Sardar Vallabhbhai Patel
National Police Academy,
Hyderabad

Cyber Crime Investigation Manual

Volume - I

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

1. Overview of Cybercrimes

1.1 Introduction to Cybercrimes

The IT revolution resulted in a phenomenal increase in the number of internet users all over the world. It helped millions of users connect online thus facilitating sharing of information. In India also there was an overwhelming increase in number of internet users. Internet in every field of the society and due to this increase in usage of Internet, a number of new crimes have evolved. Such crimes where use of computers coupled with the use of Internet is involved are broadly termed as Cyber Crimes.

If looked into practicality, it is not at all easy to define cybercrimes. In order to define such an offense, when the nature of such offense is seen, it is a combination of crime and computer. So it can be said that, 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. One legislation that deals with the offences related to such crimes in India is Information Technology Act, 2000, as amended in 2008.

1.2 Classification of Cybercrime / Important Cybercrimes.

Cyber crimes were classified by various people differently on the basis of different criterion. For the purpose of understanding the cyber crimes from the investigation point of view and the spread of the damage or impact it can have, Cybercrimes can be classified into:

a). Cybercrimes against individuals

b). Cybercrimes against organizations

c). Cybercrimes against country

Now, we will see each classification in detail.

a) <u>Cybercrimes against individuals</u>

Cybercrimes committed against individual persons include such types of crimes like transmission of Child Pornography, Harassment of any one with the use of a computer such as e-mail, Cyber Defamation, Hacking, Indecent exposure, Email spoofing, IRC Crime (Internet Relay Chat), Net Extortion, Malicious code, Trafficking, Distribution, Posting, Phishing, Credit Card Fraud and Dissemination of obscene material including Software Piracy. The potential harm of such a crime to individual person can hardly be bigger.

i) Cyber Stalking/ Cyber bullying

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.

Majority of the stalkers are the dejected lovers or ex-lovers, who then want to harass the victim because they failed to satisfy their secret desires. Most of the stalkers are men and victim female.

How do they operate?

They collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. If the stalker is one of the acquaintances of the victim he can easily get this information. If stalker is a stranger to victim, he collects the information from the internet resources such as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website.

The stalker may post this information on any website related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have sexual services. Stalker even uses very filthy and obscene language to invite the interested persons. Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and sex sites, because of which victim starts receiving such kind of unsolicited e-mails.

Some stalkers keep on sending repeated e-mails asking for various kinds of favours or threaten the victim. In online stalking the stalker can make third party to harass the victim.

Stalkers will almost always make contact with their victims through email. The letters may be loving, threatening, or sexually explicit. He will many times use multiple names when contacting the victim.

Contact victim via telephone. If the stalker is able to access the victim's telephone, he will many times make calls to the victim to threaten, harass, or intimidate them.

The fact that cyber stalking does not involve physical contact may create the misperception that it is more benign than physical stalking. This is not necessarily true. As the Internet becomes an ever more integral part of our personal and professional lives, stalkers can take advantage of the ease of communications as well as increased access to personal information. In addition, the ease of use and non-confrontational, impersonal, and sometimes anonymous nature of Internet communications may remove disincentives to cyber stalking. Put another way, whereas a potential stalker may be unwilling or unable to confront a victim in person or on the telephone, he or she may have little hesitation sending harassing or threatening electronic communications to a victim. Finally, as with physical stalking, online harassment and threats may be a prelude to more serious behaviour, including physical violence.

ii) Identity theft

Identity theft is becoming a fast growing problem in the India, as more and more ways are discovered to steal someone's identity. 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. Anyone getting a piece of personal information in a wrong way can be considered as identity thief. Identity Theft as a term refers to wrongful use of personal information with an intention of causing legal harm. The person whose Identity is used can suffer various consequences when they are held responsible for the Identity thief's actions. Personal information may include the following but it is not limited to the 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.

Different Methods /ways Identity theft can happen

- In public places people may be watching you from a nearby location by listening to your conversation if you give personal information over the telephone and is known as "shoulder surfing".
- Many people respond to "spam"– unsolicited E-mail – that request personal data by promising them some benefit.
- Don't give away your personal information in the survey forms given in restaurants/shopping malls/movie theatres as they collect this information and sell it to other parties for money.
- After shopping at super markets and medical stores retail chains in malls and other outlets insist on giving our phone number saying that it is for add on points which can be used for the next purchase which in end up in their spamming database.
- Criminals may access your private information from online shopping portals, ecommerce sites and online bank accounts and use that information against you or for self benefit.
- Criminals may access Routers without WPA encryption (Wi-Fi protected Access) and has weak and no password are vulnerable to identity thefts.
- Stealing of personal Information through Malware (Viruses, backdoors, keystroke loggers and screen scrapers).
- Identity thief always scans through all your social networking sites and also in government registers or public records to get personal information.
- Retrieving Information from computer servers that have been handled carelessly.
- Advertising Job Offers / Gift Offers / lottery through different media like whtsApp , SMS etc.
- Personal information from smart credit cards can be read though RFID (Radio Frequency Identification) device without even physical contact with the card. Stealing electronic record through a data breach.

With enough identifying information about an individual, a criminal can take over that individual's identity to conduct a wide range of crimes like:

- ❖ Submit false applications for loans and credit cards.
- ❖ Make fraudulent withdrawals from bank accounts.
- ❖ Make fraudulent use of online accounts like social media. ❖ Obtain new phone connections to carry out forgery and other frauds ❖ Obtaining other goods or privileges in your name.
- ❖ Use PAN card number to file a tax return and claim fraudulent tax return.
- ❖ Make multiple range of debts in victim's name. ❖ Fraudster uses identity to Apply and earn a job.
- ❖ Use Medical Insurance Number for discounted health care benefits or prescription drugs.
- ❖ Use children's personal information to avail government benefits.
- ❖ Fraudster can use your driving license/Passport/Aadhar Information to avail benefits in your name.

Types of Identity Theft

Stealing : Electronic wallets, purses, mail, or using other sources to gather personal information

Dumpster Diving: Getting hold of invoices, financial records or other documents containing personal information from the thrash.

Fraudulent change of address: Completing a "change of address" form to divert your mail to their new location.

Pharming: Creating fraudulent Web sites that look legitimate in order to collect personal information from consumers.

Phishing: Gathering personal information from forms that are linked from e-mails or pop-ups.

Fig.1.1: Sample Phishing page

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

Vishing: This is "voice phishing" where customers are contacted by e-mail or automated phone calls telling them that their checking accounts have been compromised. Customers are urged to call a local or toll-free number that asks you to input account information and/or your PAN card details.

Tax Identity Theft- PAN card number which is personal information of an individual is stolen for the purpose of filing a tax return and also in 'benami' transactions, purchase of luxury cars, etc.

Medical Identity Theft -Personal Information like Name or Medicare Number stolen to submit fraudulent claims to Medicare and other health insurers without your authorization.

Child Identity theft- Personal Information of a child is used by criminals to apply for government benefits, open bank and credit card accounts and apply for loan and apply for rent to live in or apply for new phone connection.

Pretexting – Identity Frauds use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.

Employment Scams – These scams advertise or send mail with a false offers of job and request for personal information and they will request you to deposit some amount from your personal account to given details in short deadline of time for assurance on job.

iii) Email Related Crimes

- **Email spoofing**: -Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation.
- **Sending malicious codes through email**: - Emails are often the fastest and easiest ways to propagate malicious code over the Internet. Hackers often bind Trojans, viruses, worms and other computer contaminants with e-greeting cards and then email them to unsuspecting persons. Such contaminants can also be bound with software that appears to be an antivirus patch.
- **Email bombing**: - Email bombing refers to sending a large amount 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.

- **Sending threatening emails**: - Email is a useful tool for technology savvy criminals thanks to the relative anonymity offered by it. It becomes fairly easy for anyone with even a basic knowledge of computers to become a blackmailer by threatening someone via e-mail.
- **Email job frauds: -** Email fraud can take the form of a *scam*. Confidence tricks tend to exploit the inherent greed and dishonesty of the victims. Email fraud targets naive individuals who put their confidence in get-richquick schemes or offers to sell popular items at 'impossibly low' prices.
- **Spamming:** - Spamming means sending multiple copies of unsolicited mails. Generally, it does not give any harm but annoying to recipient.

- **Dissemination of obscene material**: - Refers to spreading obscene materials over internet.
- **Cyber Defamation**: Cyber defamation is publishing of defamatory material against another person with the help of computers or internet. If someone publishes some defamatory statement about some other person on a website or send emails containing defamatory material to other persons with the intention to defame the other person about whom the statement has been made would amount to cyber defamation

b) Cybercrimes against Organization

The second type of Cyber-crimes classification relate to Cybercrimes against organization. The growth of internet has shown that the standard of Cyberspace is being used by individuals and groups to pressure the international governments as also to terrorize the citizens of a country. This crime obvious itself into terrorism when a human being "cracks" into a government or military maintained website. It is across the world agreed that any and every system in the world can be cracked.

i) Unauthorized access/Hacking

Hacking in simple terms means an illegal intrusion into a computer system and/or network. There is an equivalent term to hacking i.e. cracking, but from Indian Laws perspective there is no difference between the term hacking and cracking. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. 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. They extort money from some corporate giant threatening him to publish the stolen information which is critical in nature.

Government websites are the hot targets of the hackers due to the press coverage, it receives. Hackers enjoy the media coverage. For Example Web jacking: This occurs when someone forcefully takes 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

ii) Denial of Service (DoS)/Distributed Denial of Service (DDoS)

Denial-of-service (DoS) attacks typically flood servers, systems or networks with traffic in order to overwhelm the victim resources and make it difficult or impossible for legitimate users to use them.

In most respects Distributed Denial of Service (DDoS) attack is similar to a DoS attack but the results are much, much different. 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.

iii) **Computer Contamination**

Computer contaminant" means any data or program that is designed or has the capability to corrupt or destroy other data, information, image, and program contained in a computer, system or network without the knowledge or consent of the person who owns the computer or network.

WannaCry is a ransomware worm that spread rapidly across a number of computer networks in May 2017. After infecting Windows computers, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them.

Fig.1.2: Wanna Cry Ransomware Notification window

Various forms of computer contaminants are described below:

- **Virus**: A computer virus is a small program written to alter the way a computer operates, without the permission or knowledge of the user. A virus cannot be spread without a human action, (such as running an infected program) to keep it going. It spreads by sharing infected files or sending emails with viruses as attachments in the email

- **Worm**: A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer (it has the capability to travel without any human action)
- **Trojan:** A Trojan will hide within seemingly harmless programs, or will try to trick you into installing it. Trojans do not replicate by infecting other files or computers. Instead, they survive by going unnoticed. They may sit quietly in your computer, collecting information or setting up holes in your security, or they may just take over your computer and lock you out.
- **Logic bombs**: These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).
- **Key Loggers:** Key loggers are regularly used were to log all the strokes a victim makes on the keyboard. Key-loggers are most commonly found in public computers such as those in cyber cafes, hotels etc.
- **Ransomware:** Ransomware is a kind of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim. Ransomware malware can be spread through malicious email attachments, infected software apps, infected external storage devices and compromised websites.

iv) **Computer vandalism**

Vandalism means deliberately destroying or damaging property of another. Thus computer vandalism may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer or by physically damaging a computer or its peripherals.

v) **Data diddling**

One of the most common forms of computer crime is data diddling -illegal or unauthorized data alteration. These changes can occur before and during data input or before output. Data diddling cases have affected banks, payrolls, inventory records, credit records, school transcripts and virtually all other forms of data processing known.

vi) Source Code Theft

Computer source code is the most important asset of software companies. Simply put, source code is the programming instructions that are compiled into the executable files that are sold by the software development companies. As is expected, most source code thefts take place in software companies. Some cases are also reported in banks, manufacturing companies and other organizations who get original software developed for their use.

c) Cybercrimes against Country

The third type of Cyber-crimes relate to Cybercrimes against society. In this category forgery, cyber terrorism, web jacking, polluting the Youth through Indecent, Financial Crimes, Sale of Illegal Articles, Net Extortion, Cyber Contraband, Data Diddling, Salami Attacks, Logic Bombs types of crime is included. Forgery currency notes, revenue stamps, mark sheets etc can be forged using computers and high quality scanners and printers. Web Jacking hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money

i) Cyber Terrorism

Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents."

In IT Act, 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;

ii) **Sale of Illegal Articles**:

The Internet has also created a marketplace for the sale of unapproved drugs, prescription drugs dispensed without a valid prescription, or products marketed with fraudulent health claim.

1.3 Glossary of Cybercrime Terms

Back door: Secret (undocumented), hard-coded access codes or procedures for accessing information. Some back doors exist in commercially-provided software packages; e.g., consistent (canonical) passwords for third-party software accounts.

Black hat - a term used to describe a hacker who has the intention of causing damage or stealing information

Bot: a program used for a specific function such as keeping a port open or launching a flood of packets in a distributed denial-of-service attack.

Botnet: a set of bots installed (usually surreptitiously) on a number of victimized computers (zombies or slaves) to launch distributed denial-ofservice

attacks or to send spam. Cracking: malicious or criminal hacking. Unauthorized penetration of computer systems and networks, abuse of privilege, unauthorized use of services.

Cracker - a hacker who breaks into a system with the intent of causing damage or stealing data
Cracking - the process of trying to overcome a security measure

DataDiddling: modifying data for fun and profit; e.g., modifying grades, changing credit ratings, altering security clearance information, fixing salaries, or circumventing bookkeeping and audit regulations.

Data leakage: uncontrolled, unauthorized transmission of classified information from a data center or computer system to the outside. Such leakage can be accomplished by physical removal of data storage devices (diskettes, tapes, listings, printouts and photographs of screen copies or handwritten notes) or by more subtle means such as data hiding (Steganography) or even plain old human memory.

Denial-of-service (DoS) attack: overwhelming or saturating resources on a target system to cause a reduction of availability to legitimate users. On the Internet, usually involves spoofing packets or e-mail headers.

Distributed DoS (DDoS) attack: Internet-mediated attack accomplished by enlisting the services of many compromised systems to launch a denial of service (DoS).

DNS cache poisoning: modifying data in a Domain Name System (DNS) server so that calls to particular Websites or even entire domains are misdirected for fraudulent Purposes.

Easter egg: undocumented, unauthorized program functions in a production program; a kind of Trojan horse.

Exploit: a method for exploiting a vulnerability to take control of a system or otherwise compromise it. Exploits are sometimes automated in scripts.

Hacker - a person who breaks into computer systems for the purpose of stealing or destroying data

Hacking - the process of bypassing the security systems on a computer system or network and hands-on learning about any technical field, including computing.

Hacktivism: A politically- or ideologically-motivated cyber-attack or hack.

Impersonation: pretending to be authorized to enter a secure location. Examples include swaggering into a site equipped with what look like tool kits of the manufacturer of computer equipment, or pretending to be a janitor. Impersonation is a key element of social engineering.
Logic bomb: A program in which damage (the payload) is delivered when a particular logical condition occurs.

Mail-bombing: sending large numbers of unwanted e-mail messages to a single recipient or to a group of such recipients.

Malware: malicious software, including Trojan Horses, viruses, worms, logic bombs, exploits and time bombs.

Master program: in distributed denial-of-service (DDoS) attacks, a program that Communicates with implanted zombie or slave programs on compromised systems.

Payload: the unauthorized activities of malicious software.

Penetration: unauthorized access to restricted systems or resources.

Piggybacking: entering secure premises by following an authorized person through the security grid; also unauthorized access to information by using a terminal that is already logged on with an authorized ID (identification).

Pharming: misdirecting 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.

Phishing: 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.

Root kit: a script or set of scripts for gaining unauthorized root privileges (or equivalent supervisory powers) on a compromised system. Much used by script kiddies.

Sabotage: the word comes from the French for wooden shoe (sabot). Such footwear made a handy weapon for throwing into the gears of new mechanical systems that were causing unemployment during the industrial revolution of the

18th and 19th centuries. The term now means any deliberate damage to operations or equipment.

Salami theft: technique of accumulating round-off errors or other small quantities in calculations and saving them up for later withdrawal; usually applied to money, although it can be part of an inventory-theft scheme (for example).

Scavenging: using discarded listings, tapes, or other information storage media to determine useful information such as access codes, passwords, or sensitive data. Finding a listing for the source code for a new version of a popular proprietary program could be highly profitable for a computer crook. Also known as Dumpster® diving.

Scripts: any simple program, especially using a scripting or macro language; in computer crime work, however, scripts usually refer to automated systems for executing exploits.

Spamming: a popular name for e-mail sent to many unwilling recipients in order to sell products or services (or sometimes to cheat naïve customers). Those wishing to avoid offending the innocent Hormel Corporation, owners of the Spam® trademark, may refer to this indiscriminate bulk e-mail as junk e-mail or (unsolicited commercial email).

Spim: spam over instant messenger

Spit: spam over internet telephony

Spoofing: using incorrect identification; usually applied to electronic misrepresentation such as putting the wrong originating address on a TCP/IP packet. Much used in denialof-service (DoS) and distributed DoS (DDoS) attacks.

Superzapping: using powerful utility software (originally the superzap utility on IBM mainframes) to access secure information while bypassing normal controls. Debug programs, and disk editors are examples of tools used for superzapping.

Time bomb: program or batch file waits for a specific time before causing damage. Often used by disgruntled and dishonest employees who find out they're to be fired or by dishonest consultants who put unauthorized time-outs into their programs without notifying their clients. Logic bombs and time bombs are Trojan Horse programs; time bombs are a type of logic bomb.

Trojan horse: innocent-looking program that has undocumented and nefarious functions. So called by reference to Odysseus' wooden horse filled with soldiers that helped to capture Troy. Trojan Horse programs can, for example, alter data in a particular way, record passwords for later inspection, send confidential information to unauthorized destinations or open back doors into compromised systems.

Vandalism: obvious, unauthorized, malicious modification or destruction of data such as information on Web sites.

Virus: Viruses infect executable code such as programs (e.g., .EXE and .COM files under DOS), boot sectors on disks and macro programs. The viral code reproduces with the host code is loaded into memory. So called by analogy with biological viruses, which subvert the functions of normal cells. Viruses are similar to worms but reside inside programs at all times. A virus can transform an ordinary program into an unintended Trojan horse.

Vulnerability: a weakness or flaw permitting an attack on a computer system or network. Wiretapping: eavesdropping on data or voice transmissions by attaching unauthorized equipment or software to the communications medium (in the case of wires, coaxial metal cables and optical cables) or by intercepting and interpreting broadcast data (in the case of wireless phones, cellular phones, and wireless networks).

White hat - a hacker whose intentions are not criminal or malicious

Worm: program which spreads through a computer system or network by replicating (like a virus) but without integrating itself into other executable code.

Zombie: a program inserted into a vulnerable system to await further instructions; usually part of a distributed denial-of-service (DDoS) attack.

2 Information Gathering

Once a case related to cyber crime gets registered, the investigation officer needs to collect a lot of information from various sources in order to identify the suspect computer that is involved in the commission of crime and the criminals who are behind commission of the crime. Therefore, intelligence gathering is one of the major task in the course of investigation. The investigating officer will be having very few inputs, using that he has to collect maximum amount of details about the criminals or suspects. Here comes the use of various information gathering techniques.

2.1 Open Source Intelligence

Open source intelligence (OSINT) is a form of intelligence collection management that involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence.

Simply, any intelligence produced from publicly available information that is collected, exploited and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement is Open source intelligence.

Open Source Data (OSD) is the not just limited to what is available on internet. It includes the signals of all wireless communication that are there in open air, information available in printed form, broadcast or information in any other form from a primary source which Include photographs, tape recordings, satellite imagery, personal letters, online postings, etc.

OSINT essentially refers to all the techniques using which police officers can collect maximum details about the suspect or criminal from publically available information, mainly from internet.

2.1.1 Open Source Intelligence Using Mobile Number

In cases where the IO is having only the mobile numbers of the suspects or criminals, we can use the following tools which are openly available on internet to collect other details of the suspects.

a) Online recharge Sites

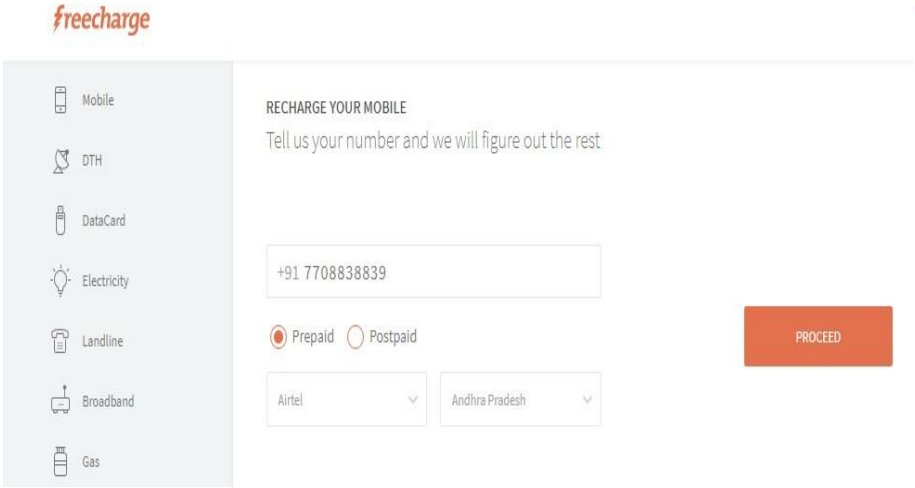


Fig.2.1: Online Recharge website showing MSP name and circle

The Online recharge websites provide the name of the mobile service provider and the telecom circle of a particular mobile number. Once, we get to

know the service provider and the telecom circle, we can send a request letter to the nodal officer for the details of the customer.

b) TrueCaller

Truecaller is a mobile application, which is a worldwide number lookup service. Which means, by this app you can find the name of the user of any Mobile number as saved in the contacts of the person who has installed this app without calling to that number.

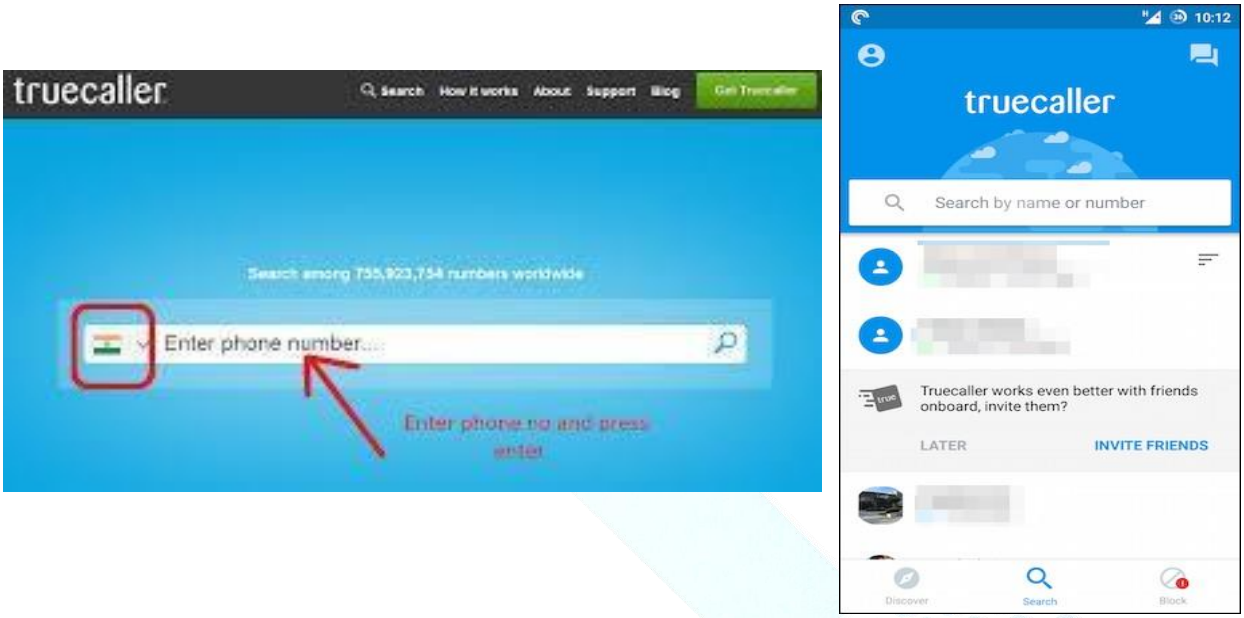


Fig.2.2: Truecaller search

Truecaller have collection of all the contacts (mobile phonebook) of its users (People who use this app) from all around the world and the public phone directories. When a person download and starts using Truecaller, this app uploads all the contacts of that person to its database. So when you search a number on Truecaller, it shows the name used by someone for saving the number in his/her phonebook.

If we come across with a number in between investigation, this service can be utilized to find out the name of the user. It has to be understood that the data on this app need not be correct always. Many times, we get the names of the persons as their nick names that are used to save the contact.

c) Facebook password reset

Facebook provides option for resetting the password using the Email/Phone number/username/ full name. If we know the phone number we can go to the password reset page of Facebook and enter the phone number in the given field. If any Facebook account is linked with this number, that account would be shown. This way we will get the full name and photos of owner of that number.

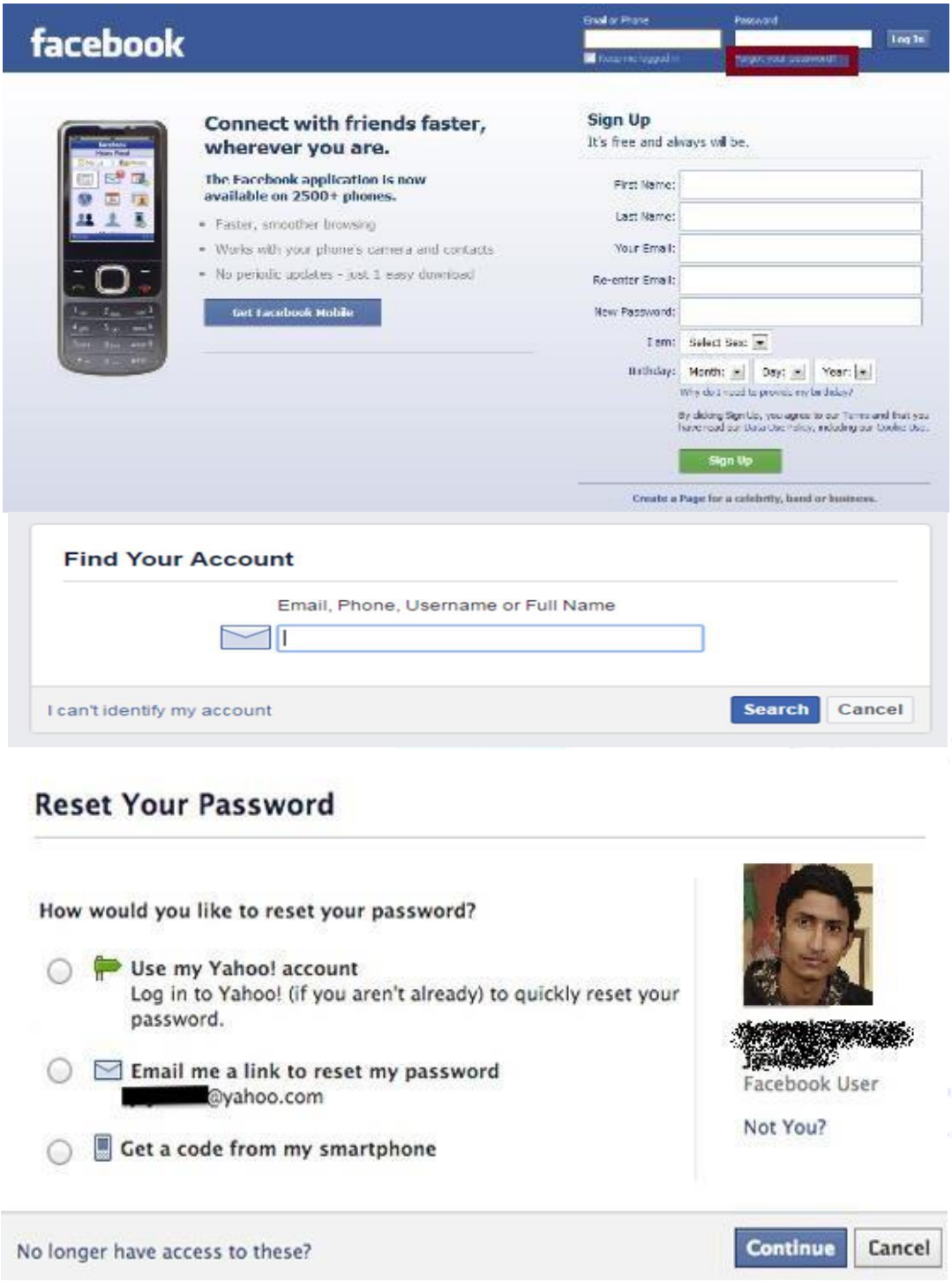


Fig.2.3: Facebook Password Reset steps

d) WhatsApp Contacts

Save the suspect's number to a smartphone in which WhatsApp is installed. If the number is having WhatsApp account, then the user profile can be viewed. This method is possible only if the user has set the privacy settings to public.

Fig.2.4: Contact details in Whatsapp

2.1.2 Open Source Intelligence Using E-Mail Address

We can use the e-mail address to search for a person over the internet.

a) People Search using pipl.com

Pipl.com is an online search engine, which can be used to find the person using the email address, social media username or phone number.

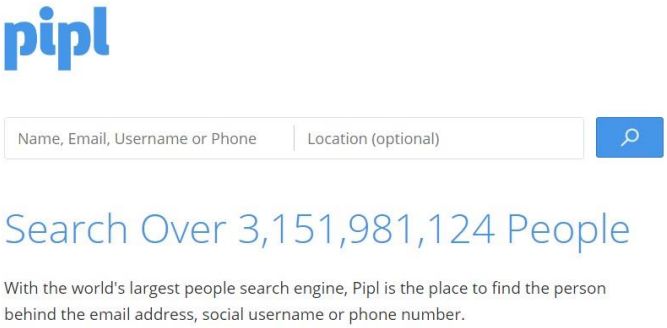


Fig.2.5: pipl search engine home page

b) Facebook password reset

Facebook provides option for resetting the password using the Email/Phone number/username/ full name. If we know the email address of a person, we can go to the password reset page of Facebook and enter the email in the given field. If any Facebook account is linked with this email, those accounts would be shown. This way we will get the full name and photos of owner of that email.

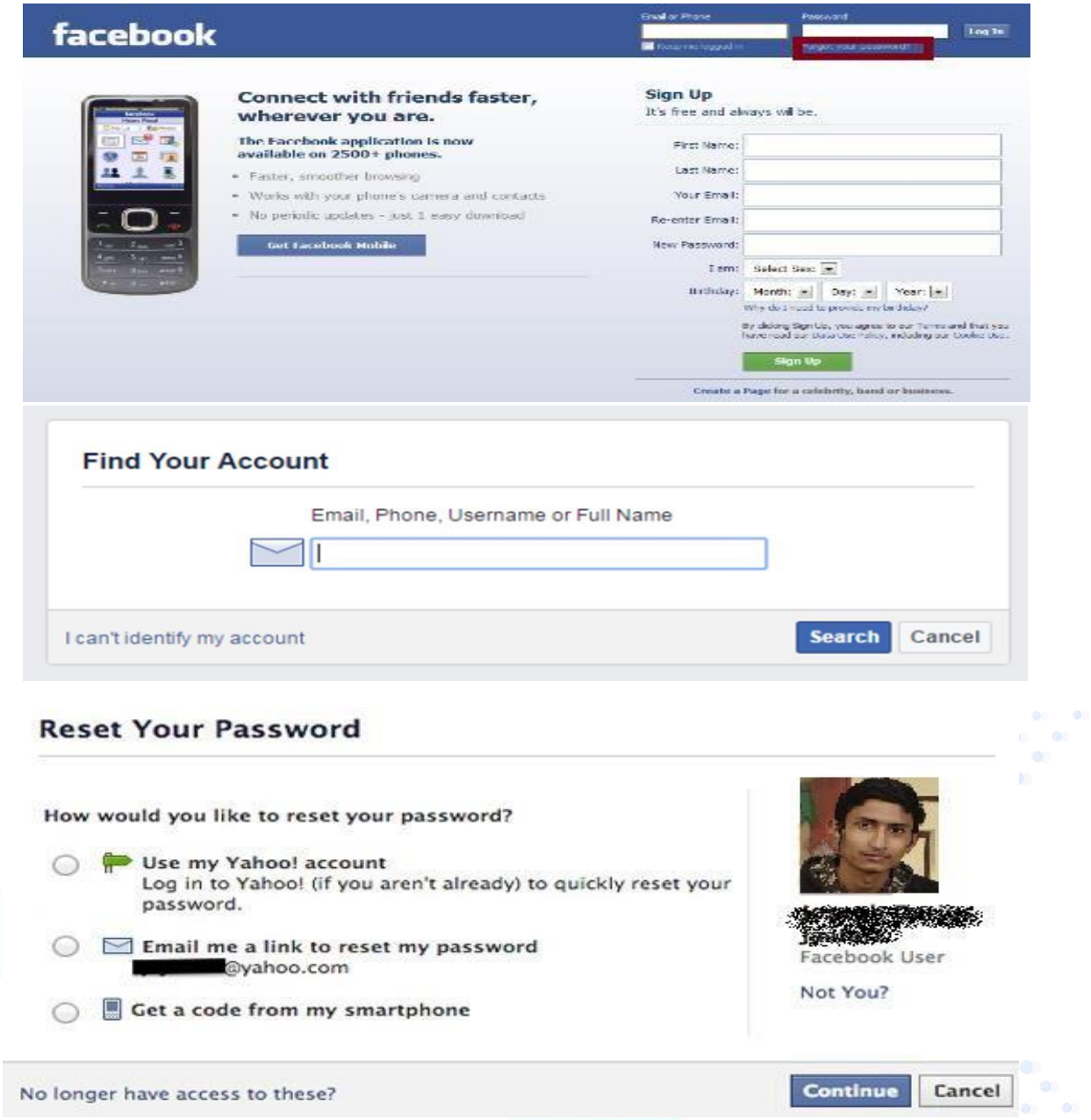


Fig.2.6: Facebook password reset using e-mail

2.1.3 Open Source Intelligence Using Search Engines

A search engine is an application that is designed to search information from the world wide web. One of the most commonly used search engine on the internet is Google, which is having more than 80% of market share. Inorder to provide the results for searches, a search engine maintains the following processes:

- Web crawling- Web search engines get their information by web crawling from site to site
- Indexing- Indexing means associating words and other definable tokens found on web pages to their domain names and HTML-based fields

▹ Searching- when a user enters a query into a search engine, the index already has the names of the sites containing the keywords, and these are instantly obtained from the index.

a) **Google search engine**

It provides various advanced search options using which one can do effective search and filter out unwanted results. It also has mechanism by which one can design custom search queries in google to get desired search results.

A Google dork query, sometimes just referred to as a dork, is a search string that uses advanced search operators to find information that is not readily available on a website. Google dorking, also known as Google hacking, can return information that is difficult to locate through simple search queries. That description includes information that is not intended for public viewing but that has not been adequately protected.

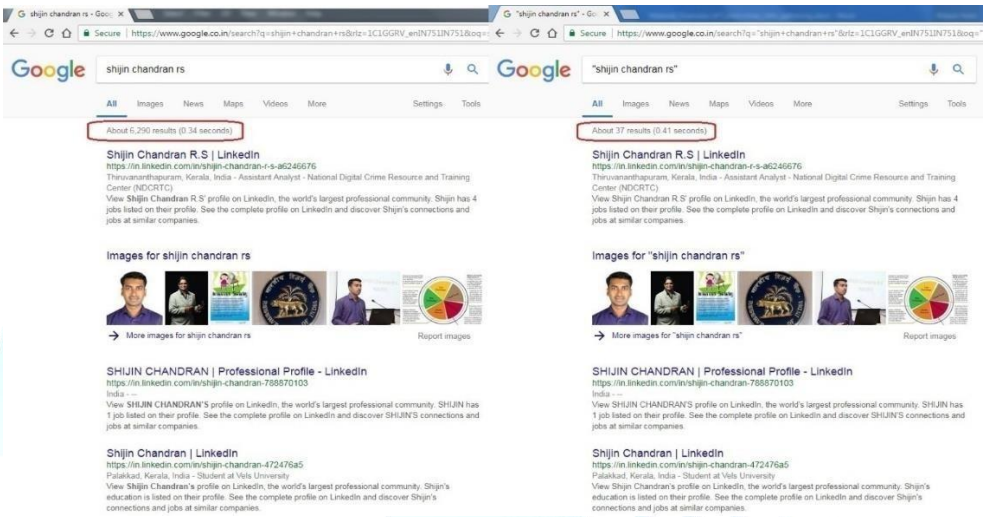


Fig.2.7: Google search with and without quotation mark

For instance, if we want to search exact name of a person or a string, we need to write it in " ". If you want to filter out unwanted results of narrow down the search, we can add the occupation, city or college of target.Just like in simple math equations, programming code, and other types of algorithms, Google Dorks has several operators that can be used for effective searching. There are far too many to include in this guide, but we will go over some of the most common operators:

- intitle – this allows one to search for pages with specific text in their HTML title. So intitle: "login page" will help a person scour the web for login pages.
- allintitle – similar to the previous operator, but only returns results for pages that meet *all* of the keyword criteria.
- inurl – allows a person to search for pages based on the text contained in the URL (i.e. "login.php").
- allinurl – similar to the previous operator, but only returns matches for URLs that meet *all* the matching criteria.

- filetype – helps a person narrow down search results to specific types of files such as PHP, PDF, or TXT file types.
- ext – very similar to filetype, but this looks for files based on their file extension.
- intext – this operator searches the entire content of a given page for keywords supplied by the person.
- allintext – similar to the previous operator, but requires a page to match *all* of the given keywords.
- site – limits the scope of a query to a single website.
- Cache - cache dork will show the cached version of the site or page of the specified site.
- Link - It will restricts results to sites containing links to the specified location.
- Inanchor - It will restricts results to sites containing liks with the specified phrase in their descriptions. inanchore dork will show all the sites which contains links with specified word or phrase.

b) Carrot search

Carrot 2 is a search engine which organizes your search results into various categories and segregates the output of your search into those categories.

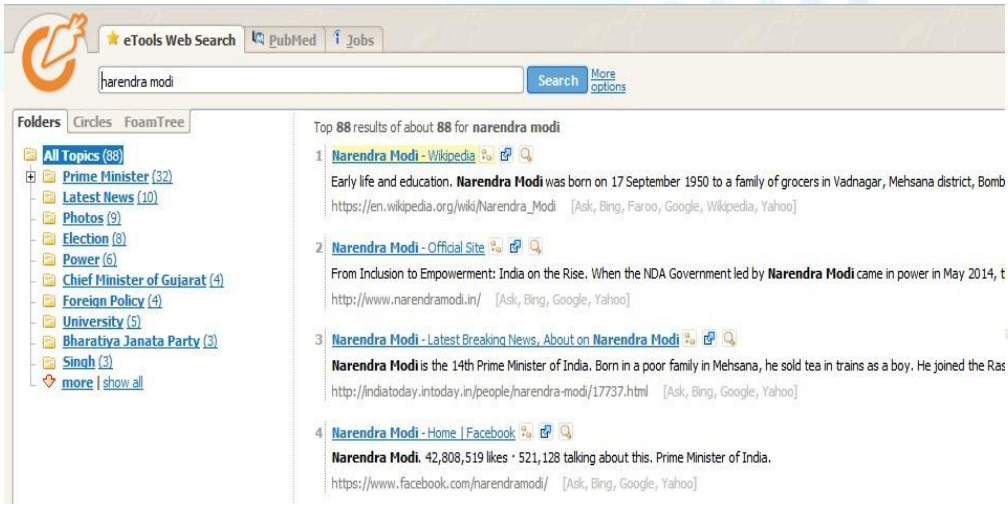


Fig.2.8: search results in carrot search engine

It can automatically cluster small collections of documents, e.g. search results or document abstracts, into thematic categories.

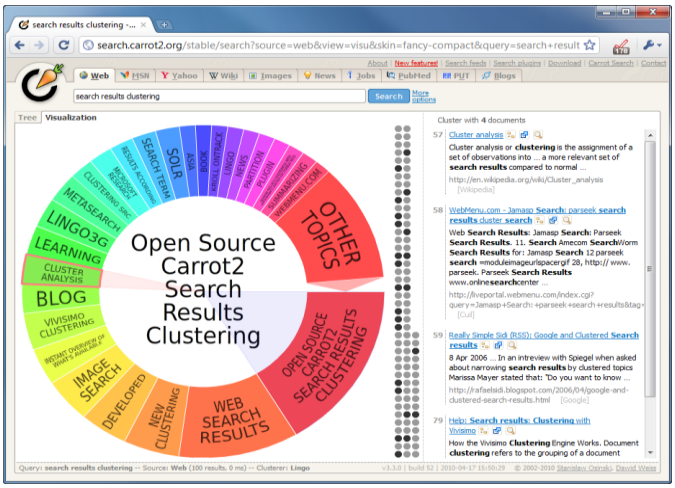


Fig.2.9: Clustered results in Carrot search engine.

2.1.4 Open Source Intelligence using images

During the course of investigation, an Investigating Officer may come across images or photos from which he needs to collect the information like who is in that picture, where it was taken, when it was taken, which camera was used to take that picture etc. Normally, the picture itself stores some such information in the form of metadata of the image or photo. It is also known as exif data of that picture. We can use open source tools for extracting these details from the photographs. For example: www.*exif.regex.info*, *https://29a.ch/photo-forensics*

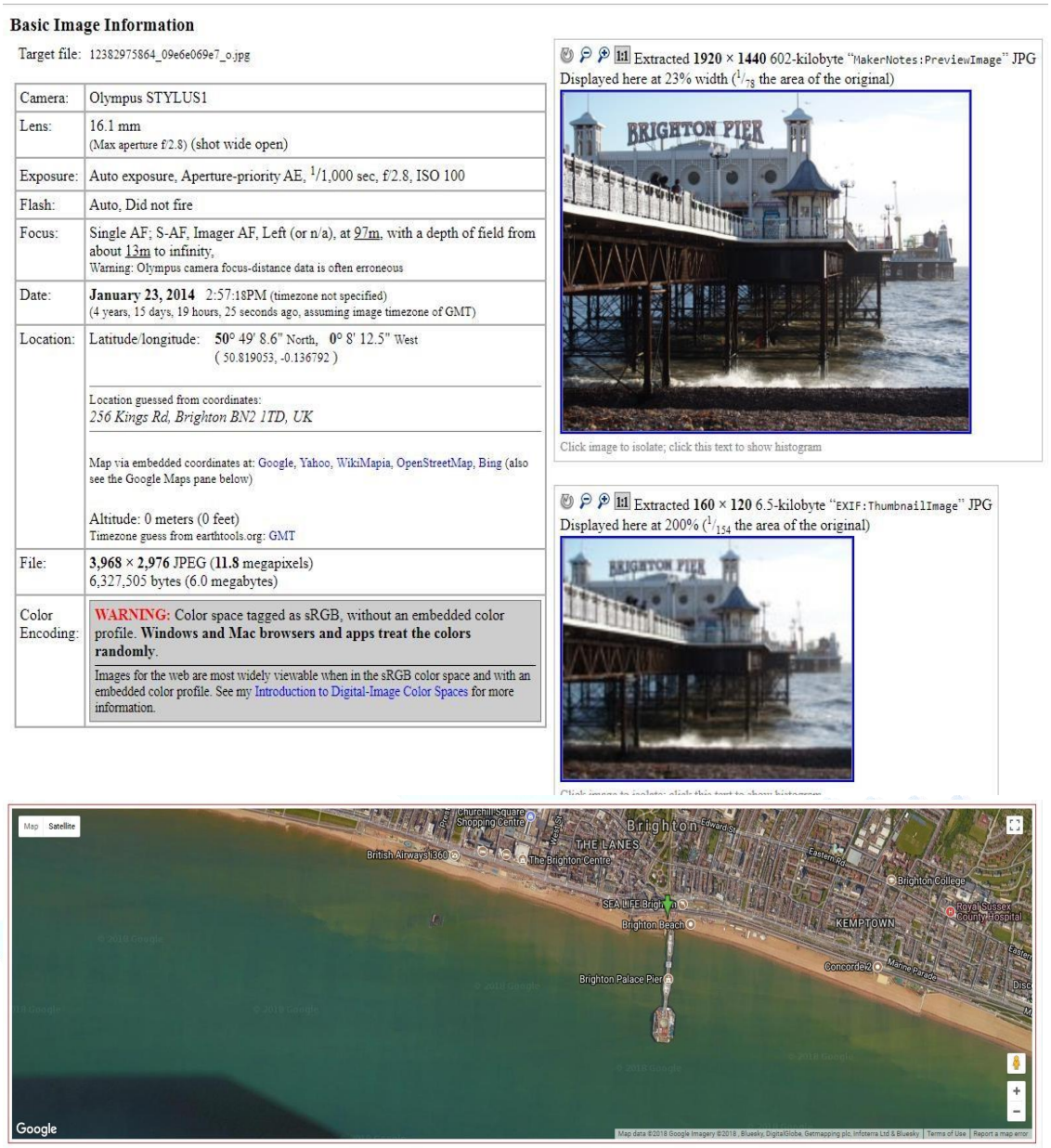


Fig.2.10: Exif data analysis results of an image

a) Reverse Image Search

We can use the picture itself to search in the internet instead of keywords. Using this way we can find out websites where same images has been uploaded or being used. This method can also be used to find out where this image has been uploaded first and where similar images are located on internet.

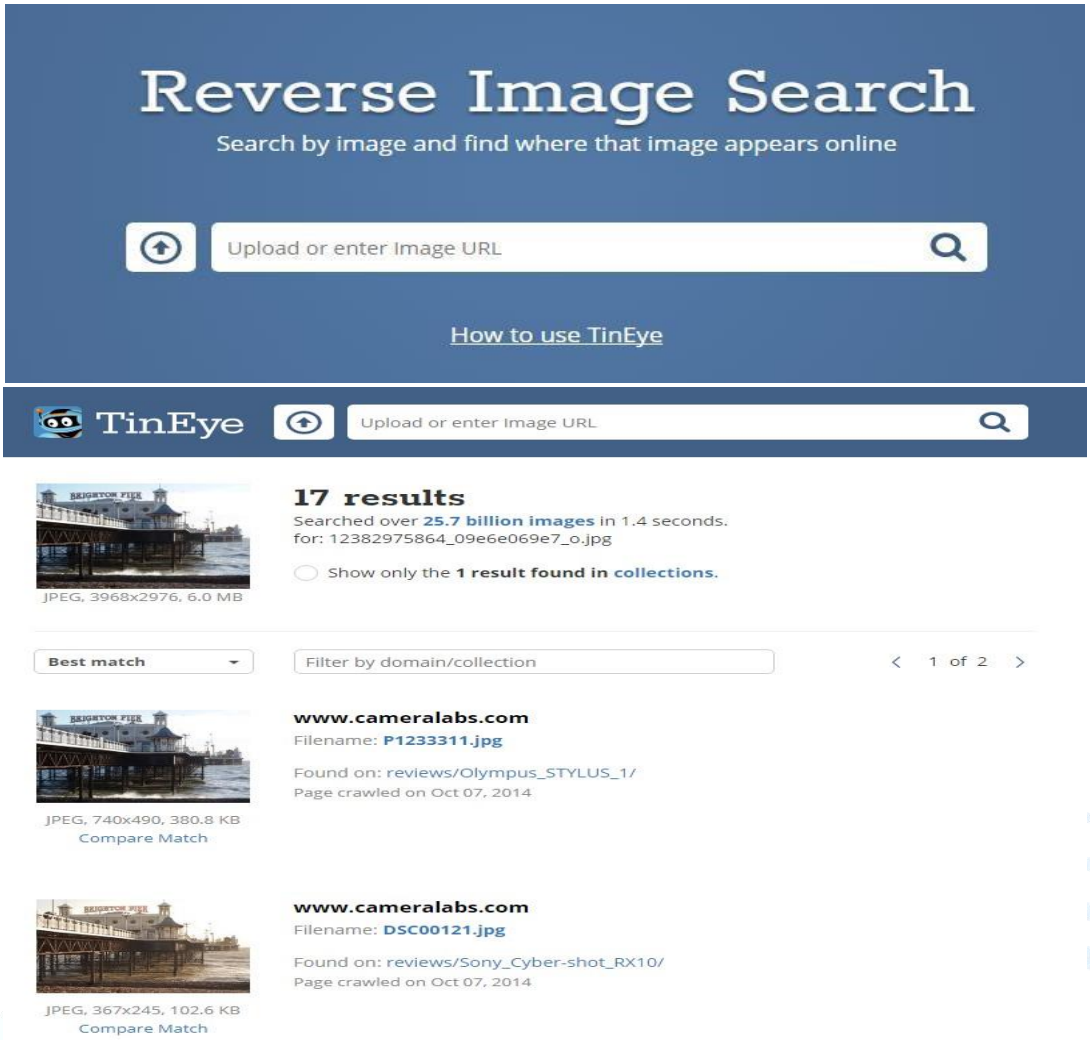


Fig.2.11Reverse image search results from Tineye.com

2.1.5 Open Source Intelligence on Facebook

Facebook is a very good source of information. Facebook users share lot of personal information through it. These publicly available details can be used to profile a person or suspect. There are many open source tools that are available which can be used to search & collect information over the Facebook. For example, Lookup-id.com, Inteltechniques.com are some such tools

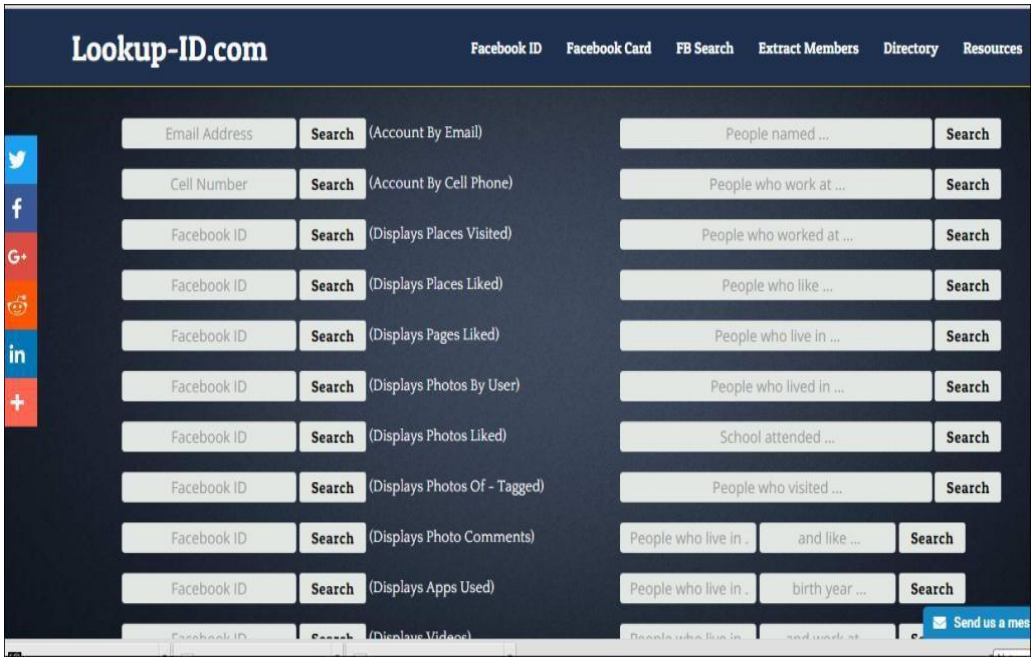


Fig.2.12: Lookup-id home page

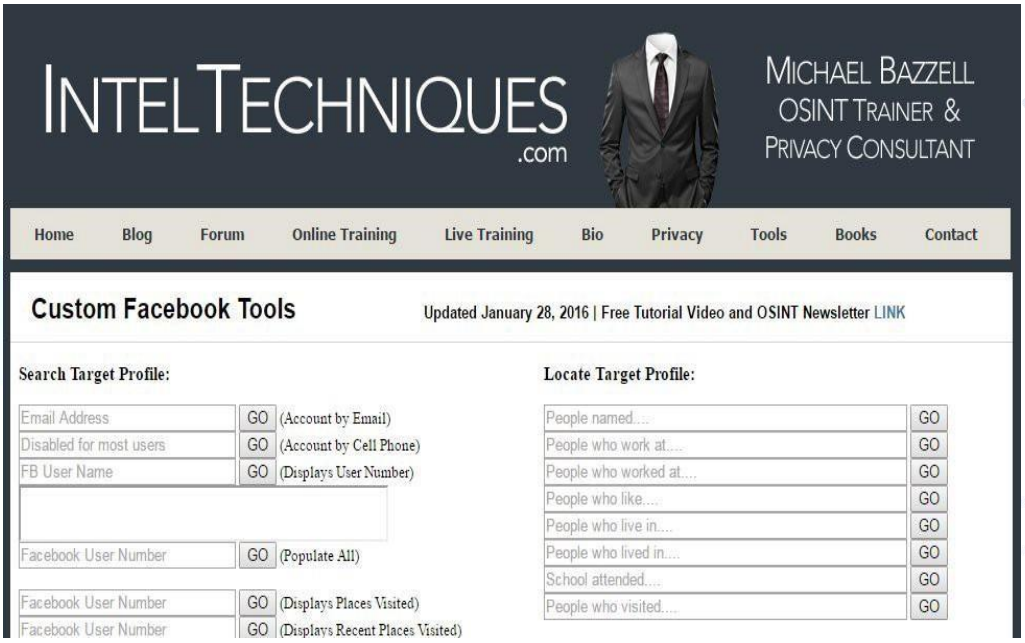


Fig.2.13: Inteltechniques home page

2.2 Information from Internet/Mobile Service Providers (ISP/MSP)

An Internet service provider (ISP) is an organization that provides services for accessing and using the Internet.

