raised and discussed between users. For example, when a gamer decides to quit from a game, he/she may want to sell the owned virtual currency by offering them in the game's forums. The way of receiving the payments is risky since many malicious users may not complete the payment or they dispute after paying. In this case, they will get their money back plus the virtual currency.

8. Some important links to Investigate about Cryptocurrency:

1. Identify the date, time and amount of the first and last transaction happening using any bitcoin public key address?

bitcoinhttps://www.blockchain.com/explorer

2. To Identify the person to whom bitcoin address belongs:

https://www.bitcoinwhoswho.com/

https://bitref.com/

https://intelx.io/

3. To identify the wallet used to perform the transactions using abitcoin address?

https://www.walletexplorer.com/

https://glasschain.org/

4. To identify frequent sender and receiver to bitcoin address

https://hashxp.org/

5. To identify the sibling transactions and bitcoin address of the same

https://hashxp.org/

6. To identify the time at which maximum transactions took place using bitcoin address

https://oxt.me/

7. To Find whether there is any relation between the two given bitcoin addresses.

https://learnmeabitcoin.com/tools/path/

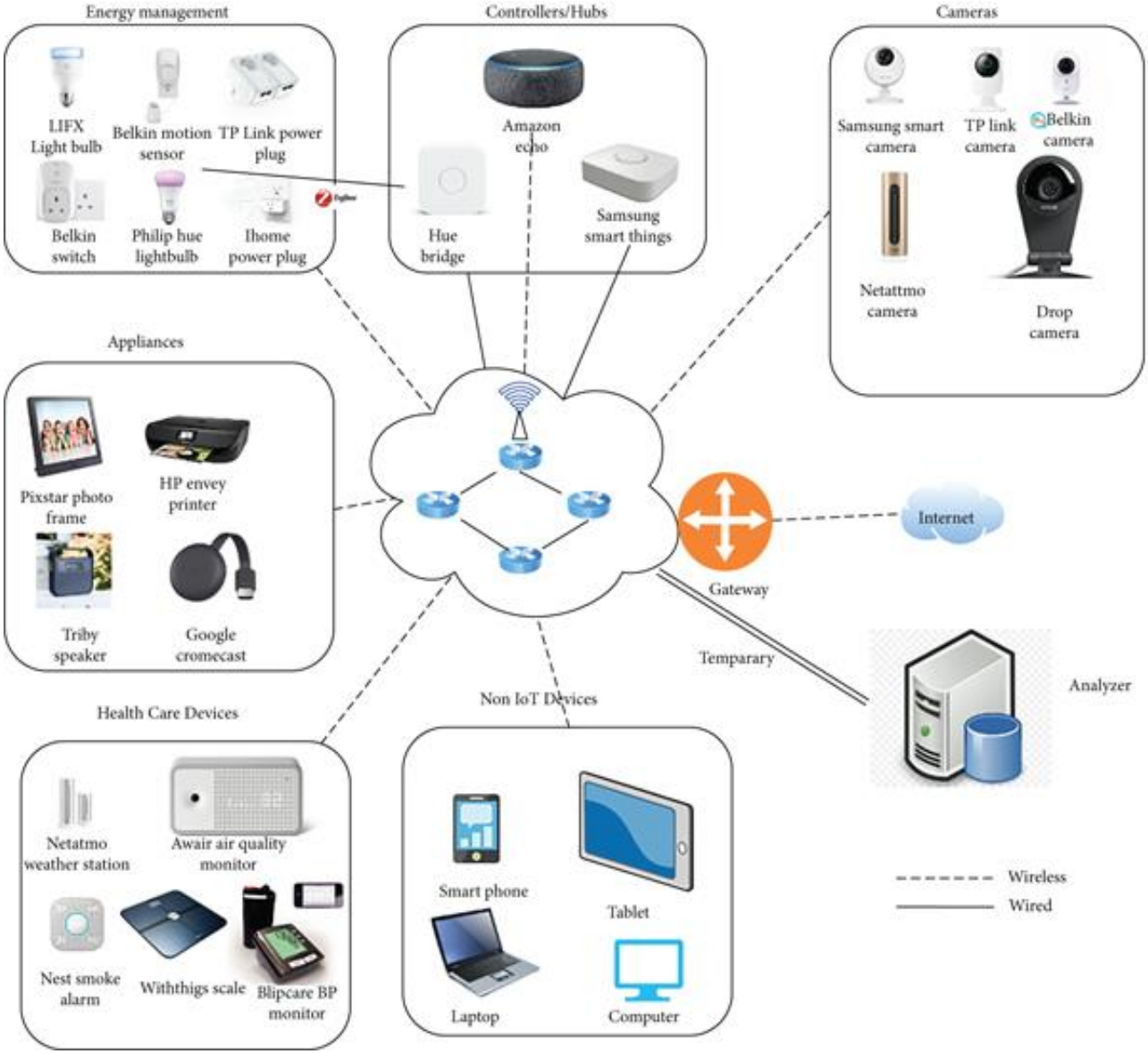
IoT & Cloud Forensics

1. What is IoT?

IoT, sometimes referred to as Internet of Everything (IoE), is the term used to describe computing devices that are web-enabled, capable of sensing, gathering, and delivering data utilising sensors, as well as the embedded communication hardware and processors. In the Internet of Things, an object is referred to as a thing if it has a device attached to it that is capable of communicating through a network with other natural, artificial, or machine-made objects. IoT makes use of cutting-edge and established robotics, networking, and sensing technologies to enable greater system integration, automation, and analysis.

A range of options for improving company and customer pleasure opens up with an expansion in the networking capabilities of machines and regular appliances utilized in different sectors, including workplaces, residences, industries, transportation, buildings, and wearable gadgets. Connectivity, sensors, artificial intelligence, tiny devices, and active involvement are a few of the crucial IoT aspects.

2. Types of IoT devices



3. Data is stored on IoT devices

i. Data About Owner

- Name
- Time zone
- Address
- Phone number(s)
- Payment information
- Your age
- Personal interests as stored in your user profile
- The location of your device or computer
- Location history, places, and routes
- Your IP addresses
- Your synced email
- Your calendar
- Acoustic model of voice characteristics

ii. Data About Contacts

- Names for stored contacts
- Nicknames for stored contacts
- Relationships for stored contacts
- Phone numbers for stored contacts
- Addresses for stored contacts
- Email addresses of stored contacts

iii. Data About Files & Activity

- Voice recordings from smart assistant
- Record of interactions and requests made via smart assistant
- Shortcuts added via the smart assistant
- Record of communications requests with your contacts Records of reviews and emails sent to the company
- Purchase history from associated parent company website or store
- Browsing history
- Your online searches
- Log of device use
- Log of content downloads
- Log of streams (video and/or music)

iv. Data About Device & Network

- Device specifications/configuration
- Information about internet-connected
- devices linked to your smart assistant
- Names of devices, homes, and members of a shared home in Apple's Home App
- Names of you and your family sharing members' devices
- Connectivity data
- Wi-Fi network details such as the name and when you're connected
- Wi-Fi credentials if synced within a smart home network
- Information about your internet service provider

4. IoT Forensics

IoT forensics is a branch of digital forensics that focuses on IoT sensors, nodes, devices, and data stored on many platforms, including connected devices, the IoT device's physical storage, and cloud storage. IoT forensics is a diverse and multifaceted approach to digital forensics because it focuses on a variety of platforms and facets of the field.

IoT forensics is a process of identification, acquisition, and analysis of digital evidence obtained from IoT devices, sensors, and nodes. IoT device data must now be retrieved and analysed for legal and investigative purposes due to the rise in cyber security threats aimed at these devices.

Investigators must concentrate on several technological factors, such as cloud forensics, network forensics, and IoT device-level forensics, in order to conduct forensics investigations on IoT devices. As a result, these factors are split into three categories: IoT, Network, and Cloud. These areas assist an investigator in gathering potential evidence from an IoT device by helping them concentrate on different areas including cloud forensics, network forensics, and device forensics. Through these areas, the investigators can potentially gather information about the impacted IoT device.

i. Steps involved in IoT forensics:

Evidence Identification and collection

The affected IoT devices at the crime scene need to be identified by an investigator. The scope of the investigation can be expanded with careful evidence identification and gathering.

a. Preservation

The investigator needs to ensure that the IoT device's evidence is appropriately stored. Before obtaining the evidence from the device during the initial search, it should not be turned off. In order to collect data from the device's hardware and software at this level, the investigator needs specialised forensic tools. In order to get sensitive information from the IoT device before it is turned off, the investigator can also do memory dumps.

b. Data Analysis

Most of the data in an IoT device is kept in the cloud or on a mobile phone that is synced with the IoT device. The investigation of devices discovered at the crime scene and cloud-stored data are both part of the evidence gathering process.

c. Presentation and Reporting

The investigation has reached its conclusion at this point. At this point, a report on the evidence and the forensics analysis process will be created, and it will be submitted in court with the actual evidence.

5. IoT Forensics Challenges

As IoT devices communicate with other devices on the same network, IoT Forensics can be difficult for the investigators.

i. Challenges in Identification, collection, and preservation of evidence

Since the majority of IoT devices operate on their own, identifying one can be difficult. Forensic investigators may have difficulties as a result of improper documentation methods for the preservation and collection of evidence for IoT devices.

ii. Challenges in Analysis of evidence

Since the majority of a device's data is saved on a cloud computing facility, a forensic investigator should also take into account the physical location of the data contained in the device to demonstrate the integrity and dependability of the evidence gleaned from it. Another challenging task for a forensic investigator is the imaging and analysis of remote data.

iii. IoT device autonomy poses some challenges

A forensic investigator may have serious concerns about an IoT device's ability to operate autonomously without human involvement. The difficulty here would be determining whether a design issue or human involvement caused the IoT gadget to malfunction.

6. Cloud Computing

The on-demand distribution of IT resources, such as computer systems, databases, storage, and applications, to users as a metered service through the internet is known as cloud computing. Numerous cloud-based services are offered by well-known cloud service providers (CSPs), including AWS, Microsoft, and Google Cloud.

i. Characteristics of Cloud Computing

- On-demand self-service
  a type of service offered by CSPs that enables on-demand provisioning of cloud resources including processing power, storage, and networks without requiring direct contact with the service providers.
- Distributed storage
  Better data reliability, scalability, and availability are provided via distributed cloud storage. However, there could be issues with compliance and security.
- Rapid elasticity
  The cloud offers scalable services that may be quickly provisioned to meet business needs. A limitless amount of resources may be deployed and redeployed by subscribers.
- Automated management
  Cloud automation speeds up the process, lowers labour expenses, and lessens the chance of human error by minimising user engagement.
- Broad network access
  On a range of devices, including laptops, smartphones, and personal digital assistants, cloud resources are accessible through the network and can be accessed using regular protocols (PDAs)
- Resource pooling
  While allocating the necessary resources to a client in accordance with their demand, the CSPs pool all resources in order to service several customers in a multi-tenant environment.
- Measured service
  Most cloud computing platforms use a "pay-per-use" metering scheme. Cloud service users either pay a monthly membership fee or a usage fee for resources like storage capacity, processing speed, and bandwidth. The resource use of clients is transparently tracked by CSPs, who also have complete control over it.
- Virtualization technology
  Resources can be scaled quickly in the cloud in a way that is not possible in non-virtualized environments thanks to virtualization technologies.

ii. Limitations of Cloud Computing

- Organizations have limited control and flexibility
- Prone to outages and other technical issues
- Security, privacy, and compliance issues
- Contracts and lock-ins
- Depends on network connections

7. Types of Cloud Computing Services

i. Infrastructure-as-a-Service

Subscribers can access basic IT resources like computing power, virtualization, data storage, and networks on-demand thanks to infrastructure-as-a-service (IaaS).
Subscribers can save money by not having to pay for things like hardware, human resources, and other expenses because CSPs are in charge of operating the underlying cloud computing infrastructure.
Examples include Azure Virtual Machines and Amazon Elastic Compute Cloud (EC2).

ii. Platform-as-a-Service

PaaS (Platform as a Service) provides a platform for creating services and applications. Although subscribers are not needed to purchase and operate the software and the infrastructure that supports it, they do have control over the installed applications and, maybe, the parameters of the application hosting environment. Dynamic scalability, automated backups, and other platform services can all be used by applications created in a PaaS environment without the need to explicitly write for them.

Examples include SAP Cloud Platform, AWS Lambda, AWS Elastic BeanStalk, and Google App Engine.

iii. Software-as-a-Service

Subscriptions to software-as-a-service (SaaS) are provided with application software on demand via the internet. It is paid for on a per-use basis by the providers, who may also charge via subscription, advertising, or user sharing.

Examples include web-based office programmes like Google Docs or Microsoft Office 365 as well as web-based email programmes like Outlook and Gmail.

8. Crimes on Cloud

A cloud crime is any illegal behaviour that uses a cloud environment as a subject, an object, or a tool.

- Cloud as a subject

  In order to steal data or introduce malware, the attackers seek to compromise the security of a cloud environment. Examples include stealing the identity of a cloud user, altering or deleting stored data without authorization, and installing malware on the cloud.

- Cloud as an object

  Attackers employ a cloud system to harm the CSP in this kind of crime; in this scenario, the cloud functions as an object. Instead of affecting the cloud environment in this example, the attacker's primary goal is to impact the CSP. For instance, DDoS attacks on the cloud may result in system failure over the entire cloud environment.