A mobile service provider (MSP) is a company that offers transmission services to users of wireless devices (smartphones and tablet PCs) through radio frequency (RF) signals rather than through end-to-end wire communication.

These service providers collect lot of information like personal details of customers, usage of services and their devices. These data are stored in their servers for

the purpose of business analysis. Some of this data would be very useful for the law enforcement agencies in investigating various crimes.
The records maintained by the service providers are,

- Subscriber Data Records (SDR)
- Customer Application Form (CAF)
- Call Detail Records (CDR)
- Internet Packet Data Records (IPDR)
- GPRS CDR
- Tower Dump Record(TDR)

The law enforcement agencies can request these records by sending notice under 91 Cr.P.C (Summons to produce document or other thing) to the service providers for the purpose of investigation.

2.2.1 Subscriber Data Records (SDR)

Subscriber Data Records (SDR) is the record maintained by the service provider which contains all the details of their customers which has been given at the time of subs cription. This record will contain name of the customer, connection number, address, circle, identity proof submitted for registration, city name, state etc.

	A	B	C	D	E	F	G	
1	CAF N	MSISDN	Customer Name	Fathers/husbands name	Date of activation	Present address	Permanent Address	Retailers name
2	212	7315065	Narendra	Mr. Ahuja	02-07-2010	Old no. 47/ New no. 88	Hyderabad	Airtel
3	213	7386589	Ramesh	Mr. Ankur Sharma	25-12-2011	H.No.8-2-693/2/28, Mith	Hyderabad	Vodafone
4	214	7396712	Suresh	Rajinikanth	26-12-2011	RMK PLAZA, 8-2-630 T	Hyderabad	Idea
5	215	7893982	Mallesh	Somesh	01-12-2011	P.S Nagr, Vijaynagar co	Hyderabad	Idea
6	216	7894440	Yellaiya	Reddy Chintal	01-12-2011	V.S.T COLONY,NACHA	Hyderabad	Airtel
7	217	8008402	Ramaiya	Vastavaiya	01-12-2011	Plot No.37, E.C.Nagar,	Hyderabad	Airtel
8	218	8008424	Katiya	Kabira	01-12-2011	HNO:4-65/2,STREET N	Hyderabad	Vodafone
9	219	8008867	Dang	Joseph Cristo	01-12-2011	H.NO-1-2-90/1/A,KAKA	Hyderabad	Idea
10	220	8026582	Amar	Pratap Singh	01-12-2011	D.No.2-20-30/1, Chilaka	Hyderabad	Idea
11	221	8121565	Akbar	Ali Jaan	01-12-2011	Deccan Swaraj Industrie	Hyderabad	Airtel
12	222	8125006	Anthony	Christopher Nolan	01-12-2011	H.No.5-14-114/2, Quada	Hyderabad	Idea
13	223	8662436	Rajesh	Rajinikanth	01-12-2011	Saraswathi Block, Triver	Hyderabad	Airtel
14	224	8662442	Naresh	Allari Komatla	01-12-2011	HNO 1-19/A, NEAR VIK	Hyderabad	Airtel
15	225	8662450	Ali	Syed Raheem Ali	01-12-2011	HNO-13-124/3 NEAR S	Hyderabad	Airtel
16	226	8662470	Razia	Nuzhath Md	01-12-2011	H.NO.7-15-12,OPP.RO	Hyderabad	Airtel
17	227	8662822	Shazia	Nuzhath Md	01-12-2011	H.No.1-91/17, FMR Con	Hyderabad	Airtel
18	228	8666660	Nazia	Nuzhath Md	01-12-2011	H.NO:42-795, CHANDA	Hyderabad	Vodafone
19	229	8790545	Fouzia	Nuzhath Md	02-12-2011	M/s Jesday Pharmaceu	Hyderabad	Airtel
20	230	8832475	Geeta	Balaiyya	03-12-2011	Sy.No.24, Mallapur Ville	Hyderabad	Airtel
21	231	8865295	Senorita	Pintos Nolan	04-12-2011	SUN BONALA ARCADE	B. Hyderabad	Airtel
22	232	8865324	Suzanne	Feroz Khan	05-12-2011	H.No.3-5-35/2, Krishna	4 Hyderabad	Vodafone
23	233	8865385	Harshdeep	Harbal Khanna	06-12-2011	VAISHNAVI COMPLEX,	Hyderabad	Vodafone
24	234	8865443	Shahnawaz Khan	Jahangir Khan	07-12-2011	H.No:3-110-1/259,Nehru	Hyderabad	Airtel
25	235	8865546	Salma	Salim Khan	08-12-2011	HNO.4-9-2,NAWAZPLA	Hyderabad	Airtel
26	236	8865952	Amir	Alibaba	09-12-2011	H.No.5-12-133/1, Manga	Hyderabad	Airtel

Fig.2.14: Sample Subscriber Data Record

2.2.2 Customer Application Form (CAF)

Customer Application Form (CAF) is the form that is filled by the customer while taking a new internet or mobile connection. This form will have details like name of the customer, photo, application number, sim number, address, circle, identity proof submitted for registration, city name, state etc.

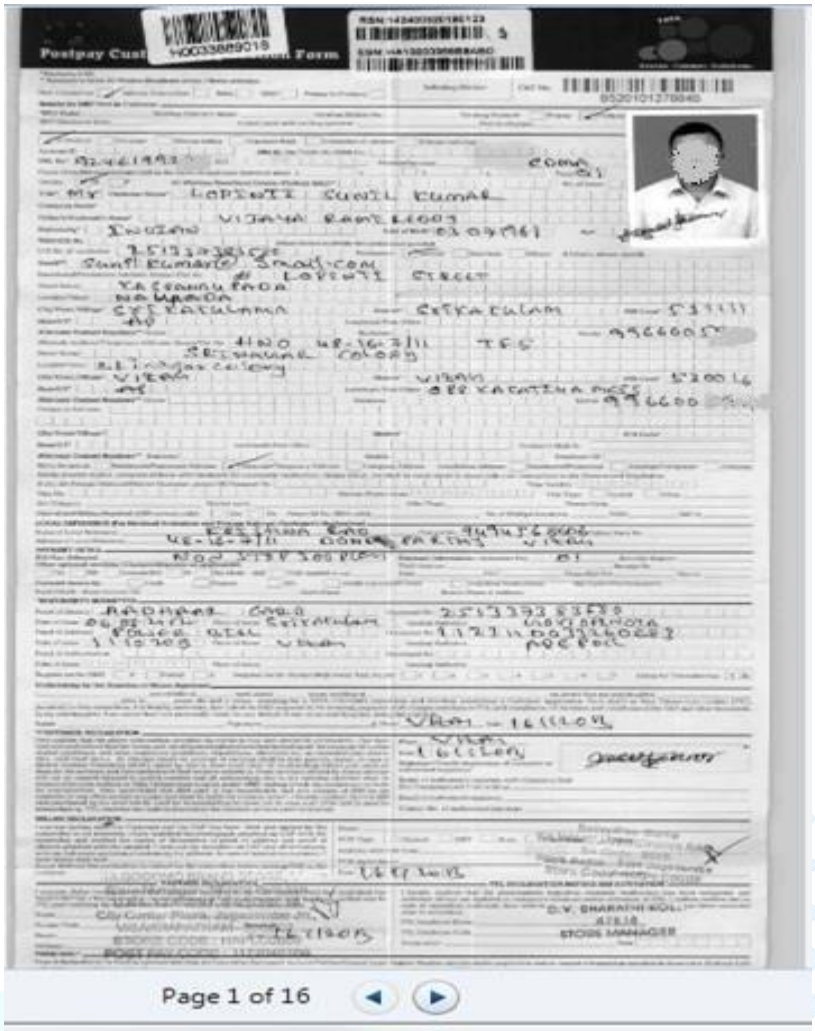
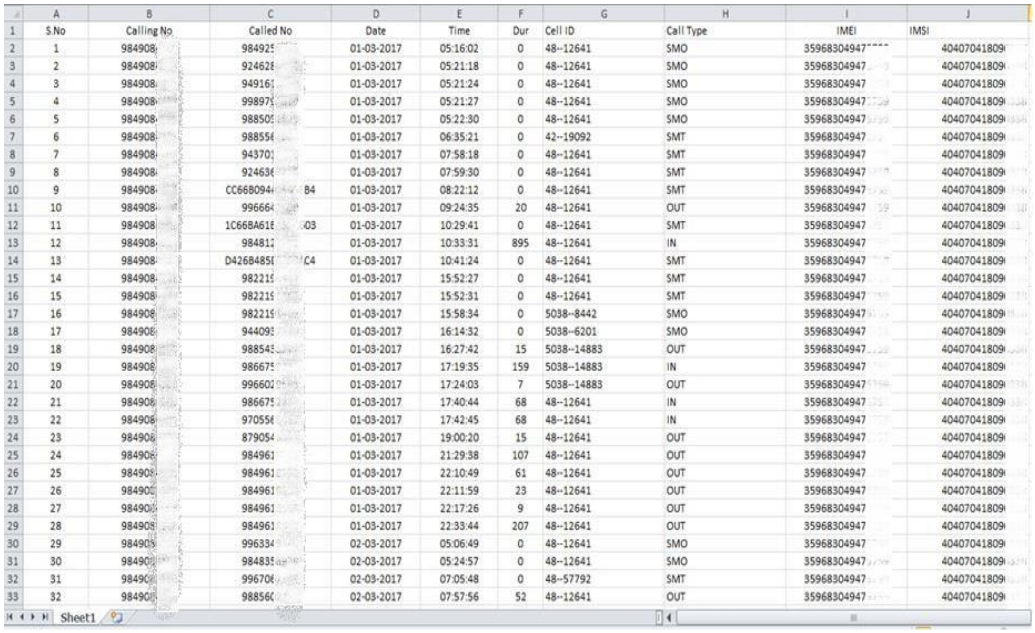


Fig.2.15: Sample Customer Acquisition Form

CAF will also provide information about the reseller or shop from where the person has taken this connection. These details will be helpful in investigating various crimes.

2.2.3 Call Detail Records (CDR)

Call Detail Records (CDR) is the record maintained by the service providers which contains all the details about the calls and sms made by the user. Service providers maintain this for business purpose and service improvement. For Law Enforcement Agencies this is very much helpful in linking the criminals with the crime. A CDR will contain lot of fields but nearly 13 column data is shared with the law enforcement agencies for the investigation purpose. A sample 13 column CDR is shown below.



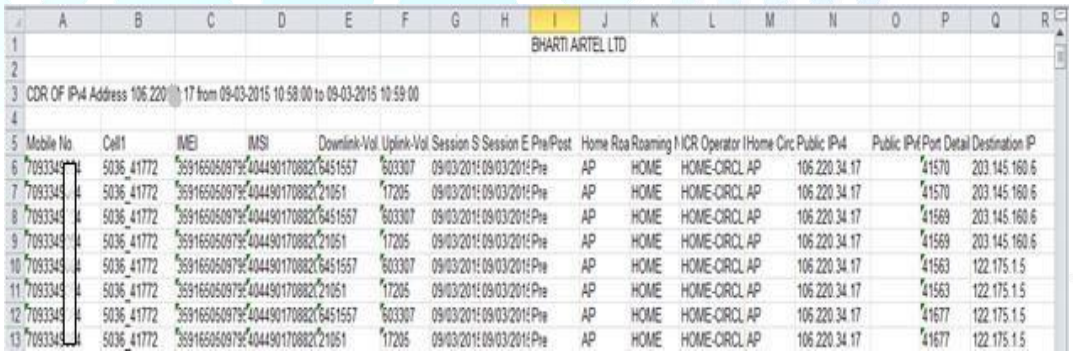
S.No	Calling No	Called No	Date	Time	Dur	Cell ID	Call Type	IMEI	IMSI
1	984908	984925	01-03-2017	05:16:02	0	48--12641	SMO	35968304947	404070418091
2	984908	924628	01-03-2017	05:21:18	0	48--12641	SMO	35968304947	404070418091
3	984908	949161	01-03-2017	05:21:24	0	48--12641	SMO	35968304947	404070418091
4	984908	998975	01-03-2017	05:21:27	0	48--12641	SMO	35968304947	404070418091
5	984908	988505	01-03-2017	05:22:30	0	48--12641	SMO	35968304947	404070418091
6	984908	988556	01-03-2017	06:35:21	0	42--19092	SMT	35968304947	404070418091
7	984908	943701	01-03-2017	07:58:18	0	48--12641	SMT	35968304947	404070418091
8	984908	924636	01-03-2017	07:59:30	0	48--12641	SMT	35968304947	404070418091
9	984908	CC668094 B4	01-03-2017	08:22:12	0	48--12641	SMT	35968304947	404070418091
10	984908	996664	01-03-2017	09:24:35	20	48--12641	OUT	35968304947	404070418091
11	984908	1C668A61E 03	01-03-2017	10:29:41	0	48--12641	SMT	35968304947	404070418091
12	984908	984811	01-03-2017	10:33:31	895	48--12641	IN	35968304947	404070418091
13	984908	D42684850 C4	01-03-2017	10:41:24	0	48--12641	SMT	35968304947	404070418091
14	984908	982215	01-03-2017	15:52:27	0	48--12641	SMT	35968304947	404070418091
15	984908	982215	01-03-2017	15:52:31	0	48--12641	SMT	35968304947	404070418091
16	984908	982215	01-03-2017	15:58:34	0	5038--8442	SMO	35968304947	404070418091
17	984908	944095	01-03-2017	16:14:32	0	5038--6201	SMO	35968304947	404070418091
18	984908	988543	01-03-2017	16:27:42	15	5038--14883	OUT	35968304947	404070418091
19	984908	986675	01-03-2017	17:19:35	159	5038--14883	IN	35968304947	404070418091
20	984908	996602	01-03-2017	17:24:03	7	5038--14883	OUT	35968304947	404070418091
21	984908	986675	01-03-2017	17:40:44	68	48--12641	IN	35968304947	404070418091
22	984908	970556	01-03-2017	17:42:45	68	48--12641	IN	35968304947	404070418091
23	984908	879054	01-03-2017	19:00:20	15	48--12641	OUT	35968304947	404070418091
24	984908	984961	01-03-2017	21:29:38	107	48--12641	OUT	35968304947	404070418091
25	984908	984961	01-03-2017	22:10:49	61	48--12641	OUT	35968304947	404070418091
26	984908	984961	01-03-2017	22:11:59	23	48--12641	OUT	35968304947	404070418091
27	984908	984961	01-03-2017	22:17:26	9	48--12641	OUT	35968304947	404070418091
28	984908	984961	01-03-2017	22:33:44	207	48--12641	OUT	35968304947	404070418091
29	984908	996334	02-03-2017	05:06:49	0	48--12641	SMO	35968304947	404070418091
30	984908	984835	02-03-2017	05:24:57	0	48--12641	SMO	35968304947	404070418091
31	984908	996706	02-03-2017	07:05:48	0	48--57792	SMT	35968304947	404070418091
32	984908	988566	02-03-2017	07:57:56	52	48--12641	OUT	35968304947	404070418091

Sheet1

Fig.2.16:Sample Call Detail Record

2.2.4 Internet Packet Data Records (IPDR)

Internet Packet Data Record (IPDR) is the record maintained by the service providers which contain the internet activity of an IP address. An IP Data Record can tell you a number of things about your incoming and outgoing network traffic. For example: Mobile number associated with IP, Destination IP Address, date, duration, uplink, downlink, Session start time, end time, etc..



BHARTI AIRTEL LTD

CDR OF IPv4 Address 106.220 17 from 09-03-2015 10:58:00 to 09-03-2015 10:59:00

Mobile No	Cell1	IMEI	IMSI	Downlink-Vol	Uplink-Vol	Session S	Session E	Pre/Post	Home Roa	Roaming N	ICR Operator I	Home Circ	Public IPv4	Public IPv4	Port Detail	Destination IP
7093345 4	5036_41772	359165050979	404490170882	6451557	603307	09/03/2015	09/03/2015	Pre	AP	HOME	HOME-CIRCL	AP	106.220.34.17		41570	203.145.160.6
7093345 4	5036_41772	359165050979	404490170882	21051	17205	09/03/2015	09/03/2015	Pre	AP	HOME	HOME-CIRCL	AP	106.220.34.17		41570	203.145.160.6
7093345 4	5036_41772	359165050979	404490170882	6451557	603307	09/03/2015	09/03/2015	Pre	AP	HOME	HOME-CIRCL	AP	106.220.34.17		41569	203.145.160.6
7093345 4	5036_41772	359165050979	404490170882	21051	17205	09/03/2015	09/03/2015	Pre	AP	HOME	HOME-CIRCL	AP	106.220.34.17		41569	203.145.160.6
7093345 4	5036_41772	359165050979	404490170882	6451557	603307	09/03/2015	09/03/2015	Pre	AP	HOME	HOME-CIRCL	AP	106.220.34.17		41563	122.175.1.5
7093345 4	5036_41772	359165050979	404490170882	21051	17205	09/03/2015	09/03/2015	Pre	AP	HOME	HOME-CIRCL	AP	106.220.34.17		41563	122.175.1.5
7093345 4	5036_41772	359165050979	404490170882	6451557	603307	09/03/2015	09/03/2015	Pre	AP	HOME	HOME-CIRCL	AP	106.220.34.17		41677	122.175.1.5
7093345 4	5036_41772	359165050979	404490170882	21051	17205	09/03/2015	09/03/2015	Pre	AP	HOME	HOME-CIRCL	AP	106.220.34.17		41677	122.175.1.5

Fig.2.17: Sample Internet Packet Data Record

From IPDR we will get the device details and mobile number associated with a particular IP Address. Using this we can track down the criminal.

2.2.5 Tower Dump Records (TDR)

Tower Dump Record is the CDR of a mobile tower. It contains all the communication (Calls&sms) details which are done udder the coverage area of a particular tower. This will contain information like the number which initiated the call/sms, the destination number, date, time in seconds, cell-ids to which mobile is connected while call/sms initiated and terminated, IMEI number of the device used,IMSI number of SIM, type of call, connection type etc. This is a very huge data hence analysis of TDR is very difficult.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Serial_No	A_Number	B_Number	Date	Time	Duration	FIRST_CELL_ID_A	LAST_CELL_ID_A	Call_Type	IMEI	IMSI	PP_PO_IN	SMS_CENTRE	FIRST_ROAMING_NETWORK		
2	1	9813188	90501844	29-Jan-12	21:00:10	86	404010065017263	404010065017263	OUT	35151504304	40401262742	PP	-	-		
3	2	8053194	96714867	29-Jan-12	21:00:13	21	404010065017263	404010065017263	OUT	35932704734	40401267842	PP	-	-		
4	3	8295087	90500189	29-Jan-12	21:00:25	1	404010065017263	404010065017263	INC	35786004905	40401266669	PP	-	-		
5	4	9991509	99910574	29-Jan-12	21:00:26	89	404010065017263	404010065017263	INC	91005260146	40401262260	PP	-	-		
6	5	9991299	89309457	29-Jan-12	21:00:50	1	404010065017263	404010065017263	SMS_OUT	35902004075	40401262348	PP	919839099999	-		
7	6	9991299	90418499	29-Jan-12	21:00:57	1	404010065017263	404010065017263	SMS_OUT	35902004075	40401262348	PP	919839099999	-		
8	7	9992776	89302976	29-Jan-12	21:00:57	294	404010065017263	404010065017263	INC	35846103005	40401267812	PP	-	-		
9	8	9813259	96714446	29-Jan-12	21:00:59	28	404010065017263	404010065035823	OUT	35499103288	40401262240	PP	-	-		
10	9	9991299	98960818	29-Jan-12	21:01:04	1	404010065017263	404010065017263	SMS_OUT	35902004075	40401262348	PP	919839099999	-		
11	10	8814004	98138523	29-Jan-12	21:01:07	863	404010065017263	404010065017263	INC	91112530543	40401262738	PP	-	-		
12	11	8814004	98138523	29-Jan-12	21:01:07	863	404010065017263	404010065017263	OUT	35481901084	40401264680	PP	-	-		
13	12	9991621	98133293	29-Jan-12	21:01:14	70	404010065017263	404010065035823	OUT	35801303900	40401266009	PP	-	-		
14	13	9991299	88180528	29-Jan-12	21:01:14	1	404010065017263	404010065017263	SMS_OUT	35902004075	40401262348	PP	919839099999	-		
15	14	9041849	99912998	29-Jan-12	21:01:16	1	404010065017263	404010065017263	SMS_INC	35902004075	40401262348	PP	919032055002	-		
16	15	8053774	88180546	29-Jan-12	21:01:20	32	404010065017263	404010065035823	OUT	35605303919	40401267825	PP	-	-		
17	16	9991299	99919340	29-Jan-12	21:01:24	1	404010065017263	404010065017263	SMS_OUT	35902004075	40401262348	PP	919839099999	-		
18	17	8818053	98130706	29-Jan-12	21:01:28	143	404010065017263	404010065017263	OUT	91111680180	40401264676	PP	-	-		
19	18	9991299	87544557	29-Jan-12	21:01:29	1	404010065017263	404010065017263	SMS_OUT	35902004075	40401262348	PP	919839099999	-		
20	19	9991954	99919180	29-Jan-12	21:01:30	25	404010065017263	404010065017263	INC	35194103549	40401266799	PP	-	-		
21	20	9991299	89508783	29-Jan-12	21:01:33	1	404010065017263	404010065017263	SMS_OUT	35902004075	40401262348	PP	919839099999	-		
22	21	9991299	90344420	29-Jan-12	21:01:42	1	404010065017263	404010065017263	SMS_OUT	35902004075	40401262348	PP	919839099999	-		
23	22	9991299	99918567	29-Jan-12	21:01:49	1	404010065017263	404010065017263	SMS_OUT	35902004075	40401262348	PP	919839099999	-		
24	23	9991299	80539900	29-Jan-12	21:01:55	1	404010065017263	404010065017263	SMS_OUT	35902004075	40401262348	PP	919839099999	-		

Fig.2.18: Sample Tower Dump

2.2.6 Information from Email Client

E-mail client is a computer program which is used to access and manage user's e-mails. While Outlook, thunderbird are the email clients that are installed in end user system while Gmail, Yahoo are examples of web based email clients. Email 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.

Every e-mail contains an e-mail header irrespective of the e-mail service provider. It is the most important part of an email for the purpose of Investigation. It includes information stamped by intermediate Email Servers and all the other metadata related to time stamps, details of sender and destination along with the Routing information of an Email.

Important e-mail header parameters are,

- Date: The date the message was originated/written.
- Message-ID: Identity of the message.
- 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 MTAs (Mail Transfer Agents) through which the message has passed

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

1. Log into your Gmail Account.
2. Open the Email whose headers you want to view.
3. Click the down arrow adjacent to the Reply link in the upper-right corner of the message.
4. Click Show Original.

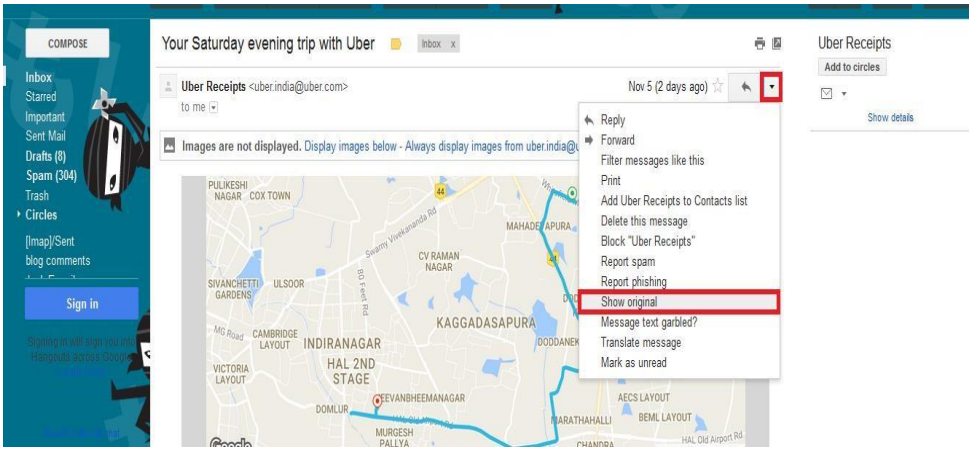


Fig.2.19: Opening e-mail header in G-mail.

A sample e-mail header is shown below.

```
Delivered-To: arif.ali.khan12@gmail.com
Received: by 10.79.148.149 with SMTP id v21csp256644ivg;
        Sat, 5 Nov 2016 07:02:16 -0700 (PDT)
X-Received: by 10.98.65.72 with SMTP id o69mr5970602pfa.128.1478354536660;
        Sat, 05 Nov 2016 07:02:16 -0700 (PDT)
Return-Path: <bounces+13641-667a-arif.ali.khan12=gmail.com@em.uber.com>
Received: from o18.email.uber.com (o18.email.uber.com. [167.89.42.140])
        by mx.google.com with ESMTPS id 201si22887982pfc.120.2016.11.05.07.02.15
        for <arif.ali.khan12@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Sat, 05 Nov 2016 07:02:16 -0700 (PDT)
Received-SPF: pass (google.com: domain of bounces+13641-667a-arif.ali.khan12=gmail.com@em.uber.com designates 167.89.42.140 as
permitted sender) client-ip=167.89.42.140;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@uber.com;
       dkim=pass header.i=@sendgrid.info;
       spf=pass (google.com: domain of bounces+13641-667a-arif.ali.khan12=gmail.com@em.uber.com designates 167.89.42.140 as
permitted sender) smtp.mailfrom=bounces+13641-667a-arif.ali.khan12=gmail.com@em.uber.com;
       dmarc=pass (p=QUARANTINE dis=NONE) header.from=uber.com
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed; d=uber.com; h=content-type:mime-version:from:cc:to:subject; s=s1;
bh=y528qpC6OuWUH2gVf8fzP6A1xNo=; b=8FtFyZsoLIfQJLOxN+hX41z//UIO2
Lt21YSQGrkXIr2SEgiJnkmr5JFG31WBeKW9GD5SJzvceJnzhgRWaNJV1hL5tIBZ5
ACusJVizUY2RwXFsPlsgLolEsgOPaRxmlrTH4rK6rgtCL/Vr98te5bVcBbT+P8eM W258TlOxU2NW6g=
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed; d=sendgrid.info; h=content-type:mime-version:from:cc:to:subject:x-feedback-id;
s=smtpapi; bh=y528qpC6OuWUH2gVf8fzP6A1xNo=; b=XTfPc25XTnWwDVMp8L
CEoUsnVfOjuKbQR84mNdeLnn4omw3VvM+cz91SHYCG51D/13nEIssTvuQFK5r47j
JyJiXzq2eqQIf8AOP1589EOlrorX4sTlhIdJdF9akC9GVTyLcESTR/chzf1tEtDI /cf6DsWtZzWI7d9asxYxXNOCc=
Received: by filter0370p1las1.sendgrid.net with SMTP id filter0370p1las1-19817-581DE666-11
```

Fig.2.20: Sample e-mail header in G-mail.

For collecting relevant information about the path the e-mail took over internet along with the details of time and ip addresses of systems at every statge, copy the e-mail header and paste it in any e-mail tracking tool which is available on internet. Some of the tools which can analyse email header data are listed below:

i. www.cyberforensics.in/OnlineEmailTracer
ii. E-mailTrackerPro **iii.** Email Lookup- Free Email Tracer

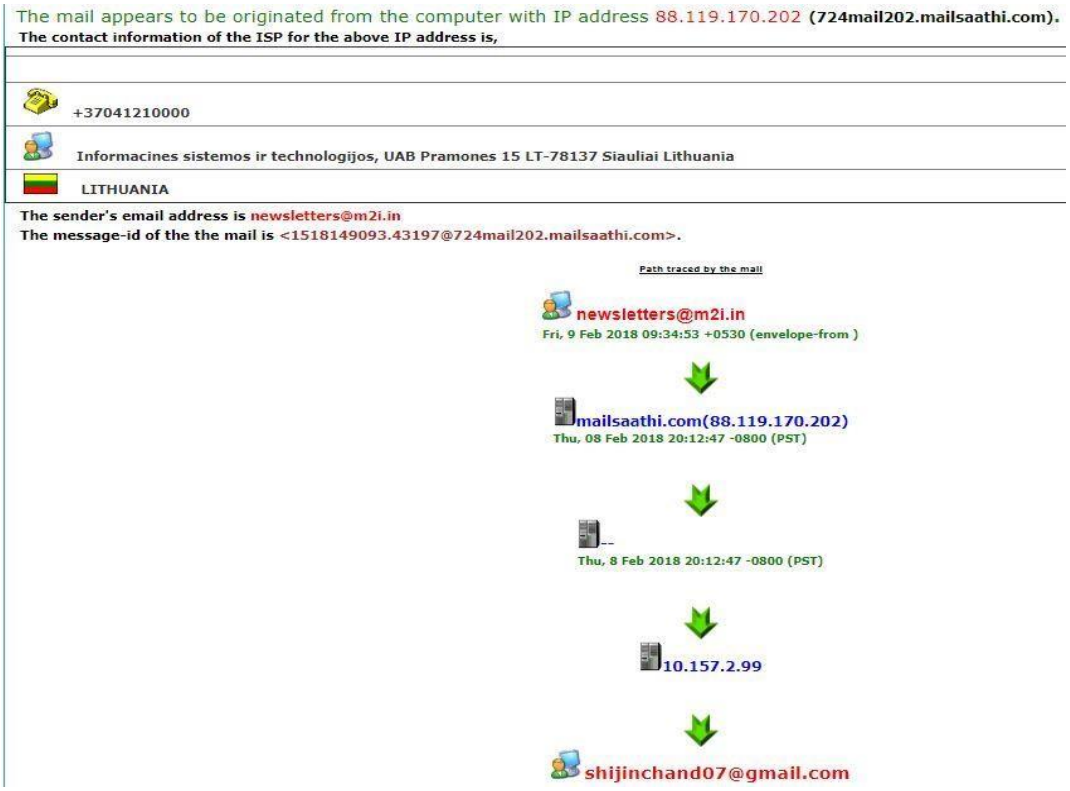


Fig.2.21: E-mail tracer output

If the user has configured the mail clients like thunderbird or outlook in his computer, all the mails will be stored in that computer itself and not on the internet. So by seizing the computer, IO can get full access to all the mails that are received in the mail account. At times, we can retrieve deleted mails also from these clients using forensic analysis of the machine.

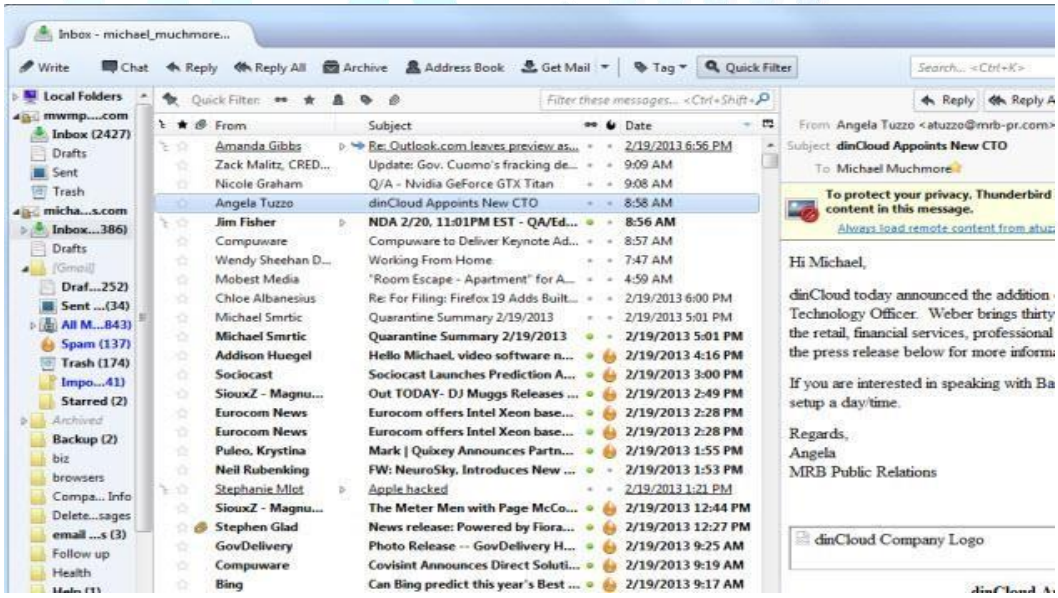


Fig.2.22:Thunderbird inbox

If the suspect is using a web based e-mail client like Gmail and Hotmail then we need to request these e-mail service providers under section 91 Cr.P.C, to give the details of the user and his communications. These service providers will give the IP addresses of the devices, which have been used by the suspect to access the mail.

Activity on this account

This feature provides information about the last activity on this mail account and any concur activity. Learn more

This account does not seem to be open in any other location. However, there may be sessic have not been signed out.

Sign out all other sessions

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	Location (IP address) [?]	Date/Time (Displayed in your
Browser	* United States (CA) ( )	5:19 pm (0 minute
Mobile	United States (CA) ( )	5:12 pm (7 minute
Browser	* United States (CA) ( )	4:54 pm (24 minut
Browser	* United States (CA) ( )	4:24 pm (55 minut

Fig.2.23: G-mail access details

2.3 Information from Social Media Networking Sites

Social media sites are very good source of information. The users share lot of personal information through it. It's also used to communicate and express the thoughts and feelings. Some of the popular social media sites are shown below.

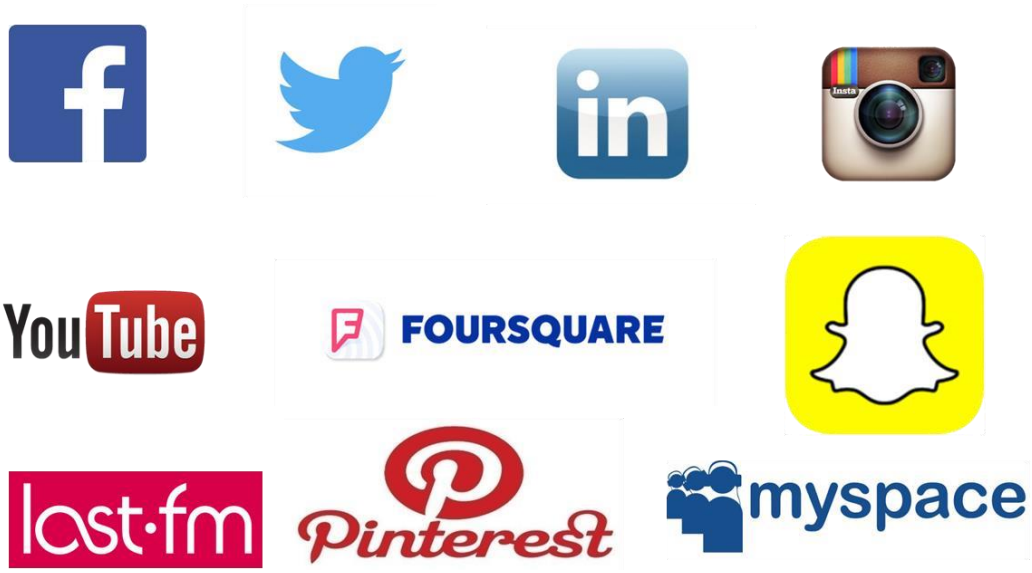


Fig.2.24: Popular Social media sites.

But if you think these are the only social media platforms then you are wrong. There are many more that are not very prominent but which are being used by different groups across the globe.

Fig.2.25:Other Social media sites present in internet

These platforms are being used by the criminals for the commission of various crimes. They use less popular sites to avoid detection. Most of the sites are hosted outside India. So, the investigation becomes more complex. Some of these websites have the dedicated divisions for giving support to the LEAs. For example, Facebook is having their legal portal www.facebook.com/records through which the LEAs can request for information regarding users.

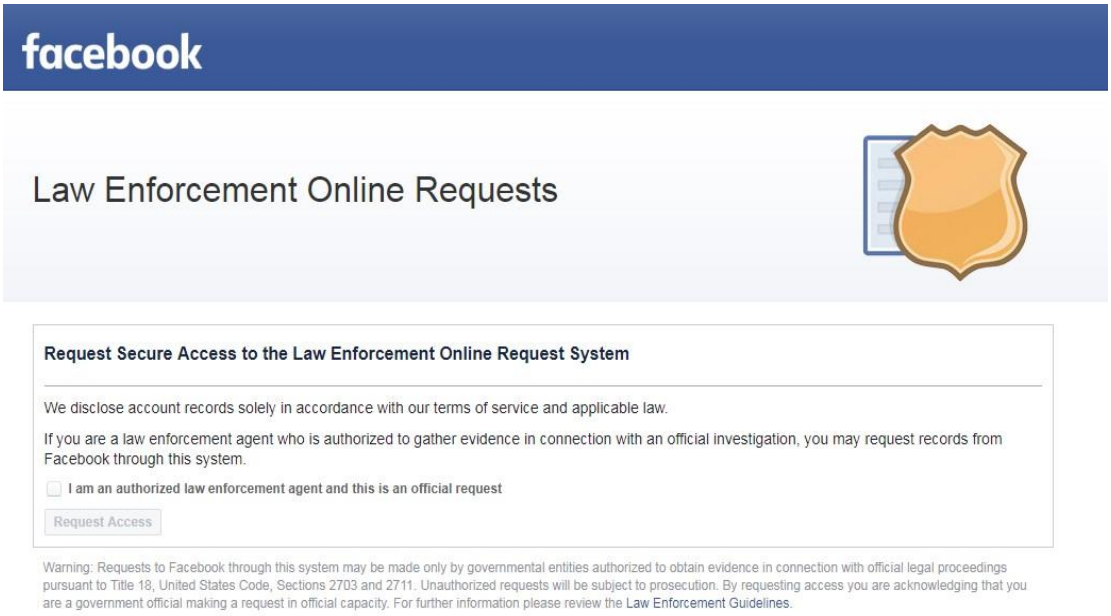


Fig.2.26: Facebook LEA Portal.

Investigating officer can request for information using the official e -mail address. Considering the type of case and intensity they will reply back.

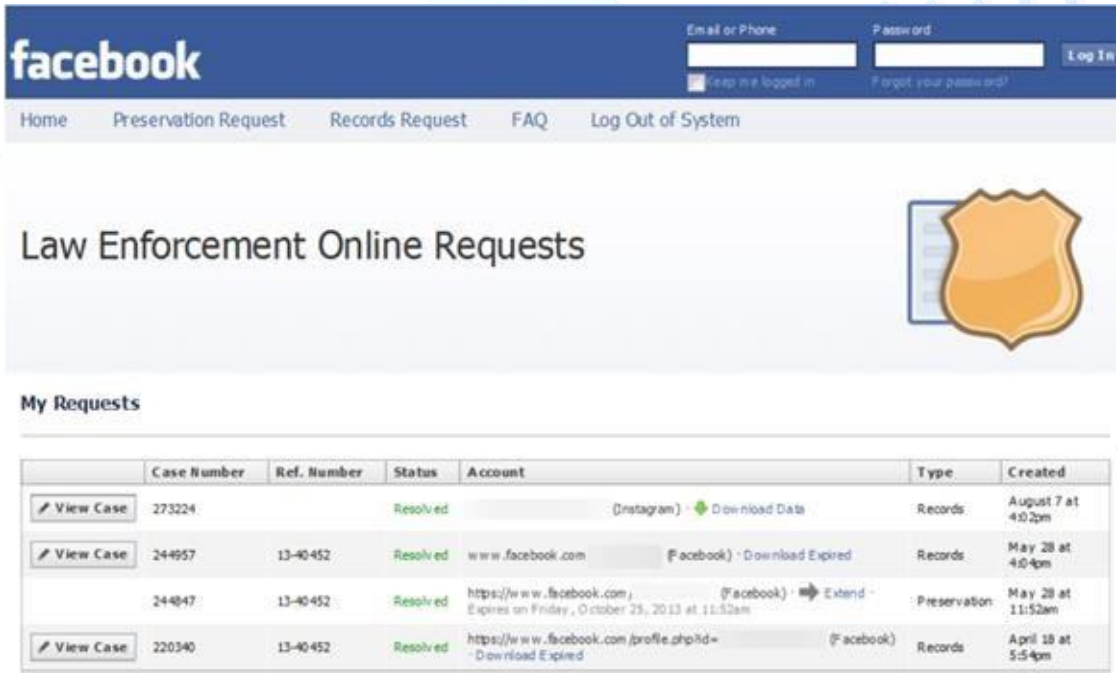


Fig.2.27: Facebook reply to LEA request.

Same like Facebook, twitter also have LEA portal:
https://help.twitter.com/forms/lawenforcement

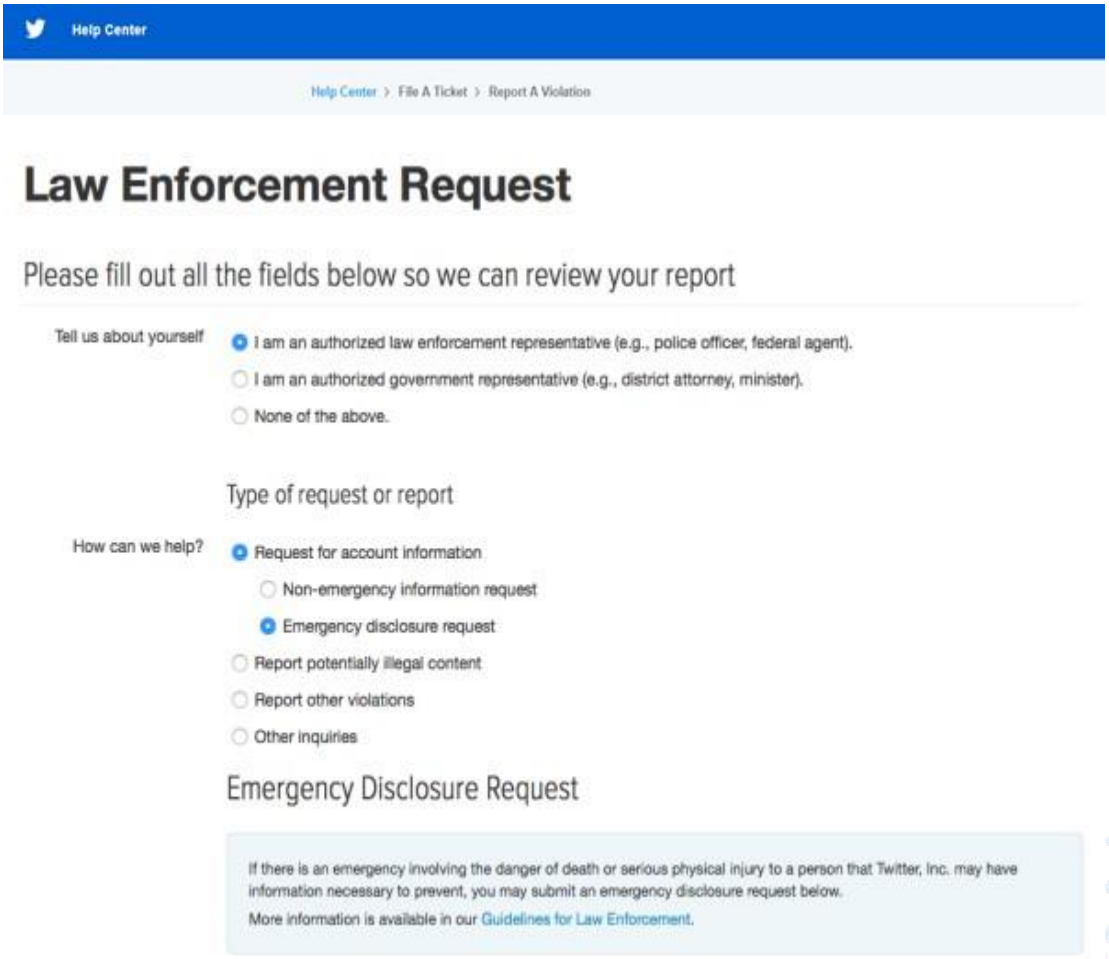


Fig.2.28: Twitter LEA portal.

2.4 Information from Financial Intuitions/Banks/wallets

There are lot of cybercrimes that are reported in which the victims lost their money from the bank/digital wallets. Criminals with technical knowledge will try to get the user credentials of account holders of various banks and by using various methods, they transfer money to some other accounts. By the time, user notices the losses incurred by him, money will be used by someone.

In such cases the LEAs can send request to the nodal officers of the respective banks/ digital wallets to provide details regarding the transactions. LEAs can also request for the account details of a suspect from them. Banks will be having complete details of their customers and their transactions. Details of some of the nodal officers of the banks are mentioned in a table at a later part of the document.

2.5 Information from Websites/Domains from Domain Host Provider

In some cases, the IO will come across with some fake websites or websites that are used by criminals to perform illegal activities. In such cases, we need to know the details such as where the website is being hosted, who is the owner, from where he is operating this website etc. In most of the cases the websites will be hosted outside India, which makes it very difficult for the investigation officers to get the details of these websites or seize the servers in which the websites are running.

We can use domain lookup services like whois which are available on internet to get the domain registration details of a particular website. For example, domain information of www.svpnpa.gov.in is shown below:

– Domain Profile

Registrant	Sardar Vallabhbhai Patel National Police Academy
Registrant Org	–
Registrant Country	IN
Registrar	National Informatics Centre (R12-AFIN) IANA ID: – URL: – Whois Server: –
Registrar Status	OK
Dates	5,095 days old Created on 2004-02-27 Expires on 2018-02-27 Updated on 2017-02-28
Name Server(s)	SR1.SVPNPA.GOV.IN (has 1 domains) SR2.SVPNPA.GOV.IN (has 1 domains)
Tech Contact	Same As Above SVPNPA Shivaram Palli, Hyderabad, Andhra Pradesh, 500052, IN administrator@svpnpa.gov.in (p) 914024015151 (f) 914024015179
IP Address	103.8[redacted].23 is hosted on a dedicated server
IP Location	- Telangana - Hyderabad - Sardar Vallabhbhai Patel National Police Academy
ASN	AS135835 SVPNPAHY-AS Sardar Vallabhbhai Patel National Police Academy, IN (registered Oct 25, 2016)
Whois History	203 records have been archived since 2007-09-13

– Website

Fig.2.30: Domain registration details of svpnpa.gov.in.

LEAs can request to the registrar of the website to give further details like the domain purchase details, details of credit/debit card used to purchase the domain, the IP address from which the person is maintaining the website etc.

2.6 Information from National Voters Service Portals

The National Voters Portal (http://www.nvsp.in/) is a place where you can search for the people who are listed in voters list in India.

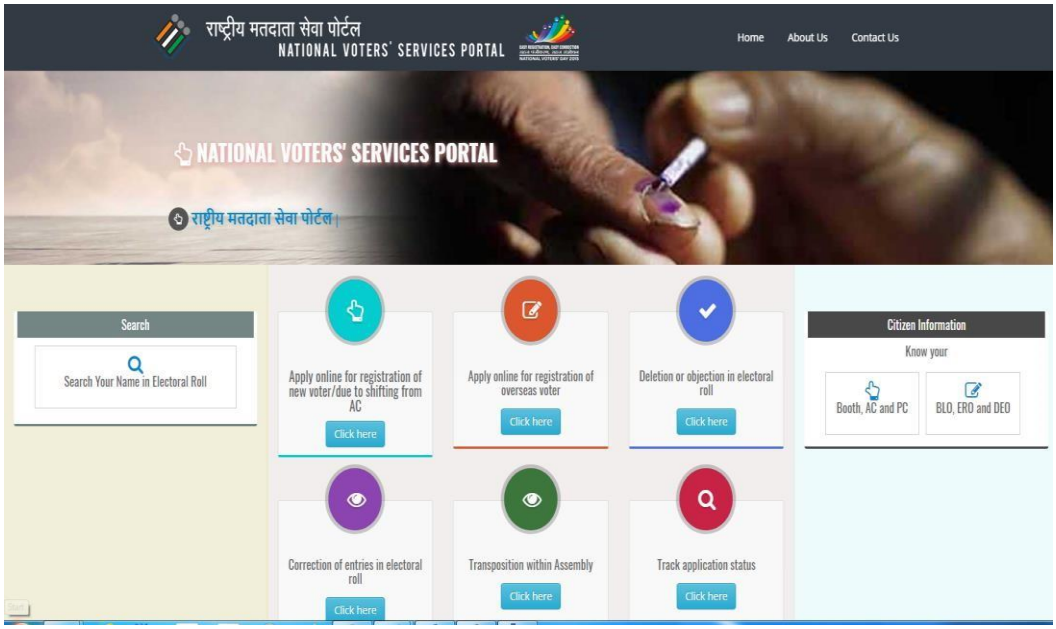


Fig.2.31: National Voters Portal Home Page.

We can search with the name/state/district/constituency name /fathers name etc. In case we know the suspects name we can sear ch on this portal. If the name is a common name in India, we will get thousands of results. We can filter it by state/district/constituency name/fathers name etc.

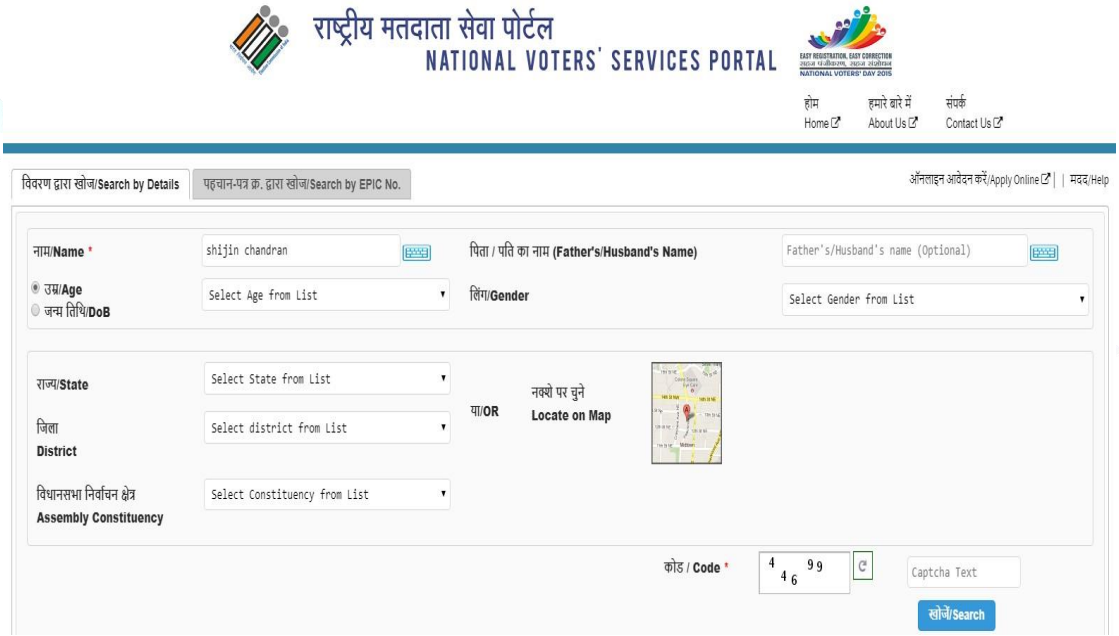


Fig.2.32: Electoral Roll Search in National Voters portal.

From the result, we will get more details of a person like Voters ID card number, polling booth, address, age, date of birth, parent name etc.