- Cloud as a tool

  When an attacker utilises a cloud account that has been compromised to target additional accounts, the cloud becomes a tool. In such circumstances, the evidentiary data may be stored on both the source and destination clouds. Example: When a crime-related piece of evidence is saved and shared in the cloud, or when a cloud is used to launch an attack against another cloud.

9. Cloud Forensics

In order to analyse any security incident, cloud forensics aims to apply the concepts and procedures of digital forensics to the cloud environment. Investigators need to be aware of the data location

and the level of access that a particular business has to the data in order to collect digital evidence in a cloud environment. This section covers cloud forensics, its significance and applications, the function of stakeholders in an investigation, and the numerous difficulties that investigators face when conducting cloud forensics.

The management of both public and private networks is a component of cloud forensics, which is the use of digital forensic investigation in a cloud context. "Digital forensics is the application of science to the identification, examination, gathering, and analysis of data while preserving the content and maintaining a strict chain of custody for the data," according to the NIST. Cloud computing has specialised ideas and is dispersed over a vast network. As a result, depending on the service offered and the deployment strategy, several forensic processes are used in cloud computing.

Each approach has a different initial stage for gathering evidence. In the SaaS paradigm, gathering application logs is entirely the responsibility of the CSP. The forensics investigation and analysis procedure can, however, be started by the investigators in IaaS by requesting the clients' virtual OS disc. Similar to private cloud services, which provide their users more control over the data and hardware infrastructure, cloud forensic investigators can physically access the digital evidence there. SaaS models on public clouds make it challenging to physically access the data, and the investigation is reliant on the audit reports and log data supplied by the CSP.

10. Challenges in Data Collection from Cloud

i. Data Location

Collecting data from the target is challenging because it is stored in different data centers and geographic regions

ii. Decreased access and data control

In each combination of cloud service and deployment model, the investigator encounters the challenge of limited access and control to the forensic data

iii. Chain of dependencies

The CSPs and most of the cloud applications often rely on other CSP(s), and the dependencies in a chain of CSP(s)/client(s) can be prominently dynamic in such conditions, cloud investigation may depend on the examination of each link in the chain and the level of complexity of the dependencies

iv. Locating evidence

Locating and collecting evidence is a challenge because data in cloud may be quickly altered or lost and there is limited knowledge regarding where or how data is stored in the cloud

v. Imaging and isolating data Description

Data imaging and isolating a migrating data target is challenging in the cloud ecosystem owing to its key characteristics: elasticity, automatic provisioning/deprovisioning of resources, redundancy, and multi-tenancy Source

vi. Data available for a limited time

Data collection and preservation of VM instances are challenging tasks owing to insufficient standard practices and tools

vii. Locating storage media

It is difficult to locate the storage media in a cloud ecosystem because it requires an in-depth understanding of the cloud architecture and implementation

viii. Evidence identification

Evidence identification is challenging because the sources/traces of evidence are either not accessible or are created or stored differently in comparison to those in non-cloud environments

ix. Dynamic storage

Often, CSPs dynamically allocate storage based on the consumer's request. This complicates the data collection process during investigation

x. Live forensics

Validating the integrity of the collected data is challenging because the data within a cloud system are volatile and frequently changing. Additionally, live forensics tools may make modifications to the suspected system Source

Metaverse & Techno-legal Challenges in Cyber Space

1. META VERSE

People can work, socialize, transact, play, and even create in the enormously scalable, persistent network of interconnected virtual worlds known as the metaverse. In order to fully immerse the user in the virtual environment, advanced virtualization and technologies (AR, VR, haptic sensors, etc.) are used. This implies that the user can interact in real time with a world that is always present and that he can access at any time.

The coexistence of hybrid and digital space is known as a metaverse. The Metaverse is a 3D web-based environment that blends virtual and augmented reality technology. In Metaverse, people can engage in any activity they like while interacting with one another in a virtual world. In this virtual, networked world, there are digital objects, decentralized metaverse NFTs, avatars, and much more. Multiple definitions of metaverses exist, each expressing a different perspective. Simply put, the term "metaverse" refers to a three-dimensional network supported by augmented and virtual reality. Persistence, self-sufficiency, infinity, interoperability, and real-time are some of its essential traits.

Metaverse is a vast notion. Metaverse applications can be utilized to gain a better viewpoint in every important field, including education, gaming, tourism, and healthcare. More than 40% of current developments in AR and VR are based on Metaverse techniques.

According to a recent metaverse development, technology can introduce holographic avatars and holograms to the metaverse together with the internet of things (IoT) and artificial intelligence (AI).

There are numerous definitions of the Metaverse that reflect a wide range of viewpoints. We must envision a three-dimensional network driven by virtual reality (VR) and augmented reality (AR) in order to rapidly understand what the term "Metaverse" means. The key qualities of the metaverse are that it is durable, self-sustaining, limitless, interoperable, and in real-time.

- It is persistent if it continues to exist despite the user's absence.
- Numerous contemporary users and VR worlds are supported by Infinite.
- Self-sustaining implies that people are able to procure their needs while also making money in the Metaverse.
- Users can transport their avatars and other virtual items between Metaverse projects with the aid of interoperability.
- Users are able to enjoy live experiences in real-time.

2. KEY TECHNOLOGIES

Virtual worlds are the focus of the metaverse. It offers an engaging method to interact and socialize while experiencing extended reality. Augmented Reality, Virtual Reality, and Mixed Reality are all parts of extended reality.

i. Augmented Reality (AR)

An interactive environment in which virtual things are superimposed over actual objects. Computer-generated perception data from several sensory modalities, including visual, aural, haptic, somatosensory, and olfactory, can be used to do this.

ii. Virtual Reality (VR)

Teleports people into a digital environment that simulates their actual presence in real-world or made-up environments. It can produce olfactory, tactile, auditory, and visual impressions.

iii. Mixed Reality (MR)

With MR, users can interact with the real environment in addition to having virtual content placed on it.

3. LAYERS OF METAVERSE

- **Layer 1: Experience –** The user interacts with gaming, commerce, sports, immersive virtual worlds, digital assets, and more throughout the experience layer. Many of these characteristics, including immersion in virtual environments, avatar identities, storytelling, and in-person social interactions, are demonstrated in gaming. Additionally, it covers a wide range of other common instances where the physical and digital worlds cross, including Zoom meetings, exercises, and more.
- **• Layer 2: Discovery –** The advertising network that consists of stores, rating systems, and social recommendations is called Discovery. Systems for incoming and outbound information sharing can facilitate discovery. Outbound discovery comprises notifications and display adverts, whereas inbound discovery includes community content platforms where consumers can learn about the preferences and suggestions made by other users. One of the important components of metaverse discovery is real-time presence, which allows users to see what other users are doing right now in the metaverse and to participate in the shared experience.
- **• Layer 3: Creator Economy –** This layer makes it possible to produce digital content such as YouTube videos without having any programming experience. The experiences offered by the creative economy will be individualized, social, immersive, and real-time.
- **Layer 4: Spatial computing –** An essential component of spatial computing is the ability for users to interact with 3D spaces, which combine real and virtual worlds. It refers to 3D engines, software, AR, VR, XR, and mapping that assist us in removing the barriers between real-world and virtual environments. The Internet of Things (IoT), speech recognition, and gesture recognition technology are also included. Users can generate an impression of physical realism using 3D engines like Unity and Unreal. Microsoft's HoloLens is a terrific illustration of what we can achieve on the spatial computing layer, whereas Omniverse by Nvidia provides a platform where creators can interact in an interoperable 3D space.
- **Layer 5: Decentralization —** Decentralization, which will allow the metaverse to be decentralised, open, and dispersed, is one of its fundamental characteristics. It consists of self-sovereign digital identity, smart contracts, open-source platforms, and blockchain technology. The metaverse needs a transparent and traceable method of carrying out transactions and interactions if it is to reach its full potential. Through blockchain, crypto assets, and NFTs, it is possible. One prominent instance of the decentralised metaverse is Decentraland, a decentralised virtual environment powered by the Ethereum blockchain and governed by a Decentralized Autonomous Organization (DAO).
- **Layer 6: Human Interface –** All technology that enhances human interactions with digital assets is referred to as human interface. It comprises wearables, gestures, speech, haptics, VR headsets, smart glasses, mobile devices, and neural networks. An excellent illustration of the same is Oculus Quest. Our interactions are becoming more digital and straightforward thanks to wearables, biosensors, and brain-computer interfaces that are 3D printed.
- **Layer 7: Infrastructure –** All technologies that enable, connect, and power digital devices are referred to as infrastructure. It covers the development of 5G computing built using microchips that are only increasing denser and quicker while also covering data centres, cloud computing, wireless, materials, and processing. The storage and computation of data have been moved closer together as a result of infrastructure progression from cloud computing to edge computing, depending on how and where it is produced and used.

4. FOUNDATIONS OF METAVERSE

i. EQUIPMENT AND INFRASTRUCTURAL FACILITIES

The proper IT infrastructure is essential given the vast volumes of data, 3D processing, and live interactivity. This comprises cloud computing, highly specialized virtualization hardware with GPU, TPU, and CPU development for the server-side hardware requirements, as well as network technologies from current 5G and upcoming 6G networks.

The consumer side is the second component, where specialized hardware is required to provide an immersive experience. Smart glasses for virtual and augmented reality, haptic feedback gear (gloves, suits, etc.), and even more powerful smartphones are required.

ii. AVATARS AND IDENTITY MANAGEMENT

A virtual world with a virtual identity may sound appealing, but genuine identity verification is necessary to ensure that it is safe and is not a "outlaw" environment. There would need to be a standard protocol and something akin to a meta-identity that could be tied to the users' own avatars and allow them to use avatars and identities across numerous virtual worlds for this to happen in many of them.

iii. REMITTANCE AND TRANSACTIONS

Every metaverse needs an ecosystem to function properly. Finding a common method of payment and transaction is necessary for this to function. Due to the possibility that each ecosystem may have its own payment and transaction methods, connecting various worlds becomes challenging on a number of levels.

iv. REGULARITY STRUCTURES AND REGULATIONS

We need social norms and regulatory structures in place, just like in the real world. One of the most difficult problems to overcome may be how to manage and enforce these regulations in a virtual environment. We must consider international norms and even laws that regulate the virtual world in order to make people feel secure.

v. EQUIPMENT AND SPECIFICATIONS

Common standards and tool sets must exist for the metaverse to be really interactive. This comprises computer languages, user-friendly design tools, widely used 3D engines, standards for the virtual reality and augmented reality industries, asset marketplace standards, transfer protocols, security standards, as well as more advanced standards like geospatial mapping.

vi. ELECTRONIC ECOSYSTEM

A functional digital economic environment is also necessary for the many use cases to be successful. Everything from advertising networks to online shops, virtual jobs, and payments for games, social interactions, eSports, and even shopping. To encourage more people and businesses to engage, develop, and share, it is crucial to establish this economic universe.

5. PROJECTS

i. METAVERSE OF GAMING - DECENTRALAND

Decentraland is a decentralized Metaverse project built on gaming that enables global users to build, discover, and exchange NFTs in a realistic and immersive virtual environment. Users can purchase real estate anywhere in the world, organize live events, play games, and engage in many other interesting activities that are also feasible in reality.

The network is entirely owned and controlled by its users and is run by a decentralized autonomous organization (DAO). Users can vote on issues like feature improvements and optimization, make important change proposals, and take part in governance. As part of its subsequent major upgrade, Decentraland will make a variety of other Metaverse projects interoperable.

ii. METAVERSE OF REAL ESTATE – UPLAND

A blockchain-based gaming Metaverse project called Upland enables the purchasing, selling, and trading of virtual assets that are linked to actual addresses. The real estate on this network is represented by NFTs, which users can acquire to become "digital landowners" and trade for UPX currencies.

Upland, a project that may be different from other Metaverse efforts now underway, aims to create a digital economy that will obliterate the distinction between the virtual and physical worlds, enabling people to take advantage of the advantages of both.

iii. VERSATILE METAVERSE - ENJIN

On the Ethereum blockchain, Enjin is a Metaverse project that supports the development of marketplaces in the future. Businesses can build decentralized NFT marketplaces, develop NFTs, integrate them, and trade them to generate money with real value based on the specialization of their company. The platform had no restrictions on the kinds of projects that could be developed, so developers could build a market for anything from games to real estate, branding, and e-commerce.

By utilizing the security features of Enjin's platform, users may conveniently store and manage their NFTs while avoiding any potential complications. The five simple phases of acquisition, minting, gaming, trading, and melting can be used to describe enjin.

6. USE CASES

i. VIRTUAL AND AUGMENTED WORKSPACES

It might be able to be in the same virtual space, collaborate, draw on a whiteboard, and even rearrange the area according to your needs rather than seeing people on a screen with some video blocks. These elements would be combined in augmented workspaces, enabling users to take part digitally in actual meetings. You would experience the people and the avatars simultaneously and be able to engage as though you were actually there if there were holograms in the space.

ii. ADVANCED BLOCKCHAIN

Decentralized or blockchain technology is necessary for the widespread use of the Metaverse across industries. Companies can create more realistic NFT marketplaces with Metaverse, enabling consumers to make wiser purchasing decisions.
While Bitcoin, Ether, and Dogecoin are all powered by blockchain technology, this technology does much more than just support and maintain currency. It facilitates the development of digital assets known as non-fungible tokens (NFTs) and dApps and can serve as a distributed ledger for recording peer-to-peer transactions.