Action	EPIC No.	Name	Age	Father's/Husband's Name	State	District	Polling Station	Assembly Constituency	Parliamentary Constituency
View Details	GYT1544972	Shijin Chandran ഷിജിൻ ചന്ദ്രൻ	30	Chandran K P ചന്ദ്രൻ കെ പി	Kerala	KANNUR	Govt. H. S.S, Kavumbhagam ,Kavumbagam	THALASSERY	VADAKARA
View Details	SNC0441915	Shijin Chandran ഷിജിൻ ചന്ദ്രൻ	23	Jayachandran ജയചന്ദ്രൻ	Kerala	PATHANAMTHITTA	St.Thomas L.P.School Manneera,Thekkutodu	KONNI	PATHANAMTHITTA
View Details	MST1596220	Shijin Chandran ഷിജിൻ ചന്ദ്രൻ	33	Chandran ചന്ദ്രൻ	Kerala	THRISSUR	Aided U P S Muriyad,Muriyad	IRINJALAKKUDA	THRISSUR
View Details	NCP0238923	Shijin Chandran ഷിജിൻ ചന്ദ്രൻ	25	Chandran ചന്ദ്രൻ	Kerala	PALAKKAD	G.B.L.P.S,TM Thara Koduvayur,Koduvayur	NENMARA	ALATHUR
View Details	ITZ1015387	Shijin Chandran ഷിജിൻ ചന്ദ്രൻ	20	Chandran ചന്ദ്രൻ	Kerala	KANNUR	Pullookkara ,Muslim LPS,Pullookkara	KUTHUPARAMBA	VADAKARA
View Details	ZFN0055095	Shijin Chandran ഷിജിൻ ചന്ദ്രൻ	29	Chandran ചന്ദ്രൻ	Kerala	ERNAKULAM	F.A.C.T (E) Upper Primary School Eloor,Eloor East	KALAMASSERY	ERNAKULAM
View Details	SDX0254458	Shijin Chandran ഷിജിൻ ചന്ദ്രൻ	26	Chandran K P ചന്ദ്രൻ കെ പി	Kerala	KANNUR	Tagore Memorial H S S , Vellora ,Vellora	PAYYANNUR	KASARAGOD
View Details	WYO0364018	Shijin Chandran K ഷിജിൻ ചന്ദ്രൻ കെ	29	Chandran ചന്ദ്രൻ	Kerala	KOZHIKODE	Govt. Upper Primary School Manasseri ,Manassery	THIRUVAMBADY	WAYANAD
View Details	UHE0342923	Shijin Chandran R ഷിജിൻ ചന്ദ്രൻ ആർ	24	Ramachandran രാമചന്ദ്രൻ	Kerala	THIRUVANANTHAPURAM	St. John's UPS, Vattiyoorkavu.,Vattiyoorkavu.	VATTIYOORKAVU	THIRUVANANTHAPURAM
View Details	ICR0317156	Shijin Chandran R S ഷിജിൻ ചന്ദ്രൻ ആർ എസ്	24	Ravikumar രവികുമാർ	Kerala	THIRUVANANTHAPURAM	M S C Lower Primary School, Pamamcodu,Pamamcodu	KATTAKKADA	ATTINGAL

Fig.2.33: Search results in National Voters Portal

വോടേര ഇന്ഫ്ോർമേശന/मतदाता सूचना/Voter Information

അവസ്ഥ/राज्य/State	Kerala
അസ്സെമ്ബ്ലീ കന്സ്ടിടുഏന്സീ/विधान सभा निर्वाचन क्षेत्र/Assembly Constituency	KATTAKKADA
നെയിം/नाम/Name	ഷിജിൻ ചന്ദ്രൻ ആർ എസ്
	Shijin Chandran R S
ഗെംദര/लिंग/Gender	M
ഇഡെന്റിതീ കാർഡ നമ്ബര/पहचान पत्र क्रमांक/EPIC No	ICR0317156
ഫത്ഹെര/ഹുസ്ബംദ്എസ് നെയിം/पिता/पति का नाम/Father's/Husband's Name	രവികുമാർ
	Ravikumar
ഭാഗം നമ്പർ/भाग संख्या/Part Number	124
ഭാഗം പേര്/भाग का नाम/Part Name	M S C Lower Primary School, Pamamcodu
വോടർ ഡ്ട് നമ്ബര/मतदाता क्रमांक/Serial No	586
പോലീംഗ സ്ഥശന/मतदान केंद्र/Polling Station	M S C Lower Primary School, Pamamcodu,Pamamcodu
പോളിംഗ് തീയതി/मतदान की तारीख/Polling Date	**No election scheduled currently**
അവസാനം അപ്ഡേറ്റ്/नवीनतम अपडेट का समय/Last Updated On	09/2/2018

Note 1 : This output is computer generated and is provided only for the information to the voter.

Note 2 : This is not an identity document.

मतदाता सूचना प्रिंट करें
Print Voter Information

Fig.2.34: Details of a voter available in National Voters Portal.

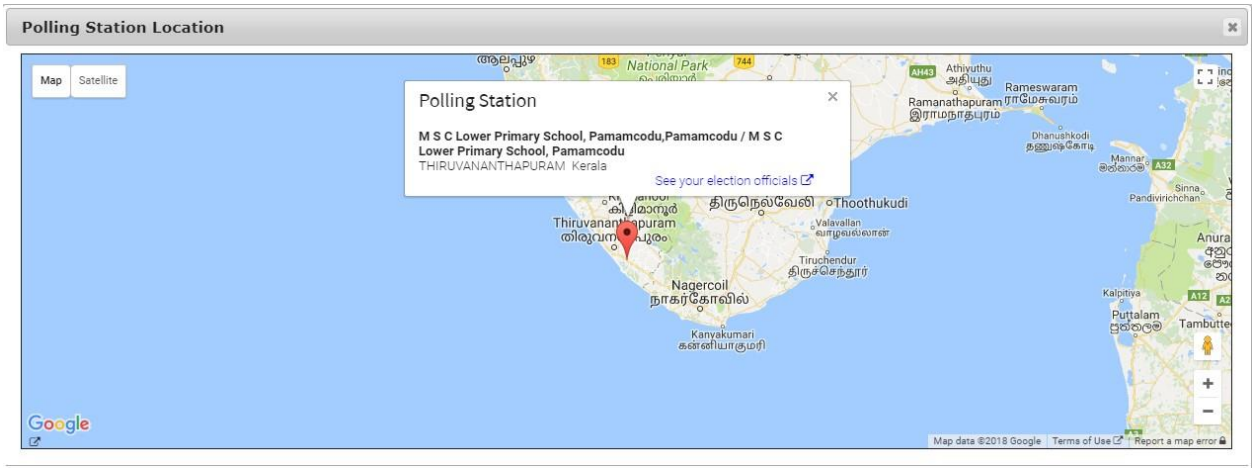


Fig.2.35: Polling Station Location

2.7 Information from Ministry of Road Transport & Highways

Motor vehicle departments will have the details of all the vehicles and driving license issued by them. At any point of investigation, if we get a vehicle number or license number, we can search for the details of owner.

MOTOR VEHICLES DEPARTMENT, KERALA
കേരള മോട്ടോർ വാഹന വകുപ്പ്

Registration Details

Enter Reg Number: KL-01-AH-4648 (Eg: KL-01-AA-7889)
Enter Chassis Number: (Last 5 values)
Enter the charactres*: rhss2x
Get

Reg Number : KL-01-AH-4648 Office: SRTO, NEYYATTINKARA

Owner Details

OwnerName	With Effect From	Guardian	Address	DealerName
RAVIKUMAR S	30-May-2005	--	--	Not Available

Tax / CESS Details

Tax License No.	Tax Paid On	Tax Paid From	Tax Paid TO	Tax Amount	Tax Paid Office	CESS Amount Paid	CESS Paid Date
9224	09-May-2016	01-Apr-2016	31-Mar-2023	Rs 1040	SRTO, NEYYATTINKARA	100	11-Apr-2008

CF Details

CF From Date	CF To Date	Issued Date	Status
25-07-2017	24-07-2018	25-07-2017	Normal

Other Details

Category	VehicleClass	Maker Name	Maker Class	C.C	BHP	Body	Cylinders
Transport	LMV - MOTOR CAB	HINDUSTHAN MOTORS LTD	HINDHUSTHAN AMBASSEDOR	0.00	0.00	SALOON	4 nos

Mfd Month	Mfd Year	Seat Capacity	ULW	Fuel	Wheel Base	Color	Registration Date	Delivery Date
May	2005	5	1200	DIESEL	0.00	CRYSTAL WHITE	02-Jun-2005	02-Jun-2005

3. Crime Scene Management

3.1 Videography and Photograph the scene of crime:

- 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 SoC 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

3.2 Isolate the scene of crime both electronically and physically, Interview the user:

- Isolate the person immediately who is working on the Computer if any, and interrogate him/her without allowing him/her touching the Computer.
- Isolate the System from the Network.
- Search the entire crime scene carefully inorder to not to miss any evidences at the crime scene.
- Collection of finger print has to be done if required.
- Visible inspection of Scene of Crime has to be done in front of technically qualified independent witnesses without touching anything.

- **Note :**At crime scene we may find the evidences in different forms of deceptive devices, which cannot be easily identified with the naked eye. The Suspect may hide the evidences in Different types of USB connectivity devices like Keychain, Locket, Bracelet, ATM Card, PowerBank, IPod, IPAD, Mobile Phone, PDA, CD/ DVD, External HardDisk (Traditional or SSD), SIM Card, SD Card or Memory Card, ..etc

3.3 If system is switched ON:

1.1.1 Connect the Portable Forensic Tools Drive (CD/ DVD/ USB/ External HardDisk ..etc) to the System and run Forensic RAM Dump Tool and Collect the RAM dump to the Sterilized media, which has been carried to the scene of crime.

1.1.2 Check whether the HardDisk (which is present in the Suspect Computer) has been Encrypted using Portable Forensic Encryption Detection Tool and load the output into Sterilized media

1.1.3 Collect the Registry Dump using the Portable Forensic Registry Dump Tool and load the output into Sterilized media

1.1.4 If possible, collect the Browser Information, System Information …etc using Portable Forensic Tool and load the output into Sterilized media

Note: All the Evidences should be collected into Sterilized or Wiped Media which has been carried to Scene of Crime.

Note: If the Investigating Officer is not technically sound enough in the collection of the evidences, he / she can take the guidance of Cyber Forensics Expert

1.1.5 After collection of all the Volatile Information, the Investigating Officer can Pull the power cable from electrical switchboard and then remove the power cable from SMPS (Switch Mode Power Sup- ply) from the back of CPU Cabinet.

1.1.6 Make sure that the system is completely turned off and then remove the back cover of the CPU cabinet using the particular screw driver.

1.1.7 Take the photograph of the Motherboard where the connectivity of all the peripherals like Hard Disk, RAM, NIC, BIOS etc….is visible and then detach the HardDisk from MotherBoard.

1.1.8 Take the Photograph of the HardDisk where Serial Number, Make & Model is clearly visible.

3.4 If the system is switched OFF:

i. Pull the power cable from electrical switchboard and then remove the power cable from SMPS (Switch Mode Power Sup- ply) from the back of CPU Cabinet.

ii. Make sure that the system is completely turned off and then remove the back cover of the CPU cabinet using the particular screw driver.

iii. Take the photograph of the Motherboard where the connectivity of all the peripherals like Hard Disk, RAM, NIC, BIOS etc….is visible and then detach the HardDisk from MotherBoard.

iv. Take the Photograph of the HardDisk where Serial Number, Make & Model is clearly visible.

3.5 Take the HASH value or capture the bit stream image:

i. Connect the Seized Hard Disk via Write Blocker to Forensic Workstation / Laptop which has been carried to the scene of crime and Calculate the Hash Value of it by using the Portable Forensic Hashing Tool in the presence of Forensic Expert

Note: If the Forensic Expert is not available at Scene of Crime and If the Investigating Officer is not technically sound in calculating the hash value, he/she has to seize and pack the Hard Disk properly and send it to FSL after noting down all the details of the Hard Disk

ii. Take an Image of Seized Media (Hard Disk / Pen drive/ SD Card...etc) using Portable Forensic Imaging Tool via Write Blocker and create atleast 3 image copies (duplicate copies)

Note: Never open / access the Original Suspect Media directly without Write Blocker, because it may tamper the Evidence data and which will not be admissible in a court of Law.

iii. Out of three Image Copies, First Image has to be sent to the Forensic Science Laboratory along with Seizure Memo, Chain of Custody Form, Questionnaire and Forwarding Note. Second image has to be kept with IO for analysis. Third image to be handed over to the accused party if requested and the Original Seized Media has to be sent to the Court along with other Original Documents at the time of submission of the Final Report.

3.6 Preparation before reaching scene of crime

i. Visualizing of Crime Scene

a) While investigating Cyber Crimes, the Investigation Officer come across various scenarios of Cyber Crimes.

b) The Crime Scene can vary from a scene with a single laptop/desktop to a Cyber Cafe to a small office network to an industry with thousands of systems connected.

c) Inorder to handle this variety of crime scenes and variety of digital evidences, the Investigation Officer should reach the crime scene with Proper Toolkit.

ii. Arrangement of Man power and Role & Responsibilities of each person.

iii. Required tool kit

iv. The Digital Forensics kit should be a portable forensics kit and should provide a complete solution for performing digital forensics Seizure, Acquisition and Analysis.

v. It should be easily carried to crime scene and can carry out on-location forensic investigations.

vi. The list of things that includes in digital forensic kit are listed below which can be used for different crime scenarios.

a) Generic tools

1. Digital Camera to take photographs of Crime Scene
2. External Sterile Media to store all the evidences collected at scene of crime
3. External CD/ DVD Driver
4. IDE & SATA Data Cables, Power Adapters, Convereters etc.
5. Multiple USB Adapter
6. Laptop Batteries
7. Back up chargers
8. Power bank
9. ScrewDriver Box

10. Magnifying Glass
11. Scissors
12. Gloves
13. Torchlight

b) Special Tools

1. Portable Workstation: A Laptop of good configuration, installed with all software tools (For Calculating Hash Values, Creating Image, Dumping the RAM Content, Analyzing a Disk, Mobile, Network & Live System Data).
2. Write Blocker to protect the Suspect Media from tampering the data while doing Hashing, Imaging and Analysis (if needed).
3. CDs / DVDs / Pendrives with Portable Software Tools can be used for Search & Seizure of Evidences from Suspect Machine.
4. Disk imaging Hardware or Software tools for taking a copy of original storage media (Suspect Media)

c) Packaging and Labelling Material

1. AntiStatic Bags for storing the seized electronic media which are prone to damage caused by electrostatic discharge.
2. Bubble Wraps for packaging the seized electronic media inorder to prevent from physical damages or scratches.
3. Tapes (ex:transparent or brown) for sealing or packaging.
4. Carton Box or Brown Colour Sheet for packaging & Labelling on it.
5. Labelling Device
6. Labelling Marker

e) Mobile equipment

1. Faraday Bag
2. SIM Card Data Extractor / Analyzer
3. SD Card / Memory Card Reader
4. Cables, Power cords for various Mobiles

f) Documentation Material

1. Search warrant has to be collected from Court (if required)
2. Seizure Memo form to document all seized material objects with model number, make, serial number and capacity

3. Chain of Custody form to fill the officer's details who has submitted the evidence and who has received the evidence at FSL.
4. 65B certificate may be obtained from the user of the system
5. Forwarding Note
6. Pen / Pencil, Eraser, Sharpener, Notepad…..etc to document the things at Scene of Crime.

Note:

- Portable Scanner and Portable printers can also be carried to Scene of crime.
- Software based or Hardware based tools can be used for Collection and Analysis of Digital Evidence.
- Forensically sound Boot disks like Helix, Paladin, DeFT...etc can also be used for collection and Analysis of Digital Evidence.
- Above mentioned list is not exhaustive. It is an indicative list which has no limit and the kit actually depends on Scene of Crime.

3.7 SOP for Mobile Devices

i. Isolate the mobile device from the network

Improper handling of a mobile device during seizure may cause loss of digital data. If the device is not handled properly, physical evidences may be contaminated and rendered useless. So, we need to secure and evaluate the scene of crime before acquiring a communication device and all areas of the scene should be searched thoroughly ensuring related evidence is not overlooked. Isolating the mobile device from other devices used for data synchronization is important to keep new data from contaminating existing data. Equipments associated with a mobile device, such as removable media, SIM cards and personal computers, may prove more valuable than the mobile device itself. Removable media varies in size and can be easily hidden and difficult to find. Personal computers may be particularly useful in later accessing a locked mobile device, if it has established a trusted relationship with the mobile device. For example, Apple incorporates a pairing process whereby an existing pairing record file can be used by some tools to access the mobile device. When interviewing the owner or user of a mobile device, consider re- questing any security codes, passwords or gestures needed to gain access to its contents. For example, a GSM device may have authentication codes set for the internal memory and/or the SIM card.

Many mobile devices offer the user ability to perform either a remote lock or remote wipe by simply sending a command (e.g., text message) to the mobile device. In order to protect that we have to isolate the phone from all the radio signals it was bounded from it.

Additional reasons for disabling network connectivity include incoming data (e.g., calls or text messages) that may modify the current state of the

data stored on the mobile device. There are few ways to isolate any mobile device. Each method has certain drawbacks:

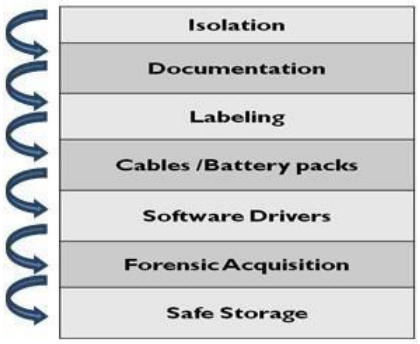


Fig.3.1 Steps in mobile device seizure

- **Airplane Mode (Only for Smartphone's):** Requires interaction with the mobile device using the keypad, which poses some risk. The technician should be familiar with the device in question and documents the actions taken (e.g., on paper or on video). Note: airplane mode does not prevent the system from using other services such as GPS in all cases.
- **Faraday Bags (feature phones):** Faraday containers may attenuate the radio signal, but not necessarily eliminate it completely .The risk of improperly sealing the Faraday container must be avoided.
- **Switch the device off**: Turning off the mobile device may activate authentication codes like PIN's and passwords which in turn takes time to break and delays the acqui- sition and analysis.
- **Use Cloned SIM Cards**: A forensic examiner clone original SIM cards to mimic the identity of them, and prevents network access to/from the handset. We call such cards as CNIC or Cellular network isolation card. Such cards also prevent the handset in erasing call logs data when a unknown/foreign SIM is inserted. If the SIM for a device is present, but requires a PUK code, a substitute SIM can be created providing acquisition to proceed without having to contact the service provider for the PUK. The values by which the mobile device correlates to the previously inserted SIM are the ICCID and the IMSI, both of them are unique and used to authenticate the user with the network. Isolation is done to all mobile/ communication devices to avoid Accidental access from the IO and to prevent remote wiping. Various mobile phone shielding devices (i.e., a tool designed to act as a Faraday cage) are used by law enforcement agencies prevent network communication to the seized devices. Examiners should test their own products to validate that they are working properly before use.

ii. Documentation:

Documenting every piece of electronic evidence with its serial number, make and model number properly in "seizure Panchnama" along with photographs of Scene Of Crime. Non-electronic materials such as invoices, manuals, and packaging material may provide useful information about the capabilities of the device, the network used, account information, and unlocking codes for the PIN. All digital devices, including mobile devices, which may store data, should be photographed along with all peripherals cables, power connectors, removable media, and connections. Make sure that correct placement of SIM Cards and other equipments are properly mentioned. If the device's display is in a viewable state, the screen's contents should be photographed and, if necessary, recorded manually, capturing the time, service status, battery level, and other displayed icons.

iii. Labeling:

Label all collected pieces of evidence at scene of crime so as to ensure proper chain of custody for every evidence article. All digital devices, including mobile devices, which may store data, should be labeled along with all peripherals cables, power connectors, removable media, and connections.

Mobile devices need to be identified by the make, model, and service provider before it is labelled. If the mobile device is not identifiable, photographing the front, back and sides of the device may be useful in identifying the make, model and current state (e.g., screen lock) at a later time.

Further means of identification may include:

- Device Characteristics: The make and manufacturer of a mobile device may be identified by its observable characteristics (e.g., weight, dimensions, and form fac- tor).
- Device Interface: The power connector can be specific to a manufacturer and may provide clues for device identification. With familiarization and experience, the manufacturers of certain mobile devices may be readily identified. Based on the size, number of contacts, and shape of the data cable interface are often specific to particular manufacturer and may prove helpful in identification.
- Device Label:
  The International Mobile Equipment Identity or IMEI is a number, usually unique, to identify mobile phones, as well as some satellite phones. It is usually found printed inside the battery compartment of the phone, but can also be displayed on-screen on most phones by entering *#06# on the dial pad. The IMEI number is a 15 decimal digits number (14 digits plus a check digit). The model and origin comprise the initial 8-digit portion of the IMEI/SV, known as the Type Allocation Code (TAC). The remainder of the IMEI is manufacturer-defined, with a Luhn check digit at the end.

  As of 2004, the format of the IMEI is AA-BBBBBB-CCCCCC-D, although it may not always be displayed this way. The IMEISV has two digits for the Software Version Number (SVN), making the format AA-BBBBBB-CCCCCC-EE

Prior to 2002, the TAC was six digits long and was followed by a two-digit Final Assembly Code (FAC), which was a manufacturer specific code indicating the location of the device's construction. From January 1, 2003 till April 1, 2004, the FAC for all phones was 00. After April 1, 2004, the Final Assembly Code was removed and the Type Allocation Code was increased to eight digits in length.

Fig.3.2 Comparison of Old and New format of IMEI

In any of the above cases, the first two digits of the TAC are the Reporting Body Identifier, which identifies the GSMA-approved group that allocated the TAC. The RBI numbers are allocated by the Global Decimal Administrator.

For example, the old style IMEI code 35-209900-176148-1 or IMEISV code 35-209900-176148-23 tells us the following:

TAC: 35-2099 - issued by the BABT (code 35) with the allocation number 2099

FAC: 00 - indicating the phone was made during the transition period when FACs were being removed.

SNR: 176148 - uniquely identifying a unit of this model

CD: 1 so it is a GSM Phase 2 or higher
SVN: 23 - The "software version number" identifying the revision of the software installed on the phone. 99 is reserved.

We can check the IMEI of any android phone in the about option directly if we have access. The screenshot is shared below.

It can also be found on the back panel by removing the battery for few of the phones.

Various sites on the Internet offer databases that provide information about the mobile device based on an identifier, such as:

- www.numberingplans.com
- http://Imei.info
- https://imeidata.net

Cable BatteryPack & Software Drivers: Collection of all proprietary attachments alongwith the device helps forensic examiners on easy access to device during acquisition. It’s a good practice to collect or search for software drivers available at scene of crime for the device seized.

iv. Transport to forensic lab

The mobile devices should be packed properly before sending them to the labs for analysis. Ensure that the device is cut off from the network and is having sufficient amount of battery charge (in case of switched on devices) is available. If not attach one power bank to charge it inside the faraday bag. Send the devices along with sufficient documents to the forensics lab.

3.8 Collecting Evidences from CCTV recordings

Before collecting the electronic data from the CCTV system following information should be documented.

1. Photographs of CCTV system and its components is to be taken.
2. Prepare sketch of Camera, System placement and position.
3. Make, Model and Serial Number of digital video recorder (DVR) or Network Video Recorder (NVR).
4. Whether system is PC based or stand-aloneor Embedded or Network based.
5. Number of recording units installed.
6. Recording capacity of the system and when it will overwrite.
7. Number of camera(s) installed and number of camera(s) active.
8. Make and model of each camera.
9. Are any Cameras Infrared /Night vision enabled sensitive? If so, identify.
10. Are any Cameras Number Plate Identification enabled? If so, identify.
11. System password, if any.
12. Date and time displayed by the system.
13. Actual current time and date (From Reference clock).
14. System Setting.
    - Image quality.
    - Frames/picture per second.
    - Recorded Image/Frame size.
    - Number of hard disk and storage capacity of each of the hard disks.
    - System Firmware version.
    - Other available System setting (e. g., event log)
16. Playback software name and version.
17. Password of software to open the concerned file, if any.
18. Whether audio being recorded? If so, how many channels are downloadable or exportable?

19. Scene contact information

- Address
- Hours of operation.
- Contact information of CCTV system installer.

20. Other information of importance.

3.8.1 Collection of Electronic Data

1. A determination should be made as to how much and what type of data needs to be retrieved from the CCTV recording system.
2. Consideration of factors like amount and type of media required and time taken in data transfer is of utmost importance.
3. Determine the possible output options, e.g.: CD/DVD writer, USB drive, ports etc.
4. Performing a test retrieval will assist in estimating the time and storage require- ments for the chosen output option.
5. Most of the DVR systems have a built-in or external CD/DVD writer to retrieve the data. In this case, following information should be kept in mind.
6. Generally, the system allows to copy the propriety viewer to the disc while burning where option may be selected manually.
7. 'Write-once' and not 'multi-session' mode should be used for taking data in CD-R/DVD-R.
8. Some system may take only CD-RW/DVD-RW. At the earliest possible time, the data should be transferred to CD-R/DVD-R.
9. After retrieval of data in CD/DVD, the data should be verified if the data of proper date and time has been retrieved.
10. If the files are retrieved in multiple CD/DVD, they should be named to ensure that the proper order of playback is identifiable.
11. The proprietary software (player) should also be provided.
12. In case the DVR system is not a build-in CD/DVD writer, an external CD/DVD writer can also be connected through a USB/Firewire/SCSI port.
13. Some CCTV systems have a compact flash card option, which is usually intended for short video sequences. If video is recovered via these drives, at the earliest possible time, all data should be transferred from compact flash card to a more permanent media and hash of the data may be calculated for reference.
14. USB / Firewire / SCSI Ports, if available, can be used to connect external drives, CD/DVD writers and legacy devices. It should first be established that the port is in working condition. Some devices may require installation of necessary drivers on the recording systems. It is advisable to contact the Operator / Manufacturer of the CCTV systems before making any of such installation.
15. Most DVR systems have a limitation on the amount of data that can be retrieved (exported/downloaded) at a time, typically 1GB or 2GB. The limit may not be specified in the system manual. It is the best

practice to keep the file under 1GB, unless it is known for sure it is capable for more.

16. Many CCTV systems have network ports and their own proprietary network viewer software which allows for multi-computer connectivity and recovery of the na- tive/proprietary recorded files. By utilizing an Ethernet crossover cable, computer and network viewer, a connection to the DVR can be established and the na- tive/proprietary file(s) are downloaded/exported.
17. In some situations, the quickest solution may appear to removethe hard drives from the system and replace them. This option should be opted carefully as there are many factors that come into play.
18. 65B Certificate and Chain of Custody Form to be filled appropriately.
19. Label, pack and transport to FSL

3.9 Collection of evidences from Network Devices

Step 1: Identify the network device (Hub, Switch, and Router Bridgeetc). If there is any difficulty to identify the network device in scene of crime, use internet search make and model number of the device.

Step 2: Take Photographs of

– Deviceindicating make and model number.

– Connected cables with serial number.

Step 3:

– If the device found in Switched off state: Collect MAC address of the all ports, MAC address is written on the device as shown in figure–.

Fig.3.2: MAC Address written on router.

– 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 4: If any information or file is collected from network administrator as shown in step 3, calculate HASH value of that file.

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

3.9.1 MODEM/WiFi Routers

Generally Modems are used for Home environment or Small organizations. We will follow the steps given below to collect information from modems/ wifi routers.

Step1: Take Photographs of MODEM indicating its make 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 is connected to the MODEM. The password for the same should be available with the Network Administrator. Every wireless modem or a wireless router contain a webpage. Using this an IO can acesses the information avilable in it. IO need to collect information as shown below 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.

3.9.2 SERVER SYSTEMS

- Check out the OS and hard disk configuration
- Note down the RAID type
- RAM Dump
- Image using the Live CD
- Soft shutdown
- Seize the entire server (Don't remove the hard disk)
- Check for the NAS or SAN
- Mainframes (Seizure is not possible)
- On sight Image with Live CD or Pen drive
- Check for the backups relevant for the time period
- Check for external storage devices like Hard disk, pendrive, flash media etc.

4. IP, Website and E-mail Investigation

4.1 Introduction to Networks

A network is any collection of independent computers that communicate with one another over a shared network medium.

- A computer network is a collection of two or more connected computers. When these computers are joined in a network, people can share files and peripherals such as modems, printers, tape backup drives, or CD-ROM drives.

- It requires protocols to perform above task. Protocol is any standard method of communicating over a network.
- **NIC**- Network Interface Card, an adapter card that is inserted into a computer, and contains the necessary software and electronics to enable the station to communicate over the network.

- **Packet**- A series of bits containing data and control information, including source and destination node addresses, formatted for transmission from one node to another.

4.2 Need of Networks:

- **Enhance Communication**: It's hard for people to work together if no one knows what anyone else is doing. A network allows employees to share files, view other people's work, and exchange ideas more efficiently. In a larger office, you can use e-mail and instant messaging tools to communicate quickly and to store messages for future reference.
- **Share Resources**: Networking of computers helps the network users to share data files. A network makes it easy for everyone to access the same file.
  - **Facilitate Centralized management:** A corporate computer network usually consists of many different electronic devices, power distribution systems, and work consoles. With centralized network management, all of these can be managed from a single control station or server. Businesses often to tend to add equipment and software to networks that can make them more complex; the number of systems to manage is sometimes so large there is a lack of connections between disparate parts. Centralized management usually makes user access, data storage, and troubleshooting more convenient.

4.2.1 Types of Networks

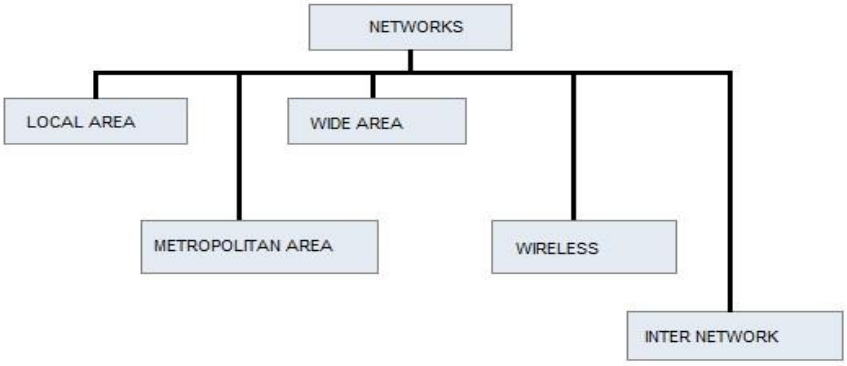


Fig.4.1 Types of Networks

4.2.3 Network protocols

Application	Description
DHCP	Dynamic Host Configuration Protocol assigns IP addresses
DNS	Domain Name System translates website names to IP addresses
HTTP	Hypertext Transfer Protocol used to transfer web pages
NBNS	NetBIOS Name Service translates local host names to IP addresses
SMTP	Simple Mail Transfer Protocol sends email messages
SNMP	Simple Network Management Protocol manages network devices
SNTP	Simple Network Time Protocol provides time of day
Telnet	Bi-directional text communication via a terminal application
TFTP	Trivial File Transfer Protocol used to transfer small amounts of data

The well known port numbers are assigned by IANA which is the Internet Assigned Numbers Authority. IANA is the same group that manages the DNS Root and IP addresses.

Fig.4.2 Various Network Protocols

Label on Column	Service Name	UDP and TCP Port Numbers Included
DNS	Domain Name Service – UDP	UDP 53
DNS TCP	Domain Name Service – TCP	TCP 53
HTTP	Web	TCP 80
HTTPS	Secure Web (SSL)	TCP 443
SMTP	Simple Mail Transport	TCP 25
POP	Post Office Protocol	TCP 109, 110
SNMP	Simple Network Management	TCP 161,162 UDP 161,162
TELNET	Telnet Terminal	TCP 23
FTP	File Transfer Protocol	TCP 20,21
SSH	Secure Shell (terminal)	TCP 22
AFP IP	Apple File Protocol/IP	TCP 447, 548

Table 1: Various Services and Port Numbers

4.3 IP Addressing

An IP (Internet Protocol) address is a unique number that is assigned to each computer (or other device) that participates in a network. This number is used to identify and locate each device.

A DHCP service is usually used to automatically assign unique IP addresses to each device. IP address can also be assigned statically – which means that the device is specifically configured to use a designated IP address.

There are two versions of IP addresses in use on the internet. These are the IPv4 and IPv6 Addresses.

IPv4: A version 4 IP address (or IPv4 address) is a 32 bit number that is usually represented in chunks of a 4 8-bit decimal bytes seperated by dots (.). For example, 192.168.0.1.

IPv6: IPv6 address is a 128 bit number tha t is usually represented in chunks of 8 hexadecimal 16 bit words, separated by colons (:).

For example, 2001:0500:0088:0200:0000:0000:0000:0010.

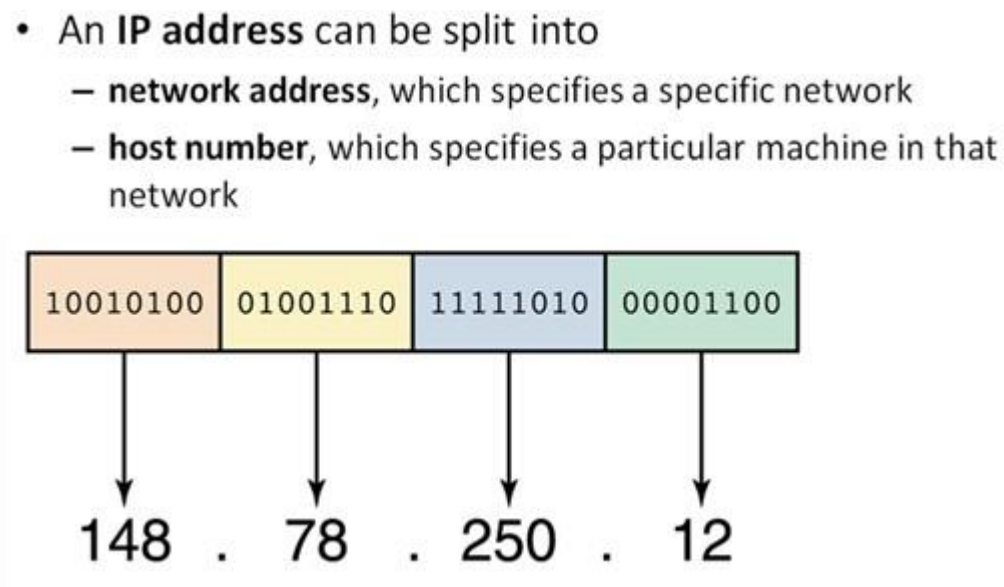


Fig. 4.3 IP v4 Structure

Each TCP/IP host is identified by a logical IP address . The IP address is a network layer address and has no dependence on the DataLink layer address (such as a MAC address of a network adapter). A unique IP address is required for each host and network component that communicates using TCP/IP.

The IP address identifies a system's location on the network in the same way a street address identifies a house on a city block. Just as a street address must identify a unique residence, an IP address must be globally unique and have a uniform format.

Each IP address includes a network ID and a host ID.

- The **network ID** (also known as a network address) identifies the systems that are located on the same physical network bounded by IP routers. All systems on the same physical network must have the same network ID. The network ID must be unique to the internetwork.
- The **host ID** (also known as a host address) identifies a workstation, server, router, or other TCP/IP host within a network. The address for each host must be unique to the network ID.

Network ID refers to any IP network ID, whether it is class-based, a subnet, or a supernet.

An IP address consists of 32 bits. Rather than working with 32 bits at a time, it is a common practice to segment the 32 bits of an IP address into four 8-bit fields called *octets* . Each octet is converted to a decimal number (the Base 10 numbering system) in the range 0-255 and separated by a period (a dot). This format is called dotted decimal notation. Table 1.10 provides an example of an IP address in binary and dotted decimal formats.

4.4 Internet Protocol

Unlike TCP, **IP is an unreliable, connectionless protocol**. IP doesn't care whether a packet gets to it's destination or not. Nor does IP know about connections and port numbers. **IP's job is too send and route packets to other computers**. IP packets are independent entities and may arrive out of order or not at all. It is TCP's job to make sure packets arrive and are in the correct order. About the only thing IP has in common with TCP is the way it receives data and adds it's own IP header information to the TCP data. The **IPv4 header** looks like this:

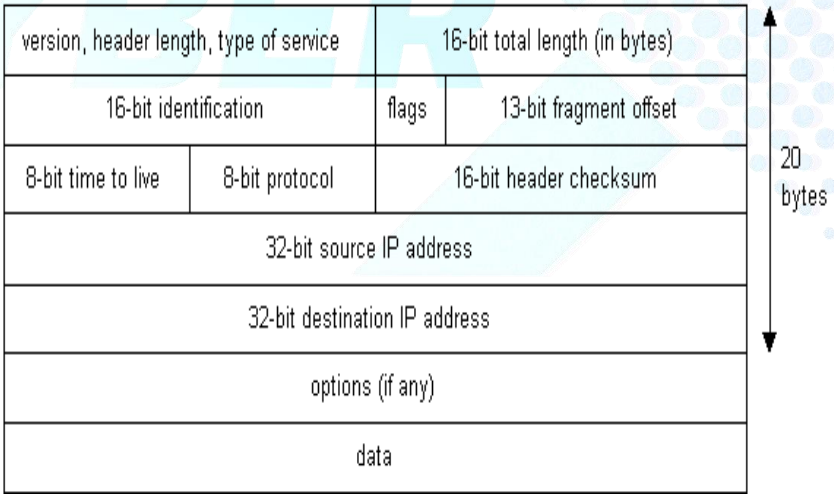


Fig.4.4 IP Header Structure

Above we see the IP addresses of the sending and receiving computers in the IP header. Below is what a packet looks like after passing through the application layer, TCP layer, and IP layer. The application layer data is segmented in the TCP layer, the TCP header is added, the packet continues to the IP layer, the IP header is added, and then the packet is transmitted across the Internet.

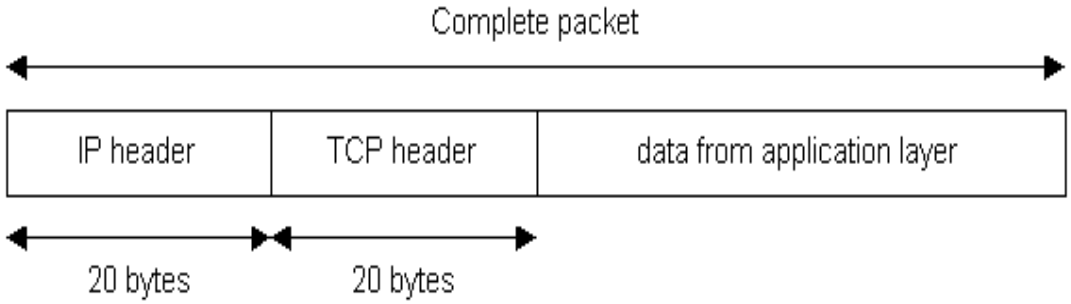


Fig.4.5 IP Packet Structure

4.4.1 IP address Classification

IP addresses are organized into classes. For convenience of humans, IP addresses are expressed in the decimal format. Every number in each class is represented as binary to computers.

The four numbers in an IP address are known as 'octets'. Each of them has eight bit positions. The octets are divided into two sections: Net and Host. The first octet represents Net for identifying the network and the Host contains the last octet. There are five IP classes.

- **Class A:** The class A is used for very large networks. There are 1 to 126 are part of this class. That means there are 126 Class A networks. Class A networks accounts for half of the total available IP addresses. supports**16 million** hosts on each of 126 networks.

- **Class B:** It is used for medium size networks. The IP address with a first octet from 128 to 191 is part of this class. Class B networks have a first bit value of 1 and a second bit value of 0 in the first octet. supports**65,000** hosts on each of 16,000 networks.
- **Class C:** Class C is used for small to middle size networks. IP address with a first octet starts from 192-223. Class C networks have a first bit value of 1, second bit value of 1 and a third bit value of 0 in the first octet. supports**254** hosts on each of 2 million networks.

- **Class D:** It has first, second and third bit value as 1 and the fourth bit as 0. The other 28 bits are used for identifying the group of computers which is intended for multicast messages.
- **Class E:** Class E is used for identification purpose. The four bits value is 1. The other 28 bits are used for identifying the group of computers which is intended for multicast messages.

4.4.2Types of IP addresses

a) Static & Dynamic IP addressing

Static IP is also called as permanent address assigned to each device in a network, whereas Dynamic IP, a temporary address assigned to the device via DHCP software. IP address assigned to your service by your cable or DSL Internet provider is typically dynamic IP. In routers and operating systems, the default configuration for clients is dynamic IP.

Dynamic IP is an IP address that is assigned automatically by the system to a device, account or user when it is connected to the network; that is, it is assigned as needed rather than in advance.

b) Private and Public IP address:

Public and private IP (Internet Protocol) addresses sometimes called "external" and "internal" IP addresses. Both provide unique identification to every device on a network.

Public external) IP address is the one that your ISP (Internet Service Provider) provides to identify your home network to the outside world. It is an IP address that is unique throughout the entire Internet. Depending on the service, a computer might have an IP address that never changes (a fixed, or static IP address). But most ISPs provide an IP address that can change from time to time (a dynamic IP address).

Private (Internal) IP address is issued by the router to each network device inside the network. This provides unique identification for devices that are within the network, such as a computer, mobile.

IP Range	Start Address	End Address	Number of Addresses
10.0.0.0/8	10.0.0.0	10.255.255.255	16,777,216
172.16.0.0/12	172.16.0.0	172.31.255.255	1,048,576
192.168.0.0/16	192.168.0.0	192.168.255.255	65,536

Fig.4.6 Private IP Address Range

4.5 Addressing modes

a) Unicast Addressing Mode:

In this mode, data is sent only to one destined host. The Destination Address field contains 32- bit IP address of the destination host. Here the client sends data to the targeted server:

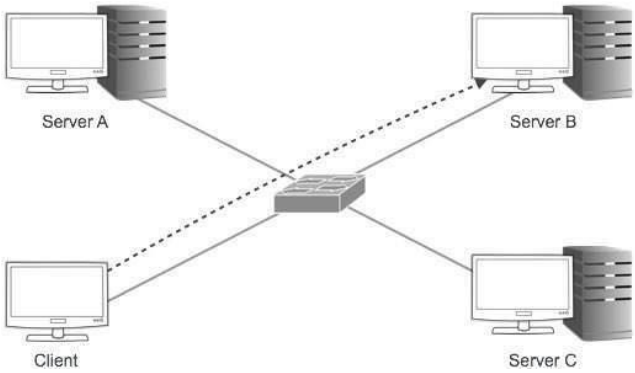


Fig.4.7 Unicast Addressing Mode

b) Broadcast Addressing Mode

In this mode, the packet is addressed to all the hosts in a network segment. The Destination Address field contains a special broadcast address, i.e.**255.255.255.255**. When a host sees this packet on the network, it is bound to process it. Here the client sends a packet, which is entertained by all the Servers:

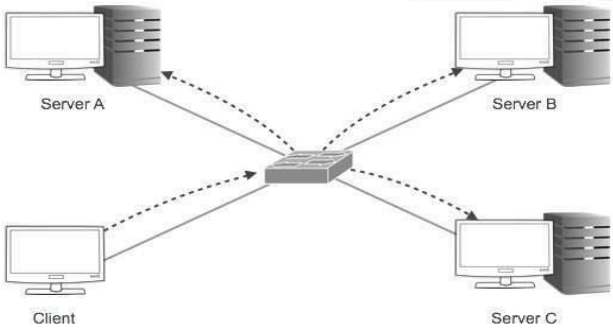


Fig.4.8 Broadcast Addressing Mode

c) Multicast Addressing Mode:

This mode is a mix of the previous two modes, i.e. the packet sent is neither destined to a single host nor all the hosts on the segment. In this packet, the Destination Address contains a special address which starts with 224.x.x.x and can be entertained by more than one host.

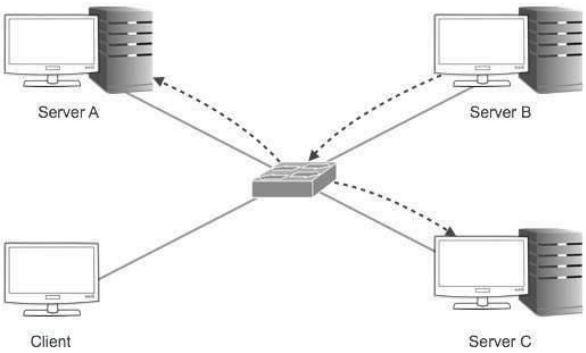


Fig.4.9 Multicast Addressing Mode

Here a server sends packets which are entertained by more than one servers. Every network has one IP address reserved for the Network Number which represents the network and one IP address reserved for the Broadcast Address, which represents all the hosts in that network.

4.6 IPv6

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP) increased to 128 bit, the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.

Address representation

The 128 bits of an IPv6 address are represented in 8 groups of 16 bits each. Each group is written as 4 hexadecimal digits and the groups are separated by colons (:). The address **2001:0db8:0000:0000:0000:ff00:0042:8329** is an example of this representation.

An example of application of these rules:
Initial address: **2001:0db8:0000:0000:0000:ff00:0042:8329** After removing all leading zeroes in each group:
2001:db8:0:0:0:ff00:42:8329
After omitting consecutive sections of zeroes: **2001:db8::ff00:42:8329**

4.7 Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) provides configuration parameters to Internet hosts like computers, smart phones,

PDA's etc whoever requests within that computer or cellular network. DHCP consists of two components:

i) a protocol for delivering host-specific configuration parameters from a DHCP server to a host and ii)a mechanism for allocation of

network addresses to hosts.

Normally the DHCP server provides the client with at least this basic information:

1. IP Address
2. Subnet Mask
3. Default Gateway

Other information can be provided as well, such as Domain Name Service (DNS) server addresses and Windows Internet Name Service (WINS) server addresses. The system administrator configures the DHCP server with the options that are parsed out to the client.

DHCP supports three mechanisms for IP address allocation. In "automatic allocation", DHCP assigns a permanent IP address to a client. In "dynamic allocation", DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address). In "manual allocation", a client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client.

Dynamic Allocation is the only one of the three mechanisms that allows automatic reuse of an address that is no longer needed by the client to which it was assigned. Thus, dynamic allocation is particularly useful for assigning an address to a client that will be connected to the network only temporarily or for sharing a limited pool of IP addresses among a group of clients that do not need permanent IP addresses. Dynamic allocation may also be a good choice for assigning an IP address to a new client being permanently connected to a network where IP addresses are sufficiently scarce that it is important to reclaim them when old clients are retired.

Manual Allocation allows DHCP to be used to eliminate the errorprone process of manually configuring hosts with IP addresses in environments where (for whatever reasons) it is desirable to manage IP address assignment outside of the DHCP mechanisms.

4.8 E-MAIL Investigation

Electronic mail (abbreviated "e-mail") is a store and forward method of electronic messages. It involves composing, sending, storing, and receiving messages over electronic communication systems.

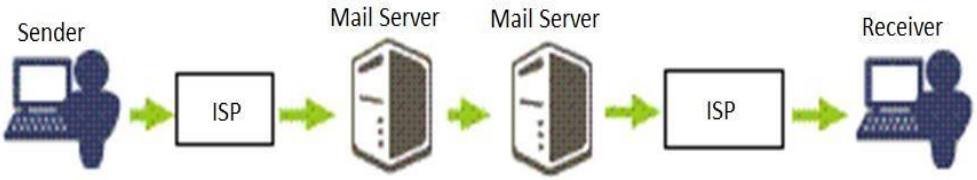


Fig.4.13: Working of E-mail

Before starting analysis of e-mails, we need to know that an email Consists of three components, namely –

- **Email Envelope** – Email is enclosed in a digital envelop analogous to envelope of a hardcopy letter.
- **Email Header**– Contains the Control and Meta Information of the email. For e.g. originator's email address, recipient's email address, email date/time, information of intermediate email servers (if any) etc.
- **Email Body** – Contains email Text/attachments.

What is e-mail tracing?

The procedure of finding the sender / originator of an e-mail is e-mail tracing.

Steps in tracing the e-mail:

- Identifying the IP address in an e-mail
- Conversion of time stamp to IST
- Tracing Internet Service Provider (ISP)
- Collecting the IP address user particulars from the ISP
- Identifying the originator of the e-mail

Imagine you receive an e-mail as follows:

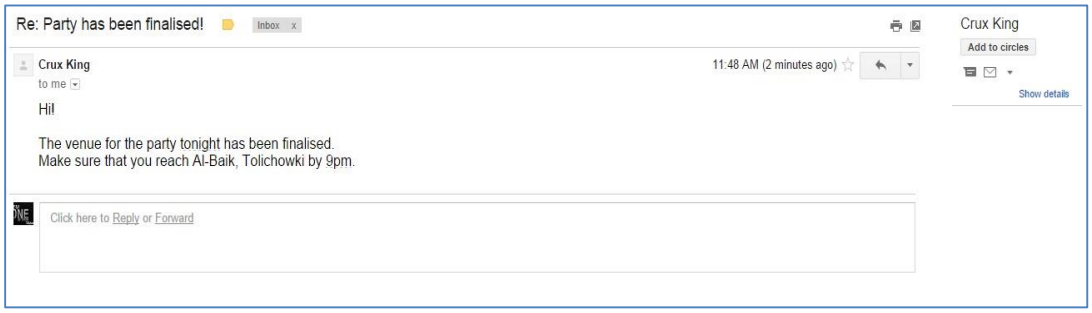


Fig.4.14: Sample E-mail

From the above e-mail what can we directly see?

- e-mail sender's name
  If we click on the small triangle we can see few more details as follows:
- sender's e-mail address
- date & time when the mail was received

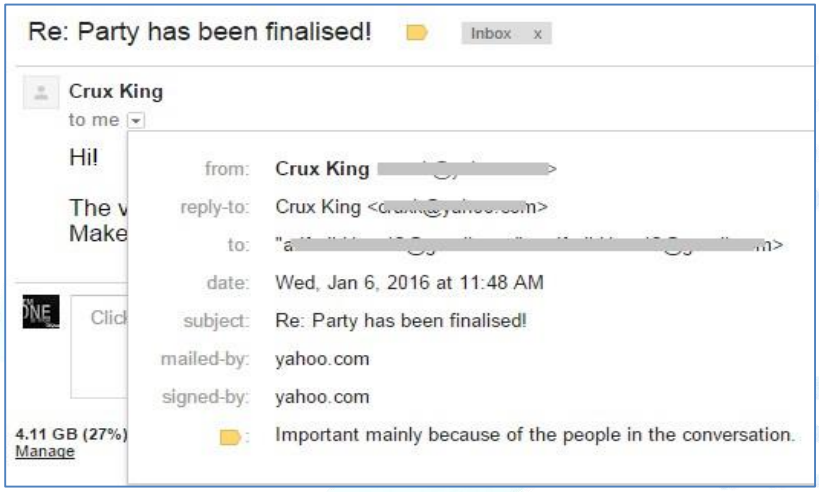


Fig.4.15: Details Available in an E-mail

In the right corner, click on the triangle beside the 'reply' button to open a drop down menu and click on 'Show original'.