With Metaverse, businesses can create NFT markets that are more engaging and authentic, allowing consumers to engage with one another, browse desired NFTs, and make smarter purchasing decisions. It has been encouraging new NFT or blockchain games where players can accumulate in-game treasures and trade them with other players since Metaverse offers a shared world of virtual space. These cutting-edge online games are created by blockchain-based game creators using the Metaverse.

iii. VENUES FOR ART AND CULTURE

Corona gave us access to several internet events and the art world in general. But what about holding virtual events where attendees might actually attend, engage in conversation, and even meet individuals online while taking in music or visual art? Making events, museums, or art exhibitions available online in a digital format could allow many more people all over the world to experience art and culture in a brand-new way. seeing the Mona Lisa in a digital Louvre's surroundings rather than merely from an internet image.

iv. DIGITAL ART WORKS

Users can create their own environment in a virtual universe using tools like Roblox and Minecraft. Many more people may have the freedom to create if the user is given the power to shape, mould, and create universes as he pleases. In such a setting, NFTs might become more important as well as the desire of people to acquire digitally produced art.

v. DIGITAL BUSINESS MODELS AND MARKETPLACES

A functional market and economic ecosystem are essential, as was previously stated. This would enable the development of entirely digital marketplaces and transactions in the metaverse. Everyone would have access to all the art they want, and auctions could be watched from anywhere in the world. Imagine being able to enter Amazon's online store and interact with the products there as if they were physically present.

Additionally, this would enable innovative new digital business models that would foresee a totally digital world and monetize these virtual spaces.

vi. LITERACY AND SCHOOL SYSTEMS

What about a class taught entirely online? Virtual experiences, instructional games, interactive walls, and much more? An interactive world can be a great benefit, especially for education and schools. It would truly be feasible to be in space, zoom to planets, and obtain information about them by simply clicking on them when we teach about our solar system. Children learn more readily when their interactions with the learning environment are enjoyable. For remote or rural locations, the metaverse may also change the game since, so long as they have internet access, they can receive the same elite education as everyone else.

vii. SOCIAL MEDIA PLATFORMS GROWTH

The creators of Meta platforms, including Mark Zuckerberg, are aware that technology is capable of far more than just facilitating social media connections. Incorporating a three-dimensional space rather than just observing people on computers or mobile devices and hearing their voices is how they envision embracing the Metaverse.

By encouraging a sense of presence among them, a platform built on Metaverse gives social media users a more immersive experience. Beyond the capabilities of the current social media world, combining virtual reality and augmented reality provides a more realistic digital experience.

Of course, social media has evolved from straightforward text-based discussions to the sharing of memories and stories, and now we are stepping into the Metaverse, a virtual world. The Metaverse's material is heavily graphical, and because users practically inhabit this world, they also become content producers.

viii. IMPROVED TRAINING AND EDUCATION

The epidemic has accelerated augmented reality and virtual reality usage in education, which has led to an increase in e-learning. It is expected to alter and enhance content distribution and learning by enabling real-time interactions in the virtual world and broadcasting data in real-time.

ix. FULL-BODY ENTERTAIMENT

Even while it doesn't seem to be applicable to business, the entertainment offered by the metaverse is grabbing a lot of attention, especially from young people, who are expected to fuel metaverse expansion.

x. PLAYFUL VIDEOGAMES

Of course, the development of immersive video games is another significant use case. Imagine "Sims" with you as a real-life character. You can play in virtual games, design your own adventure, complete your own objectives, and do a lot more. The use of haptic feedback and other VR features will enable much richer experiences that let you feel the surroundings and more.

xi. INCREASED CUSTOMER TRANSPERANCY

Customers are curious to see how the metaverse will be used and how the supply chain will evolve as 3D representations of things are developed, offered for sale, and disseminated.

xii. INCREASED COOPERATION IN PRODUCT DEVELOPMENT

It is incredibly easy for different stakeholders to develop a product, distribute it to manufacturers in the market, and refine it based on feedback, shortening the project's product life cycle.

xiii. DECREASED DANGER TO QUALITY CONTROL

More precise and enhanced product design, along with user engagement, will further reduce the production margin of error.

xiv. DESIGN OF QUICK PRODUCTION METHOD

We can easily drag and drop assets into a physics-based simulation on metaverse. Find out how to increase manufacturing efficiency and safety without the need for rigorous physical testing.

xv. PLATFORM FOR SOCIAL INTERACTION

Through immersion, users can communicate with one another and build social relationships, similar to Second Life. Through virtual rooms and worlds, users can view one another, communicate with one another, and engage in social interactions. This strategy advances social media by combining asynchronous information sharing with synchronous (live) engagement, taking it to a new level.

xvi. VIRTUAL CONFERENCES

To improve social connections, software companies like Microsoft and Meta are working to provide metaverse alternatives to typical zoom meetings for virtual meetings. Workers will soon be able to travel between offices and engage in social interaction in shared virtual worlds thanks to technological advancements.

xvii. VIRTUAL TOURISM

One of the most well-liked metaverse use cases is VR tourism, which has the potential to be widely accepted and recognized. YouTube, Netflix, and other well-known video streaming providers are modifying their platforms to enable 3D media, such as 360-degree videos.

How about exploring the world entirely from your living room? It would be a fascinating possibility to develop virtual worlds in a period when travel is constrained and climate change is a serious issue. Imagine experiencing the Swiss Alps, scaling the Himalayas, or exploring the Istanbul bazaar on your own in game-like settings. It would be feasible to go to other planets in virtual worlds, as well as to many other locations we probably can't envisage.

xviii. WORK AND LEARNING ENVIRONMENTS ONLINE

The COVID-19 pandemic has forced businesses all around the world to switch to digital communication methods. Platforms for video conferencing have also grown significantly in popularity for work-from-home situations like online learning and remote employment. The real-

time audio and visual interaction on these platforms prevent them from offering a compelling, captivating experience.

Through its graphically rich virtual world, 3-D avatars, and immersive meetings, Metaverse offers consumers a more engaging experience to alleviate this constraint. With the help of the Metaverse, we can interact with lifelike participant avatars while navigating a virtual environment rather than viewing the participants on a computer screen and conversing through microphones.

xix. VIRTUAL MARKETS AND COMPANIES

Businesses have new chances thanks to technology, which also aids in the efficient promotion of their products and services. Businesses are moving away from the two-dimensional surface of e-commerce and adopting lifelike virtualized worlds for a profound experience thanks to the growing application of the Metaverse.

Owners of e-commerce businesses can conduct trade formalities including product inspection, negotiations, and transaction closure with merchants in a virtual setting. Additionally, rather than relying on digital marketing strategies, companies can better impact customers by creating engaging and realistic marketing material.

Metaverse technology supports the production, ownership, and exchange of digital assets as well as the tokenization of physical assets, enabling cryptocurrencies and NFTs.

7. TECHNO LEGAL CHALLENGES IN CYBERSPACE

i. WHAT IS CYBERSPACE?

Although there isn't a precise definition for the phrase "CYBERSPACE," William Gibson first used it in his novel "Neuromancer" in 1984. Prior to 1984, he also wrote the book "Burning Chrome" in 1982, when he first introduced the phrase "cyberspace." Cyberspace, which was established by the internet, is a virtual or hypothetical space without physical borders or regions.

Cyberspace is a vast computer network made up of numerous networks spread out throughout the globe that use the TCP/IP protocol to facilitate communication and data exchange. It is a three-dimensional representation of a computer network's virtual space. Three layers make up cyberspace:

- Physical Layer: This layer contains the physical components of the network, such as computers, wires, etc.
- Logical Layer: In this layer, there are no physical components like cable or other wires.
- Social Layer: An additional layer over logical Layer.

ii. CYBERCRIMES

One may define cybercrimes as crimes that explicitly included computers and networks. Here are some examples of common cybercrimes:

- Child pornography: Pedophiles (those who are physically drawn to children) lure children by exposing them to explicit content before pursuing them for sexual exploitation.
- Credit card fraud is the theft of a cardholder's personal information in order to evade payment.
- Cyberstalking is the practise of threatening or harassing a victim through the internet. It is possible to stalk someone via the internet, emails, or other communication tools.
- Data Diddling: In this procedure, raw data is changed immediately before it is processed by a computer and then changed back once it is finished.
- Distribution of Malicious Software: in this a software is designed which is to perform unwanted illegal act through computer network.
- Hacking: an unlawful interruption into a computer framework and system.
- Identity fraud: it is the use of someone else’s identity for illicit purpose.
- Mail Bombs: it refers to the sending of countless E-Mails to the victim so as to crash the victim’s Email account or an E-Mail service provider.

- Password Sniffing: Password Sniffers are programs that screen and record the name and secret key of organization clients as they login, threatening security at a site.

The regulatory climate in India has always been difficult and complex. Regulations and other promotion programmes are often announced at the national level. India recently released new bills and rules touching data protection, privacy, cross-border data flows, and data localization. New bills and guidelines have been announced that have an impact on these issues and others, including data protection, privacy, and cross-border data flows. In addition to the National Cyber Security Strategy in 2020 (NCSS 2020), the GOI has also introduced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules in 2021, the Personal Data Protection Bill (PDPB) draught, the Non-Personal Data Governance Framework, and other regulations.

A digital tax is now in place in India. Equalization Levy is the name of this tax, and it is levied at a rate of 2% of the value of the consideration received or that is due to an E-commerce operator from the delivery of products or services. This was announced in March 2021 and went into effect in April of the same year.

The regulations that are currently in place to regulate information and communication technology were derived from various Acts.

- The Indian Telegraph Act of 1885,
- The Indian Wireless Telegraphy Act of 1933
- The Telegraph Wire Unlawful Possession Act of 1950
- The Cable Television Network (Regulation) Act of 1995

The Information Technology Act of 2000 regulates the internet and addresses all issues connected to data security, cybercrime, digital signatures, electronic commerce, etc. Additionally, this act forbids privacy and confidentiality violations and gives legal validity to online business activities. The Act also addresses problems with electronic transactions, hacking, network service providers, and digital signatures. It attempts to answer problems pertaining to cyberjurisdiction. This Act also covers violations and offences committed by anyone, regardless of nationality, when they were outside of India.

However, it should be emphasized that the Act is quiet on the subject of access to and exchange of personal data, which is covered by data privacy legislation in many nations. There are no particular provisions relating to individual data privacy in the current Act.

It is extremely likely that as technology develops, there will be circumstances and transactions that the IT act of 2000 mentions that won't be able to offer the people and the businesses conducting their business connected to personal data the protection and remedies they need.

The parties will ultimately have the option to sign data privacy agreements. All of this has an impact for outsourcing and BPO firms based in America and Europe, where personal data is protected by law.

The concept of privacy is essentially the right to be left alone and to have a private area free from intrusion and observation. One person's loss of privacy is another's gain in understanding, and the right to selective reveal is another definition of privacy. Personal liberty includes the right to privacy, which must also exist as a requirement for one to enjoy that right. Privacy is also crucial to living a respectable life. The three concepts of liberty, dignity, and privacy can be seen as the essential elements of a person's existence.

Every person has the right to live in freedom, without interference in their personal lives, and to have their personal information protected, which is closely tied to their right to privacy. The terms public and private should be understood in opposition to one another. Therefore, it is essential that the right to be left alone and its protection be given top priority in the current intrusive information technology age. As there is no

single comprehensive enactment, the legal provisions governing data protection must be derived from several legislative enactments.

Together, Article 19 (1) (a) and Article 21 of the constitution allow the courts to interpret the right to privacy however they see fit. After carefully examining the development of privacy laws in India, it has been determined that this law primarily developed from torts and the Constitution. Common law damages for invading one's private space can be discovered, and Article 21 provides a fair restriction for invading it.

Without a doubt, privacy is a fundamental human right that has been recognised and respected on a global scale, and it is well-established in contemporary law that privacy is an integral part of human individuality. Human rights have been enshrined in international and regional accords. In each of the aforementioned regimes, privacy occupies a key position.

The information superhighway is currently not the safest location for issues with electronic transactions. Because there are no geographic boundaries between the cybersphere and its associated criminal activities, this complicates matters because it makes it difficult to gather evidence. In the next years, privacy in the realm of the internet market will cause more harm than good. It is in everyone's best interest to maintain their right to privacy, which is a space that is unaffected by any outsiders or institutions.

Personal information might take the shape of hobbies, routines, and activities, as well as familial, educational, and communication-related information including phone and email records, medical, and financial records.

iii. PRIVACY AND DATA PROTECTION IN E-COMMERCE

a. LEGAL AND TECHNO-LEGAL CONCERNS

The right to privacy is crucial to e-Commerce and is linked to issues of security and trust, creating a serious challenge for users. The protection of user privacy during online transactions has become increasingly important over time. Legal issues relating to e-commerce transactions include the challenge of defining "privacy" and "data privacy," whereas techno-legal issues include confidentiality, tracking consumer behavior through cookies, data theft, the danger of security breaches and uninterruptible login over the internet, logic bombs/computer viruses/hacking/web bugs, telephone tapping, and CCTV monitoring issues.