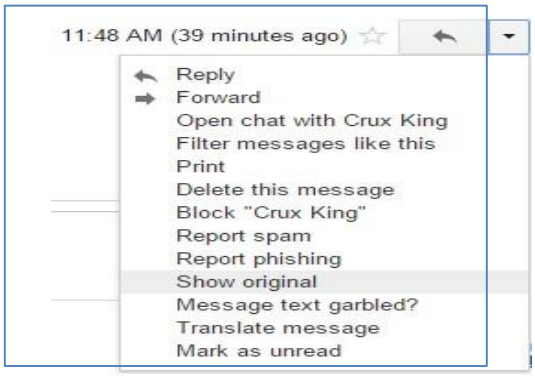
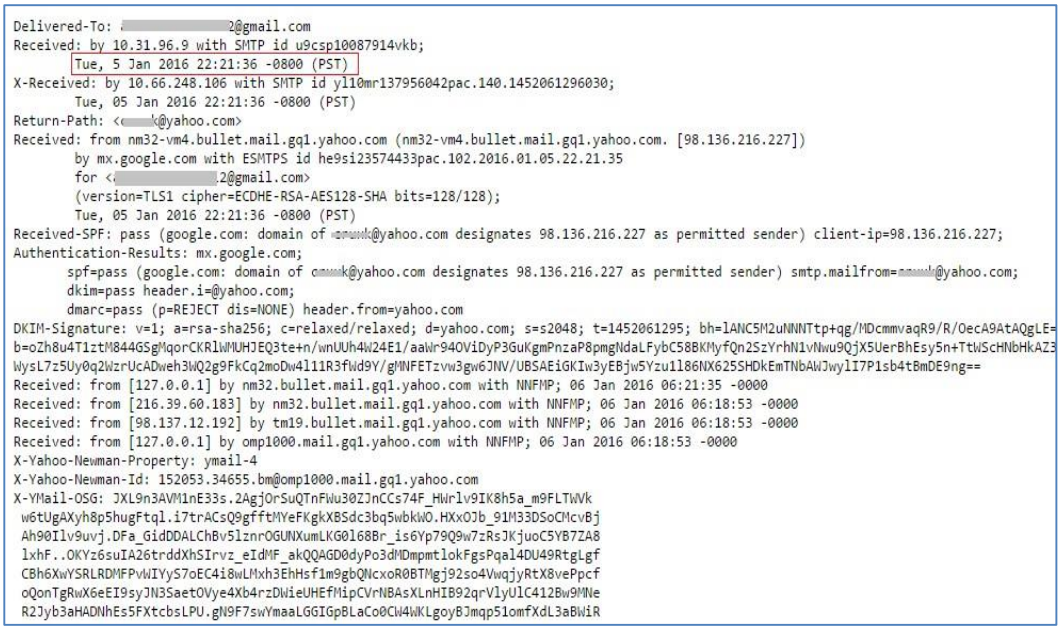


Fig.4.16: Opening E-mail header in G-mail



```
Delivered-To: [redacted]2@gmail.com
Received: by 10.31.96.9 with SMTP id u9csp10087914vkb;
        Tue, 5 Jan 2016 22:21:36 -0800 (PST)
X-Received: by 10.66.248.106 with SMTP id yl10mr137956042pac.140.1452061296030;
        Tue, 05 Jan 2016 22:21:36 -0800 (PST)
Return-Path: <[redacted]k@yahoo.com>
Received: from nm32-vm4.bullet.mail.gq1.yahoo.com (nm32-vm4.bullet.mail.gq1.yahoo.com. [98.136.216.227])
        by mx.google.com with ESMTPS id he9si23574433pac.102.2016.01.05.22.21.35
        for <[redacted]2@gmail.com>
        (version=TLS1 cipher=ECDHE-RSA-AES128-SHA bits=128/128);
        Tue, 05 Jan 2016 22:21:36 -0800 (PST)
Received-SPF: pass (google.com: domain of [redacted]k@yahoo.com designates 98.136.216.227 as permitted sender) client-ip=98.136.216.227;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of [redacted]k@yahoo.com designates 98.136.216.227 as permitted sender) smtp.mailfrom=[redacted]@yahoo.com;
       dkim=pass header.i=@yahoo.com;
       dmarc=pass (p=REJECT dis=NONE) header.from=yahoo.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1452061295; bh=lANC5M2uNNNTtp+qg/MDcmmvaqR9/R/OecA9AtAQgLE=
b=oZh8u4T1ztM844GSgMqorCKRlWMUHJEQ3te+n/wnUUh4W24E1/aaWr94OViDyP3GuKgmPnzaP8pmgNdaLFybC58BKMyfQn2SzYrhN1vNwu9QjX5UerBhEsy5n+TtWScHNbHkAZ3
WysL7z5Uy0q2WzrUcADweh3WQ2g9FkCq2moDw4l11R3fWd9Y/gMNFETzvw3gw6JNV/UBSAEiGKIw3yEBjw5Yzu1l86NX625SHDkEmTNbAWJwylI7P1sb4tBmDE9ng==
Received: from [127.0.0.1] by nm32.bullet.mail.gq1.yahoo.com with NNFMP; 06 Jan 2016 06:21:35 -0000
Received: from [216.39.60.183] by nm32.bullet.mail.gq1.yahoo.com with NNFMP; 06 Jan 2016 06:18:53 -0000
Received: from [98.137.12.192] by tm19.bullet.mail.gq1.yahoo.com with NNFMP; 06 Jan 2016 06:18:53 -0000
Received: from [127.0.0.1] by omp1000.mail.gq1.yahoo.com with NNFMP; 06 Jan 2016 06:18:53 -0000
X-Yahoo-Newman-Property: ymail-4
X-Yahoo-Newman-Id: 152053.34655.bm@omp1000.mail.gq1.yahoo.com
X-YMail-OSG: JXL9n3AVM1nE33s.2AgjOrSuQTnFWu30ZJnCCs74F_HWrlv9IK8h5a_m9FLTWVk
 w6tUgAXyh8p5hugFtql.i7trACsQ9gfftMYeFKgkXBSdc3bq5wbkWO.HXxOJb_91M33DSoCMcvBj
 Ah90Ilv9uvj.DFa_GidDDALChBv5lznrOGUNXumLKG0l68Br_is6Yp79Q9w7zRsJKjuoC5YB7ZA8
 lxhF..OKYz6suIA26trddXhSIrvz_eIdMF_akQQAGD0dyPo3dMDmpmtlokFgsPqal4DU49RtgLgf
 CBh6XwYSRLRDMFPvWIYyS7oEC4i8wLMxh3EhHsf1m9gbQNcxoR0BTMgj92so4VwqjyRtX8vePpcf
 oQonTgRwX6eEI9syJN3SaetOVye4Xb4rzDWieUHEfMipCVrNBAsXLnHIB92qrVlyUlC412Bw9MNe
 R2Jyb3aHADNhEs5FXtcbsLPU.gN9F7swYmaaLGGIGpBLaCo0CW4WKLgoyBJmqp51omfXdL3aBWiR
```

Fig.4.17: Sample E-mail Header

The e-mail headers will be displayed as above.

Information from the headers is everything which is required to analyze the e-mail.

From the above headers we can find out the time when the mail was received, and we can also ascertain whether the e-mail was legitimate or was spoofed. The line in the header under the parameter '**Received-SPF**' can help you identify if the mail was from legitimate e-mail id or was an act of spoofing. If the line says '*xxx@yahoo.com designates xx.xx.xx.xx as permitted sender*' that probably should mean that the e-mail was from legitimate e-mail id.

Additionally, the parameter 'client-ip' shown as '98.136.216.227' simply means that the e-mail was sent via the above IP address.We need to perform WHOIS lookup to get information about the above IP address.

Note: **WHOIS** is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an

Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information.

You can use any tool of sort for the same. Let us use the service from **www.who.is**

Fig.4.18: Searching an IP on Who.is

Enter the IP address found (in the e-mail header) and click on search.

The WHOIS Information will then be displayed:
The above information reveals that the IP address we searched for belongs to Yahoo! Inc. and the e-mail was a legitimate Yahoo! account and had probably been routed from legitimate Yahoo! servers.

In this case you need to send a notice to Yahoo! Inc, under 91 CrPC requesting for the IP logs of the target e-mail ID.

You get the IP logs from Yahoo, as follows:

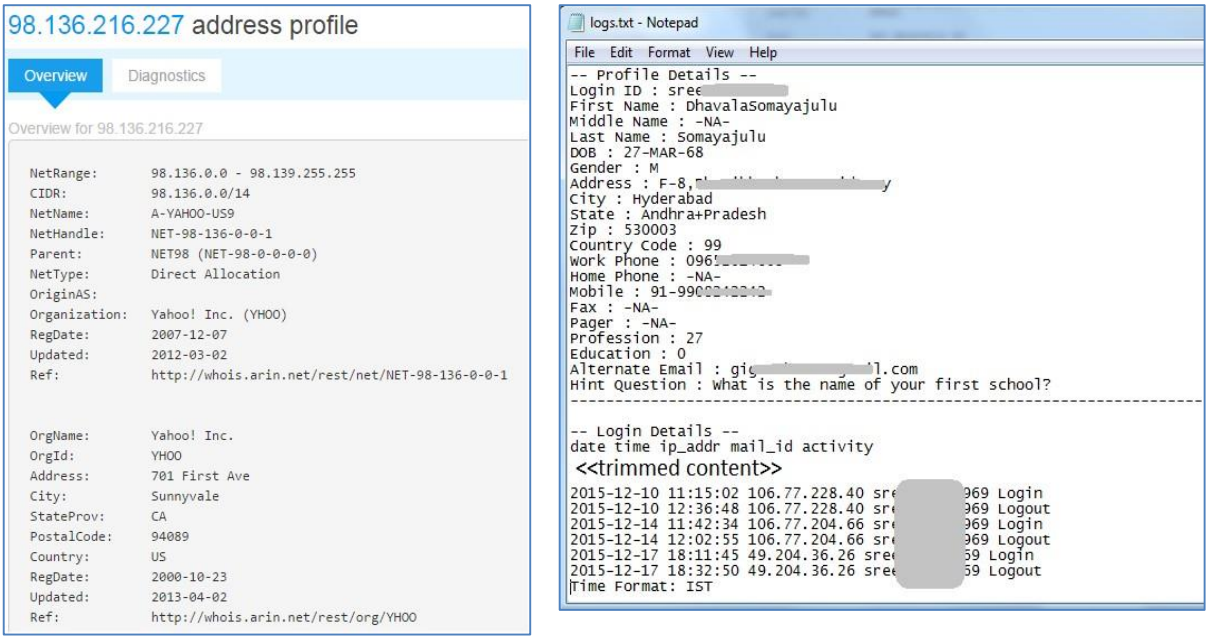


Fig.4.19: IP Log details from Yahoo

After getting the logs from Yahoo, check for the most recent IP activity, copy the IP address and make a WHOIS lookup.

In the above logs, we can see that the most recent activity was on 17-122015 around 18:00 hours and on the IP address 49.204.36.26.

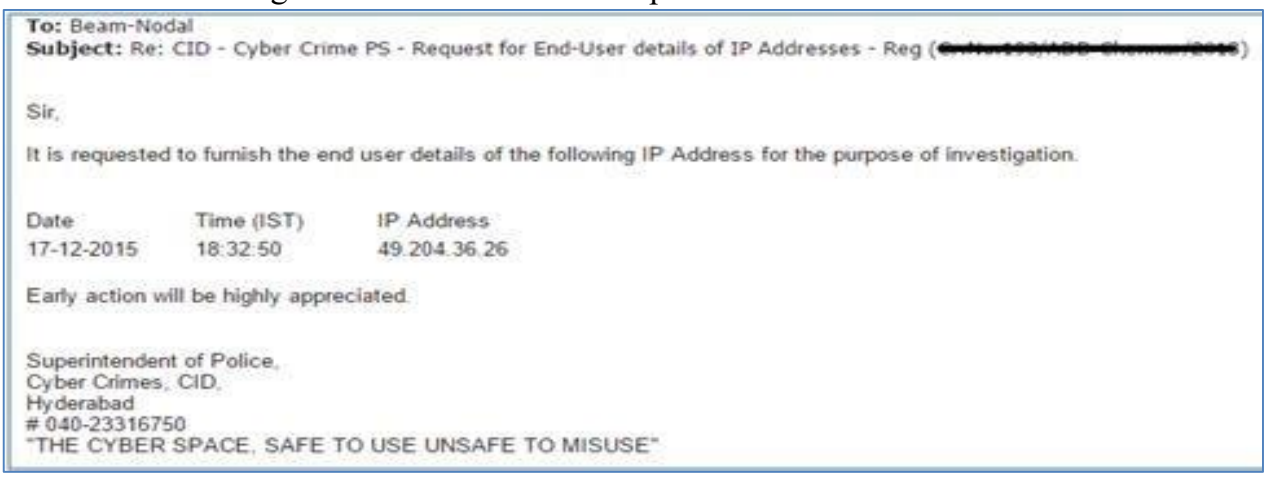
We need to check the ISP to which the above IP belongs. Perform a WHOIS lookup for that IP address.

Fig.4.20: Searching an IP in Who.is

You will be displayed with the relevant data, as follows:

Fig.4.21: IP Registration details from who.is

In the above picture we can see that the IP address belongs to Beam Telecom Pvt Ltd. We now need to send a notice to the Nodal officer of Beam Telecom requesting for the end user particulars of the IP address along with the correct timestamps.



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	49.204.36.26

Early action will be highly appreciated.

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

Fig.4.22: Sample request to ISP for IP details.

AJAY

[redacted]@beamtele.com
Right-click to interact with this contact.

[redacted]rime PS Hyderabad - Request for IP end user particulars (Cr.No.[redacted]) - Regarding.

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
[redacted]	49.204.36.26	74:44:01:99:86:0b	17-12-2015\12:56	17-12-2015\02:32	Mr. J SHIVA CHANDER
					[redacted]

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

Fig.4.23: Reply from ISP with details of customer

The Nodal officer of that ISP will reply back with end-user particulars.

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.

4.9 Grabbing Public IP of Suspect

a) URL Shortener

URL Shortener is a service provider that provides URL Shortening service. URL Shortening a procedure where a Uniform Resource Locator (URL) may be made substantially shorter in length and is will be still directed to the required page. This is done by making a redirect link on a domain that is short, which links to the webpage that has a long URL.

Step Action

Step 1: https://www.facebook.com/VINAYJAINISHERE is a long URL.

1.1 Go to https://goo.go/

1.2 Type or Paste the long URL

1.3 Click on "Shorten URL"

Fig.4.24: Google URL Shortner

Step 2: https://goo.gl/wfMdd1 is the Shortened URL using the "goo.gl" service.

2.1 New Shortened URL is generated. Use Ctrl + C to copy the URL generated

2.2 This URL can be send to be redirected to original URL

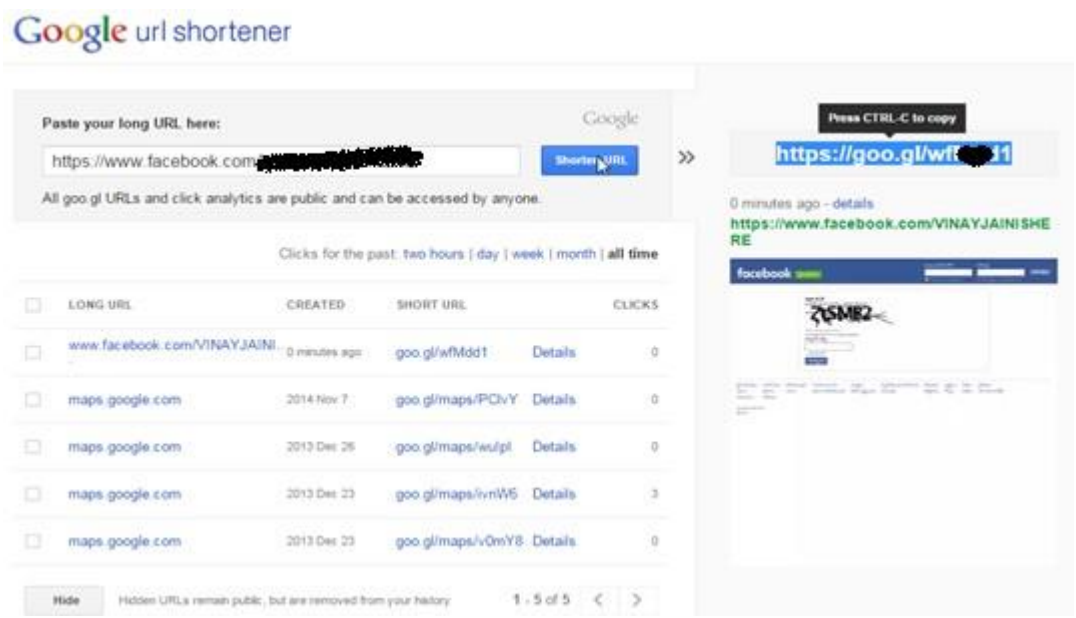


Fig.4.25: Shortened URL

Other Popular URL Shortener:

1. bit.ly (Bitly)
2. goo.gl (Google)
3. ow.ly (Hootsuite)
4. t.co (Twitter)
5. TinyURL (Gilby)
6. Tr.im (Gravity4)

Note: URL Shortener is used by LEA's or other bodies to make the redirection link small in size and to hide the IP logging URL hidden under the URL Shortener.

b) 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 a 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.

Popular IP Loggers that are in use **http://blasze.com/** and **http://iplogger.org/**

We will see how to create a tracking link using www.blasze.com

Step 1: Link to be redirected ->https://www.facebook.com/VINAYJAINISHERE

1.1 Go to http://blasze.com/ or http://blasze.tk/

1.2 Copy link to be redirected on the textbox. Click on "Submit"

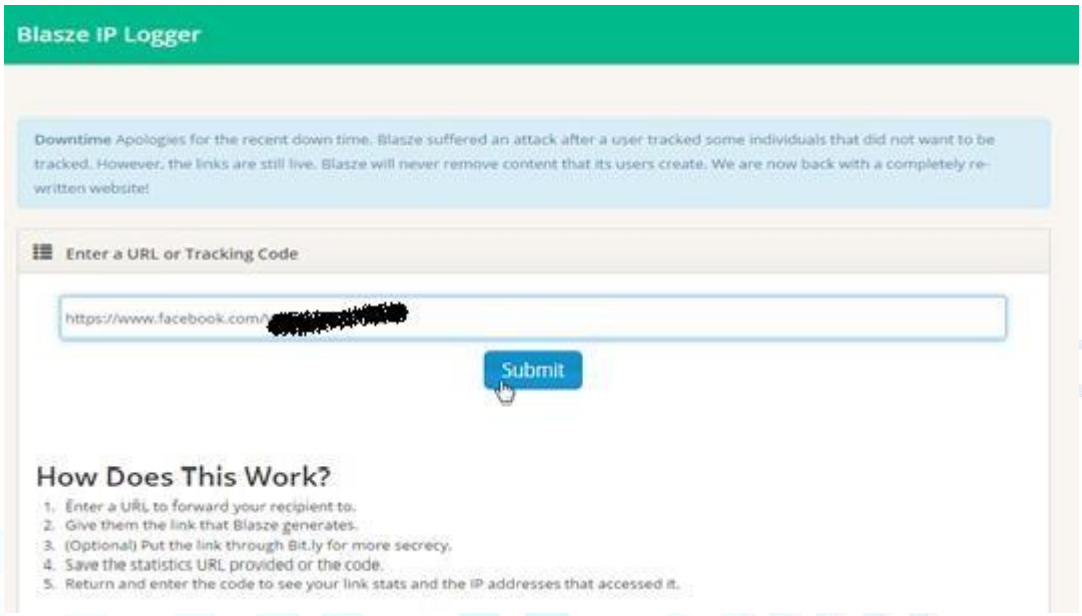


Fig.4.26: Blasze IP logger home page

Step 2: Tracking Link is: **http://blasze.tk/GML1N2** and Access Code is 3Y5RS1

2.1 Tracking Link generated is **http://blasze.tk/GML1N2**

2.2 Access Code is 3Y5RS1. This is required to get the Access Log for the generated tracking link

2.3 Tracking link needs to be shared with the suspect via Facebook of the friend's account or WhatsApp with luring message to make them click on the link given.

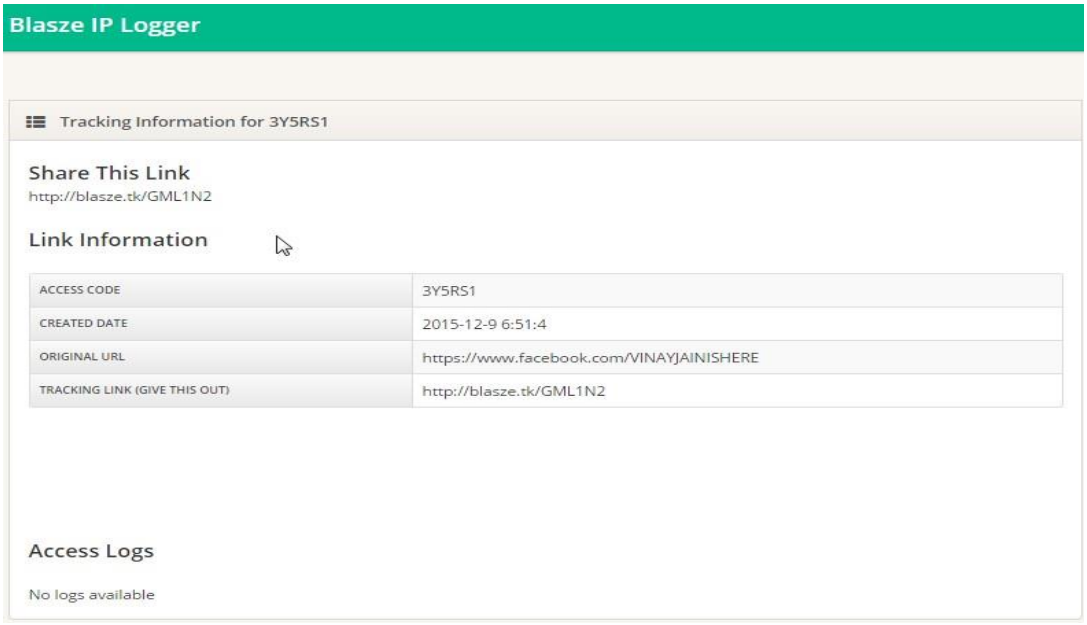


Fig.4.27: Tracking link created using Blasze

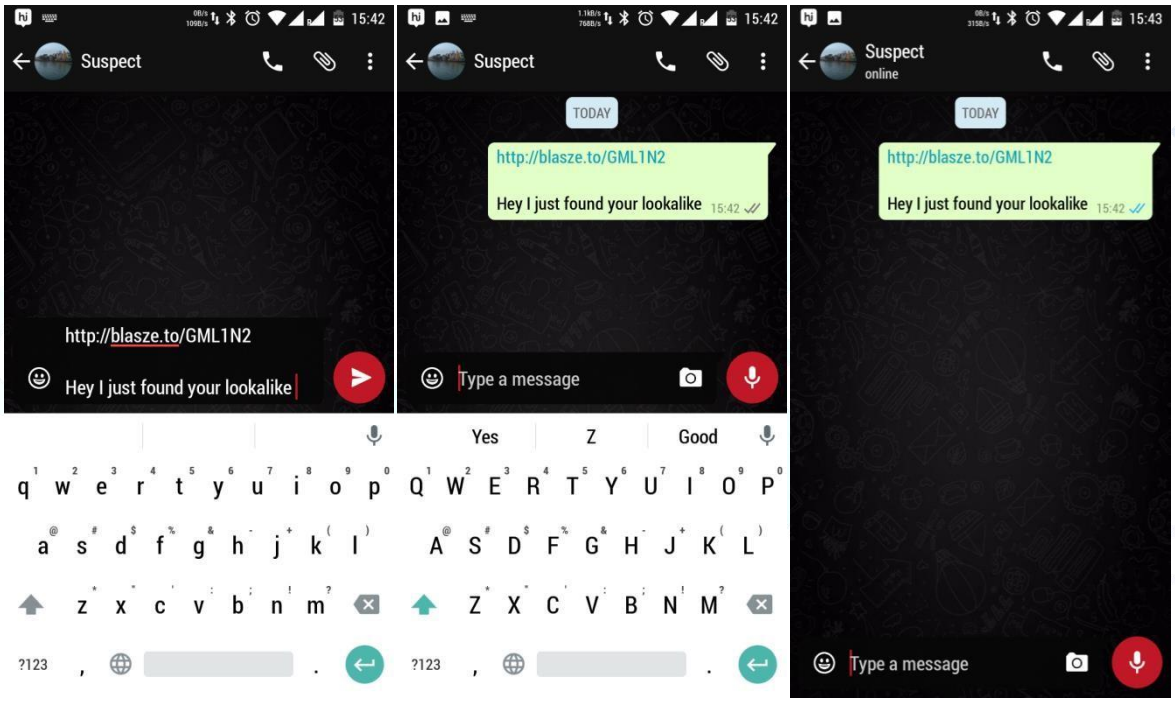
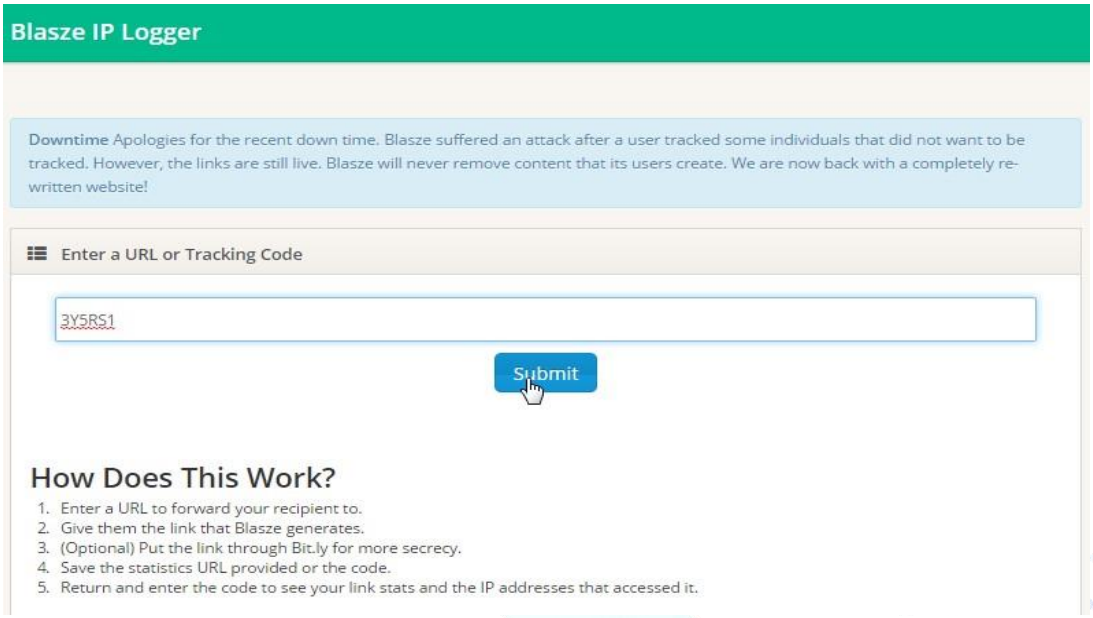


Fig.4.28: Sending Tracking Link through WhatsApp to suspect

generated

3.1 Go to http://blasze.tk /

3.2 Enter the Tracking Code 3Y5RS1. Click on Submit



Step 3: Using Access code 3Y5RS1 to get the Access Logs of the link

Fig.4.29: Entering Tracking code in Blasze

Step 4: Identifying the Public IP of the Suspect

4.1 In the Access Logs look for User Agents where browsers are used for access

4.2 Here you can identify the type of device that was used to access the link as well as the IP Address and timestamp when it was accessed 4.3 Further Link for reverse tracing the

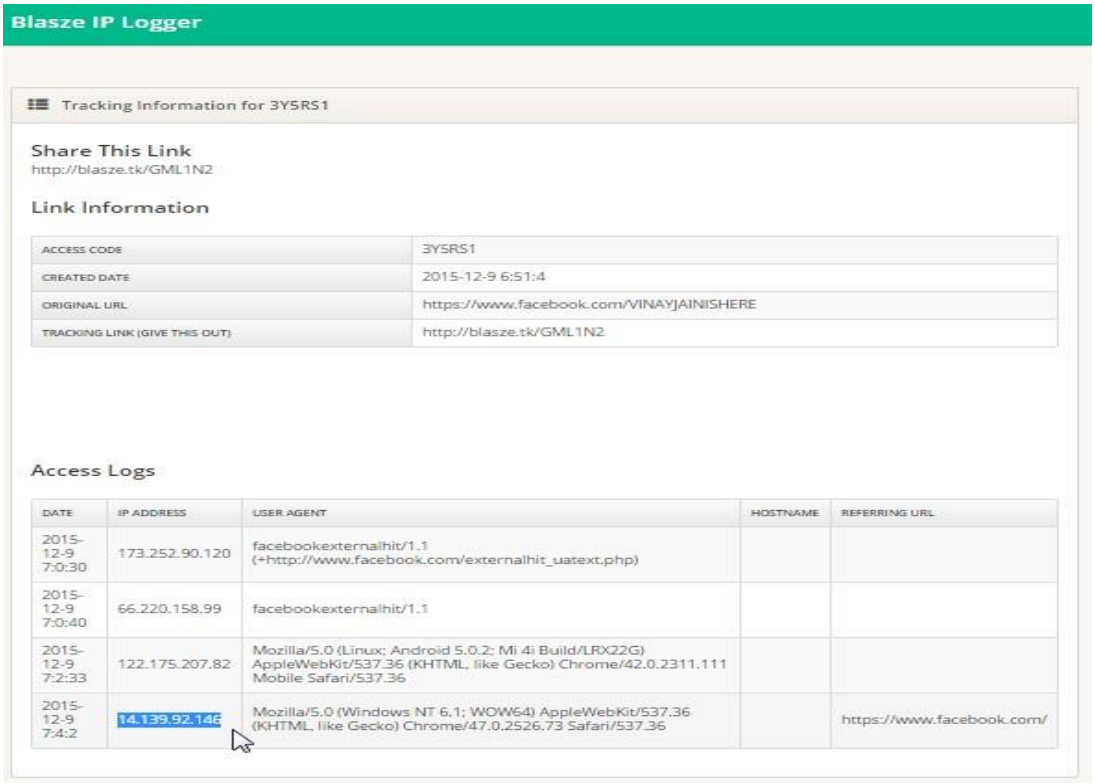


Fig.4.30: IP address of Suspect grabbed by Blasze

Note: Many a times the User Agent field helps identify the system detail of the suspect. Like in the last log the device used by the suspect is shown to be "**Micromax A300**".

For Better Function: Tracking link generated should be shortened using URL Shortener and only then it should be further used so as the Tracking activity can be masked.

4.10 Tracking of Domain Names using Whois Lookup

WHOIS Lookup

WHOIS (pronounced as the phrase *who is*) is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format. The WHOIS protocol is documented in RFC 3912.

The WHOIS service andWHOIS database are provided for information purposes only. It allows the public to check whether a specific domain name is still available or not and to obtain information related to the registration records of existing domain names.

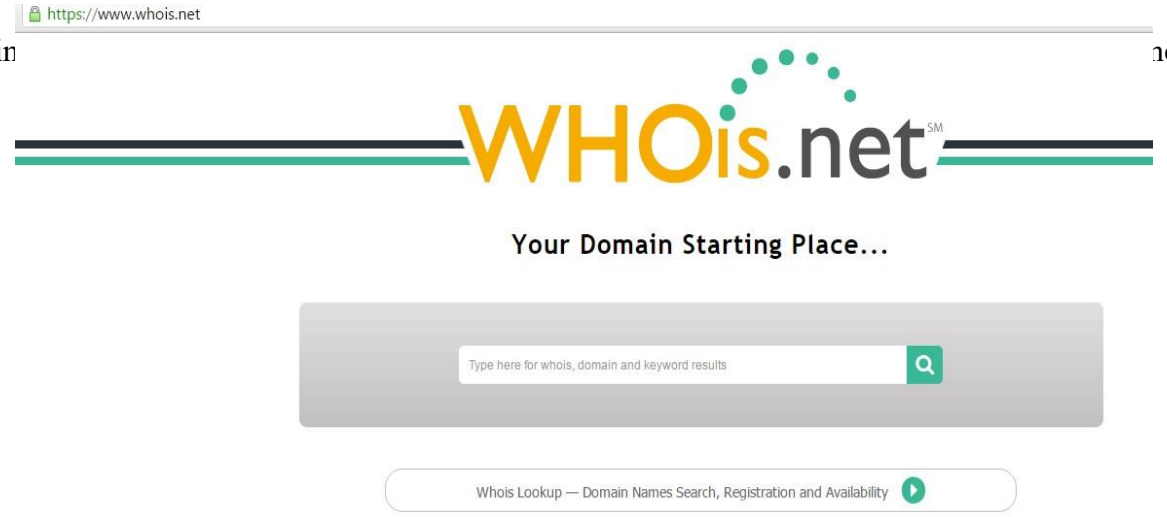


Fig.4.31: Whois.net home page

The Affirmation of commitments requires ICANN to "implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information…" The WHOIS service is a free, publicly available directory containing the contact and technical information of registered domain name holders (referred to as "registrants"). Anyone who needs to know who is behind a website domain name can make a request for that information via WHOIS. The data is collected and made available by registrars and registries under the terms of their agreements with ICANN.

WHOIS is not a single, centrally managed database. Rather, registration data is held in disparate locations and administered by multiple registries and registrars. They set their own conventions for WHOIS service, consistent with the minimum requirements established in their ICANN contacts.

The term "WHOIS" refers to protocols, services, and data types associated with Internet naming and numbering resources beyond domain names, such as Internet Protocol (IP) addresses, and Autonomous System Numbers (ASNs). The WHOIS service includes WHOIS clients, WHOIS servers, WHOIS data stores, and WHOIS data (domain name registration records). Essentially, WHOIS can refer to any of the following:

1. The information that is collected at the time of registration of a domain name or IP numbering resource and subsequently made available via the WHOIS Service, and potentially updated throughout the life of the resource;
2. The WHOIS Protocol itself, which is defined in RFC 3912; or
3. The WHOIS Services that provide public access to domain name registration information typically via applications that implement the WHOIS protocol or a web-based interface.

These ambiguities inherent in the WHOIS label complicate efforts to shape the evolution of meta-data for Internet naming and numbering. To address this, ICANN has developed more precise terminology for gTLDs, including:

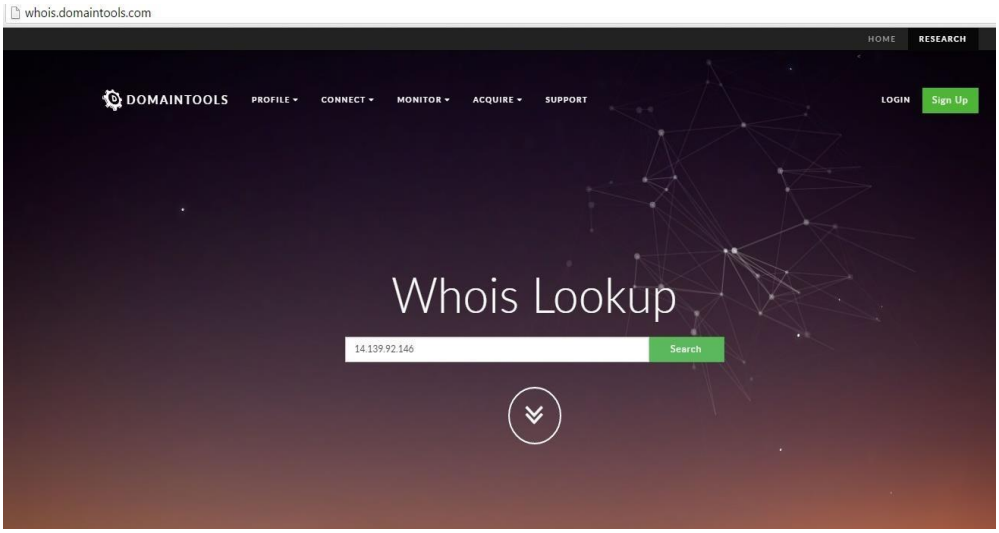
Uses of WHOIS

Internet operators use WHOIS to identify individuals or entities responsible for the operation of a network resource on the Internet. Over time, WHOIS has evolved to serve the need of many different stakeholders, such as registrants, law enforcement agents, intellectual property and trademark owners, businesses and individuals.

Stakeholders use the WHOIS service for a variety of purposes, including to:

- Determine whether a domain is available
- Contact network administrators regarding technical matters
- Diagnose registration difficulties
- Contact web administrators for resolution of technical matters associated with a domain name
- Obtain the real world identity, business location and contact information of an online merchant or business, or generally, any organization that has an online presence
- Associate a company, organization, or individual with a domain name, and to identify the party that is operating a web or other publicly accessible service using a domain name, for commercial or other purposes
- Contact a domain name registrant for the purpose of discussing and negotiating a secondary market transaction related to a registered domain name
- Notify a domain name registrant of the registrant's obligation to maintain accurate registration information
- Contact a domain name registrant on matters related to the protection and enforcement of intellectual property rights
- Establish or look into an identity in cyberspace, and as part of an incident response following an Internet or computer attack- (Security professionals and law enforcement agents use WHOIS to identify points of contact for a domain name)
- Gather investigative leads (i.e., to identify parties from whom additional information might be obtained)- Law enforcement agents use WHOIS to find email addresses and attempt to identify the location of an alleged perpetrator of a crime involving fraud
- Investigate spam- law enforcement agents look to the WHOIS database to collect information on the website advertised in the spam

Under the ICANN contracts, WHOIS can be used for any legal purpose except to enable mass unsolicited, commercial advertising or solicitations, or to enable high volume, automated, electronic processes that send queries or data to a registry or registrar's systems, except as necessary to manage domain names. We use whois lookup to identify the IP details.



IP Information for 14.139.92.142

IP Location	India Hyderabad SardarVallabhbhai Patel National Police Academy
ASN	AS55824 NKN-CORE-NW NKN Core Network, IN (registered Oct 19, 2010)
Whois Server	whois.apnic.net
IP Address	14.139.92.142

inetnum: 14.139.92.144 - 14.139.92.159 netname: NKN-SVPNPA-HYD
descr: Sardar Vallabhbhai Patel National Police Academy country: IN admin-c: NNA22-AP

Fig.4.32: Whois lookup Result of an IP

4.11 Anonymizing IP Address &Virtual Currency

Everything that is done on the Web is logged, analyzed, and used for some or other form of Intelligence gathering. To wither away from getting analyzed over internet and to obscure the identity, criminal anonymize their identity. To anonymize the internet based activities means hiding the identity or creating a fake account that doesn't contain personal information.

Following steps are some of the techniques used by criminals

LEVEL 1: Anonymous Web browsing

Hide Your IP Address- Easiest way to trace online activity. IP address easily determines the geographic location of the server and gives a rough idea about the location of the client using the connection. Also, the service provider can provide the user's activity trail. So, ways to obscure the IP Address, various services that we can use are:

1. **Use a Proxy Server:** Proxy server routes the connection through a different server so IP address of the machine isn't as easy to track as it would have been had they used a direct connection. There are thousands of proxy services mostly free, some with premium services but with a cost attached. Also most browsers support plug-ins/extensions that can provide proxy services.
2. **Use a Virtual Private Network (VPN):**a VPN is a private network that used a public address to access the internet and the activities done when connected to VPN is logged onto the VPN server not the ISP hence VPN acts as an ISP when connected to it. Hence any online service will detect the Public IP Address of the VPN instead of the client machine using the service.It gives a better level of anonymity than a proxy server would have.
3. **Use TOR.** Short form for **T**he **O**nion **R**outer. TOR is a network of virtual tunnels that allows people and groups to improve privacy and security on the Internet. The look and feel of browsing on TOR browser is somewhat same but with low broadband speed, it may feel very slow or stuck at times

LEVEL 2: Anonymous email and communication

There are core challenges in obscuring IP Addresses when sending emails. So for sending an email under privacy, risks can be mitigated by use of one of the below mentioned methods:

1. **Use an Alias:** An alias is essentially using an email forwarding address**.** When an email is send through an alias the recipient only gets the forwarding IP Address and not the real. Since all emails are forwarded on a timely basis, this prevents the privacy concern.
2. **Use a Disposable Email Account:** This can be done in either of two ways to make a disposable account with fake credentials or using services like 7 minutes mail box.

Also VPN can be used for the same.To avoid any of the above mentioned methods, we must encrypt our emails before we send them:

- **Use HTTPS in Web-based email client**. This adds SSL/TLS encryption to all the Web-based communications. It's not bulletproof,

but it definitely helps. Just make sure the URL of your webmail has an S (for Secure) after the HTTP. Gmail users, for example could use https://mail.google.com. It is also recommend using the HTTPS Everywhere extension.

- **Use PGP (Pretty Good Privacy) software**. While using HTTPS will encrypt your data on a network level, PGP software will encrypt the actual files themselves. It's a bit more complicated than other methods.

In addition to email, two chat clients mentioned below also ensure privacy to large extent:

- **TOR chat**: a lightweight and easy-to-use chat client that uses TOR's location hiding services. It uses SSL/TLS encryption.
- **Cryptocat**: a Web-based chat client that uses the AES-256 encryption standard, which is extremely hard to break. It also supports group chats, so it's perfect for chatting on a closed circuit of partners

LEVEL 3: Anonymous file transfer and sharing

Getting files from the Internet is easy, but the sender has access to your IP address when you download files. In the case of BitTorrent, there are thousands of different peers that can see IP address at any given moment. However, if done correctly, it is possible to download and share files while keeping our IP address and identity concealed.

- When downloading directly form a file hosting site like MediaFire or Mega, one can just use a proxy or VPN to obscure your IP.
- When using BitTorrent to download stuff, using a proxy or VPN will keep your identity hidden, but rather than just using any old service, we recommend using BT Guard. At its core, BT Guard is exactly the same as any other VPN or proxy service

4.12 The Basics of Onion Routing

One way to understand onion routing is to start with the concept of proxy servers. A proxy server is a server that relays your connection through that server, which basically adds a step in the path of your data packets. If someone traced your IP address, they'd see it as the proxy server's IP address instead of your home address.

But proxy servers aren't exactly anonymous. They keep logs of all the traffic that passes through, which means that they can actually point back to you if necessary. For most activities, the proxy server is fine even though it'll add a bit of latency to your connection. Your anonymity would not be entirely protected, however, if your proxy service was hit with a subpoena for your IP information.

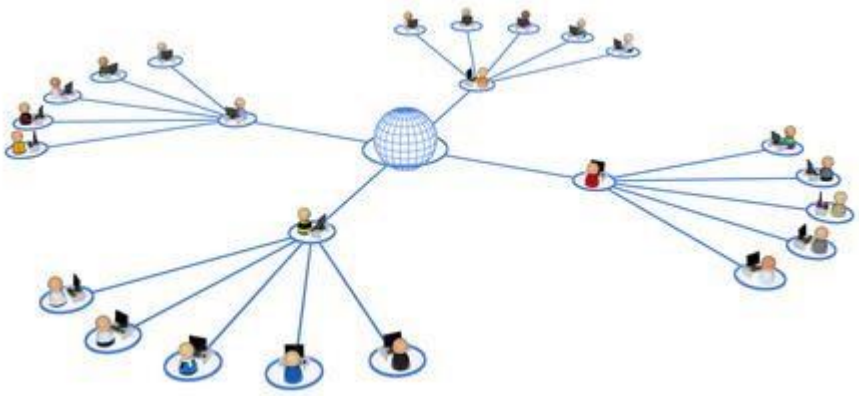


Fig.4.33: Using Proxy Server to access Internet

Onion routing is like an advanced form of proxy routing. Instead of routing through a single unprotected server, it uses a network of nodes that constantly encrypt your data packets at every step. Only at the end of this "chain" of onion nodes does your data become decrypted and sent to the final destination. In fact, only this "exit node" has the power to decrypt your message, so no other node can even see what you're sending.

Due to the multiple layers of encryption, which not-so-coincidentally resemble the layers within an onion, it's extremely difficult to trace your information back to you as the source when you use onion routing.

A Simple Example

Have you ever heard of Tor? It's a secure network that uses onion routing to keep all of your activity as encrypted and hidden as possible. Did you know that Tor actually stands for "the onion router"? If that name sounded weird to you before, now you know why it's called what it is.

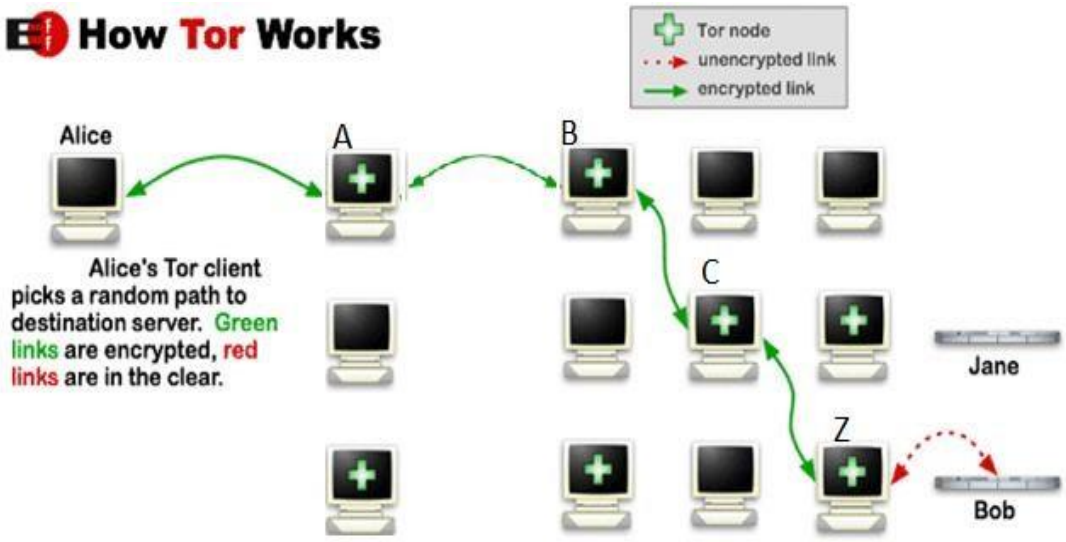


Fig.4.34: Working of TOR

Anyway, here's an example using Tor to help you visualize the process of onion routing a little better.

- Your computer has an onion routing client installed, which in this case is Tor. This client encrypts all data packets sent from your computer (Alice).
- Your computer sends a data packet to Node A.
- Node A encrypts your already-encrypted data packet and sends it to Node B.
- Node B encrypts your already-encrypted data packet and sends it to Node C.
- This cycle continues until the data packet reaches Node Z, which is the "exit node."
- Node Z decrypts all of the layers of encryption on your data packet and finally sends it off to the destination (Bob). Destination thinks your data packet originated from Node Z, not you.
- When data is sent back to you, the chain is reversed with Node Z becoming the first node and your computer being the exit node.

As you can see, the multiple layers of encryption make it really hard to break into your data packets. It's like a vault within a vault within a vault – even if you break into one, you still have to break into all of the rest.

4.15 Virtual Currencies

Virtual currencies have been around almost as long as the Internet and in the last few years they have evolved rapidly towards a product that is independent of normal currencies. With that rapid evolution has come many questions—legal,

practical, technological and otherwise—about the promise and potential of virtual currencies. Now we would provide the basics of virtual currency.

4.15.1 What are virtual currencies?

Virtual currencies (also called **crypto-currencies, virtual money**, or **digital cash**), are essentially unique, typically encrypted, computer files that can be converted to or from a government-backed currency to purchase goods and services from merchants that accept virtual currencies. You can buy these virtual currencies online using a **virtual "wallet"** on your PC or smartphone and, in some states, at kiosks and stores. Virtual currency is accepted as currency by some businesses, exchanged for cash by others, and even purchased as an investment.

4.15.2 What are the risks involved with using and investing in virtual currencies?

Exchanging Virtual Currencies

Virtual currency transactions are considered high-risk due to the vulnerability to cyber-attacks—of which there have been many. In March 2014, "Mt.Gox," the largest and best-known exchanges announced that Bitcoins (a prominent virtual currency) worth $409 million had been hacked and stolen. Mt.Gox abruptly declared bankruptcy, leaving more than one million people around the world unable to recover their funds. Virtual currency exchanges are unregulated, meaning there is little recourse to recover lost funds and, unlike deposits in insured banks and insured credit unions, there is no deposit insurance.

Types of Virtual Currencies

a) Bitcoin

Bitcoin introduced a decentralized currency system based on a peerto-peer network where currency is not issued per se; instead it is mined with advanced computers by cracking difficult math-based equations. Bitcoin can be called the trendsetter, as its success has spurred the launch of many other virtual currencies (there are more than 150 cryptocurrencies). The currencies inspired by Bitcoin are collectively called altcoins and have tried to present themselves as improvised and modified versions of Bitcoin. These currencies are easier to mine, but involve greater risk in terms of lesser liquidity, acceptance and value retention. Here are five digital currencies picked from the IOT.

b) Litecoin

Litecoin, the second largest cryptocurrency in the world was launched in the year 2011. It was created by Charlie Lee, a MIT graduate and former

Google engineer and can be described as the second-incommand to Bitcoin. Litecoin is based on an open source global payment network that is not controlled by any central authority and uses "scrypt" as a proof of work, which can be decoded with the help of CPUs of consumer grade. Litecoinhas a faster block generation rate and well as more rewards per block as compared to Bitcoins.

c) Darkcoin

Darkcoin is a more secretive version of Bitcoin. Though Bitcoins are anonymous when compared to traditional money, there is still a record of all transactions ever carried out in a ledger “blockchain” which can reveal a lot of information. Darkcoin offers more anonymity as it works on a decentralized mastercode network that makes transactions almost untraceably. Launched in January 2014, Darkcoin has an increasing fan following in a short span of time. This cryptocurrency was created and developed by Evan Duffield and can be mined using a CPU or GPU.

d) Peercoin

Peercoin, also referred to as PPCoin, Peer-to-Peer Coin and P2P Coin, was created by software developers Sunny King (a pseudonym) and Scott Nadal. It was launched in August 2012 and was the first digital currency to use a combination of proof-of-stake and proof-of-work. The coins are initially mined through the commonly-used proof-of-work hashing process but as the hashing difficulty increases over time, users are rewarded with coins by the proof-of-stake algorithm, which requires minimal energy for generating blocks. This means that over time, the network of Peercoin will consume less energy. Peercoin is an inflationary currency since there is no fixed upper limit on the number of coins.

e) Dogecoin

Dogecoin is another currency from the family of cryptocurrencies that recently turned a year old (launched in December 2013). Dogecoin, which has a ShibuInus (a bread of a Japanese dog) as its logo, was created by Billy Markus and Jackson Palmer. Dogecoin presents itself broadly based on the Bitcoin protocol, but with modifications. It uses scrypt technology as a proof-of-work scheme. It has a block time of 60 seconds (1 minute) and the difficulty retarget time is four hours. There is no limit to how many Dogecoin can be produced i.e. the supply of coins would remain uncapped. Dogecoin deals with large numbers of coin that are lesser in value individually, making the currency more accessible with a low entry barrier and fit for carrying out smaller transactions.

f) Primecoin

Primecoin is an altcoin with a difference. Developed by Sunny King (who also developed Peercoin), its proof-of-work is based on prime numbers, which is different from the usual system of hashcash used by most cryptocurrencies based on the Bitcoin framework. It involves finding special long chains of prime numbers (known as Cunningham chains and bi-twin chains) and offers greater security and mining ease to the network. These chains of prime numbers are believed to be of great interest in mathematical research.

5. Communication Device Based Investigation

A communication device is a hardware-based equipment that can be used to send and receive information in the form of analogue or digital signals. These devices can either be wired or wireless and nowadays very portable (that is handheld or wearable). Typical examples of communication devices are Smartwatches, Mobile Phone, Satellite Phone, GPS etc. These devices today are compact forms of computers with high performance, huge storage, and enhanced functionalities. They are the most personal electronic device a user accesses. These devices can be used for a range of tasks such as they are used to perform simple communication tasks like calling and texting, providing support for Internet browsing, e-mail, taking photos and videos, creating and storing documents, identifying locations with GPS services, and managing business tasks.

As new features and applications are incorporated into these devices, the amount of information stored on the devices is continuously growing. As a result, these devices have become portable data carriers, and they keep track of all your moves. Mobile phones are the most used amongst these devices and with the increasing prevalence of mobile phones in peoples' daily lives and in crime, data acquired from mobile phones has become an invaluable source of evidence for investigations relating to criminal, civil, and even high-profile cases. It is rare to conduct a digital forensic investigation that does not include a phone. For example, Mobile device call logs and GPS data were used to help solve the attempted bombing in Times Square, New York, in 2010.

The science behind recovering digital evidence from digital communication devices is called as **digital forensics**. Whereas digital evidence is defined as the information and the data that is stored on, received, or transmitted by an electronic device that is used for investigations. Digital evidence encompasses any and all digital data that can be used as evidence in a case. **Digital forensics** is a branch of forensic science which focuses on the recovery and investigation of raw data residing in electronic or digital devices.

5.1 Mobile Interception & Authorization

Mobile devices use different technology and different hardware equipment for the purpose of their use. For example, they might use different technology in communicating that is CDMA or GSM or may have different hardware components according to the handset model or the manufacturing company, for example, Apple may use the different patented features to that of Samsung. As a result, there have to be few different specifications on interception related to the nature of the Mobile technology used in the question. Telecommunication Engineering Centre (TEC) is the body of Department of Telecommunication of Government of India (DoT) which formulates the standards and specifications of various products as well as interfaces which will interface with the Indian Telecom Networks.

Lawful interception is a legal requirement of any state irrespective of the technology. As a legally sanctioned official access to private communications, Lawful Interception is a security process in which a service provider or a network operator collects and provides the law enforcement officials with intercepted communications of private individuals or any organizations. In India, the lawful interception is carried out in accordance with Section 5(2) of the Indian Telegraph Act read with Rule 419(A) of the IT Rules.

5.2 Indian Telegraph Act 1885

Section 5: Power for Government to take possession of licensed telegraphs and to order interception of messages

(1) On any public emergency, or in the interest of the public safety, the Central Government or a State Government may, take temporary possession (for so long as the public emergency exists, or the interest of the public safety requires the taking of such action) of any telegraph established, maintained or worked by any person licensed under this Act.