Privacy relates to the individual, whereas cyber security is more complicated and encompasses the entire ecosystem. In spite of several amendments that have modified as well as added new or additional sections to provide a comprehensive law governing e-Commerce, it has miserably failed to give a precise and universally accepted definition of the term "Privacy" and "Data Privacy," and as a result, has generated a great deal of controversy. Over the years, thinkers, research scholars, and the general public have become overburdened with the issues pertaining to Privacy and Data Protection in the internet world.

The only anticipated solution for containing the legal, techno-legal, and regulatory difficulties is a comprehensive regulation that addresses the emerging dangers to privacy and data protection in eCommerce.

b. CONCERN WITH CONFEDENTIALITY

In cases where a body corporate neglects to ensure adoption of reasonable security practices to protect individuals' personal data, Sections 72 and 72A of the Information Technology Act of 2000 prescribe penal provisions for breaches of confidentiality, enabling an aggrieved person to file a lawsuit for damages before the Adjudicating Authority designated under Section 46 of the Act.

iv. LEGAL CONCERN IN TECH INDUSTRY

With every new idea that hits the market, technology continues to advance. Massive technical advancements have occurred over the past 50 years, from the general adoption of colour television to the development of the internet and cryptoassets. The law is frequently playing catch-up in this dynamic, unexpected, and innovative environment. This means that companies must examine major patterns to see where legislative change may occur.

Technology has an impact on individual privacy and continues to change how we perceive privacy. 15 People have different ideas about what privacy is, but by thinking about the taxonomy of privacy in connection to various forms, we may clear up the confusion over what privacy actually is.One of the most important developments attained by human beings is the creation of internet. Most important impact has been in the transmission of information. As there exist multiplayer's in the locale of the internet. It is, therefore, sometimes described as the 'information technology communications anarchy' 16. Many scholars are of the view that onus of proving right to privacy falls under those who objects it.

v. CLOUD COMPUTING

From the perspective of data security and privacy, cloud computing presents a significant legal danger. All tech companies should take into account the full data lifecycle, from generation to transfer and storage, while utilising cloud computing.

When relying on cloud computing, other crucial factors include making sure that strong contracts, internal policies, and insurance are in place to help manage lawsuit risks and regulatory scrutiny. International servers are available from a number of large cloud solution providers. This must be taken into account when developing data rules, and applicable regulations governing transnational data transfers must be followed.

vi. PROTECTION OF DATA

For tech companies, data protection reigns supreme. Your reputation could suffer and you run the danger of losing business if you are not on top of this. Strong and clear policies, such as those governing privacy and cookies, are essential.

Nearly all tech companies will utilise and handle personal data (including the data of their staff). Drone cameras, facial recognition, and other cutting-edge technology frequently ignore the reality that they are processing personal data.

Therefore, it is essential that technological products are developed in accordance with privacy rules, to safeguard users and reduce the likelihood of legal challenges and severe fines. A data breach is always a possibility.

Therefore, it is crucial to make sure that you have practical rules and procedures to successfully handle any breach.

The Information Commissioner's Office is the governing body for data-related offences. It posts helpful content on its website.

vii. ENVIRONMENTAL SOCIAL AND GOVERNANCE(ESG)

Stakeholder expectations are always rising, and there is a growing reliance on digital products. We are witnessing governments become more and more involved in ethics and accountability as a result of these rising demands. It is crucial that digital companies think about how to increase their ESG accountability. The impact of any legal change on stakeholders, particularly investors, will be lessened by ensuring their satisfaction.

Businesses should generally aim to do the following when taking ESG into account:

- Conduct an assessment of their operations to identify and prioritise appropriate ESG areas;
- Ensure that ESG is discussed at the board level and that the board is kept informed of requirements and information on ESG issues so that changes can be made;
- Address technology, regulatory, and monitoring of specific ESG requirements;
- Improve corporate reputation by unmistakably demonstrating ESG compliance.

There are numerous ways to accomplish this, but it is advised to have a clearly visible outward-facing ESG policy; properly negotiate contracts with suppliers and other partners, taking into account their ESG compliance and making sure that doing business with them won't damage a company's brand.

viii. INFORMATIONAL PROPERTY(IP)

For tech companies, IP protection should come first. Particularly if you are working with outside developers, you should have precise paperwork to verify IP ownership. IP rights can, in theory, only be transferred in writing. You should explicitly indicate in a document that you will own all intellectual property developed by the developer if you outsource any development.

As tech businesses are founded around their intellectual property, we also advise completing thorough due diligence checks on the third-party providers and having any contracts evaluated before signing.

You should carefully consider how to safeguard your IP from users both in the Metaverse and the real world. If you discover a breach of intellectual property, you should file a claim right away.

ix. INVESTMENT

The bulk of tech companies will need funding to expand and improve their product. To safeguard themselves and their company when investors are involved, founders must seek legal counsel early on.

When discussing essential product knowledge, confidentiality agreements are crucial for tech companies. It has been demonstrated that hiring attorneys early on will save money in the long run. Since they have likely encountered such problems before, they can provide wise business advise.

It is important to keep in mind that if investment paperwork are not in your best interest, you could unknowingly give up a lot of influence over your company. Therefore, it is best to consult attorneys as soon as possible.

8. THE INFORMATION TECHNOLOGY ACT 2000 DEALS WITH AS:

i. HACKING

a. Section 66 C: This law addresses identity theft and stipulates that anyone who uses another person's electronic signature, password, or other unique identification feature fraudulently or dishonestly faces up to three years in prison and a fine of up to INR 1,000,000 in addition to other penalties (Rupees One Lakh)

b. Provision 66 E: This section states that anyone who willfully or knowingly violates someone else's privacy by taking, publishing, or transmitting a photo of their private area without that person's agreement will face up to three years in prison or a fine of not more than INR 200,000/- (Indian Rupees Two Lakh) or with both.

ii. SPAMMING

Cybersecurity privacy is at risk in this sector as well, which is a growing issue for all internet users. It is a tool used by abusers to assist them when they frequently send emails to a specific address or addresses. It is known as an unsolicited mass e-mail or an unsolicited commercial e-mail.

When there is no prior relationship between the parties and the recipient has not given their express consent to receive the communication, it is deemed to be of this sort and must be unsolicited. Since everyone contributes to the expense of running the internet, it is nearly identical to unsolicited telephone marketing calls with the exception that users pay for a portion of the message.

Spam is primarily commercial advertising. It is a kind of bulk mail that is acquired by businesses that focus on building email distribution lists from the sender's perspective. In order to retrieve email addresses, the commercial websites gather information through automated searches. Cookies are used and data mining is used to assist them.

Section 43:

These are also referred to as web beacons, which are file objects that are added to web pages or emails in order to track user activity and act as a form of spyware. The online advertising sector favours the more comprehensible terms clear GIFS, invisible GIFs, and beacon GIF over the term "web bugs."

Due to its transparency, ability to blend in with the background, and small size, it is frequently unnoticeable to the user. An IMG element that loads from a different web server than the rest of the page may usually be found if the user examines the website's source version.

iii. WEB BUGS

When an email user accesses his email inbox and reads the message the web bug can call home, the user may be able to report back the time and date they had opened it. By using this method, the sender is made aware of this information. Although advocates for online privacy are against the use of bugs generally, they can be used for good, such as to monitor copyright infringement on the Internet.

If a web bug is installed in a computer without the owner's or state's consent, a penalty will be applied in accordance with sections 43(b) and (c) of the IT Act, 2000.

Section 43:

For damage to the computer, computer system, etc., there are penalties and compensation.

If someone downloads, copies, or extracts data, computer databases, or information from a computer, computer system, or computer network without the owner's or another person in charge of those items' permission, this includes data held or stored on any removable storage medium; and causes to be introduced any computer contaminant or computer virus into any computer, computer system, or internet.

iv. INTERNET STALKING

It is a phrase for tracking someone's online activities, such as their movements and clicks, while they are browsing or surfing. An organisation might do this to profile a possible client, while a potential criminal would do it to gather data for illegal purposes. As a result, it has been deemed a violation of privacy, and if it is done with the intent to commit a crime, the usual rules must be followed to deal with the crime and any linked activity. However, regulations governing this kind of criminal behaviour, such as privacy violations, have not yet been created.

The harassment caused by the stalker can also be mental, physical, racial, religious, sexual, or any other type of harassment. As a result, another type of linked field of invasion of the privacy of internet users, or Netizens, is brought about by cyber harassment as a crime. Cybercrime of a serious character, breaching the priceless and incredibly private, touchy area of one's privacy on the cyber network, is the violation of the privacy of online transactions. As more people use computers and the internet, cyberstalking is now [14] becoming more and more prevalent.

v. PHISHING AND PHARMING

These are the names of fake emails that trick users into disclosing their private information. Phishing, which involves sending an email to a user while pretending to be a valid internet address with a reason usually to verify personal information or private information, is a method of identifying theft and obtaining personal data.

Phishing is a term used to describe this kind of email scam. By sending the user an email that somehow instructs them to visit a website, the user may be requested to update personal information that the legitimate organization already knows, such as passwords or credit card details. Usually, the email will mention the consequences for not clicking the link, such as the possibility of your account being closed.

vi. DATA ACQUISITION

Today, databases can reach terabyte sizes because to the information technology sector's rapid development. But sometimes, because the datasets are so large, it is challenging to draw a meaningful conclusion. Data mining has been the most recent answer to this issue.

Data mining comes in two flavours: descriptive and predictive. In general, descriptive models are used to build meaningful subgroups like a demographic cluster by describing trends in existing data. Predictive models, on the other hand, can be used to forecast explicit values that are based on patterns identified from previous outcomes.

vii. KEY ISSUES AND EMERGING TECHNOLOGIES

Security concerns, ethical concerns, a lack of standardisation, globalisation, and the emergence of new technologies provide challenges for the IT sector, the law, and the government of India, among other significant issues.

viii. NEW TECHNOLOGY DEVELOPMENT

As more people utilise the internet, ICT technology advances. Therefore, as more people utilise the internet, crime rates are rising. The new Act needs to be revised in front of the technology, which is a major concern for cyber lawyers and the GoI. India has the second-highest percentage of internet users in Asia.

ix. ETHICAL CONCERNS

Another problem that makes hacking more difficult is the lack of ethical hacking experts that can spot a hacker's vulnerability. The difficulty is in producing more ethical hackers who are aware of laws and complaints.

x. USE OF SOCIAL NETWORKS IN EXPANDING

Another aspect of cybercrime is the use of social networks and media like Facebook. Social media is used by people to exchange data. The retention of customer data by service providers is against IPR. Data misuse results in criminal activity. The difficulty lies in managing and implementing the legislation on the service provider's and the social media partner's platforms. To lessen the misuse of Data, a legal framework should be put in place for the customers, service providers, and social media partners. Crime Branch of India is establishing more cybercrime cells in India to help and educate the populace. The rate of internet use and Facebook statistics for India are shown in the table below.

xi. LACK OF GLOBALIZATION AND STANDARDS

Cyberspace-related laws are not uniform or universal. For terrorism and cybercrime, different nations have varied laws and penalties. The difficult part is making cyber law a global concern and enforcing a standard law across all borders and jurisdictions.

xii. SECURITY CONCERNS

The data are digitally stored in cyberspace. The system must be more secure so that only authorised users can access the data. Due to lax protection, illegal acts take place where an unauthorised individual can access the data. Cyber Law in India has different lawsuits in ITA-2008 and punishments under IPC for this kind of criminal activity. The Indian government started implementing several cyber security policies. A tech-legal corporation and law firm called Perry4Law and Perry4Law's Techno Legal Base (PTLB) has identified numerous weaknesses in Indian cyber security initiatives that have paralysed [2]. The business should be legally organised with intellectual property rights (IPR) laws in place, such as copyright for software and organisation trademarks.

Security risks related to intellectual property include the distribution of unlicensed software and the theft of digital trademarks. The government of India has new hurdles in maintaining adequate policy control over time through a technological legal framework and sound legal procedure. Without any parliamentary supervision or permission, Indian security and intelligence services are in charge of many cyber security-related projects. India needs to classify its cyberlaw, and this requires

intelligence, transparency, and reforms. It should be normalised by GoI over time. These agencies cannot be awarded cyber immunity without it. India must secure its cyberspace while balancing civil freedoms and needs for national security.

Volume - I

- Overview of Cybercrimes
- Information Gathering
- Crime Scene Management
- IP, Website and E-mail Investigation
- Communication Device Based Investigation
- Investigation of Financial Frauds
- Social Media Investigation
- Windows & Network Forensics

Volume - II

- Mobile Phone Investigation & Forensics
- IPDR and VoIP Investigation
- Cyber Security & Framework

Volume - III

- Disk Forensics
- Operating System Forensics (Windows, Linux & Mac)
- Browser Forensics
- Servers and RAID configuration
- Investigation of Digital Payment Frauds
- Virtual currencies and Crypto currencies
- Open-Source Intelligence

Volume - IV

- Malware and network forensics
- Dark web and cryptocurrency
- Advance Digital Forensics

Volume - V

- Trending Modus Operandi of Cybercrimes
- Acquaintance to Web Server and technology
- Investigation of E-Mails
- Cyber Law and Admissibility of Digital Evidence
- Digital crime Scene management
- Social media Monitoring and Sentiment Analysis
- Dark Web & Cryptocurrency Investigation
- New Technologies (Cloud, Metaverse, IoT) Investigation & Challenges