(2) On any public emergency, or in the interest of the public safety, if it is necessary or expedient so to do in the interests of the:

– sovereignty and integrity of India,
– the security of the State,
– friendly relations with foreign States or
– public order or
– for preventing incitement to the commission of an offence,

the Central Government or a State Government by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order.

Rule 419 A of Indian Telegraph Rules

Salient Features:

(1) Directions for interception of any message or class of messages under subsection

(2) of Section 5 of the Indian Telegraph Act, 1885 shall not be issued except by an order made by the -

- Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India and
- Secretary to the State Government in-charge of the Home Department in the case of a State Government.
- In unavoidable circumstances, such order may be made by an officer, not below the rank of a Joint Secretary to the Government of India, who has been duly authorized by the Union Home Secretary or the State Home Secretary, as the case may be.

Provided that in emergent cases

— for operational reasons or in remote areas where obtaining of prior directions for interception of message or class of messages is not feasible;

prior approval of the Head or the second senior-most officer of the authorized security i.e. Law Enforcement Agency at the Central Level and the officers authorised in this behalf, not below the rank of Inspector General of Police at the state level

BUT the concerned competent authority shall be informed of such interceptions by the approving authority within three working days and that such interceptions shall be got confirmed by the concerned competent authority within a period of seven working days.

If the confirmation from the competent authority is not received within the stipulated seven days, such interception shall cease.

(3) While issuing directions under sub-rule (1) the officer shall consider the possibility of acquiring the necessary information by other means and interception orders shall be issued only when it is not possible to acquire the information by any other reasonable means.

(4) The interception directed shall be the interception of any message or class of messages as are sent to or from any person or class of persons or relating to any particular subject whether such message or class of messages are received with one or more addresses, specified in the order, being an address or addresses likely to be used for the transmission of communications from or to one particular person specified or described in the order or one particular set of premises specified or described in the order.

(6) The directions for interception shall remain in force unless revoked earlier, for a period not exceeding sixty days from the date of issue and may be renewed but the same shall not remain in force beyond a total period of one hundred and eighty days.

(-) All the requisitioning security agencies shall designate one or more nodal officers, not below the rank of SP or Addl. SP or the officer of the equivalent rank to authenticate and send the requisitions for an interception to the designated officers of the concerned service providers to be delivered by an officer, not below the rank of Sub-inspector of Police.

(-) The service providers shall designate two senior executives of the company in every licensed service area/ State/ Union Territory as the nodal officers to receive and handle such requisitions for an interception.

(-) Designated nodal officers of the service providers shall forward in every fifteen days a list of interception authorizations received by them for confirmation of the authenticity of such authorizations.

(-) Review Committee constituted by The Central Government/ the State Government Review Committee constituted by the Central Government shall consist of the following, namely:

(a) Cabinet Secretary — Chairman
(b) Secretary to the Government of India, In-charge, Legal Affairs — Member
(c) Secretary to the Government of India, Department of Telecommunications — Member

Review Committee constituted by the State Government shall consist of the following, namely:

(a) Chief Secretary — Chairman
(b) Secretary Law/Legal Remembrance In-charge, Legal Affairs — Member
(c) Secretary to the State Government (other than the Home Secretary) — Member

(-) The Review Committee shall meet at least once in two months and record its findings whether the directions issued under sub-rule (1) are in accordance with the provisions of sub-section (2) of Section 5 of the said Act.

(-) Records pertaining to such directions for interception and of intercepted messages shall be destroyed by the relevant competent authority and the authorized security and Law Enforcement Agencies every six months unless these are, or likely to be, required for functional requirements.

5.3 Procurement and review of lawful interception order under Rule 419A:

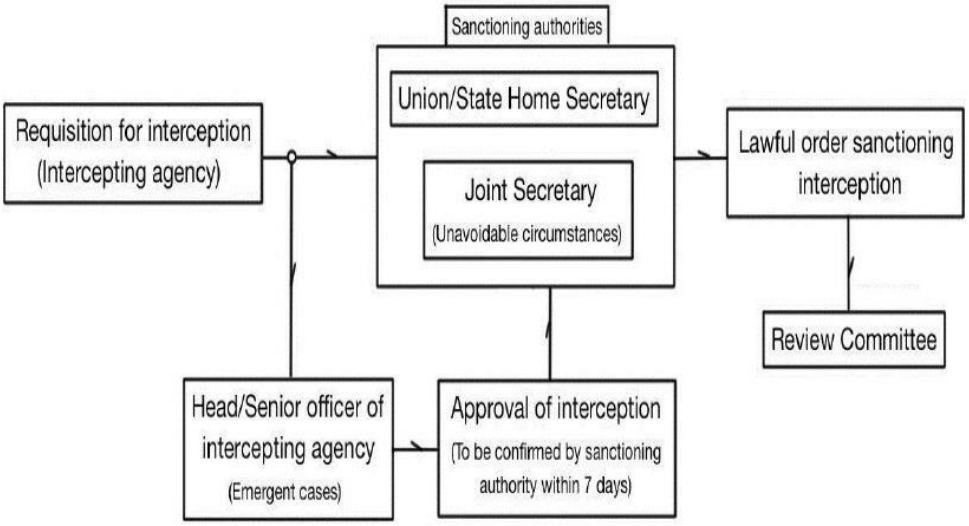


Fig.5.1: Lawful Interception Procedure

i. Intelligence Bureau,
ii. Narcotics Control Bureau,
iii. Directorate of Enforcement,
iv. Central Board of Direct Taxes,
v. Directorate of Revenue Intelligence,
vi. Central Bureau of Investigation,
vii. National Investigation Agency,
viii. Research & Analysis Wing (R&AW),
ix. Directorate of Signal Intelligence, Ministry of Defence- for Jammu & Kashmir, North East & Assam Service Areas only

 State Agencies:

i. Director General of Police, of concerned state
ii. Commissioner of Police, Delhi for Delhi Metro City Service Area only.

Call data records (CDRs) can be sought under the statutory provisions contained in Section 92 of the Code of Criminal Procedure, 1973 or Section 5(2) of the Indian Telegraph Act, 1885 read with Rule 419 A of Indian Telegraph (Amendment) Rules, 2007.

5.4 Legal Interception of Communications by Law Enforcement Agencies

Indian laws do not allow disclosure of information pertaining to authorised interception and communications data. Section 5 (2) of the Indian Telegraph Act 1885 – read with rule 419 (A) of Indian Telegraph (Amendment) Rules 2007 obliges telecommunications service providers to maintain extreme secrecy in matters concerning lawful interception. Under Rule 25(4) of the IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 (Interception Rules) and Rule

11 of the IT (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 (the 'Traffic Data Rules'),
'strict confidentiality shall be maintained' in respect of directions for lawful interception, monitoring, decryption or collection of data traffic.

5.5 Central Monitoring System (CMS)

Centralized access to the country's telecommunications network. Prior to the CMS, all service providers in India are required to have Lawful Interception Systems installed at their premises in order to carry out targeted surveillance of individuals by monitoring communications running through their networks. After CMS, all Telecom Service Provider's (TSP's) in India are required to integrate Interception Store & Forward (ISF) servers with their pre-existing Lawful Interception Systems.

These ISF servers are then connected to the Regional Monitoring Centres (RMC) of the CMS. Each Regional Monitoring Centre (RMC) in India is connected to the CMS. CMS involves the collection and storage of data intercepted by TSPs in central and regional databases. All data intercepted by TSPs is automatically transmitted to RMC, and subsequently automatically transmitted to the CMS.
Thus, CMS authority can have centralized access to all data intercepted by TSPs all over India, but that the authority can also bypass service providers in gaining such access. Unlike in the case of so-called "lawful interception" where the nodal officers of TSPs are notified about interception requests, CMS allows for data to be automatically transmitted to its data centre, without the involvement of TSP's.

Evolution of Interception Mechanism

• Tape Interception Recorders- TIR

Fig.5.2: Tape Interception Recorders

• Digital Voice Recorders

Fig.5.3:Digital Voice Recorders

• Mobile Phones Diversion
• Voice loggers- SIM-based/ Landline based

Fig.5.4:Voice loggers

• Switch-Based Monitoring System (SBMS)-

By using TIR's, Digital Voice Recorders, Diversion's and Voice loggers it was possible to intercept call content (Active call). For call related information LEA's had to rely on CDR's. However, with the use of SBMS, it is possible to intercept both call content as well as call related information such as location, missed calls, SMS, internet traffic etc. This way real-time monitoring of the calls, unified view for voice, fax, SMS, GPRS and any other internet (EDGE/UMTS/LTE) sessions is possible. SBMS is highly secured and provides multi-level passwords and secures the network while using so. SBMS can be used for GSM, CDMA, PSTN and ILD networks.

It can be used to identify targets based on Telephone Number, MSISDN, IMEI and IMSI. This way SBMS can be used to intercept calls interception of data, analysis of data, interpretation of data, this information can be then used to zero down the suspect's behaviour and movement that is whether static or moving.

Evidence that can be obtained from a Mobile Phone:

- Evidence inside of SIM - Contacts, SMS and Location.
- Evidence in Mobile Equipment – Contacts, SMS, Call History, Images, Videos and any other user files.
- Evidence in the network – Call Logs, SMS logs, location, GPRS, tower dump, subscribers name and address.

5.6 Call Detail Record

As discussed earlier Mobile phones today are very commonly used and are due to the usage they are almost treated as a unique identification of their user. Mobile phone users now use them for various purposes such as calls, messages, social media along with this they are also used by many for their banking and e-wallets, they are also used for entertainment and gaming purposes. Due to the usage of mobile phones in the society for a wide range of applications, certain antisocial elements use this as a tool to perform antisocial activities or crimes.

Fortunately, all Telecommunication Service Providers maintain a log of any activity done using a mobile phone. One of these logs is called as Call Detail record (CDR), it is mandatory for all the service providers to provide a CDR whenever requested by an investigation officer from any Law enforcement agencies within the country. CDR comes very handily in investigating methods of crimes including some of the most sophisticated one as well. CDR provides a great deal of information about the telephonic behaviour of the SIM card holder which helps the police investigating the crime in a systematic fashion.

With the help of a CDR following information can be obtained:

- The phone number of the subscriber originating the call (Caller/sender)
- The phone number receiving the call (Receiver)
- Date and time
- The call duration
- Call type (voice, SMS, etc.)
- Other details (call drop reasons, QoS etc.)
- Billing information
- Roaming details
- Cell location (at the start of the call)
- Cell location (at the end of the call)
- International Mobile Equipment Identity (IMEI)
- International Mobile Subscriber Identity (IMSI)

With the above information, it is easier to track the activity of a criminal/suspect and to find out any accomplices in the real time.

Current Telecom Providers in India:

Fig.5.6: Mobile Service Providers in India

Airtel - http://www.airtel.in/applications/xm/FixedLineNodalOfficer.jsp

Aircel - http://www.aircel.com/AircelWar/appmanager/aircel/ap?_nfpb=true&_pageLabel=P44001200312651712160 76

BSNL - http://www.bsnl.co.in/opencms/bsnl/BSNL/about_us/consumer_griev.html

Idea - http://www.ideacellular.com/customer-care/regulatory/cellular-appellateauthority

Jio - http://www.jio.com/en-in/contact-us#horizontalTab1

MTNL - http://www.mtnl.net.in/contact.html

Reliance Communications - http://www.rcom.co.in/Rcom/personal/customercare/appellate-authority.html

Tata docomo – https://www.tatadocomo.com/en-in/nodal-appellate

Tata Indicom - https://www.tataindicom.com/en-in/nodal-appellate

Telenor - https://www.telenor.in/lite/maharashtra-&-goa/p/contact-us

Vodafone - https://www.vodafone.in/help-support/

For any other service providers - http://www.trai.gov.in/consumer-info/list-of-appellateofficer

5.7 Guidelines for Requesting CDRs

- On identification of suspect mobile number the investigating officer has to identify the Service Provider Service Provider “of that number". The best way to find the service provider of a particular number is by maintaining SDR (Subscriber Data Record) of TSP (Telecomm service providers) across India. The State should maintain an updated record of all SDR. Once the identification of service provider is done, a request letter is given to the MSP through the concerned officer. Follow all rules and regulations prescribed by authority from time to time.
- Every request for CDRs will be approved by the officer concerned in writing.
- A register will be maintained to keep the time of getting the request, when it was forwarded to the service provider and when the CDR was received.
- Joint or Special commissioner (special cell) will authorise a few officers in every police unit, who can send requests to service providers for call details of a mobile number from their official emails.
- No SMS, telephone call or fax request will be entertained unless an original copy of request signed by the competent authority is produced by the telecom operator. If the request is made through official email ID of the competent authority, a physical copy needs to be produced before the nodal authority of Telecom Company within 48 hours.

NOTE: It is necessary to understand various types of services provided by the service provider before asking them for the logs of various services. Different service providers use different formats to provide their CDR's.

5.8 Different types of CDR:

a) Normal CDR:

It is a detailed record of calls & SMS that are sent and received. The general format of 13 field CDR required from Telecom Service Provider is as shown in Figure 2.78. It is most commonly requested for investigation purposes. However, the format of CDR varies for various service providers. In the request for CDR, the date, time and duration for which CDR is requested has to be mentioned.

CALL DETAILS FOR THE MOBILE NUMBER:XXXXXXXXXX FOR PERIOD :DD/MM/YY TO DD/MM/YY												
CALLING A PARTY TELEPHONE NUMBER	CALLED B PARTY TELEPHONE NUMBER	CALL DATE	CALL TIME	CALL DURATION IN SEC	FIRST CELL ID OF PARTY A	LAST CELL ID OF PARTY A	CALL TYPE	IMEI OF A	IMSI OF A	TYPE OF CONNECTION	SMS CENTER NUMBER	FIRST ROAMING NETWORK CIRCLE OF A
1	2	3	4	5	6	7	8	9	10	11	12	13

Fig.5.7: Format of 13 field column CDR

However, in many cases, the MSP's provide CDR's which are not normalized and are as shown below.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Strictly Confidential													
2	Report Run Date :31-03-2017 12:15:10													
3	IDEA Cellular Limited - Andhra Pradesh													
4	K.L.K.Estate, Fateh Maidan Road,													
5	Hydrabad - 500001. Andhra Pradesh. India.													
6	Call details for MSISDN : +918464923771													
7	Category : Post-Paid													
8	IMSI : 404070545876095													
9	From Date 01-02-2017 00:00:00 To Date 31-03-2017 12:15:06													
10	Calling Party	Called Number	Date	Time	Duration	First Cell I	Last Cell ID	Call Type	IMEI	IMSI	Type of Connection	SMSC Number	Roaming Network	2G/3G Call Access Type
11	918464923771	'058595	18/03/2017	21:30:16	0	40407-64-	N/A	SMO	'91122025	####	PP	919848001104	N/A	2G
12	918464923771	'IA-IDEA	19/03/2017	14:56:29	0	405852-11	N/A	SMT	'91122025	####	PP	919844047138	Idea Tamilnadu &	2G
13	918464923771	'IA-IDEA	19/03/2017	14:56:33	0	405852-11	N/A	SMT	'91122025	####	PP	919844047138	Idea Tamilnadu &	2G
14	918464923771	'IA-IDEA	19/03/2017	14:56:36	0	405852-11	N/A	SMT	'91122025	####	PP	919844047138	Idea Tamilnadu &	2G
15	918464923771	'IA-IDEA	19/03/2017	01:55:32	0	405852-11	N/A	SMT	'91122025	####	PP	919844047138	Idea Tamilnadu &	2G
16	918464923771	'IA-IDEA	19/03/2017	01:55:44	0	405852-11	N/A	SMT	'91122025	####	PP	919844047138	Idea Tamilnadu &	2G
17	918464923771	'IA-50325	20/03/2017	18:13:27	0	405852-25	N/A	SMT	'91122025	####	PP	919844198441	Idea Tamilnadu &	2G
18	918464923771	'TD-FACEBK	20/03/2017	18:34:59	0	405852-25	N/A	SMT	'91122025	####	PP	919032355002	Idea Tamilnadu &	2G
19	918464923771	'IX-IDEA	20/03/2017	19:41:39	0	405852-25	N/A	SMT	'91122025	####	PP	919844198441	Idea Tamilnadu &	2G
20	918464923771	'121113	20/03/2017	20:10:00	28	405852-25	N/A	MOC	'91122025	####	PP	N/A	Idea Tamilnadu &	2G
21	918464923771	'IA-IDEA	21/03/2017	21:52:25	0	40444-125	N/A	SMT	'91122025	####	PP	919844047138	Idea Karnataka	2G
22	918464923771	'IA-IDEA	21/03/2017	21:52:40	0	40444-125	N/A	SMT	'91122025	####	PP	919844047138	Idea Karnataka	2G
23	918464923771	'IA-612345	22/03/2017	09:01:21	0	40444-95(	N/A	SMT	'91122025	####	PP	919848201212	Idea Karnataka	2G
24	918464923771	'917731862592	30/03/2017	11:33:02	0	40444-95(	N/A	SMT	'91140110	####	PP	919848001104	Idea Karnataka	2G
25	918464923771	'9642613391	30/03/2017	11:35:29	61	40444-95(	40444-9501-	MTC	'91140110	####	PP	N/A	Idea Karnataka	2G

Fig.5.8: Example of a normal CDR.

b) GPRS CDR

General Packet Radio Service (GPRS). Details of internet use& its location. It contains information associated with the internet usage of the requested number using mobile internet. General Format of 16 field column GPRS CDR required from Telecom Service Provider is as shown in below Figure.

GPRS CDR															
MSISDN	SOURCE_IP_ADDRESS	SOURCE_IP6_ADDRESS	SOURCE_PORT	PUBLIC_IP_ADDRESS	TRANSLATED_IP_ADDRESS	PUBLIC_IP_PORT	DESTINATION_IP_ADDRESS	DESTINATION_PORT	START_DATE_TIME_PUBLIC_IP	END_DATE_TIME_PUBLIC_IP	STATIC_DYNAMIC_IP_ADDRESS	USER_ID	MAC_ID	PGW_ADDRESS	CGI_ID
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Fig.5.9: GPRS CDR Format.

An example of GPRS CDR is as shown below.

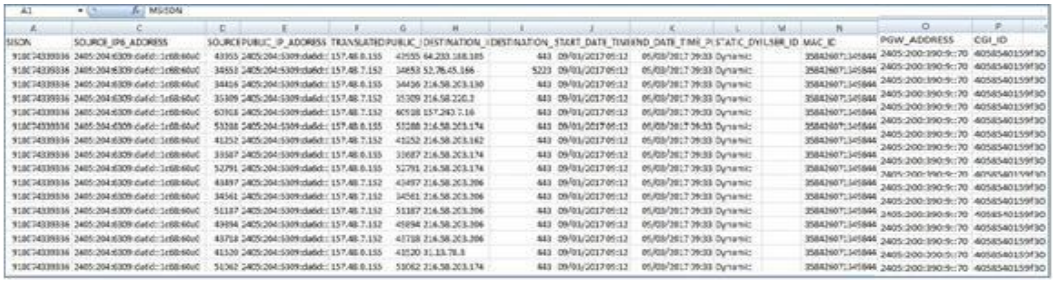


Fig.5.10: Internet sessions and their corresponding locations in GPRS CDR.

c) Tower CDR (Tower Dump):

Contains all transactional details of calls and SMS that happened in the given duration under particular cell tower or base transceiver station. In certain cases where no suspect is identified with regard to a crime, the Investigating Officer(IO) would collect the tower location (Tower ID) where crime Scene falls and details of calls of a particular duration are obtained. While fetching tower dump of a particular area, tower dump of all Service providers has to be collected. To identify all the Towers serving crime scene, the IO would have to use "Cell ID Finding" tools. Some are software based, whereas some are hardware based. For example, NetMonitor (mobile software) and Spectra (hardware). General Format of 13 field column Tower CDR required from Telecom Service Provider is as shown in below Figure.

TOWER DUMP												
CALLING NO	CALLED NO	DATE	TIME	DUR (S)	CELL 1	CELL 2	CALL TYPE	IMEI	IMSI NO	TYPE	SMSC	ROAM NW
1	2	3	4	5	6	7	8	9	10	11	12	13

Fig.5.11: Different Fields in Tower dump CDR.

An example of Tower CDR is shown below Figure.

Calling No	Called No	Date	Time	Dur(s)	Cell1	Cell2	Call Type	IMEI	IMSI No	Type	SMSC	Roam Nw
9629189736	8754873404	12/02/2017	00:54:36	10	25--37804	37804	OUT	3.52E+14	4.05E+14	PREPAID	-	-
9629189736	4566293805	12/02/2017	00:56:15	14	25--37804	37804	OUT	3.52E+14	4.05E+14	PREPAID	-	-
14A68A643C1E0	9790643850	12/02/2017	01:16:29	0	25--37804	-	SMT	3.59E+14	4.05E+14	PREPAID	9.84E+09	-
9025431972	7708665259	12/02/2017	02:10:34	44	25--37804	37804	IN	9.11E+14	4.05E+14	PREPAID	-	-
9025431972	7708665259	12/02/2017	02:26:56	24	25--37804	37804	IN	9.11E+14	4.05E+14	PREPAID	-	-
7639965749	9677440392	12/02/2017	03:01:50	9	25--37804	37804	IN	3.55E+14	4.05E+14	PREPAID	-	-
8940559343	9677440392	12/02/2017	03:29:28	12	25--37804	37804	IN	3.55E+14	4.05E+14	PREPAID	-	-
9159860663	9600864501	12/02/2017	03:36:55	103	25--37804	37804	IN	3.55E+14	4.05E+14	PREPAID	-	-
9994682626	9655811731	12/02/2017	04:33:56	39	25--37804	37804	OUT	3.55E+14	4.05E+14	PREPAID	-	-
9600961817	9944814613	12/02/2017	04:51:06	13	25--37804	37804	OUT	3.59E+14	4.05E+14	PREPAID	-	-
9600961817	9944814613	12/02/2017	04:51:06	14	25--37804	37804	IN	3.6E+14	4.05E+14	PREPAID	-	-
9629378863	8122686919	12/02/2017	05:02:38	101	25--37804	37804	OUT	3.58E+14	4.05E+14	PREPAID	-	-

Fig.5.12: Example of Tower Dump.

d) GPRS DUMP (3G, 4G/Internet Dump)

The details of all the internet activities of a subscriber are provided in the GPRS Data Record/GPRS Dump. An IO must request for a GPRS dump of a particular mobile number for a particular duration. The attributes available in a GPRS CDR are as shown in Figure.

GPRS CDR															
MSISDN	SOURCE_IP_ADDRESS	SOURCE_IP6_ADDRESS	SOURCE_PORT	PUBLIC_IP_ADDRESS	TRANSLATED_IP_ADDRESS	PUBLIC_IP_PORT	DESTINATION_IP_ADDRESS	DESTINATION_PORT	START_DATE_TIME_PUBLIC_IP	END_DATE_TIME_PUBLIC_IP	STATIC_DYNAMIC_IP_ADDRESS	USER_ID	MAC_ID	PGW_ADDRESS	CGI_ID
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Fig.5.13: Different fields of GPRS Dump.

An example of a GPRS Dump is shown below.

MSISDN	SOURC	TRANSLATED_	PUBLIC	DESTINATION_IP	DESTIN	START_DATE_TIM	SOURCE_I	SOURCE_PORT	TRANSLATED_IP_	PUBLIC_IP_PORT
918074339336	43955	157.48.0.165	43955	64.233.188.105	443	09/03/2017 09:12	10.116.128	43955	157.48.0.166	43955
918074339336	34653	157.48.7.162	34653	52.76.45.166	5223	09/03/2017 09:12	10.116.128	34653	157.48.7.163	34653
918074339336	34416	157.48.0.165	34416	216.58.203.130	443	09/03/2017 09:12	10.116.128	34416	157.48.0.166	34416
918074339336	35309	157.48.7.162	35309	216.58.220.2	443	09/03/2017 09:12	10.116.128	35309	157.48.7.162	35309
918074339336	60918	157.48.7.162	60918	157.240.7.16	443	09/03/2017 09:12	10.116.128	60918	157.48.7.162	60918
918074339336	53288	157.48.0.165	53288	216.58.203.174	443	09/03/2017 09:12	10.116.128	53288	157.48.0.166	53288
918074339336	41252	157.48.7.162	41252	216.58.203.162	443	09/03/2017 09:12	10.116.128	41252	157.48.7.163	41252
918074339336	33687	157.48.0.165	33687	216.58.203.174	443	09/03/2017 09:12	10.116.128	33687	157.48.0.165	33687
918074339336	52791	157.48.0.165	52791	216.58.203.174	443	09/03/2017 09:12	10.116.128	52791	157.48.0.165	52791
918074339336	43497	157.48.7.162	43497	216.58.203.206	443	09/03/2017 09:12	10.116.128	43497	157.48.7.162	43497
918074339336	34561	157.48.7.162	34561	216.58.203.206	443	09/03/2017 09:12	10.116.128	34561	157.48.7.162	34561
918074339336	51187	157.48.7.162	51187	216.58.203.206	443	09/03/2017 09:12	10.116.128	51187	157.48.7.162	51187
918074339336	49894	157.48.7.162	49894	216.58.203.206	443	09/03/2017 09:12	10.116.128	49894	157.48.7.162	49894

Fig.5. 14: Example of GPRS Dump.

e) Subscriber Details Record (SDR)

There are various other documents that are provided by the Telecom Service Provider's which are required for proper analysis of call Data record(CDR). Subscriber Data Record (SDR)s is a record of document collected and details filled by a consumer at the time of purchase of SIM card. There are many fields in an SDR, a few relevant are shown in the Figure. The information on other fields in an SDR can be referenced in the following link.

http://www.dot.gov.in/sites/default/files/Instructions%20on%20Verification%20of%20New%20Mobile%20Subscribers%20%281%29.PDF?download=1

SDR												
CAF NO.	MSISDN	CUSTOMER NAME	FATHERS/ HUSBANDS NAME	DATE OF ACTIVATION	PRESENT ADDRESS	PERMANENT ADDRESS	RETAILERS NAME	CURRENT STATUS	CITY	STATE	DOC _TYP _POA	DOC _TYPE _POI
1	2	3	4	5	6	7	8	9	10	11	12	13

Fig.5.15: Format of relevant fields in an SDR.

An example of SDR is shown in below figure.

	Customer Name	Fathers/husbands name	Date of activation	Present address	Permanent	Retailers name	Current Status	City	State	Doc_Type_Po/	Doc_Type_Poi	
2	Narendra	Mr. Ahuja	02/07/2010	Old no. 47/ New no. 8	Hyderabad	Airtel	Active	Hyderabad	Telangana	Registered Leas	Registered Partnership Deed	
3	Ramesh	Mr. Ankur Sharma	25/12/2011	H.No 8-2-693/2/28, M	Hyderabad	Vodafone	Active	Hyderabad	Telangana	Bank Pass Book	Registered Partnership Deed	
4	Suresh	Rajinikanth	26/12/2011	RMK PLAZA, 8-2-630	Hyderabad	Idea	Active	Hyderabad	Telangana	Bank Pass Book	Voter Identity Card	
5	Mallesh	Somesh	01/12/2011	P.S Nagr, Vijaynagar	Hyderabad	Idea	Active	Hyderabad	Telangana	Bank Pass Book	Registered Partnership Deed	
6	Yellaiya	Reddy Chintal	01/12/2011	V.S.T COLONY,NACI	Hyderabad	Airtel	Active	Hyderabad	Telangana	Bank Pass Book	Registered Partnership Deed	
7	Ramaiya	Vastavaiya	01/12/2011	Plot No.37, E.C.Naga	Hyderabad	Airtel	Active	Hyderabad	Telangana	Bank Pass Book	Voter Identity Card	
8	Katiya	Kabira	01/12/2011	HNO:4-65/2,STREET	Hyderabad	Vodafone	Active	Hyderabad	Telangana	Bank Pass Book	Registered Partnership Deed	
9	Dang	Joseph Cristo	01/12/2011	H NO-1-2-90/1/A,KAK	Hyderabad	Idea	Active	Hyderabad	Telangana	Bank Pass Book	Registered Partnership Deed	
10	Amar	Pratap Singh	01/12/2011	D.No.2-20-30/1, Chila	Hyderabad	Idea	Active	Hyderabad	Telangana	Bank Pass Book	Voter Identity Card	
11	Akbar	Ali Jaan	01/12/2011	Deccan Swaraj Indust	Hyderabad	Airtel	Active	Hyderabad	Telangana	Bank Pass Book	Registered Partnership Deed	
12	Anthony	Christopher Nolan	01/12/2011	H.No.5-14-114/2, Qua	Hyderabad	Idea	Active	Hyderabad	Telangana	Bank Pass Book	Registered Partnership Deed	
13	Rajesh	Rajinikanth	01/12/2011	Saraswathi Block, Tri	Hyderabad	Airtel	Active	Hyderabad	Telangana	Bank Pass Book	Registered Partnership Deed	
14	Naresh	Allari Komatla	01/12/2011	HNO 1-19/A, NEAR V	Hyderabad	Airtel	Active	Hyderabad	Telangana	Bank Pass Book	Voter Identity Card	
15	Ali	Syed Raheem Ali	01/12/2011	HNO-13-124/3 NEAR	Hyderabad	Airtel	Active	Hyderabad	Telangana	Bank Pass Book	Voter Identity Card	
16	Razia	Nuzheth Md	01/12/2011	H.NO.7-15-12,OPP.R	Hyderabad	Airtel	Active	Hyderabad	Telangana	Bank Pass Book	Passport	
17	Shazia	Nuzheth Md	01/12/2011	H.No.1-91/17, FMR C	Hyderabad	Airtel	Active	Hyderabad	Telangana	Bank Pass Book	Passport	
18	Nazia	Nuzheth Md	01/12/2011	H.NO:42-795, CHANC	Hyderabad	Vodafone	Active	Hyderabad	Telangana	Bank Pass Book	Passport	
19	Fouzia	Nuzheth Md	02/12/2011	M/s Jesday Pharmac	Hyderabad	Airtel	Active	Hyderabad	Telangana	Bank Pass Book	Passport	
20	Geeta	Balaiyya	03/12/2011	Sy.No.24, Mallapur V	Hyderabad	Airtel	Active	Hyderabad	Telangana	Bank Pass Book	Passport	

Fig.5.16: Example of SDR.

f) Customer Application Form (CAF)

This document contains the name, a passport sized photograph, location of purchase of SIM card and address details of the Subscriber as filled by him/her. An example of Customer Application Form is shown in Figure

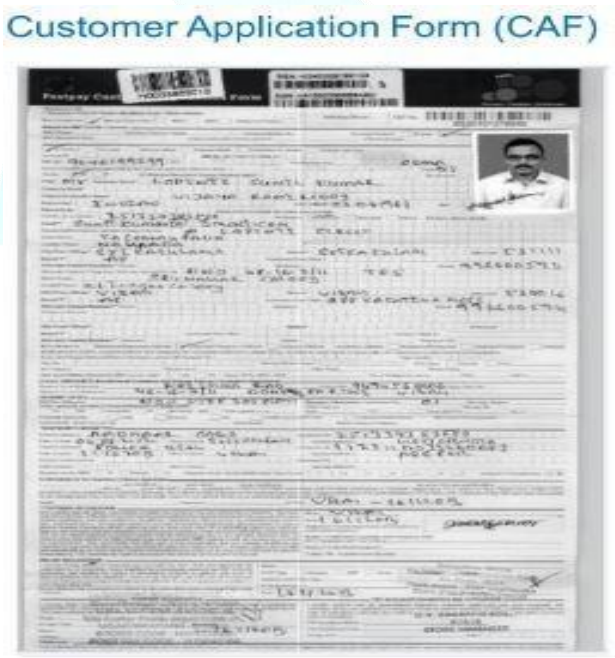


Fig.5.17: Example of a Customer Application Form.

g) Internet Protocol Details Record (IPDR)

An IPDR can tell, a number of things about incoming and outgoing network traffic. It is a data record of all the network traffic at a Particular IP at the Particular point in time. The general format for an IPDR is as shown in Figure.

IPDR																
Mobile No.	Cell 1	IMEI	IMSI	Downlink-Vol.	Uplink-Vol.	Session Start-Time	Session End-Time	Pre /Post	Home Roaming Circle	Roaming Network Indicator	ICR Operator Name	Home Circle	Public IPv4	Public IPv6	Port Detail	Destination IP
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

Fig.5.18: Format of an IPDR

An example of an IPDR is as shown below.

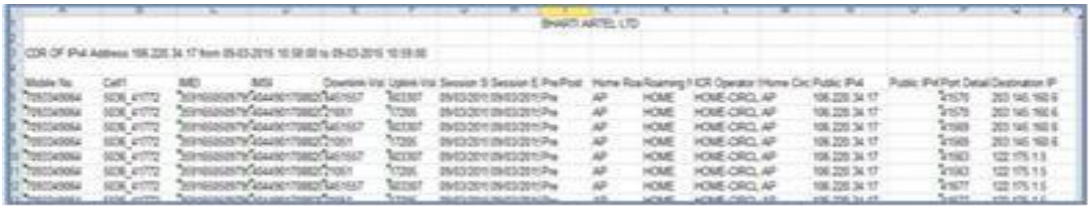
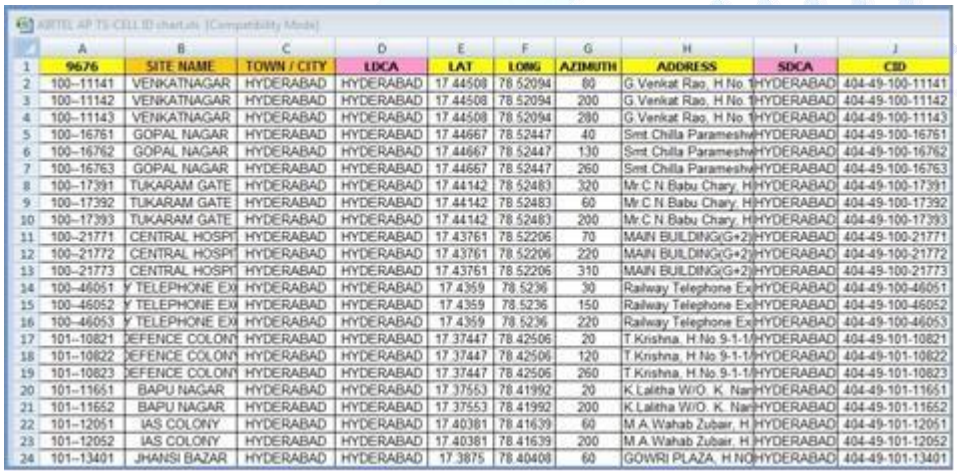


Fig.5.19: Example of an IPDR.

h) Cell ID Chart

A Cell ID chart is a record of all the Cell Tower(s) belonging to a Mobile Service Provider which includes the Cell ID, Latitude, Longitude, Address, etc of all the Towers. Every Service Provider has their own Cell ID chart. The service providers provide the updated list of Cell IDs to the LEA(s) as and when there are new Towers installed or any change in the previous towers. An example of Cell ID chart is as shown in Figure.



	A	B	C	D	E	F	G	H	I	J
1	9676	SITE NAME	TOWN / CITY	LDCA	LAT	LONG	AZIMUTH	ADDRESS	SDCA	CID
2	100--11141	VENKATNAGAR	HYDERABAD	HYDERABAD	17.44508	78.52094	80	G.Venkat Rao, H.No.1	HYDERABAD	404-49-100-11141
3	100--11142	VENKATNAGAR	HYDERABAD	HYDERABAD	17.44508	78.52094	200	G.Venkat Rao, H.No.1	HYDERABAD	404-49-100-11142
4	100--11143	VENKATNAGAR	HYDERABAD	HYDERABAD	17.44508	78.52094	280	G.Venkat Rao, H.No.1	HYDERABAD	404-49-100-11143
5	100--16761	GOPAL NAGAR	HYDERABAD	HYDERABAD	17.44667	78.52447	40	Smt.Chilla Parameshv	HYDERABAD	404-49-100-16761
6	100--16762	GOPAL NAGAR	HYDERABAD	HYDERABAD	17.44667	78.52447	130	Smt.Chilla Parameshv	HYDERABAD	404-49-100-16762
7	100--16763	GOPAL NAGAR	HYDERABAD	HYDERABAD	17.44667	78.52447	260	Smt.Chilla Parameshv	HYDERABAD	404-49-100-16763
8	100--17391	TUKARAM GATE	HYDERABAD	HYDERABAD	17.44142	78.52483	320	Mr.C.N.Babu Chary, H	HYDERABAD	404-49-100-17391
9	100--17392	TUKARAM GATE	HYDERABAD	HYDERABAD	17.44142	78.52483	60	Mr.C.N.Babu Chary, H	HYDERABAD	404-49-100-17392
10	100--17393	TUKARAM GATE	HYDERABAD	HYDERABAD	17.44142	78.52483	200	Mr.C.N.Babu Chary, H	HYDERABAD	404-49-100-17393
11	100--21771	CENTRAL HOSPI	HYDERABAD	HYDERABAD	17.43761	78.52206	70	MAIN BUILDING(G+2)	HYDERABAD	404-49-100-21771
12	100--21772	CENTRAL HOSPI	HYDERABAD	HYDERABAD	17.43761	78.52206	220	MAIN BUILDING(G+2)	HYDERABAD	404-49-100-21772
13	100--21773	CENTRAL HOSPI	HYDERABAD	HYDERABAD	17.43761	78.52206	310	MAIN BUILDING(G+2)	HYDERABAD	404-49-100-21773
14	100--46051	Y TELEPHONE EX	HYDERABAD	HYDERABAD	17.4359	78.5236	30	Railway Telephone Ex	HYDERABAD	404-49-100-46051
15	100--46052	Y TELEPHONE EX	HYDERABAD	HYDERABAD	17.4359	78.5236	150	Railway Telephone Ex	HYDERABAD	404-49-100-46052
16	100--46053	Y TELEPHONE EX	HYDERABAD	HYDERABAD	17.4359	78.5236	220	Railway Telephone Ex	HYDERABAD	404-49-100-46053
17	101--10821	DEFENCE COLONY	HYDERABAD	HYDERABAD	17.37447	78.42506	20	T.Krishna, H.No.9-1-1	HYDERABAD	404-49-101-10821
18	101--10822	DEFENCE COLONY	HYDERABAD	HYDERABAD	17.37447	78.42506	120	T.Krishna, H.No.9-1-1	HYDERABAD	404-49-101-10822
19	101--10823	DEFENCE COLONY	HYDERABAD	HYDERABAD	17.37447	78.42506	260	T.Krishna, H.No.9-1-1	HYDERABAD	404-49-101-10823
20	101--11651	BAPU NAGAR	HYDERABAD	HYDERABAD	17.37553	78.41992	20	K.Lalitha W/O. K. Nar	HYDERABAD	404-49-101-11651
21	101--11652	BAPU NAGAR	HYDERABAD	HYDERABAD	17.37553	78.41992	200	K.Lalitha W/O. K. Nar	HYDERABAD	404-49-101-11652
22	101--12051	IAS COLONY	HYDERABAD	HYDERABAD	17.40381	78.41639	60	M.A.Wahab Zubair, H	HYDERABAD	404-49-101-12051
23	101--12052	IAS COLONY	HYDERABAD	HYDERABAD	17.40381	78.41639	200	M.A.Wahab Zubair, H	HYDERABAD	404-49-101-12052
24	101--13401	JHANSI BAZAR	HYDERABAD	HYDERABAD	17.3875	78.40408	60	GOWRI PLAZA, H.NO	HYDERABAD	404-49-101-13401

Fig.5.20: An example of Cell ID Chart.

i) IMEI Database

A collective database that cross-examinesan IMEI (International Mobile Equipment Identity) number found in CDRs to the corresponding device details mostly model number and manufacturer. IMEI database is maintained by Mobile

Service Providers to maintain a Black List/White List so as to block/allow a mobile phone from accessing their Network.

j) RAW CDR

It is a CDR which contains more details than a normal CDR with attributes such as OUTTRUNK, INTRUNK, INSWITCH, OUTSWITCH, etc.
This is requested in investigating cases involving spoofed calls. The general format of RAW CDR is as shown in Figure.

RAW CDR										
CALLING NUMBER	CALLED NUMBER	CALL DATE	TIME	DURATION	OUTFRAME NAME	INTRUNK NAME	IN SWITCH	OUT SWITCH	LRN	NETWORK
1	2	3	4	5	6	7	8	9	10	11

Fig.5.21: Format of RAW CDR.

An Example of RAW CDR is as shown in Figure.

								OUTSWITCH NAME			
		DISHNET WIRELESS LTD				CONFIDENTIAL					
Report Generation Date & time				27-09-2017							
Call Detail records for ILD No:				85690[illegible]1							
Period of call Details Records			01-09-2017	to	27-09-2017						
CALLING NUMBER	CALLED NUMBER	CALL DATE	TIME		DURATION	OUTTRUNKNAME	INTRUNK NAME	INSWITCH	OUTSWITCH	LRN	NETWORK
912266[illegible]0	60173402[illegible]0	09-09-2017	2:23:30 PM		30	M800	TTSL-Hyderaba	Mumbai	Mumbai		
912266[illegible]0	60173402[illegible]0	09-09-2017	2:40:12 PM		28	M800 TELECOM	TTSL-Hyderaba	Mumbai	Mumbai		
60173402[illegible]0	917778420[illegible]7	20-09-2017	6:30:11 PM		5	DWL Hyderabad	MAXIS TELECO	Mumbai	Mumbai	3070	Idea
Reference No.	2776285[illegible]0										
				This is a System generated report and needs no signature.							

Fig.5.22: Example of RAW CDR

5.7.3 Different Fields Available in CDRs

Fields in CDR	Explanation
Calling Number	Details of those numbers to which made the calls (Outgoing calls & Outgoing SMS)
Called Number	Details of those numbers which received the calls (Incoming Calls) Some MSPs provide this data under B_ Number Column.
Date	Date on which calls/SMSs were originated/received
Time	Time on which the transactions were made (calls/SMS/MMS). Some Service Providers record it in12hour format, whilesomerecordin24hourformat
Duration	Duration of all calls (in Seconds).
Cell ID	Mobile Tower information from which the calls were made/received

Call Type	•Incoming call(INC) •Outgoing Call(OUT) •Incoming SMS(SMS-INC) •Outgoing SMS(SMS-OUT) The Symbols for the type of call i.e. INC, OUT, SMS-IN SMS-OUT might change with different MSP's.
IMEI	International Mobile Equipment Identity (IMEI) is a number to identify the Mobile phone device. Every Mobile phone device is having a unique IMEI. It is usually printed on the phone in the back panel. It can also be found by dialling *#06#
IMSI	International Mobile Subscriber Identity (IMSI) is a unique number stored in SIM. It gets its relevance in CDR analysis by the fact that two SIM cards may be having one mobile number, but no two SIMs will be having same IMSI number.
Connection Type	There can be two types of connections •Prepaid (PRE) •Postpaid(PO)
SMS Centre	SMS Centre is responsible for sending/receiving the text messages for a telephone network. When someone sends/receives an SMS, it gets stored in SMS Centre from which it is delivered to the recipient.

There are many MSP's (Mobile Service Provider) in India. It has been observed that the format and type of the file in which the MSPs provide the CDRs are not same. In fact, every MSP might have its own format in which it provides the CDR's.

- MS Excel format (.xls, .xlsx)
- Text format (.txt)
- Comma Separated Value format (.csv)
- HTML format (.html)
- PDF Format (.pdf)

Junk Numbers in CDR

There are some junk numbers found in the CDR. CDRs, you may find some junk hexadecimal numbers in either Calling/Called numbers, as follows:

- 1446BC65381C0613
- 549697C8>0BCC56

These numbers are nothing but some automatically generated SMSs from various entities like Companies, promotional SMS, Alerts etc.

5.7.5 Things to be done before Analysis

Analysis of a CDR is best performed using Pivot table feature of MS Excel 2007/2010. However, there are following steps to be performed before we begin with CDR Analysis with Pivot table.

i) CDR format conversion

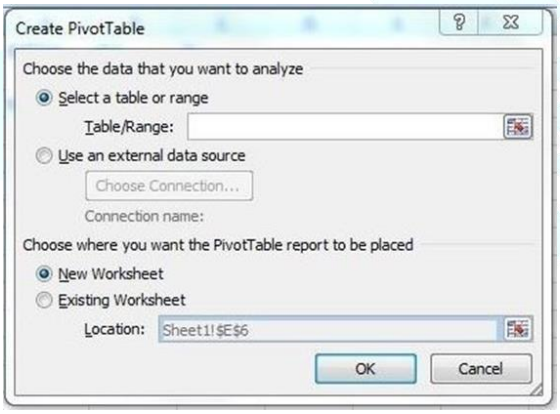
As discussed above, CDRs may come in different formats depending upon the MSP. For analysis purpose we must convert it into either MS Excel format (.xls/.xlsx) or Comma Separated Value (.csv) format.

a) Creating a Pivot Table

A pivot table is a data analysis and summarization tool found in MS Excel. After the CDR is converted into MS Excel or CSV format, a pivot table needs to be created. The Pivot table can be created as follows:

Arrange the data in proper order (ascending) based on the time, date and make sure the 1st column (or) the "Calling Number" or "A party" consists of only the numbe$_r$ whose CDR we are analysing. The "Called Number" or "B Party" consists of all other numbers.

ii) Now go to Insert tab and click on the pivot table. We get a prompt showing "Create pivot table" and click OK. It will create a new pivot table in a new worksheet.



i)

Fig.5.23: Pivot table creation using MS Excel.

a) Drag the "Called No." field into the leftmost bottom box named as row labels.
b) – Drag the "Call Type" field into the rightmost upper box named as column labels.
c) – Drag the "Calling No." field into 'Σ' summation Values column and click on it & select "value field settings".

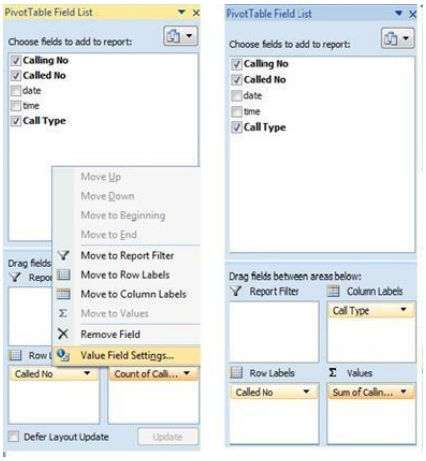


Fig.5.24: Screenshot of Pivot Table Field List.

iii) After choosing Value Field Settings the following window appears in which Select the type of calculation required to summarize. Here Count is chosen and click Ok as shown in Figure.

Fig.5.25: Screenshot of Pivot Table "Value Field Settings"

iv) Select the grand total until the last row, go to options and click sort largest to smallest. Get the number which has the highest count that the accused has called.

b) Mapping Tower Locations

i) To find out the tower location of any Cell ID, first of all, go to the desired CDR, select the 'Cell ID' column, then right-click on it, select the copy option and take a new worksheet then paste it.

ii) The formula for tower location analysis is

VLOOKUP(A2,[workbookname.xls]worksheetname!$A:$H,8,0) Where 8th column is number of r.

Note: Replace 'workbookname' with the actual workbook name and replace 'worksheetname' with the actual worksheet name.

iii) Copy and paste the above-mentioned formula in the 2nd column of the Excel worksheet document. The Cell ID chart is in the first column of the same Excel sheet.

iv) Select the bottom of the first cell, click on '+' sign to apply the formula to the complete column.

v) In this way, we can import all the tower locations of city, district, state and azimuth as well.

5.9 Analysis of CDR

The CDR may consist of hundreds, thousands or even lakhs of call records. Analysis of a CDR is a compulsory process to get useful information out of it. CDR Analysis is usually performed to get the following information (but not limited to) from a CDR.

I. Top few numbers on which a mobile number user is calling frequently (Outgoing calls).
II. Top few numbers from which a mobile number user is getting calls frequently (incoming calls).
III. Top few maximum duration calls.
IV. 1-5 seconds calls.
V. Night location of mobile number user.
VI. How many SIM cards mobile number user has changed.
VII. How many Mobile sets mobile number user has used.
VIII. Calls made during a particular time period (e.g. 10 AM – 6 PM), etc.

a) Multiple CDRs Analysis

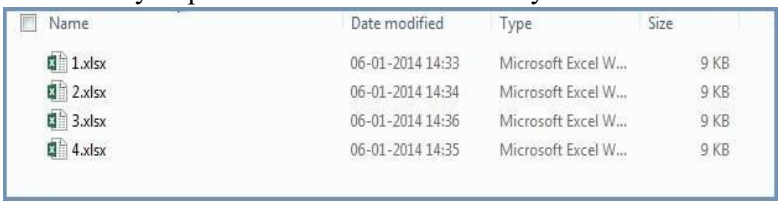
Multiple CDR Analysis is very useful in cases where there is more than one suspect in a case. The CDRs of the suspect(s) can be analysed to find out

- Whether they were in touch with each other.
- Is there any number to which all or some of the suspects are communicating.

MS Excel again can be used to analyse multiple CDRs.

Step 1:

For multiple CDR Analysis place all the CDRs to be analyzed in one folder.



Screenshot showing placement of all the CDRs in one folder

Step 2:

Create a MASTER file to append all the calling numbers and called numbers of all the CDRs placed in the folder for analysis.

Screenshot of excel sheet with a master file

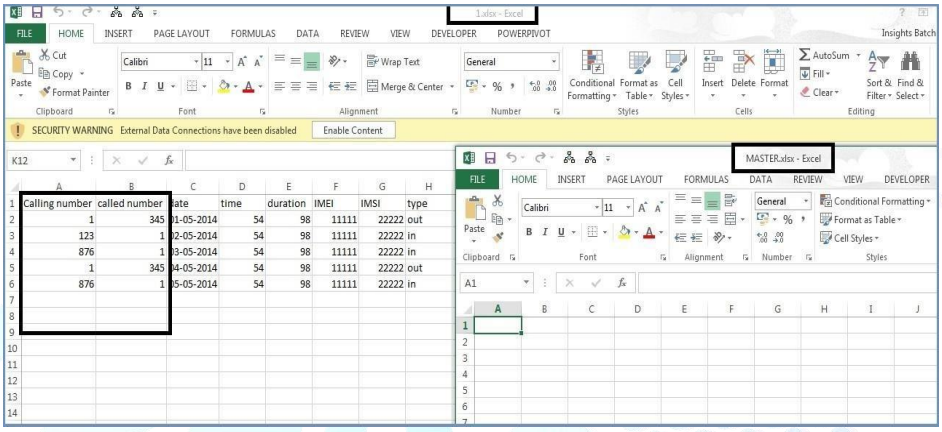
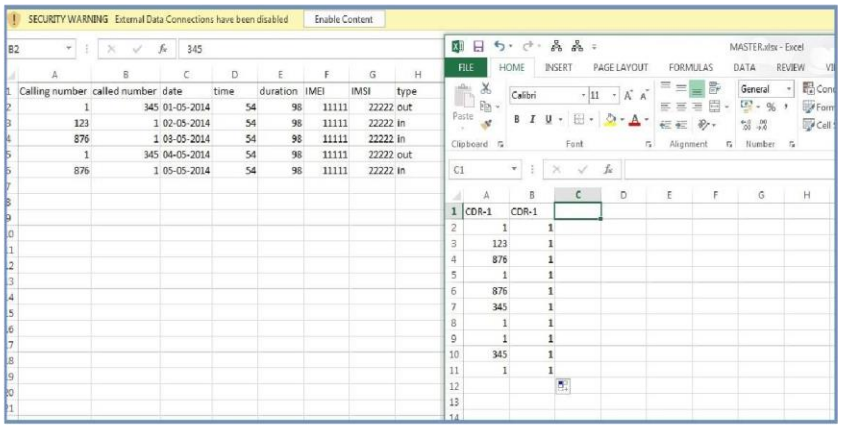
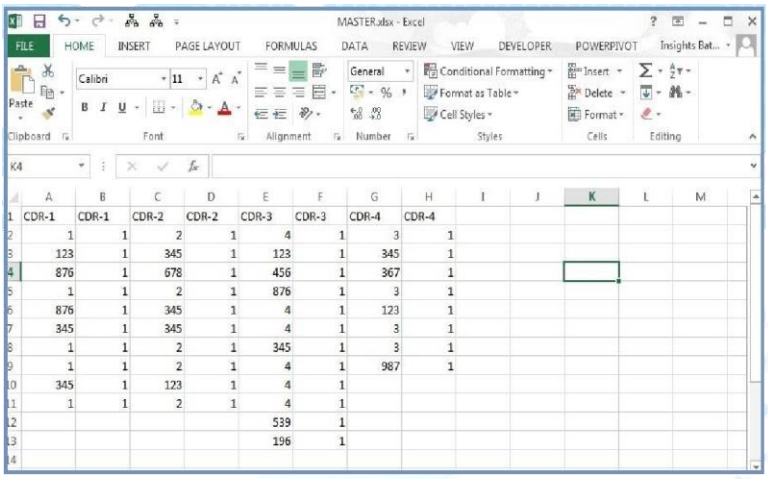


Fig.5.26: Multiple CDRs Analysis – 1



Screenshot of master file showing called numbers and calling numbers copied into Masterfile from CDR-1

In the above screenshot, the numbers of First CDR (1.xlsx) in calling number and called number fields were copied and appended in 'CDR-1' column A in master file. Another column with the same name as Column A was created and filled with number '1'. The same exercise should be done for all the CDRs. Finally, after adding data from four CDR, the MASTER.xlsx would be like the Screenshot below.



Screenshot showing addition of all called and calling numbers from all CDRs into MASTER.xlsx

Fig.5.27: Multiple CDRs Analysis – 2

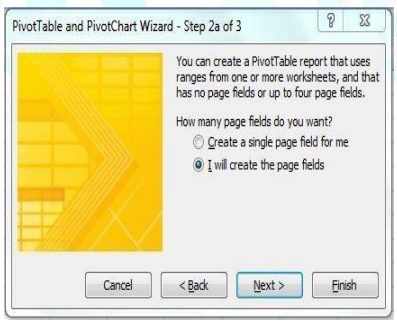
Step 3:

Press ATL + D and then P. The following window would appear.

Screenshot of window after execution of step 3 in Multiple CDR Analysis

Step 4:

Select Multiple Consolidation Ranges option from the window which appears after executing step 3 and press Next. Then the following window would appear.

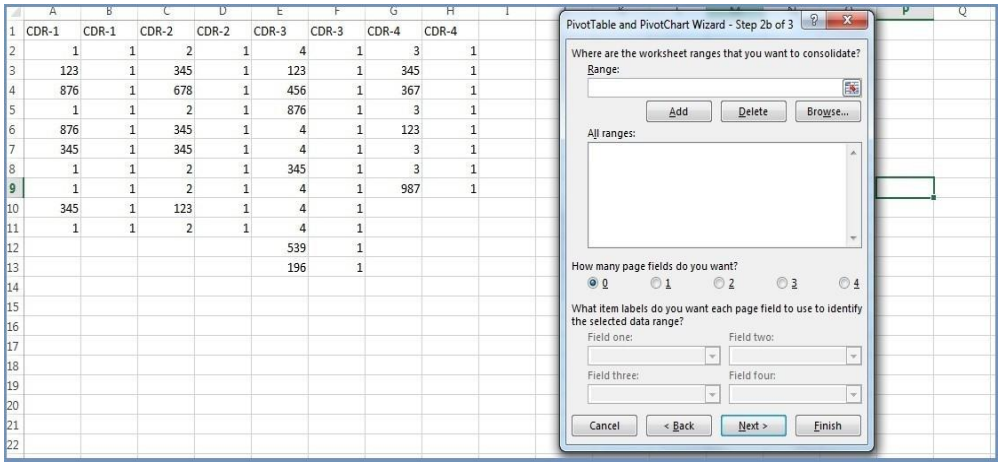


Screenshot of window after execution of Step 4 in Multiple CDR Analysis

Fig.5.28: Multiple CDR Analysis – 3

Step 5:

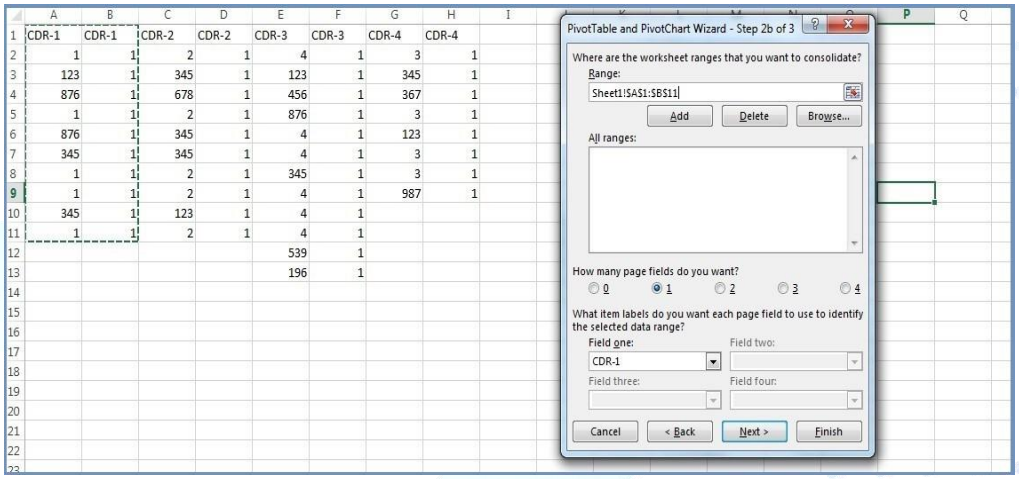
Move on by clicking on the option “I will create the page fields” and click on Next. Following window will appear.



Screenshot of MASTER.xlsx with window of 'PivotTable and PivotChart Wizard'

Step 6:

Select the range of data from the CDR-1 and click on Add. Then select '1' as the page field, Write 'Field one' as CDR-1.

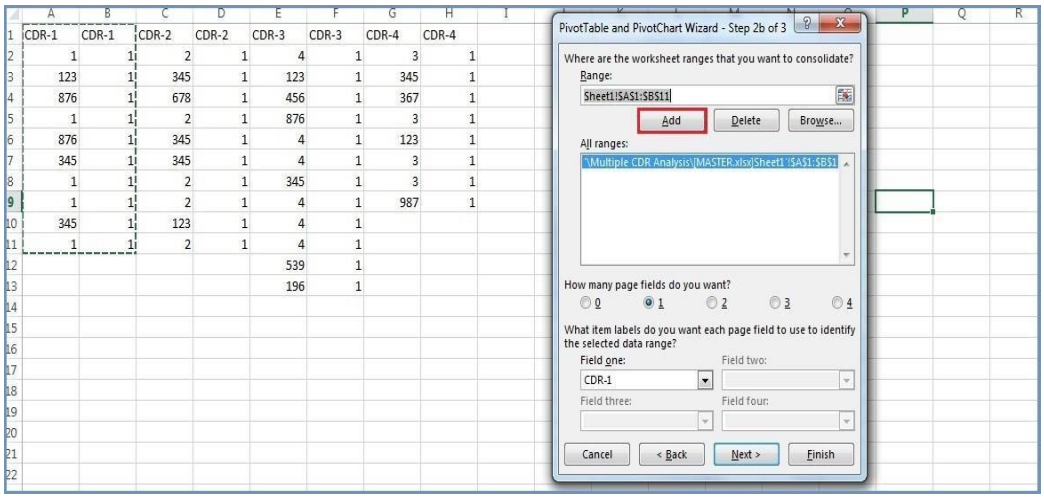


Screenshot of MASTER.xlsx with window showing execution of step 6

Fig.5.29: Multiple CDR Analysis – 4

Step 7:

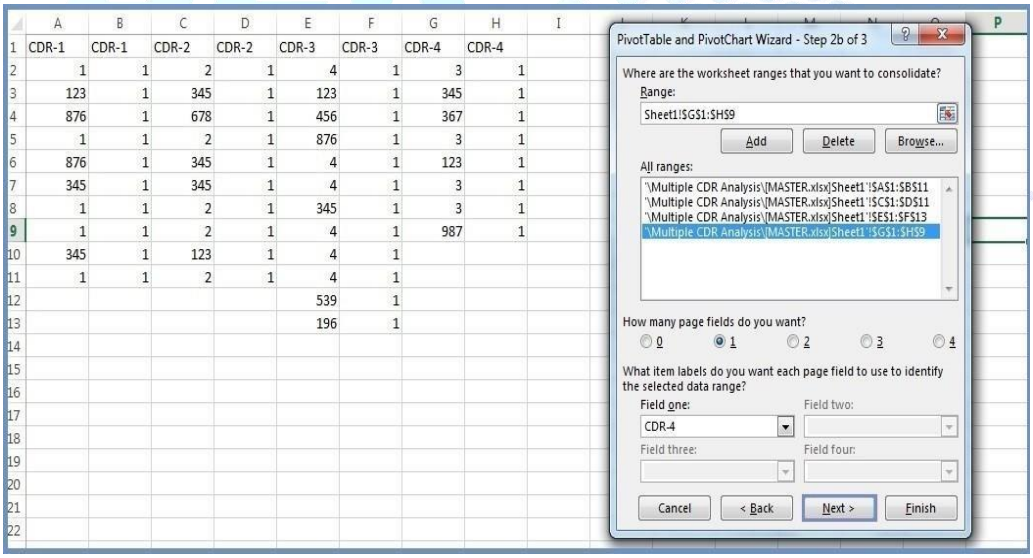
After execution of step 6, click on 'Add' button in the pivot table wizard.



Screenshot of MASTER.xlsx with window showing execution of step 7

Step 8:

Similarly, data from all the CDRs to be selected and added into it.

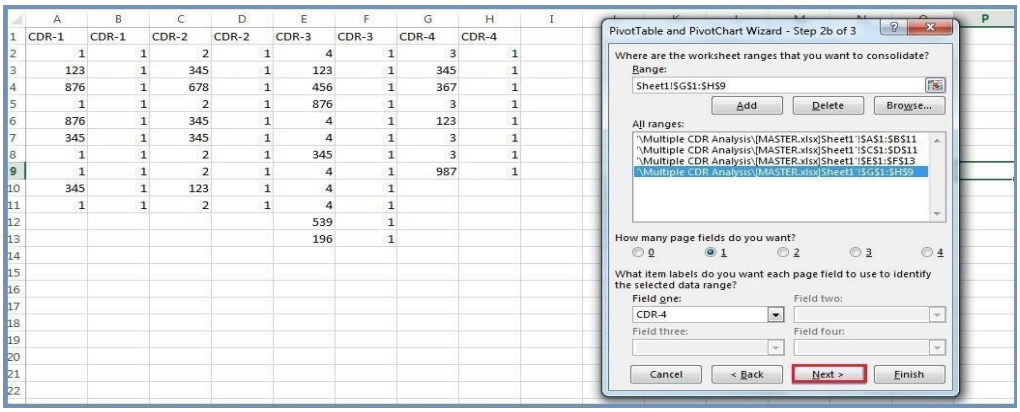


Screenshot of MASTER.xlxs with pop up window showing addition of data from all CDRs

Fig.5.30: Multiple CDRs Analysis – 5

Step 9:

After adding all CDRs to the pivot table wizard move on by clicking on Next.

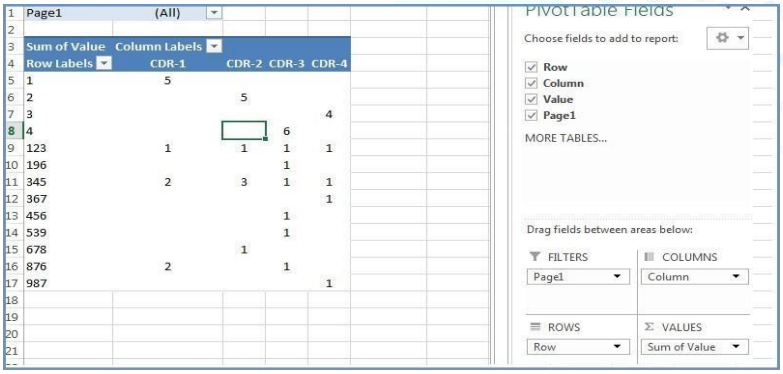


After execution of step 9 following window appears indicating to finish the process.

Screensh ot of dialog box indicating to finish the step

Step 10:

Cli ck on Finish. The resulting screen looks like this



Screenshot of Final Result Screen

Here following analysis can be made that, number's "123" and "345" are interacting with all 4 CDR that, number "876" is interacting with CDR-1 and CDR-3.

Fig.5.31: Multiple CDRs Analysis – 6

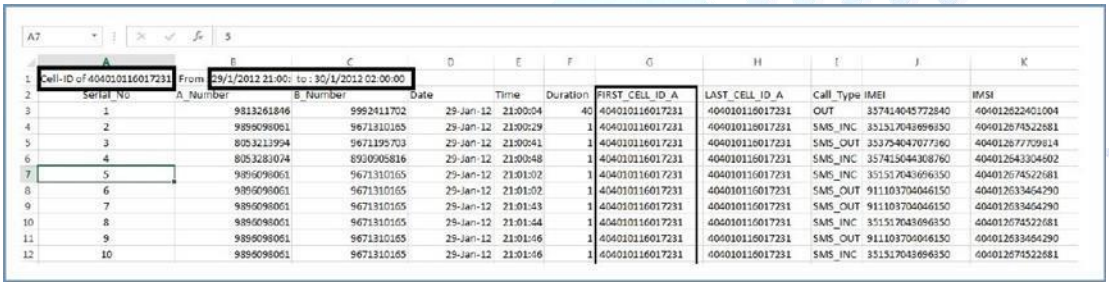
5.10 Tower Dump Analysis

Tower Dump Analysis is a very important tool in the investigation. It is especially helpful when there are no suspects for a crime, and only a few peripheral details are available with the investigation agency.

Examples –

- An FIR is registered with police; electricity wires were stolen from various villages in the district. Police, in this case, had no suspect in hand, but only the places of crime and tentative time of the crime (during the night).
- A major theft was reported by a dealer of Pure Ghee. More than 500 tins of Ghee (each weighing 20 KG) worth around 30 lakhs was stolen. In this case, the CCTV footage, police could see that although the thieves covered their faces, they made few calls.
- In a kidnapping case, police only knew about the route followed by the kidnappers, after the boy (who was kidnapped) told them about the route.

A tower dump analysis in these cases helps us figure out the suspects. A sample tower Dump of Vodafone is as shown in below figure.



Cell-ID of 404010116017231	From	29/1/2012 21:00:	to :	30/1/2012 02:00:00								
Serial_NO	A_Number	B_Number	Date	Time	Duration	FIRST_CELL_ID_A	LAST_CELL_ID_A	Call_Type	IMEI	IMSI		
1	9813261846	9992411702	29-Jan-12	21:00:04	40	404010116017231	404010116017231	OUT	357414045772840	404012622401004		
2	9896098061	9671310165	29-Jan-12	21:00:29	1	404010116017231	404010116017231	SMS_INC	3515170436963 50	404012674522681		
3	8053213994	9671195703	29-Jan-12	21:00:41	1	404010116017231	404010116017231	SMS_OUT	353754047077360	404012677709814		
4	8053283074	8930905816	29-Jan-12	21:00:48	1	404010116017231	404010116017231	SMS_INC	357415044308760	404012643304502		
5	9896098061	9671310165	29-Jan-12	21:01:02	1	404010116017231	404010116017231	SMS_INC	3515170436963 50	404012674522681		
6	9896098061	9671310165	29-Jan-12	21:01:02	1	404010116017231	404010116017231	SMS_OUT	911103704046150	404012633464290		
7	9896098061	9671310165	29-Jan-12	21:01:43	1	404010116017231	404010116017231	SMS_OUT	911103704046150	404012633464290		
8	9896098061	9671310165	29-Jan-12	21:01:44	1	404010116017231	404010116017231	SMS_INC	3515170436963 50	404012674522681		
9	9896098061	9671310165	29-Jan-12	21:01:46	1	404010116017231	404010116017231	SMS_OUT	911103704046150	404012633464290		
10	9896098061	9671310165	29-Jan-12	21:01:46	1	404010116017231	404010116017231	SMS_INC	3515170436963 50	404012674522681		

Fig.5.32: A sample Vodafone tower dump.

From the above figure, it is clear that this tower dump belongs to Tower ID: 404010116017231 which is owned by Vodafone, Haryana. The duration for which the dump was requested is also given.

5.10.1 Objectives of Tower Dump Analysis

- The precise reason for any tower dump analysis is to find out the suspect. In short, tower dump is the CDR of a tower.

- The most important query often asked by the investigators is – How to find common numbers amongst many tower dumps collected from different places. It helps in understanding about those people who are on run (after the kidnapping, chain snatching, vehicle theft etc.) or who are involved in crimes at different locations.

- For this purpose, it is necessary to uniform the format for the tower dumps that are needed to be analysed. Tower dump formats of different service providers can vary from one another so to avoid any mismatch of the data it is always better to create a new master file for analysis.

- Below steps are done to the analysis of a multiple towers dumps for Vodafone network, similarly, this can be implemented for any other service provider or a group of service providers, but the master file format needs to be updated accordingly.

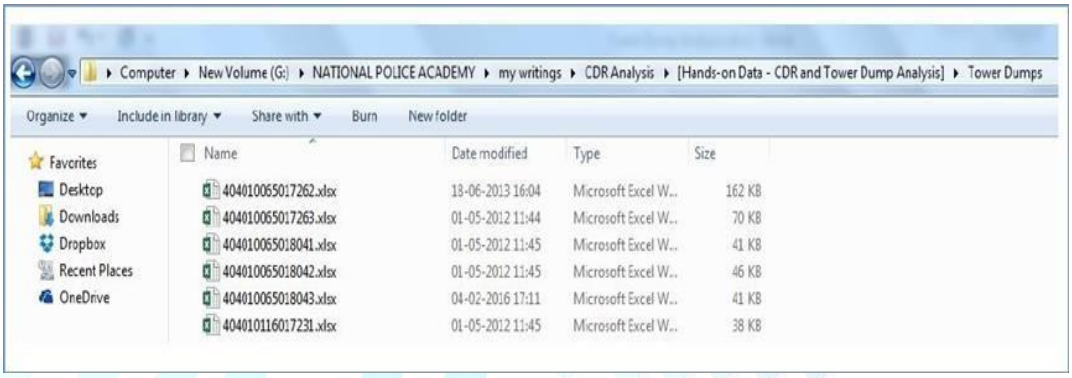


Fig.5.33: Multiple towers dump to be analysed are kept in a folder.

5.10.2 Analysis of Tower Dumps ToR find common Numbers

Here, it can be seen that in the First call, A_Number (also known as calling number) (i.e. 9813261846) is calling B_Number (also known as a called number) (i.e. 9992411702).

Now the question arises that out of these two numbers, which one was using the Tower, at the time of the call. The answer to this question lies in the type of this call. The call type is OUT. It means the tower made an outgoing call. Hence, A _Number was using the tower to make a call.

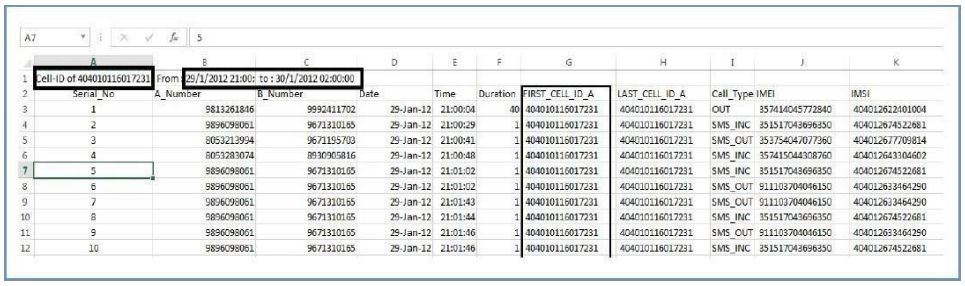
In the next example: – In Serial_No 2, A_Number (i.e. 9896098061) is making a call to B_Number (i.e. 9671310165). However, the call type is SMS_INC, i.e. SMS incoming. It means, tower received an SMS. In that case, B_number received the SMS and hence, it was in the Tower. So, if we generalize this concept, whenever tower makes an outgoing call or SMS, A_number is using the tower, and when the tower receives an incoming call or SMS, B_number is using the tower.

Step 1:

Merge the data - The tower dumps should be merged into single worksheet.

Step 2:

Identify the Target numbers of the Tower - This is a tricky step, which involves a small understanding of how a tower stores the call. For example – Few calls in the abovementioned Tower Dumps are given.



	A	B	C	D	E	F	G	H	I	J	K
1	Cell-ID of 404010116017231	From:	29/1/2012 21:00:	to : 30/1/2012 02:00:00							
2	Serial_No	A_Number	B_Number	Date	Time	Duration	FIRST_CELL_ID_A	LAST_CELL_ID_A	Call_Type	IMEI	IMSI
3	1	9813261846	9992411702	29-Jan-12	21:00:04	40	404010116017231	404010116017231	OUT	357414045772840	404012622401004
4	2	9896098061	9671310165	29-Jan-12	21:00:29	1	404010116017231	404010116017231	SMS_INC	351517043696350	404012674522681
5	3	8053213994	9671195703	29-Jan-12	21:00:41	1	404010116017231	404010116017231	SMS_OUT	353754047077360	404012677709814
6	4	8053283074	8930905816	29-Jan-12	21:00:48	1	404010116017231	404010116017231	SMS_INC	357415044308760	404012643104602
7	5	9896098061	9671310165	29-Jan-12	21:01:02	1	404010116017231	404010116017231	SMS_INC	351517043696350	404012674522681
8	6	9896098061	9671310165	29-Jan-12	21:01:02	1	404010116017231	404010116017231	SMS_OUT	911103704046150	404012633464290
9	7	9896098061	9671310165	29-Jan-12	21:01:43	1	404010116017231	404010116017231	SMS_OUT	911103704046150	404012633464290
10	8	9896098061	9671310165	29-Jan-12	21:01:44	1	404010116017231	404010116017231	SMS_INC	351517043696350	404012674522681
11	9	9896098061	9671310165	29-Jan-12	21:01:46	1	404010116017231	404010116017231	SMS_OUT	911103704046150	404012633464290
12	10	9896098061	9671310165	29-Jan-12	21:01:46	1	404010116017231	404010116017231	SMS_INC	351517043696350	404012674522681

Illustration of Step 2 for analysing tower dumps

Steps 3:

Create a column of target numbers.
Idea is to create a new column, which will only have those numbers which were using the tower for making or receiving calls.

Insert a new column. Name it as – "Target numbers".

- Sort the column "Call Type".
- Copy all A_numbers into the "Target numbers" column for outgoing calls/sms.
- Copy all B Numbers into the "Target Numbers" column for incoming calls/sms.

After performing this step, the tower dump should look like the Screen shot shown in figure.

Figure showing Illustration of step 3

Fig.5.35: Multiple Tower Dumps Analysis-II

Step 4:

Create a Pivot Table

Note Please refer to the earlier section about how to create a Pivot Table.

After creating the pivot table, the tower dump looks like as shown in Figure 2.113

Figure showing illustration of Step 4

Step 5:

Drag Target number into Row label.

Figure showing illustration of step 5

It can be seen that all the target numbers are arranged row-wise.

Fig.5.36: Multiple Tower Dumps Analysis-III

Step 6:

Drag First Cell ID into Column Label

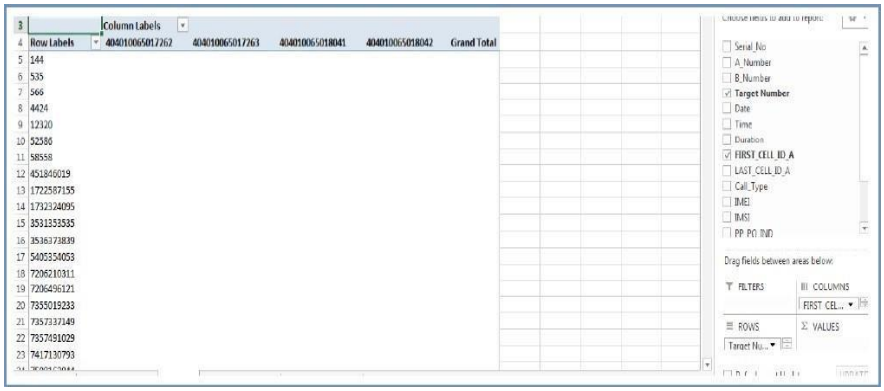


Illustration of step 6 of Tower Dump Analysis

It is seen here that all the Tower IDs included are arranged column wise.

Step 7:

Drag any field into the values field and take a count.

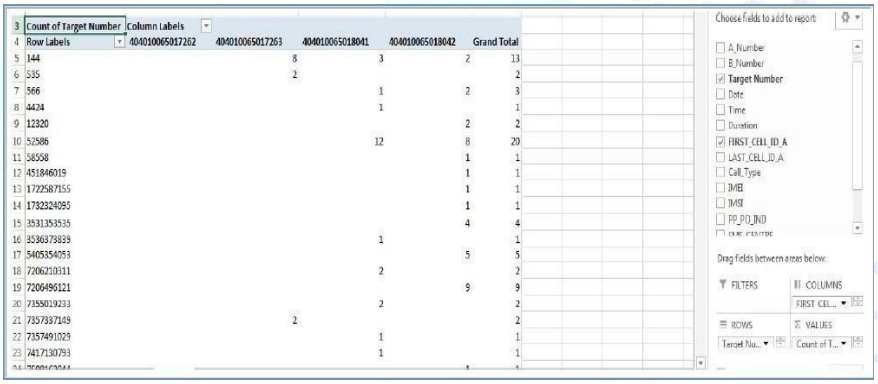
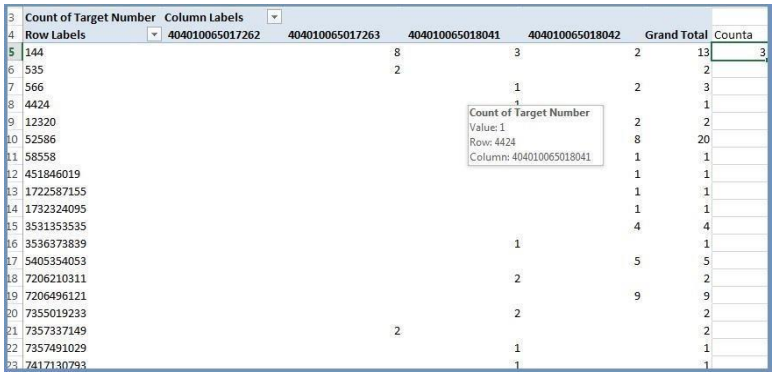


Illustration of Step 7

Fig.5.37: Multiple Tower Dumps Analysis-IV

Step 8:

Use 'Counta' function. Counta is used to find out the count of towers which the mobile number was communicating with.



Count of Target Number	Column Labels				
Row Labels	404010065017262	404010065017263	404010065018041	404010065018042	Grand Total	Counta
144		8	3	2	13	3
535		2			2	
566			1	2	3	
4424			1		1	
12320				2	2	
52586				8	20	
58558				1	1	
451846019				1	1	
1722587155				1	1	
1732324095				1	1	
3531353535				4	4	
3536373839			1		1	
5405354053				5	5	
7206210311			2		2	
7206496121				9	9	
7355019233			2		2	
7357337149		2			2	
7357491029			1		1	
7417130793			1		1	

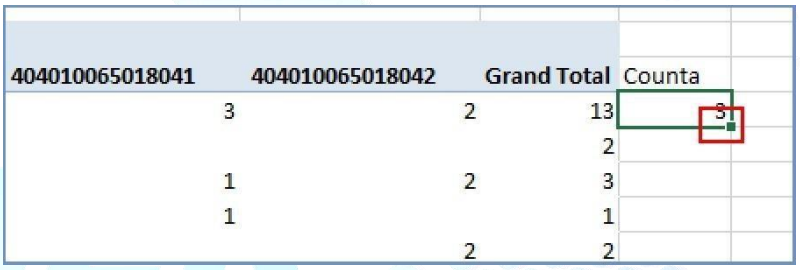
Count of Target Number
Value: 1
Row: 4424
Column: 404010065018041

Figure 2.11: Screenshot showing illustration of Step 8

It is given after the Counta function is executed that, out of 4 Tower IDs, number 144 was available in 3 Tower IDs.

Step 9:

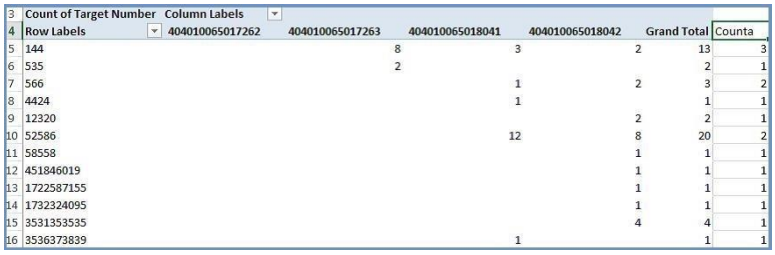
Copy the formula for all the Target numbers.



404010065018041	404010065018042	Grand Total	Counta
3	2	13	3
		2	
1	2	3	
1		1	
		2	2

Illustration of Step 9

Double click on the bottom right corner of the first cell under the column 'Counta'.



Count of Target Number	Column Labels				
Row Labels	404010065017262	404010065017263	404010065018041	404010065018042	Grand Total	Counta
144		8	3	2	13	3
535		2			2	1
566			1	2	3	2
4424			1		1	1
12320				2	2	1
52586			12	8	20	2
58558				1	1	1
451846019				1	1	1
1722587155				1	1	1
1732324095				1	1	1
3531353535				4	4	1
3536373839			1		1	1

Figure indicating action of click on Rectangle

Fig.5.38: Multiple Tower Dumps Analysis-V

Step 10:

Apply a filter on 'Counta' column. Select 'Counta' cell Go to Data -> click on Filter

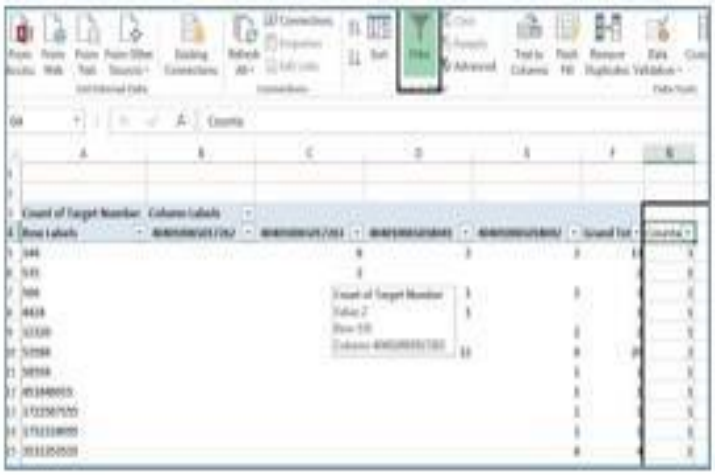


Illustration of step 10

Step 11:

Filter 'CountA' for all the numbers which are available in 3 or more than 2 towers.

Illustration of step 11

The above steps give a clear idea of how to perform tower dump analysis.

Fig.5.39: Multiple Tower Dumps Analysis-VI

5.11 IPDR Analysis

An IPDR is a record of all internet activity of mobile subscribers at one point in time when they are assigned some specific IP address. An IPDR can tell you a number

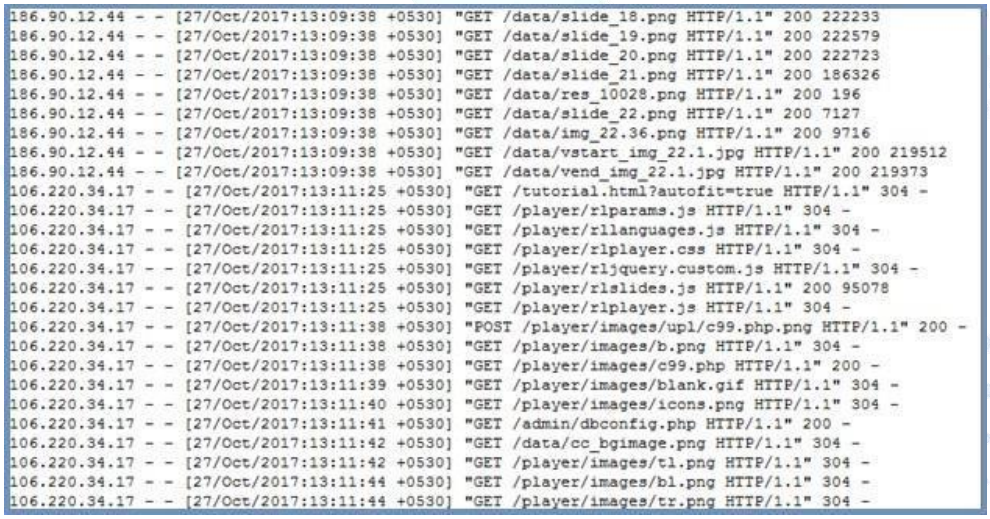
of things about your incoming and outgoing network traffic like Source and Destination IP Address, Time of access, source and destination ports, and also the Mobile number to which the IP Address was assigned.

Every website a user visit keeps a record of the IP address of the user who visited. If some website gets hacked, the victim can provide the Logs of the website to Law Enforcement Agencies who will then find out the ISP. If the ISP belongs to a Mobile Service Provider, the LEA will request for the IPDR of that IP for that date and time.

Consider the following scenario:

- A website luna.carawebs.com was allegedly hacked on 27th October 2017 at around
- 1:10-1:20 pm and was reported by the owner.

- The Cyber Cell requests for the Access Logs of the website from the person-in-charge of maintaining the logs of luna.carawebs.com and receives it which is as follows:



```
186.90.12.44 - - [27/Oct/2017:13:09:38 +0530] "GET /data/slide_18.png HTTP/1.1" 200 222233
186.90.12.44 - - [27/Oct/2017:13:09:38 +0530] "GET /data/slide_19.png HTTP/1.1" 200 222579
186.90.12.44 - - [27/Oct/2017:13:09:38 +0530] "GET /data/slide_20.png HTTP/1.1" 200 222723
186.90.12.44 - - [27/Oct/2017:13:09:38 +0530] "GET /data/slide_21.png HTTP/1.1" 200 186326
186.90.12.44 - - [27/Oct/2017:13:09:38 +0530] "GET /data/res_10028.png HTTP/1.1" 200 196
186.90.12.44 - - [27/Oct/2017:13:09:38 +0530] "GET /data/slide_22.png HTTP/1.1" 200 7127
186.90.12.44 - - [27/Oct/2017:13:09:38 +0530] "GET /data/img_22.36.png HTTP/1.1" 200 9716
186.90.12.44 - - [27/Oct/2017:13:09:38 +0530] "GET /data/vstart_img_22.1.jpg HTTP/1.1" 200 219512
186.90.12.44 - - [27/Oct/2017:13:09:38 +0530] "GET /data/vend_img_22.1.jpg HTTP/1.1" 200 219373
106.220.34.17 - - [27/Oct/2017:13:11:25 +0530] "GET /tutorial.html?autofit=true HTTP/1.1" 304 -
106.220.34.17 - - [27/Oct/2017:13:11:25 +0530] "GET /player/rlparams.js HTTP/1.1" 304 -
106.220.34.17 - - [27/Oct/2017:13:11:25 +0530] "GET /player/rllanguages.js HTTP/1.1" 304 -
106.220.34.17 - - [27/Oct/2017:13:11:25 +0530] "GET /player/rlplayer.css HTTP/1.1" 304 -
106.220.34.17 - - [27/Oct/2017:13:11:25 +0530] "GET /player/rljquery.custom.js HTTP/1.1" 304 -
106.220.34.17 - - [27/Oct/2017:13:11:25 +0530] "GET /player/rlslides.js HTTP/1.1" 200 95078
106.220.34.17 - - [27/Oct/2017:13:11:25 +0530] "GET /player/rlplayer.js HTTP/1.1" 304 -
106.220.34.17 - - [27/Oct/2017:13:11:38 +0530] "POST /player/images/upl/c99.php.png HTTP/1.1" 200 -
106.220.34.17 - - [27/Oct/2017:13:11:38 +0530] "GET /player/images/b.png HTTP/1.1" 304 -
106.220.34.17 - - [27/Oct/2017:13:11:38 +0530] "GET /player/images/c99.php HTTP/1.1" 200 -
106.220.34.17 - - [27/Oct/2017:13:11:39 +0530] "GET /player/images/blank.gif HTTP/1.1" 304 -
106.220.34.17 - - [27/Oct/2017:13:11:40 +0530] "GET /player/images/icons.png HTTP/1.1" 304 -
106.220.34.17 - - [27/Oct/2017:13:11:41 +0530] "GET /admin/dbconfig.php HTTP/1.1" 200 -
106.220.34.17 - - [27/Oct/2017:13:11:42 +0530] "GET /data/cc_bgimage.png HTTP/1.1" 304 -
106.220.34.17 - - [27/Oct/2017:13:11:42 +0530] "GET /player/images/tl.png HTTP/1.1" 304 -
106.220.34.17 - - [27/Oct/2017:13:11:44 +0530] "GET /player/images/bl.png HTTP/1.1" 304 -
106.220.34.17 - - [27/Oct/2017:13:11:44 +0530] "GET /player/images/tr.png HTTP/1.1" 304 -
```

Fig.5.40: Sample Access Log of a Website

In the above screenshot of the Access Logs from the Website Administrator, an instance of uploading a file can be seen from the IP 106.220.34.17, and then later again the user with the IP Address 106.220.34.17 is accessing a file from the "admin" directory.

Having the input from the complainant that the site was hacked around 1:10-1:20 pm, we can find only this IP in the log with multiple requests to the website. This IP can be noted down as suspicious.

- Next, find out the Service Provider of the IP noted.
- Perform a WHOIS IP lookup of that IP address found in the access logs.

There are many websites to perform WHOIS lookup. Here we are going to use one such website, namely whois.domaintools.com to find out details of

suspected IP address, copy the IP address and Go to whois.domaintools.com and paste the IP address, it will show the ISP to which it belongs to, as shown in the figure below:

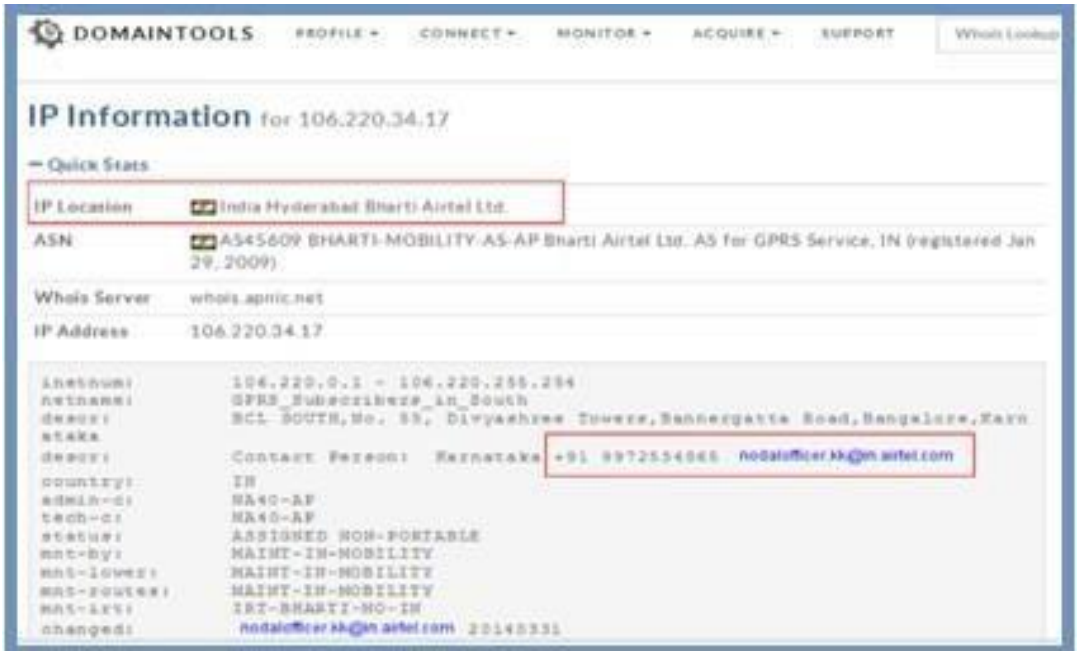


Fig.5.41: ISP information of a particular IP address

From the above figure, it is found that the IP address belongs to Bharti Airtel Ltd.

Here, the email address and mobile number of the concerned person will be available who will assist in contacting the respective nodal officer who is authorized to provide

Required details to Law Enforcement Agencies.

Then record the IP address, date to request IPDR for further investigation. Request the IPDR of the above-mentioned IP address for the said date and time from the respective Nodal Officer. The format of mailing the Nodal officer is as follows:

To: Airtel-Nodal
Subject: Re: CID - Cyber Crime PS-Request for IPDR details of IP address

Sir,
It is requested to furnish the IPDR details of the following IP Address for the purpose of investigation.

Date	Time	IP Address
27-10-2017	13:11:38	106.220.34.17

Early action will be highly appreciated.

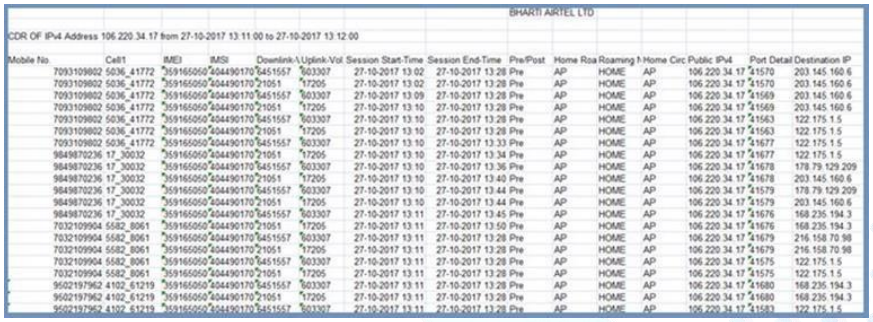
Superintendent of Police,
Cyber Crimes, CID.
Hyderabad.
#040-23316750
"THE CYBER SPACE, SAFE TO USE UNSAFE TO MISUSE"

Fig.5.42: Format of mail to a nodal officer.

As there is a limited pool of IP address assigned to a Service Provider, they make use of the concept of Network Address Translation (NAT) to share one Public IP address with many subscribers. For this reason, in the case of requesting end-user particulars of the Mobile IP, the service providers cannot determine one specific user, and hence provide a complete IPDR of that IP for a period of 1-5 mins which contains details of all the subscribers which were assigned the requested IP address for a period of time. You will receive the IPDR from the Nodal officer as shown below.

Fig.5.43: Format in which IPDR is received from Nodal Officer.

Open the IPDR and check if it was provided for the right date and time



BHARTI AIRTEL LTD

CDR OF IPv4 Address 106.220.34.17 from 27-10-2017 13:11:00 to 27-10-2017 13:12:00

Mobile No	Cell1	IMEI	IMSI	Downlink-V	Uplink-Vol	Session Start-Time	Session End-Time	Pre/Post	Home Roa	Roaming N	Home Circ	Public IPv4	Port Detail	Destination IP
	7093109802	5036_41772	359165050	404490170	5451557	303307	27-10-2017 13:02	27-10-2017 13:28	Pre	AP	HOME	AP	106.220.34.17	41570	203.145.160.6
	7093109802	5036_41772	359165050	404490170	21051	17205	27-10-2017 13:02	27-10-2017 13:28	Pre	AP	HOME	AP	106.220.34.17	41570	203.145.160.6
	7093109802	5036_41772	359165050	404490170	5451557	303307	27-10-2017 13:09	27-10-2017 13:28	Pre	AP	HOME	AP	106.220.34.17	41569	203.145.160.6
	7093109802	5036_41772	359165050	404490170	21051	17205	27-10-2017 13:10	27-10-2017 13:28	Pre	AP	HOME	AP	106.220.34.17	41569	203.145.160.6
	7093109802	5036_41772	359165050	404490170	5451557	303307	27-10-2017 13:10	27-10-2017 13:28	Pre	AP	HOME	AP	106.220.34.17	41563	122.175.1.5
	7093109802	5036_41772	359165050	404490170	21051	17205	27-10-2017 13:10	27-10-2017 13:28	Pre	AP	HOME	AP	106.220.34.17	41563	122.175.1.5
	7093109802	5036_41772	359165050	404490170	5451557	303307	27-10-2017 13:10	27-10-2017 13:33	Pre	AP	HOME	AP	106.220.34.17	41677	122.175.1.5
	9849870236	17_30032	359165050	404490170	21051	17205	27-10-2017 13:10	27-10-2017 13:34	Pre	AP	HOME	AP	106.220.34.17	41677	122.175.1.5
	9849870236	17_30032	359165050	404490170	5451557	303307	27-10-2017 13:10	27-10-2017 13:36	Pre	AP	HOME	AP	106.220.34.17	41678	178.79.129.209
	9849870236	17_30032	359165050	404490170	21051	17205	27-10-2017 13:10	27-10-2017 13:40	Pre	AP	HOME	AP	106.220.34.17	41678	203.145.160.6
	9849870236	17_30032	359165050	404490170	5451557	303307	27-10-2017 13:10	27-10-2017 13:44	Pre	AP	HOME	AP	106.220.34.17	41579	178.79.129.209
	9849870236	17_30032	359165050	404490170	21051	17205	27-10-2017 13:10	27-10-2017 13:44	Pre	AP	HOME	AP	106.220.34.17	41579	203.145.160.6
	9849870236	17_30032	359165050	404490170	5451557	303307	27-10-2017 13:11	27-10-2017 13:45	Pre	AP	HOME	AP	106.220.34.17	41676	168.235.194.3
	7032109904	5582_8061	359165050	404490170	21051	17205	27-10-2017 13:11	27-10-2017 13:50	Pre	AP	HOME	AP	106.220.34.17	41676	168.235.194.3
	7032109904	5582_8061	359165050	404490170	5451557	303307	27-10-2017 13:11	27-10-2017 13:28	Pre	AP	HOME	AP	106.220.34.17	41679	216.158.70.98
	7032109904	5582_8061	359165050	404490170	21051	17205	27-10-2017 13:11	27-10-2017 13:28	Pre	AP	HOME	AP	106.220.34.17	41679	216.158.70.98
	7032109904	5582_8061	359165050	404490170	5451557	303307	27-10-2017 13:11	27-10-2017 13:28	Pre	AP	HOME	AP	106.220.34.17	41575	122.175.1.5
	7032109904	5582_8061	359165050	404490170	21051	17205	27-10-2017 13:11	27-10-2017 13:28	Pre	AP	HOME	AP	106.220.34.17	41575	122.175.1.5
	9502197962	4102_61219	359165050	404490170	5451557	303307	27-10-2017 13:11	27-10-2017 13:28	Pre	AP	HOME	AP	106.220.34.17	41680	168.235.194.3
	9502197962	4102_61219	359165050	404490170	21051	17205	27-10-2017 13:11	27-10-2017 13:28	Pre	AP	HOME	AP	106.220.34.17	41680	168.235.194.3
	9502197962	4102_61219	359165050	404490170	5451557	303307	27-10-2017 13:11	27-10-2017 13:28	Pre	AP	HOME	AP	106.220.34.17	41583	122.175.1.5

Fig.5.43: Sample IPDR to check Date and Time.

The above figure shows the IPDR of the required date and time with a range of 1 minute. Hence, this IPDR is relevant and we can start analyzing this.

Step 1:

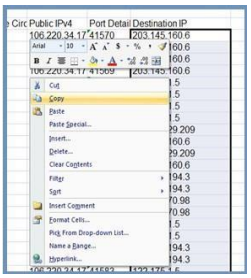
Identify the services/websites accessed by the subscribers from the "Destination IP" column.

Step 2:

A manual WHOIS lookup for every IP can be done, but to make it quick you can perform "Bulk IP lookup". There are so many websites on the internet which provide this service. One popular website is infobyip.com

Step 3:

Copy all the IP addresses from the "Destination IP" column.



Illustrating Step 3

Step 4:

Go to infobyip.com/ipbulklookup.php and paste all the copied IP addresses in the box, and click on "lookup" as follows:

Illustrating Step 4

Fig.5.44: IPDR Analysis - 1

Step 5:

The list of services/websites hosted on the IP addresses will be displayed.

IP	Domain	Country	Region	City	ISP	ASN
203.145.160.6	abts-tn-dynamic-006.160.145.203.airtelbroadband.in	India	07		Bharti Airtel Ltd., Telemedia Services	AS24560
203.145.160.6	abts-tn-dynamic-006.160.145.203.airtelbroadband.in	India	07		Bharti Airtel Ltd., Telemedia Services	AS24560
203.145.160.6	abts-tn-dynamic-006.160.145.203.airtelbroadband.in	India	07		Bharti Airtel Ltd., Telemedia Services	AS24560
203.145.160.6	abts-tn-dynamic-006.160.145.203.airtelbroadband.in	India	07		Bharti Airtel Ltd., Telemedia Services	AS24560
122.175.1.5	telemedia-ap-static-005.1.175.122.airtelbroadband.in	India	00	Chandanagar	Bharti Airtel Ltd., Telemedia Services	AS24560
122.175.1.5	telemedia-ap-static-005.1.175.122.airtelbroadband.in	India	00	Chandanagar	Bharti Airtel Ltd., Telemedia Services	AS24560
122.175.1.5	telemedia-ap-static-005.1.175.122.airtelbroadband.in	India	00	Chandanagar	Bharti Airtel Ltd., Telemedia Services	AS24560
122.175.1.5	telemedia-ap-static-005.1.175.122.airtelbroadband.in	India	00	Chandanagar	Bharti Airtel Ltd., Telemedia Services	AS24560
178.79.129.209	luna.carawebs.com	United Kingdom	H9	London	Linode, LLC	AS63949
203.145.160.6	abts-tn-dynamic-006.160.145.203.airtelbroadband.in	India	07		Bharti Airtel Ltd., Telemedia Services	AS24560
178.79.129.209	luna.carawebs.com	United Kingdom	H9	London	Linode, LLC	AS63949
203.145.160.6	abts-tn-dynamic-006.160.145.203.airtelbroadband.in	India	07		Bharti Airtel Ltd., Telemedia Services	AS24560

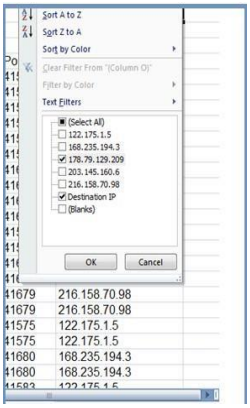
Figure 2.124: Screenshot Illustrating Step 5

Step 6:

From the above list, identify the IP addresses belonging to the victim's website. As seen in the figure, 178.79.129.209 belongs to the victim's website luna.carawebs.com. Note it down.

Step 7:

Apply filter on "DestinationIP" column to see only the subscribers who were accessing 178.79.129.209 as shown below:



Illustrating Step 7

Fig.5.45: IPDR Analysis - 2

Step 8:

You can then see only the list of subscribers who were accessing the victim's website.

Figure showing list of subscribers.

Step 9:

From the above figure it is clear that there was only one subscriber who was accessing the victim's website and was using the mobile number 984970xxxx to commit the offense.

Note: GPRS may have the same investigation (using the destination IP)

Fig.5.46: IPDR analysis - 3

Once the Mobile number is identified an IO can then request CDR or SDR and CAF for the same number and can analyse suspect's behaviour. In certain cases, the IP address can be of a broadband connection (ISP) in which case the IO can request the subscriber details such as his name, address and

contact number if any from the ISP directly. From then onwards usual investigation techniques can be used by the IO to solve the case.

5.12 VOIP (Voice Over IP)

VoIP (voice over IP) is the transmission of voice and multimedia content over Internet Protocol (IP) networks. In simplest term, it is the use of a telephone over the internet network. VoIP is commonly used nowadays as it is reasonably cheaper compared to that of the traditional resource (traditional phone calls) as the single network is used to carry voice and data traffic rather than having to use two different networks. A lot of applications and mobile networks now use VoIP services for their use. Following is a list of few software applications that use VoIP for their services:

1. Skype

   With Skype, you can make calls to another Skype user for free. It also lets you call conventional phones for very low rates. The best feature of the Skype, which makes it better than other apps in its class, is its Video chat and video conference options. Although many other apps also offer these features, none is as effective as Skype.

2. Facebook Messenger

   Facebook messenger is one of the few apps which lets you communicate with another user for free. It is offering text, voice message recordings, HD calls, snap photos and videos, stickers, group chats, and now even video calling for free.

3. Whatsapp
   Whatsapp lets users communicate with another WhatsApp user using their mobile number (their MSISDN) for simple and multimedia text messaging, audio recordings, file sharing, HD audio and video calls for free.

Primarily these three apps are used extensively and are closely followed by their competitors such as Viber, Line, Telegram, Google Duo and Tango supporting similar features.

These apps when used by the user create a lot of artefacts which are available on the device which was used by the user. Hence it is important to do a proper seizure of the devices from the scene of a crime. VoIP traffic can be identified from an IPDR or GPRS dump.

i) A VoIP session invitation is sent to a client by the user to participate either in a call or any other VoIP related services.
ii) The client then acknowledges that they have received an invite request.

- Step – 2 Information transfer

i) Once the connection is established and necessary acknowledgement has received the transfer of information can start. (That is when a user accepts a call or opens a message he can then start communicating or download the content that is being transferred.)
ii) The transfer of information continues as long as the session is active once either of the users indicates to terminate the session (user wants to end the call, or the message is downloaded/uploaded completely) the session can be terminated.

- Step – 3 Connection Termination

i) Cancel request is used to stop any pending request.

- Step – 4 Record Transaction

i) The details of this transaction are then registered by service providers of both the client and the other user.

5.12.2 VoIP analysis

VoIP analysis can be done at different levels using different methods as indicated below.

i) Real-time raw data decoding and reconstruction:
This is possible by intersecting the traffic between an active VoIP session. This method is also known as the Man in The Middle (MITM) attack. By this method, HTTPS/SSL traffic needs to be reconstructed for analysing the real-time data.
ii) Logs/Trace evidence to the network communication:
In this method with the help of network logs such as CDRs, IPDRs web addresses and IP addresses can be analysed to get routing information of the communication.
iii) Decode endpoint devices
Once the device is seized use the device for examining the artefacts. Analyse fragments of chats, time, duration and any traffic on ports.

VoIP can use different servers for the communication to happen, they may use proxy servers, redirect servers, registrar servers and location servers

for this purpose it is important to examine the IP addresses that are available in the logs. Below is a sample of VoIP log.

```
INVITE sip:1006@10.100.13.139:5060 SIP/2.0
Via: SIP/2.0/UDP 10.100.12.230:56727;
branch=z9hG4bK-d8754z-ae78c05f8f58042a-1--
-d8754z-;rport
Max-Forwards: 70
Contact: <sip:1004@10.100.12.230:56727;
rinstance=a8c18539cb50ec97>
To: <sip:1006@10.100.13.139:7020>
From: <sip:1004@10.100.13.255:5060>;tag=f11afe5a
Call-ID: M2JhYjBjMGRkYzQzNTA2ZmFm
YWU4MzViN2NiOTVlMTA.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE,
REGISTER, SUBSCRIBE,
NOTIFY, REFER, INFO, MESSAGE
Content-Type: application/sdp, Supported: replaces
User-Agent: 3CXPhone 4.0.13679.0
```

Fig.5.47: sample VoIP Log

Following are few special interests for CDR on VoIP communications:

1. WhatsApp runs over the SSL TCP/443 and uses 4244, 5222, 5223, 5228, 5242 50318, and 59234.

2. Skype uses port number 32535 for all incoming connections and 40031 for all outgoing connections by default.

3. Communication on TCP Port 5222 is generally done by ICQ based messengers.

5.13 Search and seizure of Mobiles/Tablets

5.13.1 Acceptable operating procedures

i) <u>Isolation</u>

Improper handling of a mobile device during seizure may cause loss of digital data. If the device is not handled properly, physical evidences may be contaminated and rendered useless. So, we need to secure and evaluate the scene of crime before acquiring a communication device and all areas of the scene should be searched thoroughly ensuring related evidence is not overlooked. Isolating the mobile/tablet device from other devices used for data synchronization is important to keep new data from contaminating existing data. Equipment's associated with a mobile device, such as removable media, SIM cards and personal computers, may prove more valuable than the mobile device itself. Removable media varies in size and can be easily hidden and difficult to find. Personal computers may be particularly useful in later accessing a locked mobile device, if it has established a trusted relationship with the mobile device. For example,

Apple incorporates a pairing process whereby an existing pairing record file can be used by some tools to access the mobile device. When interviewing the owner or user of a mobile device, consider requesting any security codes, passwords or gestures needed to gain access to its contents. For example, a GSM device may have authentication codes set for the internal memory and/or the SIM card.

Many mobile devices offer the user ability to perform either a remote lock or remote wipe by simply sending a command (e.g., text message) to the mobile device. In order to protect that we have to isolate the phone from all the radio signals it was bounded from it. Additional reasons for disabling network connectivity include incoming data (e.g., calls or text messages) that may modify the current state of the data stored on the mobile device.

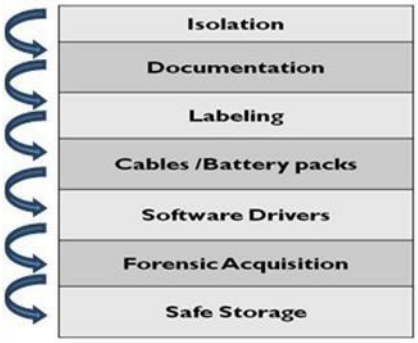


Fig.5.48: Illustration of step by step process of mobiles/tablets search and Seizure

There are few ways to isolate any mobile device. Each method has certain drawbacks:

- **Airplane Mode (Only for Smartphone's):** Requires interaction with the mobile device using the keypad, which poses some risk. The technician should be familiar with the device in question and documents the actions taken (e.g., on paper or on video). Note: airplane mode does not prevent the system from using other services such as GPS in all cases.
- **Faraday Bags (feature phones):** Faraday containers may attenuate the radio signal, but not necessarily eliminate it completely .The risk of improperly sealing the Faraday container must be avoided.
- **Switch the device off**: Turning off the mobile device may activate authentication codes like PIN's and passwords which in turn takes time to break and delays the acqui- sition and analysis.
- **Use Cloned SIM Cards**: A forensic examiner clone original SIM cards to mimic the identity of them, and prevents network access to/from the handset. We call such cards as CNIC or Cellular network isolation card. Such cards also prevent the handset in erasing call logs data when a unknown/foreign SIM is inserted. If the SIM for a device is present, but requires a PUK

code, a substitute SIM can be created providing acquisition to proceed without having to contact the service provider for the PUK. The values by which the mobile device correlates to the previously inserted SIM are the ICCID and the IMSI, both of them are unique and used to authenticate the user with the network. Isolation is done to all mobile/ communication devices to avoid Accidental access from the IO and to prevent remote wiping. Various mobile phone shielding devices (i.e., a tool designed to act as a Faraday cage) are used by law enforcement agencies prevent network communication to the seized devices. Examiners should test their own products to validate that they are working properly before use.

ii) Documentation

Documenting every piece of electronic evidence with its serial number, make and model number properly in "seizure panchnama" along with photographs of Scene of Crime. Non-electronic materials such as invoices, manuals, and packaging material may provide useful information about the capabilities of the device, the network used, account information, and unlocking codes for the PIN. All digital devices, including mobile devices, which may store data, should be photographed along with all peripherals cables, power connectors, removable media, and connections. Make sure that correct placement of SIM Cards and other equipment's are properly mentioned. If the device's display is in a viewable state, the screen's contents should be photographed and, if necessary, recorded manually, capturing the time, service status, battery level, and other displayed icons.

iii) Labelling

Label all collected pieces of evidence at scene of crime so as to ensure proper chain of custody for every evidence article. All digital devices, including mobile devices, which may store data, should be labelled along with all peripherals cables, power connectors, removable media, and connections. Mobile devices need to be identified by the make, model, and service provider before it is labelled. If the mobile device is not identifiable, photographing the front, back and sides of the device may be useful in identifying the make, model and current state (e.g., screen lock) at a later time.

iv) Further means of identification

- Device Characteristics: The make and manufacturer of a mobile device may be identified by its observable characteristics (e.g., weight, dimensions, and form factor).

- Device Interface: The power connector can be specific to a manufacturer and may provide clues for device identification. With familiarization and experience, the manufacturers of certain mobile devices may be readily identified. Based on the size, number of contacts, and shape of the data cable interface are often specific to particular manufacturer and may prove helpful in identification.

- Device Label: The International Mobile Equipment Identity or IMEI is a number, usually unique, to identify mobile phones, as well as some satellite phones. It is usually found printed inside the battery compartment of the phone, but can also be displayed on-screen on most phones by entering *#06# on the dial pad. The IMEI number is a 15 decimal digits number (14 digits plus a check digit). The model and origin comprise the initial 8-digit portion of the IMEI/SV, known as the Type Allocation Code (TAC). The remainder of the IMEI is manufacturer-defined, with a Luhn check digit at the end.

We can check the IMEI of any android phone in the about option directly if we have access. The screenshot is shared below.

Fig.5.49: Checking of IMEI of an android phone

It can also be found on the back panel by removing the battery for few of the phones.

Fig.5.50: IMEI inside a phone.

Various sites on the Internet offer databases that provide information about the mobile device based on an identifier, such as:

- www.numberingplans.com
- http://Imei.info
- https://imeidata.net

v) Cable Battery Pack & Software Drivers

Collection of all proprietary attachments along with the device helps forensic examiners on easy access to device during acquisition. It's a good practice to collect or search for software drivers available at scene of crime for the device seized.

5.14 Mobile Forensics

Mobile forensics is a branch of digital forensics related to the recovery of the digital evidence from the mobile devices. Forensically sound is a term used extensively in the digital forensics community to qualify and justify the use of a particular forensic technology or methodology. The main principle for a sound forensic examination of digital evidence is that the original evidence must not be modified. This is extremely difficult with mobile devices. Some forensic tools require a communication vector with the mobile device, thus standard write-block protection will not work during forensic acquisition. Other forensic acquisition methods may involve removing a chip or installing a bootloader on the mobile device prior to extracting data for forensic examination.

In cases where the examination or data acquisition is not possible without changing the configuration of the device, the procedure and the changes must be tested, validated, and documented. Following a proper methodology and guidelines is very crucial in examining the mobile devices as it yields the most valuable data. As with any evidence gathering, not following the proper procedures during the examination can result in loss or damage of the evidence or render it inadmissible in the court.

The mobile forensics process is broken into three main categories: **seizure**, **acquisition**, and **examination/analysis.** If the phone is locked by a PIN or a password or is encrypted, the examiner will be required to bypass the lock or determine the PIN to access the device. Mobile phones are networked devices and can send and receive data from different sources, such as telecommunication network (mobile network), Wi-Fi access points, and Bluetooth. So, if the phone is in a running state, a criminal can securely erase the data stored on the phone by executing a remote wipe command.

Mobile device forensic acquisition can be performed using multiple methods, which are defined later. Each of these methods affects the amount of analysis required, which will be discussed in greater detail in the upcoming chapters. Should one method fail, another must be attempted. Multiple attempts and tools may be necessary in order to acquire the most data from the mobile device.

Mobile phones are dynamic systems that present a lot of challenges to the examiner in extracting and analysing digital evidence. The rapid increase in the number of different kinds of mobile phones from different manufacturers makes it difficult to develop a single process or a tool to examine all types of devices. Mobile phones are continuously evolving as existing technologies progress and new technologies are introduced. Furthermore, each mobile is designed with a variety of embedded operating systems. Hence, special knowledge and skills are required from forensic experts to acquire and analyse the devices.

5.14.1 Forensics Acquisition

Forensic Acquisition can be done by IO or Forensic Examiner at crime scene itself or Forensic Science Laboratory. There are various techniques for acquisition like logical, physical etc that are discussed in this document. The type of mobile device and data to be extracted generally dictates which tools and techniques should be used in an investigation. The classification system used in this section provides a framework for forensic examiners to compare the extraction methods used by different tools available in the market today to acquire data. This comparison is only to understand the difference between the methods. Nowadays all forensic tools support extraction either wired (USB, RS232) or wireless (IrDA, Bluetooth and WIFI) connection.

1. **Screen Captures**: Use a camera to take pictures of what's on the screen. Sometimes this is the only way. Formally, we call this method as manual extraction method. In this extraction, it is impossible to recover deleted information. Some tools have been developed to provide the forensic examiner with the ability to document and categorize the information recorded more quickly. Nevertheless, if there is a large amount of data to be captured, a manual extraction can be very time consuming and the data on the device may be inadvertently modified, deleted or overwritten as a result of the examination. Manual extractions become increasingly difficult and perhaps unachievable when encountering a broken/ missing LCD screen or a damaged/missing keyboard interface or device is configured with foreign language unknown to the examiner.

2. **Logical Extraction**: – Extracting the data on the device that we see and can access on the device. Call logs, phone books, SMS messages, pictures, email, browsing etc

3. **Physical Extraction or Hex Dumping**: – Extracting data from the physical memory of the device, and removable memory – raw data. This raw data or raw dump stored in flash memory or NAND flash is extracted into an external drive as a raw image or binary image (usually in .bin format). We also call this method as Hex dumping. Physical analysis is the way to recover deleted information, as it gives the examiner a physical view in hex format and provides the ability to logically view the entire image in a categorical fashion after parsing. But it is difficult and sparsely supported by any forensic tool. This technique involves uploading a modified boot loader (or other software) into a protected area of memory (e.g., RAM) on the device.

This upload process is accomplished by connecting the mobile device's data port to a flasher box or a forensic tool like UFED and XRY, and the forensic tool is in turn connected to the forensic workstation. A series of commands is sent from the forensic tool to the mobile device to place it in a diagnostic mode. Once in diagnostic mode, the tool captures all (or sections) of flash memory and sends it to the forensic workstation over the same communications link used for the upload. Some tools work this way, or they may use a proprietary interface for memory extractions and also extracts the data into proprietary format.

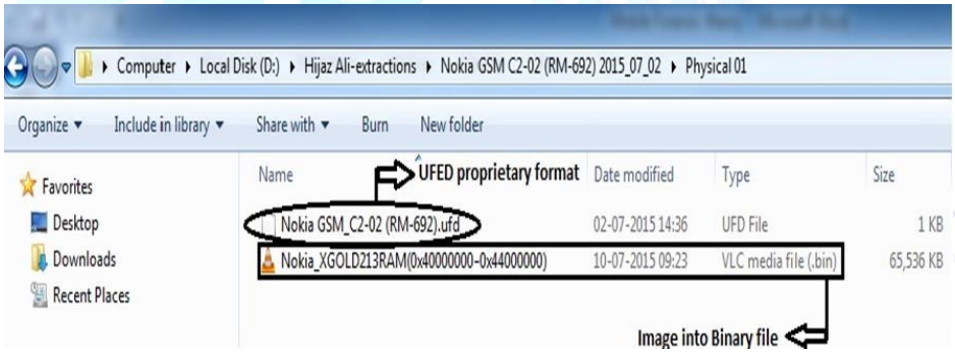


Fig.5.51: Image acquisition using UFED

Physical extraction is also called as JTAG extraction (Joint Test Action Group) which is a common test interface and has been a standard for many manufacturers. JTAG defines an interface to test processor, memory and other semi-conductor chips inside the handset. An examiner can communicate using special purpose programmer device to probe defined test points and acquire image out of locked or devices that have minor damages where we cannot use data ports properly. The only difference between Physical extraction and JTAGging (called informally) is we have to dismantle the mobile device to obtain access through wiring connections. All these physical acquisitions are made with the help of

flasher boxes. The graphic below depicts the screenshot of UFED's physical extraction into binary file.

4. **File System Extraction**: – Extracting data from the directory structure of the device, i.e., it may work on file system and retrieve data like hidden-files, deleted data sometimes. Many recent tools like UFED are involving these techniques into their tools due to diversity of mobile operating systems developed (e.g., Android based devices). File system extraction allows an examiner to view the file structure of the device operated under the device in a directory and sub-directory manner.

a) What if your device (SIM & Handset) is damaged?

The handset obtained at Scene of Crime is damaged by one of the following reasons like:

- Explosion
- Fire
- Water
- Acid/Chemical Reaction etc.

We need to look data into the silicon chip (Either BGA or TSOP chip) embedded on the board of the handset. It can be done only be heating or by chemical treatment. We call this method as Chip removal method.

CHIP-OFF: These extractions require physical removal of flash memory from the handset and perform the acquisition. Once it is removed from the handset, image is taken from the contiguous memory location into binary form and it will be analysed later. It absolutely replicates the same process of imaging a hard drive in our traditional forensics. Due to the risks involved in chip-off extractions (like we are unable to rearrange the chip on to the memory again after removal in our forensic laboratories) JTAG extractions more preferred. Forensic examiner also performs methods like Micro-Read in which recording of the physical observation of gates on NAND and NOR chips is done with the help of microscope. This is done only when we can't image a flash memory using Chip-off method. This method is applied only for high-profile cases like national security. Currently there are no proprietary tools to do such type of extractions which require team of qualified experts, proper equipment and in-depth knowledge in the domain as well as case.

Safe Storage: All the isolated devices which are seized should be properly packed in a bubble wrap or with any material that won't damage the evidentiary value of the device. Due to the volatile nature of some mobile devices, they should immediately be sent to a forensic laboratory for processing and the power requirements should be discussed with the evidence custodian. We can carry power banks with us while acquiring the

device to equip them with enough power until they reach the laboratory. All evidence should be in sealed containers in a secure area with controlled access.

Precautions followed during data acquisitions at SOC:

1. Handle phones properly so as to maintain the fingerprints if any.
2. Turn of the device wireless capabilities (i.e put the phone in airplane mode) so that unwanted interaction can be stopped.
3. Take photos of the crime scene which include cradles, cell phones, wires, connectors, etc.
4. If the phone is compromised (i.e. immersed in liquid), remove the battery and then seal it in a bag along with the liquid in which it was immersed. (Both separately packed)
5. Search for papers, sticky-notes, diaries and any other evidences which may give out passwords or other vital information.
6. Label all the wires, connectors and devices and bag them with evidence.
7. Make sure to fill the chain of custody forms for each evidence item that is being bagged.

5.15 Memory Types in Featured Mobile Handsets

Mobile devices contain both non-volatile and volatile memory. Volatile memory (i.e., RAM) is used for dynamic storage and its contents are lost when power is drained from the mobile device. Non-volatile memory is persistent as its contents are not affected by loss of power or overwriting data upon reboot. For example, solid-state drives (SSD) that stores persistent data on solid-state flash memory.

Mobile devices typically contain one or two different types of nonvolatile flash memory. These types are NAND and NOR. NOR flash has faster read times, slower write times than NAND and is nearly immune to corruption and bad blocks while allowing random access to any memory location. NAND flash offers higher memory storage capacities, is less stable and only allows sequential access.

Memory configurations among mobile devices have evolved over time. Feature phones were among the first types of devices that contained NOR flash and RAM memory. System and user data are stored in NOR and copied to RAM upon booting for faster code execution and access. This is known as the first generation of mobile device memory configurations.

As smartphones were introduced, memory configurations evolved, adding NAND flash memory. This arrangement of NOR, NAND and RAM memory is referred to as the second generation. This generation of memory configurations stores system files in NOR flash, user files in NAND and RAM is used for code execution.

The latest smartphones contain only NAND and RAM memory (i.e., third generation), due to requirements for higher transaction speed, greater storage density and lower cost. To facilitate the lack of space on mobile device mainboards and the demand for higher density storage space (i.e., 2GB – 128GB) the new Embedded MultiMedia Cards (eMMC) style chips are present in many of today's smartphones.

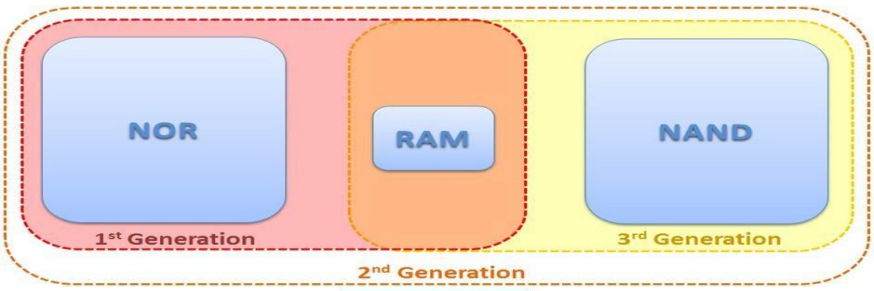


Fig.5.52: RAM Generations

RAM is the most difficult to capture accurately due to its volatile nature. Since RAM is typically used for program execution, information may be of value to the examiner (e.g., configuration files, passwords, etc.). Mobile device RAM capture tools are just beginning to become available.

NOR flash memory includes system data such as: operating system code, the kernel, device drivers, system libraries, memory for executing operating system applications and the storage of user application execution instructions. NOR flash will be the best location for data collection for first generation memory configuration devices.

NAND flash memory contains: PIM data, graphics, audio, video, and other user files. This type of memory generally provides the examiner with the most useful information in most cases. NAND flash memory may leave multiple copies of transaction-based files (e.g., databases and logs) due to wear levelling algorithms and garbage collection routines. Since NAND flash memory cells can be re-used for only a limited amount of time before they become unreliable, wear levelling algorithms are used to increase the life span of Flash memory storage, by arranging data so that erasures and re-writes are distributed evenly across the SSD.

Garbage collection occurs because NAND flash memory cannot overwrite existing data, the data must first be erased before writing to the same cell.

5.16 Analysis process:

Analysis process begins with examiner knowing about the case details and brief facts about the case he is going to investigate. Examination process involves taking the copy or image file of the mobile handset seized. This file is imported into various forensic tool kits to bring out the desirable artefacts found totally dependable on the type of case. We will see a different type of artefacts from different memory modules belongs to the mobile device.

Fig.5.53:Various Storage Locations in a Mobile Phone

Artefacts Collected from SIM:

SIM itself is a great piece of evidence.

- Usually name of the network provider is available or printed on the front face of the SIM and a unique identification number called as ICCID (Integrated Circuit Card ID) is printed on the rear side. This ICCID is a 20-bit number which is used to identify the manufacturer of the SIM.
- •Generally, a SIM can be locked with PIN (Personal Identification Number) providing security from unauthorized access. If a user tries to enter a PIN through three attempts, the card automatically gets locked.
- •This PIN can be bypassed, and SIM card can be accessed only by 8digit PUK (personal unblocking code) number which is fixed and kept by the network operator. Therefore, investigator can always access a SIM by asking its PUK number from the operator.
- •SIM card is having its own File system in which there is a directory structure defined. LOCI (Location Information), a file contains information about LAI (location area Identifier) which gives us info about mobiles current location.
- •This LAI info is retained in the SIM even when the cell phone / Mobile is switched off. A phone will store this LAI on its SIM card, so it knows what location it's in and to be able to receive service. If a phone were to change to a new Location Area, it stores the new LAI in the SIM card, adding to a list of all the previous LAIs it has been in.
- •It is possible for an investigator to determine in which location area the mobile was located when it was operating last time. All this Information can be extracted from the SIM extraction devices available with any mobile forensic tool (Ex: UFED, MPE).

Artefacts Collected from Mobile Phone and Memory Card:

- Contacts, Calls (dialled, missed, received)
- Text Messages (SMS) & Multimedia (MMS)
- Times / Dates
- Pictures, Audio and Video Images
- Tasks / Notes / Calendars
- Application Files
- Bluetooth Pairing
- Maps, GPS Locations
- E-mail, browser history, keyboard cache, bookmarks
- Smartphone 'App' data – Facebook, Skype, Gmail, WhatsApp etc….
- Usernames, passwords, personal and corporate sensitive data

Artefacts Collected from

Network provider: – Subscriber name and address

- Phone number associated with SIM
- Billing account details
- Telephone number (MSISDN)

- Tower Location (BTS Address) & Services allowed

Challenges in extraction of forensic evidence from communication devices:

- ❖ Hardware is getting complex day by day as technology is evolving which is a bigger challenge for forensic examiner to identify and extract the evidence.
- ❖ Flash Memory or Integrated Storage – no hard disks available to remove and copy.
- ❖ Huge diversity of Operating systems makes difficult to get support from the mobile phones forensic tools.
- ❖ It is difficult to find the boot loaders for all the variety of operating systems and mobile architectures. Hence physical extraction may not be possible always.
- ❖ No standard protocol for data extraction.
- ❖ Different Data Cables and Data Communication Ports.
- ❖ China Made Phones creates challenges with their wide variety of proprietary operating systems and chipsets like Mediatek, Spredtrum and infinium to name a few.
- ❖ All Chinese made phones don't support data transfer due to the proprietary made cables for accessory profit.
- ❖ New Smartphone 'Apps' create secondary layers of data and additional challenges also stores a set of data on the cloud.

Forensic tools:

Forensic tools are solutions available for acquiring, retrieving and preserving the evidence from wide variety of handsets. These tools are continuously updated and provide methods to extract data. There are some of the popular tools out of which Cellebrite-UFED, XRY, MPE+ are used by several federal agencies and forensic science laboratories.

Fig.5.54: Mobile forensics tools

- Pictures of the phone and individual components and labels with identifying information
- Status of the phone received
- Make, model and identifying information
- Tools used during analysis

6. Investigation of Financial Frauds

6.1 Types of financial frauds

a) OTP Frauds

As a measure to increase the security of the electronic transactions that are happening through the internet and various payment applications, the concept of multi factor authentication was introduced in all the electronic transactions. One of the most common techniques used in the multi-factor authentication of the financial transactions in electronic form is the One Time Password (OTP). In this process, the user authentication is performed by sending a OTP from the payment portal to the mobile number attached to the account of the user.

In the OTP frauds, the OTP generated by the payment portal is captured or taken by the fraudster from the user by adopting various techniques. One of the most common techniques used by them is by calling the user and asking them to share the OTP in the pretext that they require this for unlocking the card/attaching the aadhar/approval of loan and so on. Also, there are techniques by which the user's mobile is infected with malware that can forward the OTP automatically to the fraudsters or a mechanism by which fraudsters can read or access the OTP delivered to the mobile of the user.

Modus operandi:

- The fraudster calls the victim saying he was making some online registration and had entered the phone number of the victim by mistake since the two numbers were similar. And asks the victim to share the code received on the phone, so that he could complete the registration. Whereas the fraudster is actually trying to reset to online bank account of his target using the One Time Password (OTP).

Investigation:

1. The crime committed by stealing the OTP and using it for doing fraudulent financial transactions is considered to be Identity theft, the penal provisions for this crime are covered under Sec 66C of the Information Technology Act 2000. On receiving such a complaint, an FIR has to be registered under sec 66C along with sections 406, 420, 379 IPC, whichever is relevant.
2. The investigation of these cases has to be proceeded on the basis of the calls received from the fraudster if he/she has called and taken the OTP. The IO has to take the CDR and customer identity details of the owner of the SIM and proceed with investigation. But, in most of the cases it is found that the SIM cards used by the fraudster for these purposes are not registered using genuine name and addresses. In such case, we need to further the investigation of the case by analysing the call details of the IMEI traces, tower locations and other information that can be collected in this regard.
3. If the fraudster used the OTP that he has stolen for making a bank transaction or changing the password of online banking services, then we need to request the bank for the details of the accounts into which money was withdrawn or transferred. Once we identify the account particulars, we will continue the investigation in this line. If no transaction was done but they have changed the password of the online account, immediately bank need to be alerted to block the transactions from the account temporarily. Then, we proceed to collect the details of the IP address of the machine that is used to make those changes in the profile or password of the account.
4. Once, we receive the IP address of the device that is used to make the fraudulent online transactions, we can find out the ISP, who has allocated the IP address. Then we would approach the ISP for collecting the details (name, physical address, mobile and email attached, the location from which device was connected to the internet etc) of the person on whose name this IP was allocated.
5. These are some of the ways by which we identify the suspect device that was used to do the transaction.
6. Now it is the task of the IO to proceed and seize the device.
7. Once the device is seized, we can acquire the data from the device forensically and analyse for collecting evidences such as the web sites visited, details of credit cards if he/she has stored on it and other relevant digital evidences required for proving the involvement of the device in the commission of the offence.
8. After that, IO has to collect required evidences for connecting the suspect to the suspect device. This can be done by collecting all the circumstantial evidences related to the commission of the offence.

b) Job Frauds

Many of us would have received messages in our mobile phones requesting us to apply for job with working from home and payment of good salaries. We would have

seen lot of advertisements that were received in our mail box or posted on social media sites. Though we cannot tell that all these are frauds, job frauds using electronic media would look something like this. There can be a website where in fraudster could ask all the persons to register with all the personal information of people and they can collect lot of information, they can collect some money promising them placements in lucrative positions in prime companies. If people are defrauded by using these techniques through online platforms, they are considered to be job frauds.

In this kind of frauds, scammers trick victims into handing over your money by offering you a 'guaranteed' way to make fast money or a high paying job for little effort.

Modus operandi:

The fraudster would post recruitment advertisements over social media site or send personal e-mails to the victim asking them to pay some fees as a deposit to secure the job.

Investigation:

1. In all such cases, the IO can take leads from various places and proceed for investigation of the cases. These include
   a. If the victim received communication from the fraudster through email, we would collect the details of the email id, take the copy of the email along with the header following proper established procedures. Collect the details of the persons who were contacted by the victim and collect their KYC details. If the victim paid money through any bank account, collect KYC details of the account holder and investigate. To find the origin of the email and locate the user of the e-mail account, the procedure to be followed is explained in the e-mail investigation unit.
   b. If a website is being run by the fraudster for advertising or registration for jobs and other purposes, then we would find the details of the IP address of the server from which the website is being hosted, details of the owner of the website such as name, address, email, contact etc. We have to collect the details of the owners of the domain name as well following procedures mentioned in the 'internet investigation' unit. The evidences of existence of such a website with all the pages has to be saved by taking an offline copy of the website using various tools.

c) ATM/debit/credit card Frauds

The ATM cards are widely used for money withdrawals, shopping on the online site, paying money at the Point of sale machines etc. Credit cards, debit cards and smart cards are some of the examples of the ATM cards. As the use of ATM cards is increasing day by day, it poses a great amount of risk and frauds caused by the misuse of these cards. Fraudster performs various techniques in order to get the details of the ATM and uses the credential to do the fraudulent transactions.

Modus operandi:

- Commission of ATM frauds has two key aspects: firstly, getting access to the card or the data stored on the card and secondly getting the pin of the card. A criminal can get these through various methods. Some of them are discussed below.

Stealing cards:

One of the ways a fraudster can get access to the ATM card of the victim is by stealing it and use the card to perform fraudulent transactions.

Card skimming:

The ATM cards generally have a magnetic strip on it, which contains some of the electronic data which is used to authenticate when we use the ATM card to perform for any kind of payment. Fraudsters install ATM skimmers to the ATM machines or the POS machines, which scan the electronic data present in the magnetic strip as the victim perform the transactions on the ATM machine or the POS machine.

Buying card details from internet:

There are a lot of websites available on the internet as well as on the Dark web where people sell the ATM card details of various users which were gained by hacking into the banks database or by posting a fraudulent website and getting the credentials from it.

All the above mentioned techniques are used to get the details of the ATM card. From here on the fraudster can use the details to do some online transactions or he can make duplicate ATM cards by embedding the electronic data onto the empty cards with magnetic strip.

Investigation:

1. On receiving the complaint, the first step an IO need to do is to block the ATM card temporarily by calling the corresponding bank, so that the fraudster is not allowed to make any other transactions.
2. If the fraudster does any online transaction using the ATM card then the IO can contact the online portal on which the transaction was made asking for the IP address of the system used to make transaction along with the personal details of the person, which are collected by the portal.
3. Suppose the fraudster transferred the money to some different account, then IO has to identify the account to which the amount was transferred from the victim's bank statement and proceed to the bank asking for KYC documents of the account holder.
4. In case the fraudster has used a duplicate ATM card and performed any kind of withdrawals at any of the bank ATMs, IO can proceed by asking the bank the statement of the victim account and identify the location of the ATM machine from where the withdrawal occurred and take out the CCTV footage for the respective duration and identify the fraudster.

d) Hacking of Bank Accounts

Hacking in simple terms means illegal intrusion into a computer system without the permission of the computer user. If one can get access to the credentials of the account holders of different banks, we know that they can use them to do the transactions online or otherwise. So, it is a practice that fraudsters collect the details of the bank account

by hacking the bank servers, payment gateways, user machines that are being used for doing online transactions, e-commerce sites etc. For the purpose of hacking, fraudsters may make use of any vulnerable services running on the victim's machine or send any kind of malicious program that infects the victim's machine.

Modus operandi:

- Fraudsters take advantage of the software vulnerability present in user system or in the bank application to fetch the login credentials and perform the fraudulent transactions.
  - **Using Key-Loggers**

    Key-Logger is a piece of software which once installed on any system, it tracks or logs all the key strokes made by the victim using the keyboard and sends this data to the fraudster. Whenever a user enters his/her credentials in the key-logger infected machine, the fraudster receives the credentials sitting in remote location.

  - **Using Malware**

    Malware is nothing but a software program, which, when run on the computer, it makes the system perform the tasks that an attacker wants it to do.

I. PoS RAM scraping malware

- These malwares infects the point of sale (PoS) machines and capture the credit/debit card information stored in the RAM and send it to the fraudster who is sitting in some remote location.

II. ATM malware

- These malwares infects the ATM machines and perform some unusual activities such as stopping the ATM machine to dispense or dispense all the money that is available inside the ATM when the fraudster give some instruction to the ATM.

III. Malwares infecting bank's server

These malwares infects the bank servers and send the database of the user details, user credentials etc to the fraudster who is sitting in some remote location.

Investigation:

1. Whenever a case related to stealing of the bank account credentials of a person through the process of hacking is reported, police officer need to register an FIR as per sections 43(a), 43(b), 43(g) r/w 66, 66C of IT Act and sections 379, 406, 420, 467, 468, 471 of IPC, whichever is relevant.
2. We then need to identify the computer that was hacked for stealing the account details. We know that, when a computer system is hacked/compromised, there is a significant amount of evidence that will be available in the form of logs in the computer as well as the network it is connected to. IO should collect the bit-by-bit copy of the infected/ compromised system. From the image acquired, an IO should extract the logs and analyze them in order to identify

the IP address and the details of the fraudster. We need to analyse the machine to find out all the other information that the fraudster has stolen.

3. If we get to know the vector used by the fraudster such as email, social media, website etc, we can collect further details about the activities performed by the fraudster by investigating the respective platforms. The processes to be followed by the IO for investigating the platforms are discussed in the other units in detail.

e) Identity Theft

In this kind of frauds, fraudster uses various techniques in order to get the personal information of the victim such as login credentials of Internet banking; ATM pins etc and uses this personal information of the victim to perform fraudulent transactions causing financial loss to the victim. Fraudster performs the identity theft in the following ways:

Phishing

Phishingis an attempt made by the fraudsters, where he sends the link of the page of a fake bank website to the victim either by mail/SMS or over social media sites in order to steal the personal information of the victim such as Customer ID, PIN, Credit/Debit Card number, Card expiry date, CVV number, etc. In recent years, phishing has emerged as one of the biggest threats to individuals and to the economy as well.

Modus operandi:

1. In these cases, fraudsters normally create a fake website that looks similar to a banking website or a e-commerce website and sends a link to the victim by email/SMS asking them to enter the credentials to verify the account status or change the password etc. Once the victim enters the credentials in that site, the fraudster receives those credentials and uses it to perform fraudulent transactions. Investigation:

1. These crimes are considered as identity theft, the penal provisions for this crime are covered under Sec 66C of the Information Technology Act 2000. On receiving such a complaint, an FIR has to be registered under sec 66C along with sections 406, 420, 379 IPC, whichever is relevant.
2. The IO should collect the url which was received by the victim and identify the location of the phishing website. We would also collect the details such as the IP address of the server from which the website is being hosted, details of the owner of the website such as name, address, email, contact etc. We have to collect the details of the owners of the domain name as well following procedures mentioned in the ‘internet investigation’ unit. The evidences of existence of such a website with all the pages has to be saved by taking an offline copy of the website using various tools.

Smishing

Smishing involves obtaining the personal information of the victim using SMS text messages or tricking a user into downloading a Trojan horse, virus or other malware onto their cell phone or other mobile device.

Modus operandi:

In Smishing, the fraudster send a SMS to the victim with Link asking the victim to go to the link and register for securing their account or verifying the credentials with the bank server as a security check-up.

Investigation:

1. These crimes are considered as identity theft, the penal provisions for this crime are covered under Sec 66C of the Information Technology Act 2000. On receiving such a complaint, an FIR has to be registered under sec 66C along with sections 406, 420, 379 IPC, whichever is relevant.
2. As the victim receives the message via SMS, IO can proceed to investigate based on the SMS received from the. An IO has to take the CDR and customer identity details of the owner of the SIM and proceed with investigation. But, in most of the cases it is found that the SIM cards used by the fraudster for these purposes are not registered using genuine name and addresses. In such case, we need to further the investigation of the case by analysing the call details of the IMEI traces, tower locations and other information that can be collected in this regard.

Vishing

Unlike traditional phishing attacks where the fraudster uses fake emails or link manipulation to get the information from the victim, vishing is when a fraudster tries the call the victim in order to get the information from the victim. There are a number of techniques used, e.g., concern that one of your accounts may be vulnerable, a threat that you have not paid a bill, an offer of a reward or prize,

Modus operandi:

The Victims receive call from the fraudster saying that they are the representatives from the banks/E-commerce sites and asking them to reveal the banking credentials so that they can verify the account.

Investigation:

1. These crimes are considered as identity theft, the penal provisions for this crime are covered under Sec 66C of the Information Technology Act 2000. On receiving such a complaint, an FIR has to be registered under sec 66C along with sections 406, 420, 379 IPC, whichever is relevant.
2. As the fraudster communicates with the victim by calling him/her, IO can precede the investigation by taking the CDR and customer identity details of the owner of the SIM.

f) Insurance Frauds

Insurance fraud occurs when individuals deceive an insurance company, agent or other person to try to obtain money to which they are not entitled. It happens when someone puts false information on an insurance application and when false or misleading information is given or important information is omitted in an insurance transaction or claim.

There are two types of insurance frauds:

Hard Fraud: Someone deliberately fakes an accident, injury, theft, arson or other loss to collect money illegally from insurance companies.

Soft Fraud: Normally honest people often tell "little white lies" to their insurance company. Many people think it's just harmless fudging. But soft fraud is a crime.

Modus operandi:

Fraudsterfurnish false documents and manipulation in citing the cause of death as part of the adopted by to claim insurance benefits Ex:

- Billing for services that were not provided
- Performing medically unnecessary services
- Altering claim forms, medical documentation, etc.
- Billing for a service that costs more

A payment gateway is a service which acts as a middle man when a buyer wants to make the payment to the seller. Payment gateways provide a secure medium/channel for making the transaction.

These gateways transmit the transaction details such as the banking credentials, whether there is sufficient balance for the transaction to proceed etc.

Just like in the physical world, where we use Point of sale machines to make the payment to the seller, we use payment gateways to make the online transactions and complete the payment. Some of the payments gateways are Bill Desk, CC Avenue, and Citrus etc

Modus operandi:

Fraudster creates a fake payment gateway web page which looks and behaves similar to the genuine payment gateway website and sends it to the victim. The victim thinking the fake website sent by the fraudster as genuine enters his credentials. The fraudster receives those credentials and performs the fraudulent transactions.

Investigation:

1. These crimes are considered as identity theft, the penal provisions for this crime are covered under Sec 66C of the Information Technology Act 2000. On receiving such a complaint, an FIR has to be registered under sec 66C along with sections 406, 420, 379 IPC, whichever is relevant.

2. We would identify the phishing page and then we would find the details of the IP address of the server from which the website is being hosted, details of the owner of the website such as name, address, email, contact etc. We have to collect the details of the owners of the domain name as well following procedures mentioned in the 'internet investigation' unit. The evidences of existence of such a website with all the pages has to be saved by taking an offline copy of the website using various tools.
3. Suppose the fraudster has used the credentials to make any transaction on the payment gateway, IO can get the transaction id from the victim, which can be obtained from the bank statement. Then the IO can request the details such as for what purchase did the fraudster made the transaction from the E-commerce website and request the details such as IP address, bank account etc of the fraudster from the payment gateway.

h) Digital Wallets

As the online mode of payments has increased to make cashless transactions, multiple ways to make the payments has also increased. One such mode of payment is digital wallets/Virtual wallets/mobile wallets. Similar to the physical wallets we use in our daily life, digital wallets acts as a container where we can store your digital information about various credit/debit card, load money from your bank account to the digital wallets and get coupons etc.

Using these digital wallets, one can pay the bills, book tickets on various platforms, transfer fund from one account to other etc, providing convenience to the user by not allowing him/her to stand in long queues to pay the bills. Digital wallets allows user to pay these bills from anywhere in the world connected to the internet

There are many applications like PayTM, Freecharge wallet, SBI buddy, ICICI pockets, Mobikwik, PayUMoneyetc which provide the digital wallets service.

Modus operandi:

In these kinds of frauds, the fraudster creates fake mobile wallet apps and uploads it to the internet for people to download. People over the internet thinking the fake mobile wallet app as genuine app download and try to use it for transactions giving away their credential. The fraudster receives those credentials and performs the fraudulent transactions.

Investigation:

1. These crimes are considered as identity theft, the penal provisions for this crime are covered under Sec 66C of the Information Technology Act 2000. On receiving such a complaint, an FIR has to be registered under sec 66C along with sections 406, 420, 379 IPC, whichever is relevant.
2. On receiving the complaint, we would identify the fake app that is being hosted and then we would find the details of the IP address of the server from which the website is being hosted, details of the owner of the website such as name,

address, email, contact etc. We have to collect the details of the owners of the domain name as well following procedures mentioned in the

'internet investigation' unit. The evidences of existence of such a website with all the pages has to be saved by taking an offline copy of the website using various tools.

Investigating abraod

The processes to be followed by the IO for investigating abroad are discussed in the below link in detail.

Below are the list of nodal officers whom to approach:

NODA OFFICERS OF DIFFERENT BANKS IN INDIA

ORGANISATION	NODAL OFFICER	PHONE NO	EMAIL_ID
ANDHRA BANK	NODAL OFFICER		frmg@andhrabank.co.in
AXIS BANK	AJAY CHAKOTE	7893966698	Ajay.Chakote@axisbank.com
BANK OF BARODA	GM (OPERATIONS)		gm.ops.ho@bankofbaroda.com
HDFC BANK	SOMASEKHAR	9347052868	SomaSekhar.RaoDaduwai@hdfcbank.com
HSBC BANK	NODAL OFFICER	9703227575	nodalofficerinm@hsbc.co.in
HSBC BANK	HSBC		srinivas1naidu@hsbc.co.in
ICICI BANK	P NARASIMHA RAO	9000601267	narasimharao.ponnam@icicibank.com
ICICI BANK	K V RANGACHARY	9949612251	rangachary.kv@icicibank.com
ING VYSYA BANK	NODAL OFFICER		nodalofficer@ingvysyabank.com
IOB	IOB		creditcard@iobnet.co.in
KOTAK	ESCALATIONS		escalations@kotak.com
KOTAK	SHIVKUMAR	9885031691	shivkumar.sundaram@kotak.com
KOTAK	SUPPORT		service.bank@kotak.com
PNB	DGM		skbansal@pnb.co.in
PNB	GM		vsrinivasan@pnb.co.in
SBH	CM (GRIEVANCES)		cmgrievances@sbhyd.co.in
SBI	AGM (VIGILANCE)		agmvig.lhohyd@sbi.co.in
SBI	HELP LINE - HYDERABAD		helpline.lhohyd@sbi.co.in
SBI	AGM		agmcustomer.lhohyd@sbi.co.in
SBI-CARDS	CEO-SBI CARDS		CEO@sbicard.com
SBI-CARDS	NODAL OFFICER		Nodalofficer@sbicard.com
SCB	NODAL OFFICER		principal.nodalofficer@sc.com

Table 3: List of Nodal Officers of Various Banks

Nodal officers of various Internet Service Providers

ORGANISATION	NODAL OFFICER	PHONE NO	EMAIL_ID
ACTTV	NODAL OFFICER		nodalofficer@acttv.in
BEAM CABLE	AJAY BANDA	9542445244	ajay.banda@beamtele.com
BEAM CABLE	BEAM		nodal.term@beamtele.com
BSNL	NARAYANA	9490120744	sdetecvig@bsnl.co.in
EXCELL MEDIA	RAMA	9866316212	ramakrishna@excellmedia.net
NETX	ADITYA		skept@netxconnect.com
PIONEER ONLINE	NODAL OFFICER		support@pol.net.in

SIFY	NODAL OFFICER		luithelp@sify.com
SKYTEL	RAJ KUMAR		rajskytel@gmail.com

SOUTHERN ONLINE	SOL		support@sol.net.in
SRITEL	VAMSI		vamsi@sritel.in
TIKONA	SAMPAT JAYDEEP		jaydeep.sampat@tikona.in
VAINAVI	PADMAJA		padmaja@vainavi.net
VAINAVI	NODAL OFFICER		nodal@vainavi.net
VSNL	SECTION VIGILANCE		VIGILANCE.mumbai@tatacommunications.com
YOUTELE	NODAL OFFICER		idc@youbroadband.co.in
ZYTEL	ANIL KUMAR		anilkumar.ch@zyetel.com

Nodal officers of various online platforms

ORGANISATION	NODAL OFFICER	PHONE NO	EMAIL_ID
ARZOO	RAJESH		rajesh.m@arzoo.com
BHARAT MATRIMONY	NODAL OFFICER		legal@consim.com
CLEARTRIP	SUPPORT		hotelcs@cleartrip.com
CLEARTRIP	MANGESH		mangesh.bhanu@cleartrip.com
EBAY			contactIndiafit@ebay.com
EBAY	MOHAN	9867712149	kchaudhary@ebay.com
FLIPKART	CUSTOMER SUPPORT		cs@flipkart.com
FLIPKART	NODAL OFFICER		grievance.officer@flipkart.com
IRCTC	CUSTOMER CARE		care@irctc.co.in
MOBIKWIK	NIKHIL		support@mobikwik.com
MOBIKWIK	AMIT		amit@mobikwik.com
MOBIKWIK	TAMANNA		tamanna@mobikwik.com
MOBIKWIK	HEENA		heena@mobikwik.com
OLX	OLX		grievanceofficer@olx.in
OLX	OLX INTERNATIONAL		complaints@council.bbb.org
PAYTM	RAHUL		rahul.bali@paytm.com
PAYTM	SECURITY		security@paytm.com
RECHARGEITNOW	GANESH		ganesh.garg@rechargeitnow.com

RECHARGEITNOW	CUSTOMER CARE		care@rechargeitnow.com
RECHARGEITNOW	SARAT		sharat.jain@rechargeitnow.com
RECHARGEITNOW	MAHESH		mahesh.agarwal@estel telecom.com
WAY2SMS	RAJASEKHAR	9390036006	support@way2online.com
PAYTM			cybercell@paytm.com
PAYU			reportfraud@payu.in disutes@payu.in care@payu.in
IRCTC			itaf@irctc.co.in care@irctc.co.in
MOBIKWIK			fraudalerts@mobikwik.com risk@mobikwik.com
BOOKMYSHOW			helpdesk@bookmyshow.com riskmanagement@bookmyshow.com
OLA CABS			cybercrimeescalations@olacabs.com anik@legaltrb.com security@olacabs.com
FREECHARGE			risk.team@freecharge.com care@freecharge.in
SBI eBUDDY			epg.cms@sbi.co.in dm1it.cms@sbi.co.in alert.buddy@sbi.co.in agm.nodcyb@sbi.co.in

Table 4: Nodal officers of various Internet Service Providers

Nodal officers of various Payment gateway

ORGANISATION	NODAL OFFICER	PHONE NO	EMAIL_ID
BILL DESK	GENIUS		genius@billdesk.com
CCAVENUES	NODAL OFFICER		risk@ccavenue.com

Table 5: Nodal officers of various Payment gateway

7. Social Media Investigation

7.1 SOCIAL MEDIA

Social media is the collective of online communications channels dedicated to community-based input, interaction, content-sharing and collaboration. Websites and applications dedicated to forums, micro blogging, social networking, social bookmarking, social circulation, and wikis are among the different types of social media.

Social media changes constantly – **Twitter,** now one of the most popular social media platforms, didn't even exist ten years ago. And the dynamics of social media use can be complicated. Different social media platforms are more popular among different demographic or geographic groups. Agencies should not simply think of social media as venue to obtain evidence of a crime, but also as a tool for gathering intelligence. The intelligence can be useful for a variety of law enforcement functions, including counterterrorism, gang enforcement, policing protests, and monitoring drug trends.

The number of social media sites is astounding and ever-increasing. Some of the more popular applications include: Facebook, Instagram, Kik, Snapchat, Tagged, Twitter, Myspace, Vine, Linkedin, flickr, vimeo, Google+, tumblr, Skype, Stickam, Youtube, Sina Weibo, Craigslist, Bebo, Sony Playstation Network, XBox Live!, iMessage, mIRC, Viber, Wickr, Vibe, Whatsapp, TigerText, Yahoo Messenger, AIM, Omegle, WeChat, and ooVoo. Investigators will need to determine a user's username and password for most of these services to obtain more information on a specific user.

There are several resources that can help agencies data mine and analyze information from social media websites. One useful site is Media Sonar, which is an application that provides a location-based social media investigations' platform for law enforcement. Another is Sociospyder, which is software available exclusively to law enforcement and intelligence agencies that "mines open source intelligence (OSINT) from Facebook, Twitter, LinkedIn, YouTube and Google+."

- **Facebook** is a popular free social networking website that allows registered users to create profiles, upload photos and video, send messages and keep in touch with friends, family and colleagues. According to statistics from the Nielsen Group, Internet users within the United States spend more time on Facebook than any other website.
- **Twitter** is a free microblogging service that allows registered members to broadcast short posts called tweets. Twitter members can broadcast tweets and follow other users' tweets by using multiple platforms and devices.
- **Google+** (pronounced Google plus) is Google's social networking project, designed to replicate the way people interact offline more closely than is the case in other social networking services. The project's slogan is "Real-life sharing rethought for the web."

- **LinkedIn** is a social networking site designed specifically for the business community. The goal of the site is to allow registered members to establish and document networks of people they know and trust professionally.
- **Pinterest** is a social curation website for sharing and categorizing images found online. Pinterest requires brief descriptions but the main focus of the site is visual. Clicking on an image will take you to the original source, so, for example, if you click on a picture of a pair of shoes, you might be taken to a site where you can purchase them. An image of blueberry pancakes might take you to the recipe; a picture of a whimsical birdhouse might take you to the instructions.
- **Instagram**is a free online program and social network that enables users to take, edit and share photos with other users via Instagram's own platform, email, and social media sites including Twitter, Facebook, Tumblr, Foursquare and Flickr.
- **YouTube**is a free video-hosting website that allows members to store and serve video content. YouTube members and website visitors can share YouTube videos on a variety of web platforms by using a link or by embedding HTML code.
- **WhatsApp Messenger** is a cross-platform instant messaging application iPhone, Black Berry, Android, Windows Phone and Nokia smartphone users to exchange text, image, video and audio messages for free.

7.2 Investigation on social media platforms

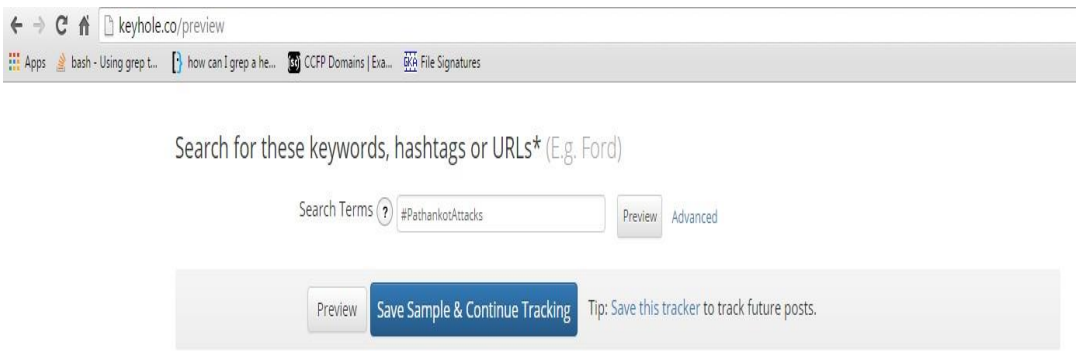
7.2.1 Information Gathering via Social Media Analysis:

There are lots of online tools, some of them shown below

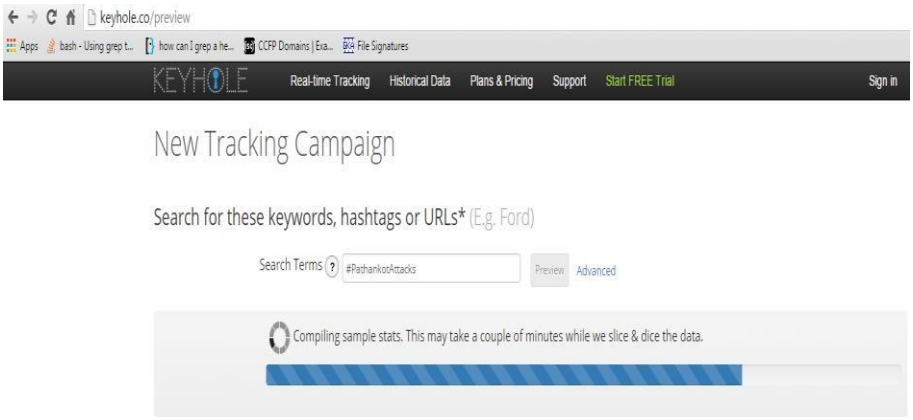
i) Keyhole.co – An online tool which focuses on Twitter hashtags and keywords to gather intelligence out of them and presents a report accordingly.

Go to www.keyhole.co

Enter the keyword or hashtag of interest. (Here, its #PathankotAttacks)



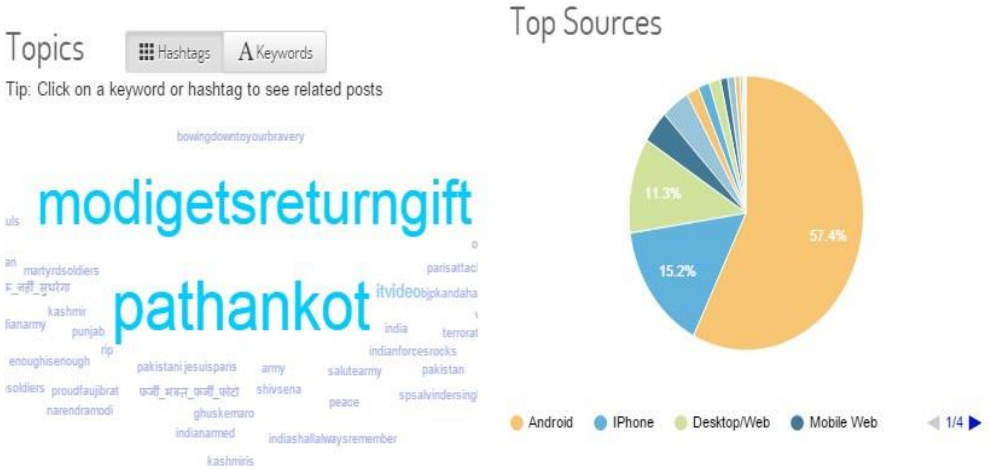
1. Click on ‘Preview’



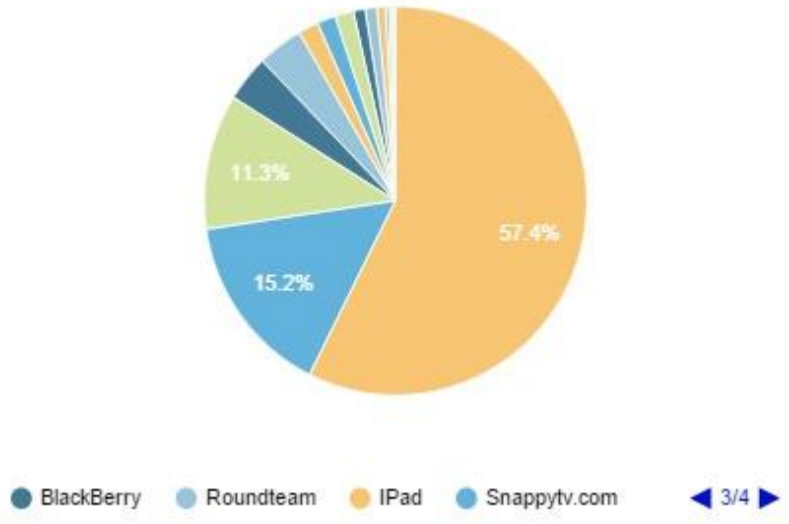
2. Let the statistics load.

3. You will be displayed with relevant results which contain the details like Timeline, Top Posts, share of posts, demographics, popular keywords, etc.

4. Further, you can see the word-cloud revolving around the hashtag you specified and also the various platforms

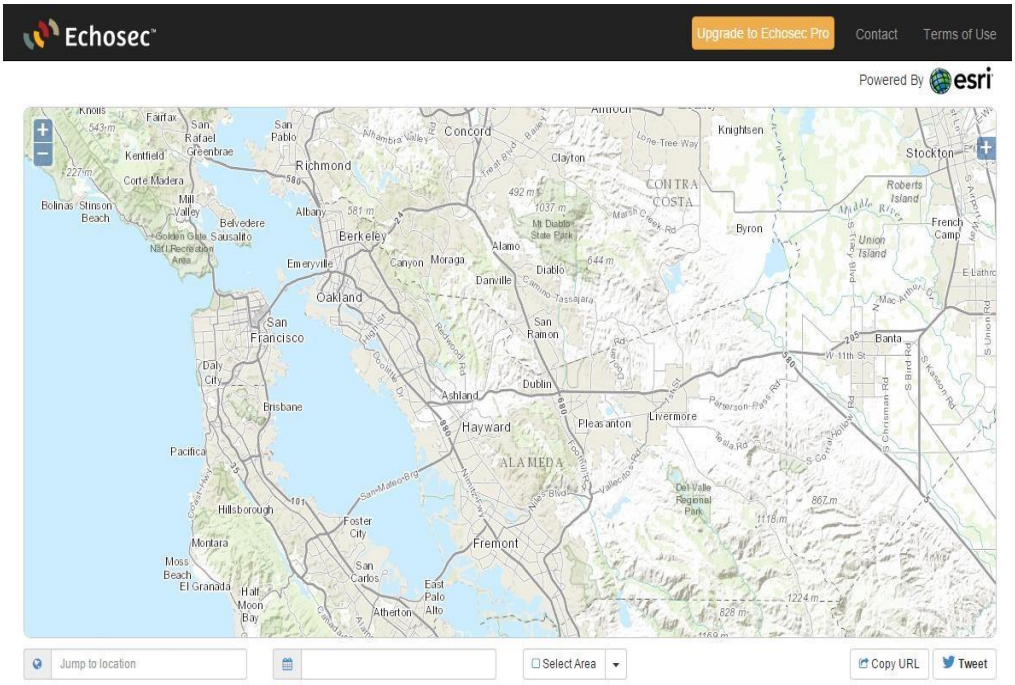


5. (Operating Systems) and devices from which the tweets were made.

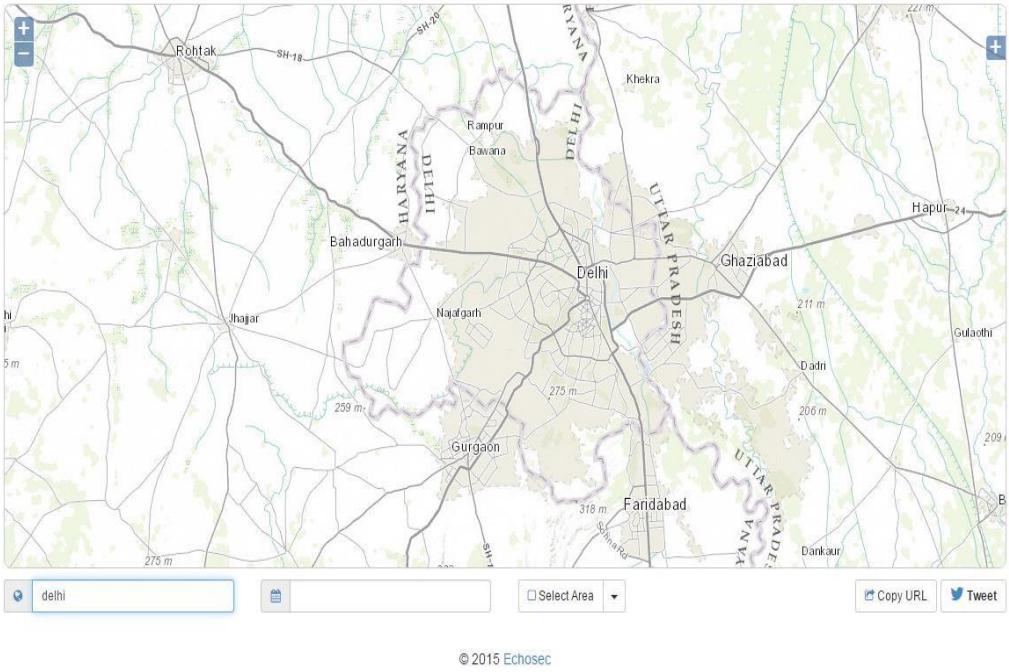


ii) Echosec.net– An online tool which does location based search and tries to discover the activities on social media taking place in a specified location

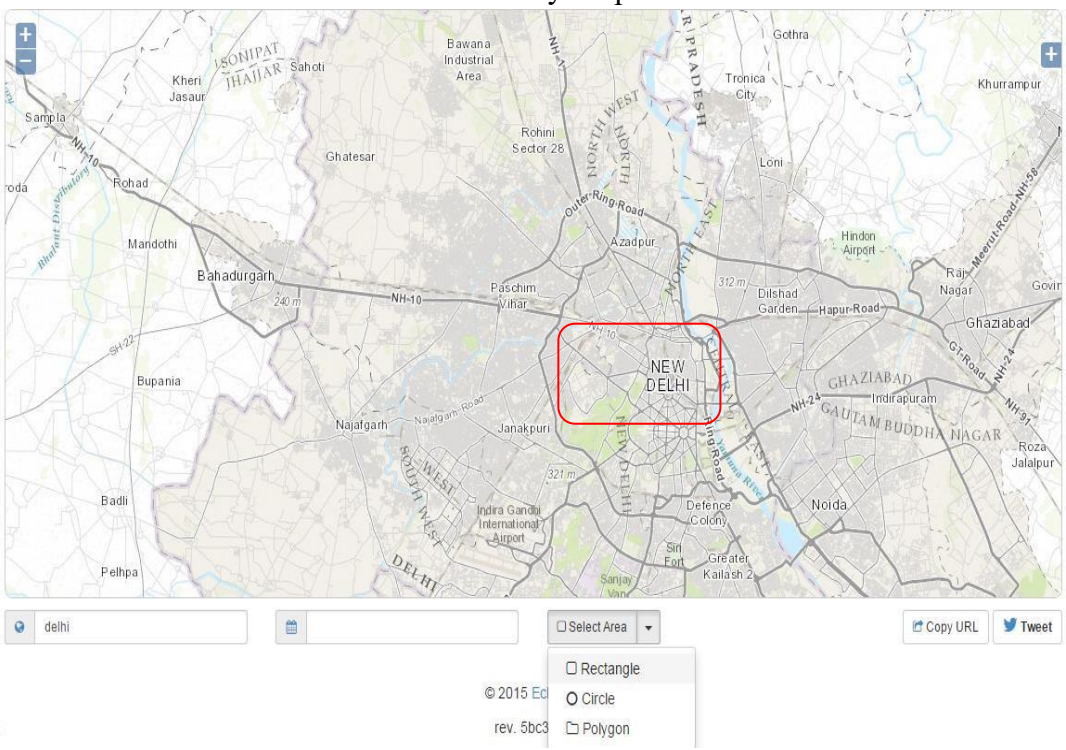
1. Go to www.echosec.net



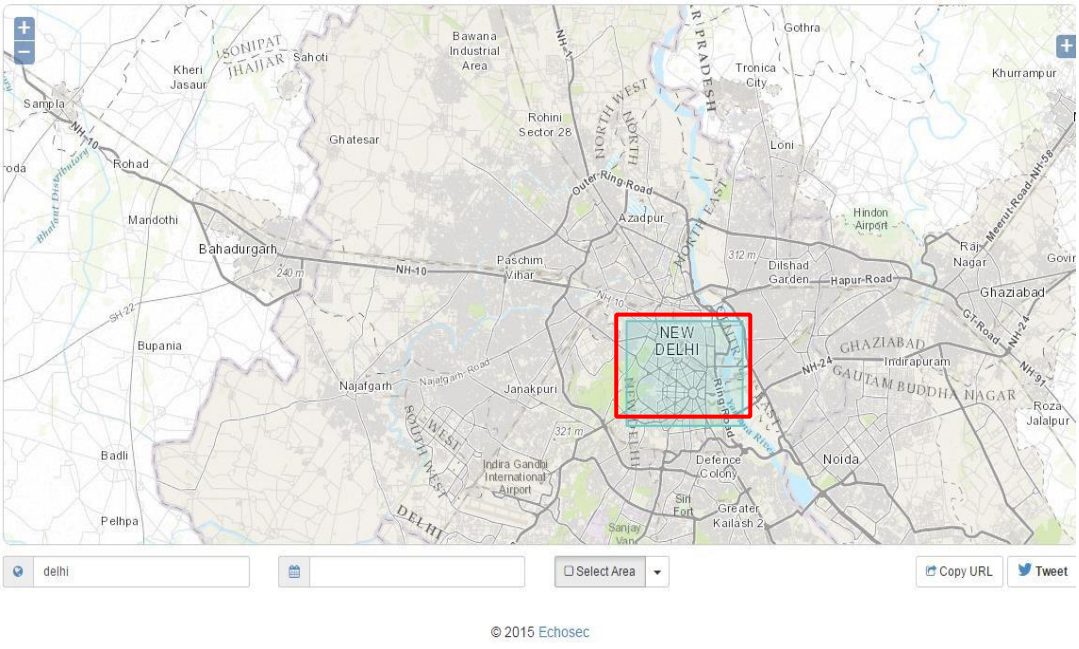
2. Type an area and hit enter



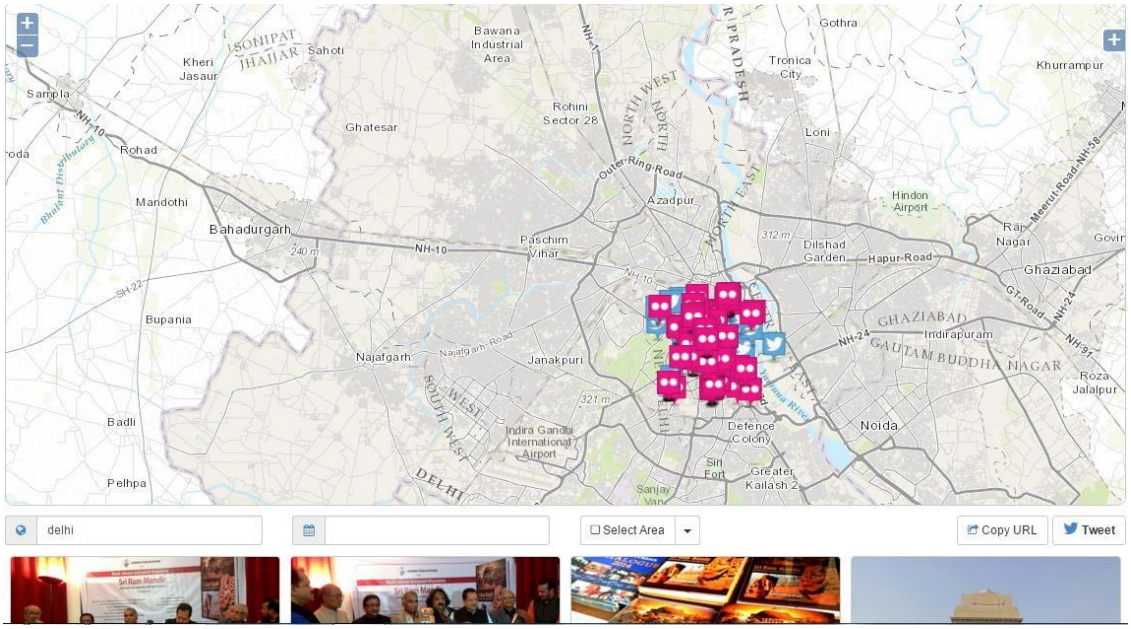
3. Now click on ‘Select area’ and choose any shape.



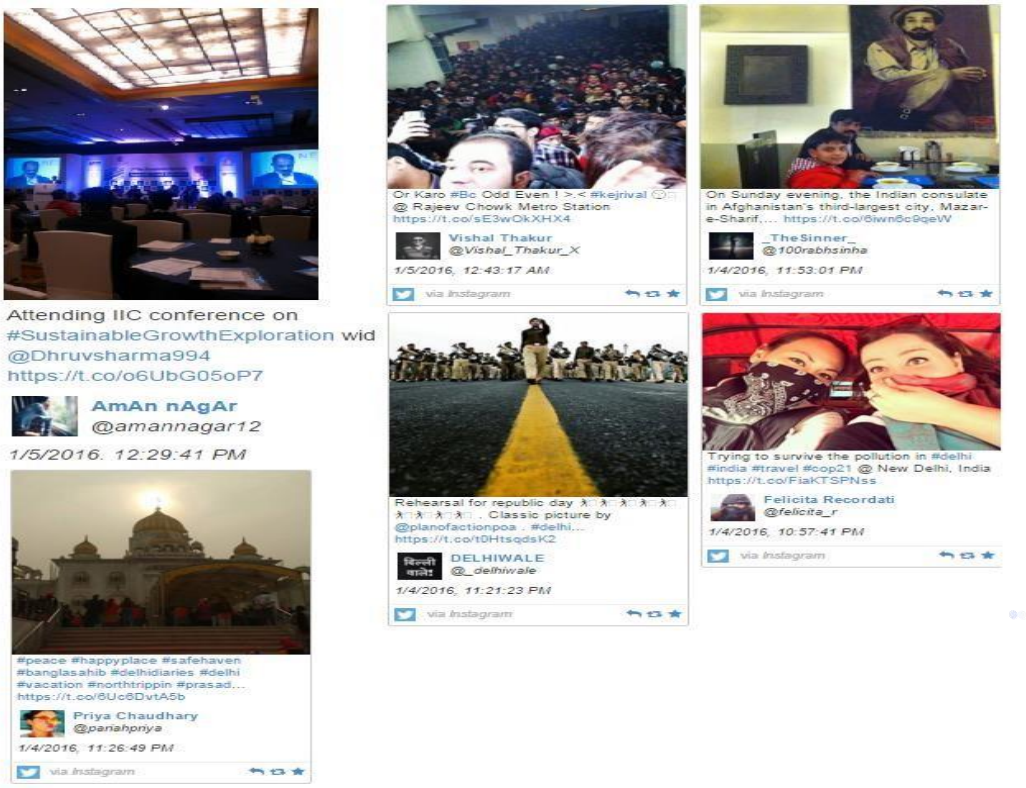
4. Draw over an area to select it.



5. You will be shown the tweets corresponding to that area.



6. Scroll down to see what juicy information you can get.



For example, from the above results one can find out that there is an IIC conference in some place around, and also that the Rajeev Chowk Metro station is exploding with lots and lots of people mocking at Delhi CM's 'Odd-Even day' system. We can also see there is a rehearsal going on for the Republic Day parade.

Although we cannot guarantee that every tweet is listed in the output, but this can be considerably acceptable intelligence data which we can gather from social media.

iii) TrueCaller

Truecaller lets you search beyond your phonebook, identify unknown incoming calls, block calls you don't want to receive, and make relevant contact suggestions based on time and place – so you never have to leave the service to find the right contact.

* See who is calling if you don't have their number in your phonebook
* Block unwanted calls from spam callers and telemarketers
* Search for any number in the world to see who it belongs to
* You can now copy a number anywhere and it will notify you who it belongs to
* Get in touch with people via name search (Premium feature)
* Tweet and Follow a person on Twitter directly from Truecaller
* Yelp! integration for faster business search results
* + more features to make your phone smarter

Truecaller NEVER uploads your phonebook to make it searchable or public. 3G or WIFI is required for Truecaller Caller ID to work. Operator charges may apply.

*** The block text feature is currently not supported for devices with Android 4.4 (KitKat).**

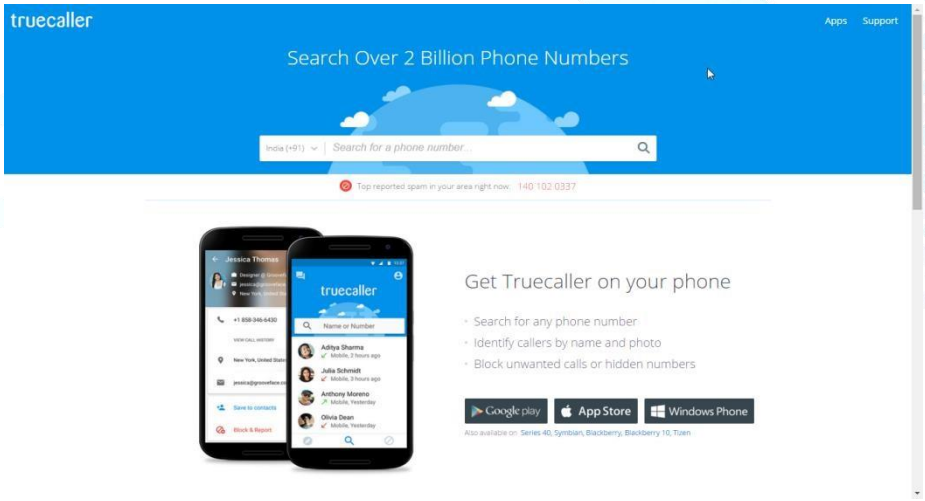


Fig.7.3 Truecaller home page

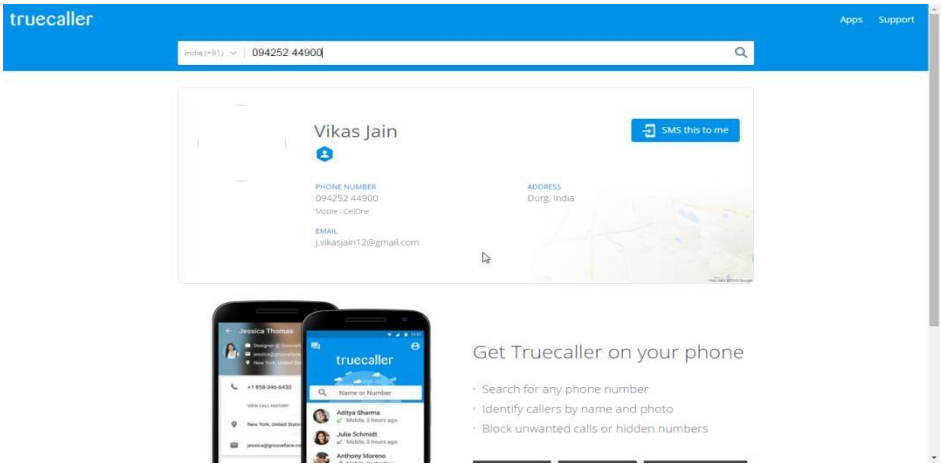


Fig.7.4: Truecaller search result iv) Maltego

With the continued growth of technologies and infrastructure associated with web services, the threat picture of your "environment" is not always clear or complete. In fact, most often it's not what we know that is harmful - it's what we don't know that causes the most damage.

Maltego is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates. Maltego's unique advantage is to demonstrate the complexity and severity of single points of failure as well as trust relationships that exist currently within the scope of your infrastructure.
The unique perspective that Maltego offers to both network and resource based entities is the aggregation of information posted all over the internet - whether it's the current configuration of a router poised on the edge of your network or the current whereabouts of your Vice President on his international visits, Maltego can locate, aggregate and visualize this information.

Maltego offers the user with unprecedented information. Information is leverage. Information is power. Information is Maltego.

What does Maltego do?

- Maltego is a program that can be used to determine the relationships and real world links between:
  - People
  - Groups of people (social networks)
  - Companies ○ Organizations ○ Web sites ○ Internet infrastructure such as:
    - Domains
    - DNS names
    - Netblocks ▪ IP addresses ○ Phrases ○ Affiliations ○ Documents and files
- These entities are linked using open source intelligence.
- Maltego is easy and quick to install - it uses Java, so it runs on Windows, Mac and Linux.

- Maltego provides you with a graphical interface that makes seeing these relationships instant and accurate - making it possible to see hidden connections.

- Using the graphical user interface (GUI) you can see relationships easily - even if they are three or four degrees of separation away.
- Maltego is unique because it uses a powerful, flexible framework that makes customizing possible. As such, Maltego can be adapted to your own, unique requirements. **What can Maltego do?**

- altego can be used for the information gathering phase of all security related work. It will save you time and will allow you to work more accurately and smarter.
- Maltego aids you in your thinking process by visually demonstrating interconnected links between searched items.
- Maltego provide you with a much more powerful search, giving you smarter results.
- If access to "hidden" information determines your success, Maltego can help you discover it. **What Maltego cannot do?**

- Maltego cannot parse restricted network for factual data.
- Maltego cannot look for information that is not in public domain.
- Maltego cannot look for connection or information without available authorization credential.
- Maltego cannot parse deep web for information mining.

7.3 Taking Archive of Various Social Media Platform

7.3.1 Facebook Archive

Facebook is a social networking platform which provides website as well as few applications to connect users from around the world with their friends and family online. Users can create content such as text, images, and videos or can live broadcast events of their day today life with their friends or to public users. Users can join common interest groups where they can communicate with other users with similar interest. Facebook is having more than 240 million users from India and is also the leading country for highest number of users on Facebook network globally.

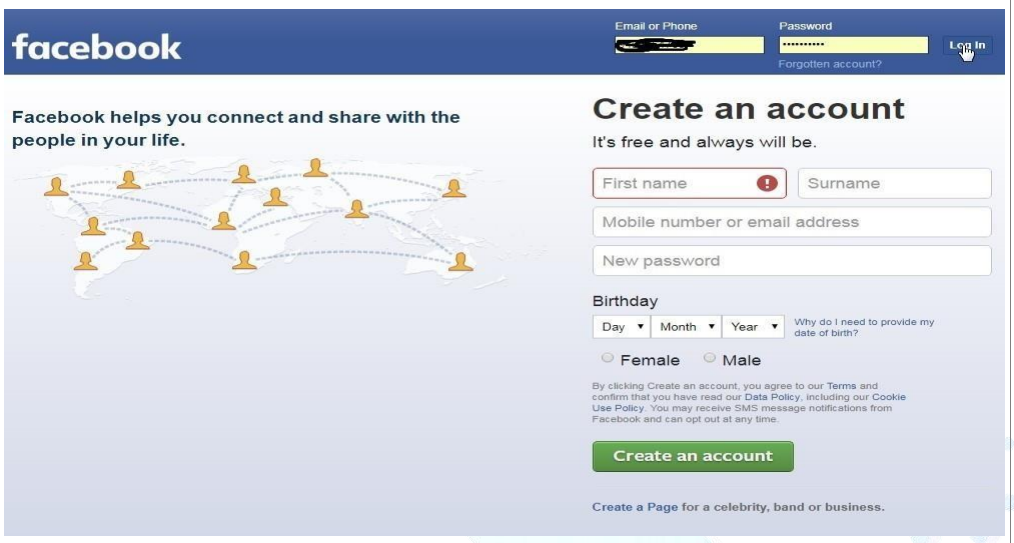
As Facebook has become so common within Indian users it is widely being used by antisocial elements for causing criminal activities or antisocial activities on Facebook. Facebook stores all the data that is created by the user on their websites or applications. This data can be very useful in solving any investigations involving Facebook user. For such a reasons law enforcement agencies can request data of a user for specific date from Facebook by providing 91CrPc with the legal team of Facebook. However if an investigating officer has the Facebook username and password of a criminal's or a suspects profile then they can download this data offline themselves by using Facebook achieve functionality. In order to make an offline copy of all the activities done by Facebook user account, the investigating officer can go through the

following steps. Please note this process is only possible when the Investigating Officer (IO) knows login ID & password of the user account.

In order to make an offline copy of all the activities done by facebook user account we can go through the following steps. This is possible only when the Investigating Officer (IO) knows login ID & password of the user account. Steps to create a Facebook archive:

Step1:

Log into Facebook using the required ID and password.



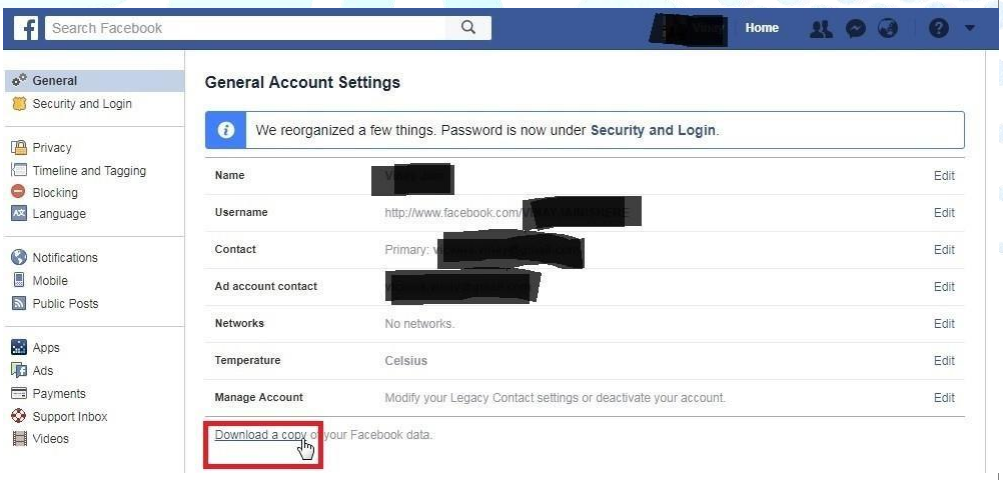
Screenshot of login page of Facebook

Use the drop down menu to select "Settings" options.

ScreenshotIllustrationofStep2ofFacebookArchive

Step3:

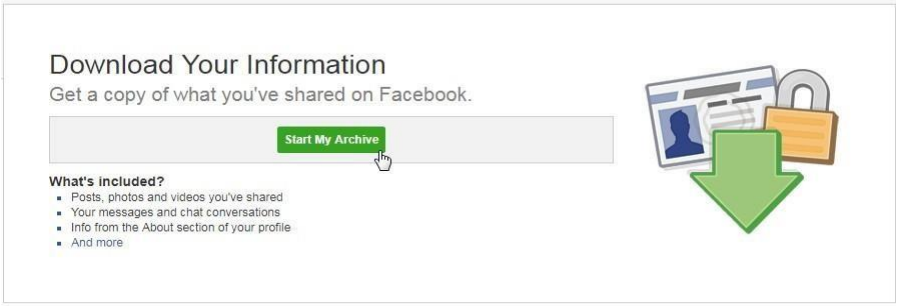
Under"GeneralAccountSettings"selecttheoption"Downloadacopy"asshowninb elow screenshot.



Screenshot of Facebook page with General Account settings

Step4:

Proceed by Selecting the option "Start MyArchive" as shown in below screenshot



Screenshot showing 'how to get a copy of information shared in a particular account'

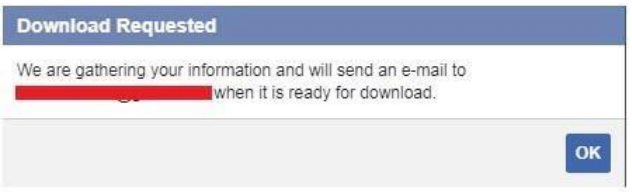
Step5:

Click "Start My Archive" button on popup window which proceeds Step4.

Popup window asking to click on 'Start my Archive'.

Step6:

If you are doing this archive for the first time an archive will be created by Facebook and a link will be sent to the registered email. As shown below:



ScreenshotIllustartingstep6

If an archive is done before on this profile then it will straightaway take you to a download link as shown below:

ScreenshotIllustarting step7

Step7:

OnceyouclickDownloadArchiveyouwillreceiveaprompttorenteryourpassword: Here re-enter the password and click on "Submit"

Screenshot Illustrating step7

Step8:

Once you click submit, if the password is correct then the download will start and de- pending on the size of the data it can finish in few minutes. Finally once the download is finish you will see below screenshot:

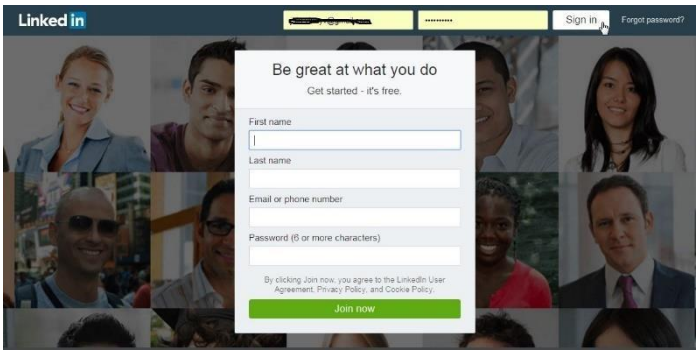
Screenshot Illustrating step 8

7.3.2 LinkedIn Profile Archive

LinkedIn is a business and employment-oriented social networking service that operates via websites and mobile apps. It is mainly used for professional networking, including employers posting jobs and job seekers posting their CVs. LinkedIn allows members (both workers and employers) to create profiles and "connections" to each other in an online social network which may represent real-world professional relationships. Members can invite anyone (whether member or not) to become a connection. The "gated-access approach" (where contact with any professional requires either an existing relationship or an introduction through a contact of theirs) is intended to build trust among the service's members. Although LinkedIn is intended for professional network, some users can misuse LinkedIn to create fake job offers and use it to crook users on the network. In such cases data can be requested of a user from LinkedIn by contacting theirlegalteambyproviding91CrPcanddetailsof the incident. LinkedIn also provides a feature by which a user can download their data offline just like Facebook. If an investigating officer knows the username and password of the suspect or a criminal then this can be used to retrieve the archive from LinkedIn for analyzing the data. In order to make an offline copy of all the activities done on LinkedIn user account investigation officer can go through the following steps of making an offline copy of LinkedIn archive:

Step1:

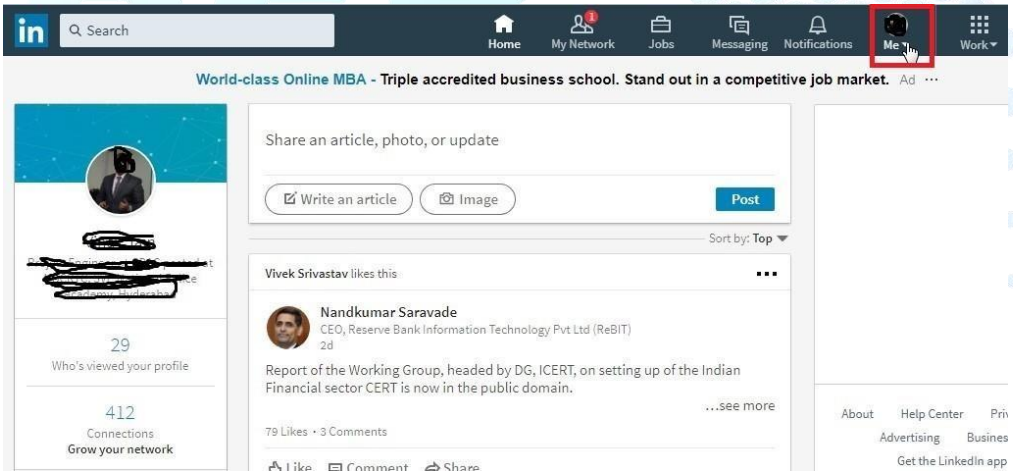
Log into LinkedIn using the required ID and password.



Screenshot of LinkedIn page

Step2:

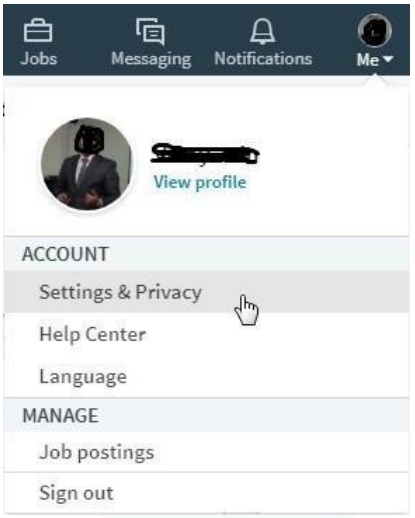
Click on profile picture on top-right to open the drop down menu as highlighted in the below screenshot.



Screenshot of LinkedIn page after login

Step3:

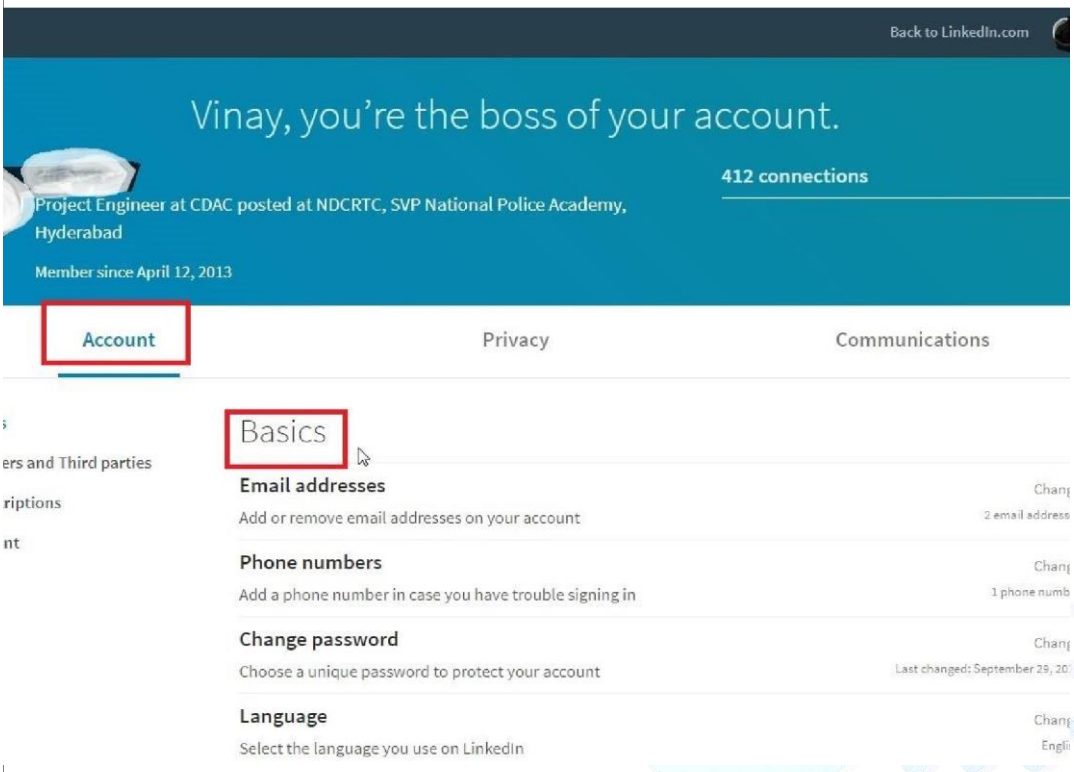
Select "Settings and privacy" option as highlighted in the below screenshot.



Screenshot of drop down menu from profile picture

Step4:

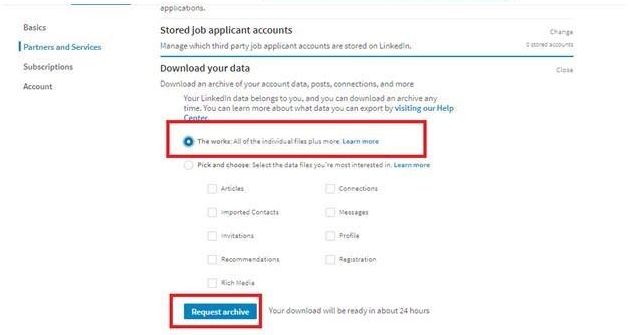
down on "Basics" Section



Screenshot Illustrating Step3 of LinkedIn Archive

Step5:

Click "Download your data" as shown in below screenshot.



Screenshot Illustrating Step 5

Step6:

Click "The works" under" Download your data" for all data related to the pro below screenshot

to download the arcl and then click “Request archive” button. As shown in

Screenshot Illustrating step 6

Step7:

Enter Password and “Done" as shown in below screenshot.

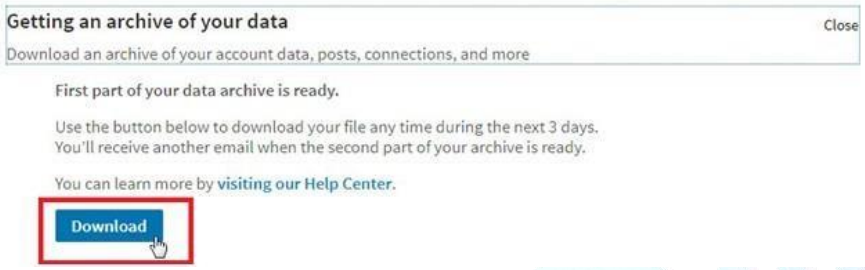
Screenshot Illustrating the result page after step 7

Step8:

If the profile has never done an archive it will take at least few minutes for LinkedIn to prepare the archive. An email will be sent to the registered user account once the archive is ready. Please wait till the archive is ready for the download.

Screenshot Illustrating Step 8 ofLinkedIn Archive

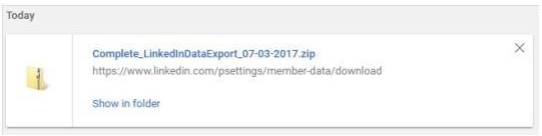
If the profile has been archived before then archive can be ready in some cases and thus the download will be ready. In such cases, you can click on the download button to get the offline copy of the data. Or you can click the link that is sent to registered email once the archive is ready for download.



Screenshot Illustrating Step 8

Step9:

Once you click download button depending on the size of data and speed of your internet connection it may take several minutes for the download to finish. Once the download is finished you will see a screen like below.



ScreenshotIllustratingStep9

An investigating officer can then analyze the data from this zip file and present it as an evidence in the court if required.

7.3.3 Acquire Twitter Profile Archive

Twitter is an online news and social networking service where users post and interact with messages, "tweets", and restricted to140 characters. Registered users can post tweets, but those who are unregistered can only read them. Users access Twitter through its website interface, SMS or a mobile device app.

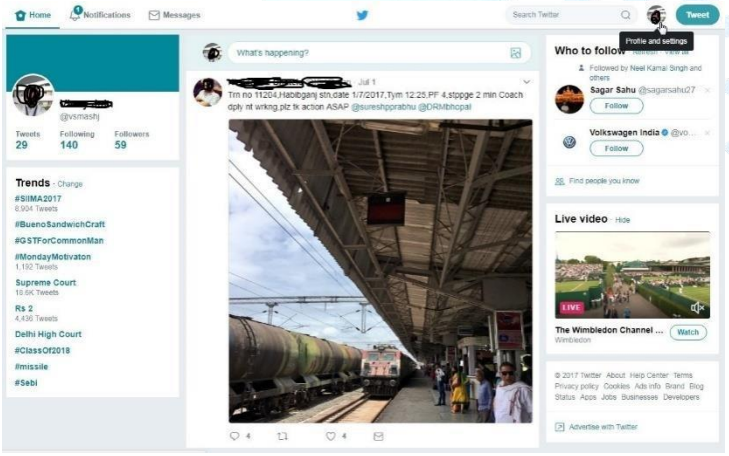
Step1:

Login to Twitter using the required ID and password.

Screenshot of ’login page of Twitter’

Step2:

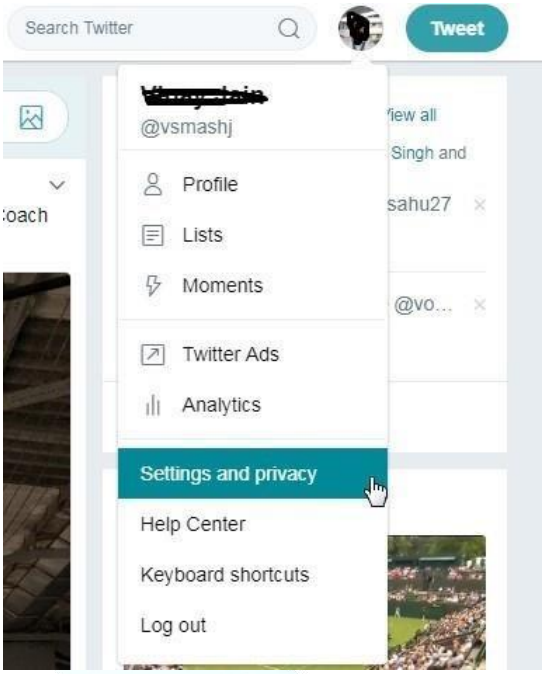
Click on profile picture on top-right to open the drop down menu.



Screenshot of ‘twitter logged in’ page by user

Step3:

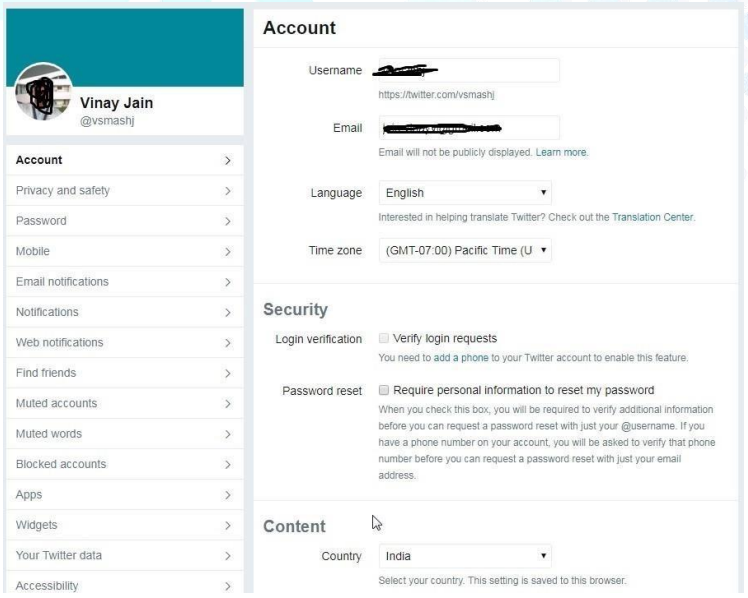
Select "Settings and privacy" option.



Screenshot of drop down menu from profile picture

Step4:

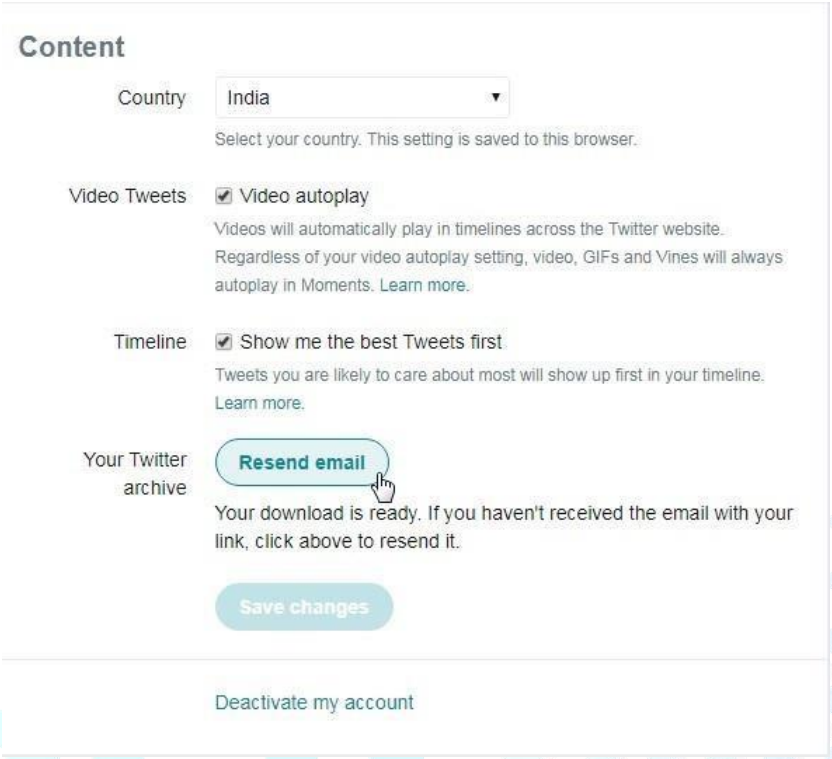
Scroll down on" Content" Section



Screenshot Illustrating step 4

Step5:

Click "Resend email" or "Create Archive" to provide a link to download archive.



Screenshot Illustrating Step 5

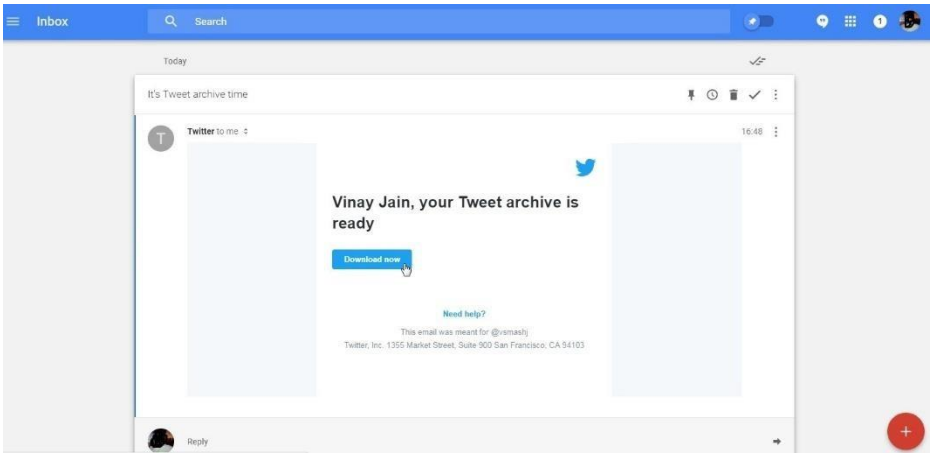
Step6:

Open the linked email account to download the archive by using the link.

Screenshot Illustrating Step 6 of Twitter Profile Archive

Step7:

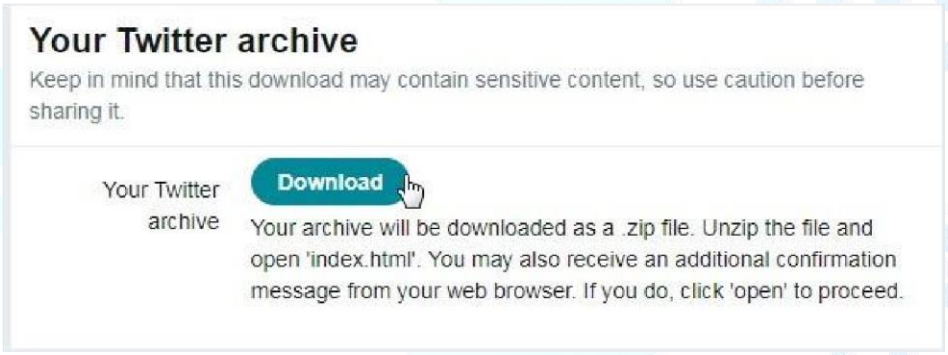
Click on the Download now



Screenshot Illustrating Step 7 of Twitter Profile Archive

Step8:

Pop up window with 'your twitter archive' comes with action of clicking Download.



ScreenshotIllustratingStep8

Step9:

Download complete and popup window with the url link shown and also the archive ready in folder.

Screenshot illustrating step 9 of Twitter Profile Archive

7.4 Reporting Objectionable content over Social Media

For reporting objectionable content over social media like Facebook, Twitter, Tagged etc., the investigating officer needs to know the login credentials.

7.4.1 Facebook

Once you login, go to the profile which you find to be objectionable.

Step1:

Click on icon of three dots as shown in the following picture and select "Report".

Screenshot of example of objectionable content in social media

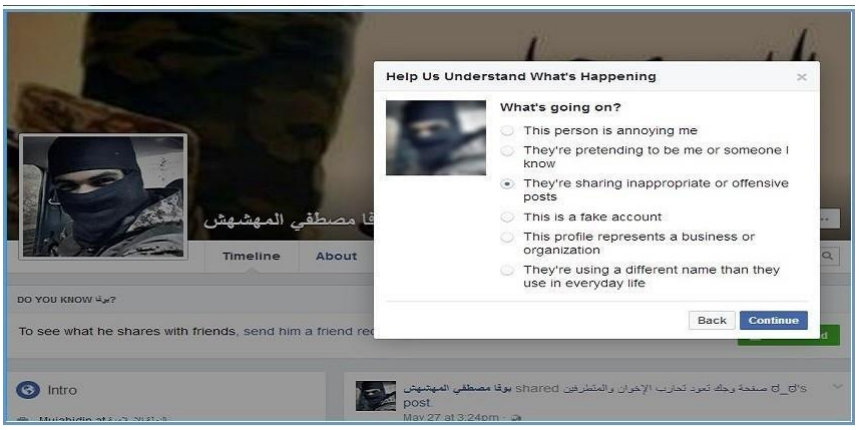
Step2:

Select the option "Report this profile".

Note: If the content is related to nudity or pornography select "Nudity and pornography", else if it is depicting sexual activities, then select "Sexually Suggestive", else select "Other"

Step3:

Select "They're sharing inappropriate or offensive posts".



Screenshot of example of objectionable content in social media with pop up dialog for 'They're sharing inappropriate or offensive posts'

Step4:

Proceed by choosing any options on the type of content to be reported and then click on

'continue'.

Screenshot of example of objectionable content in social media with pop up dialog for 'Nudity and pornography'

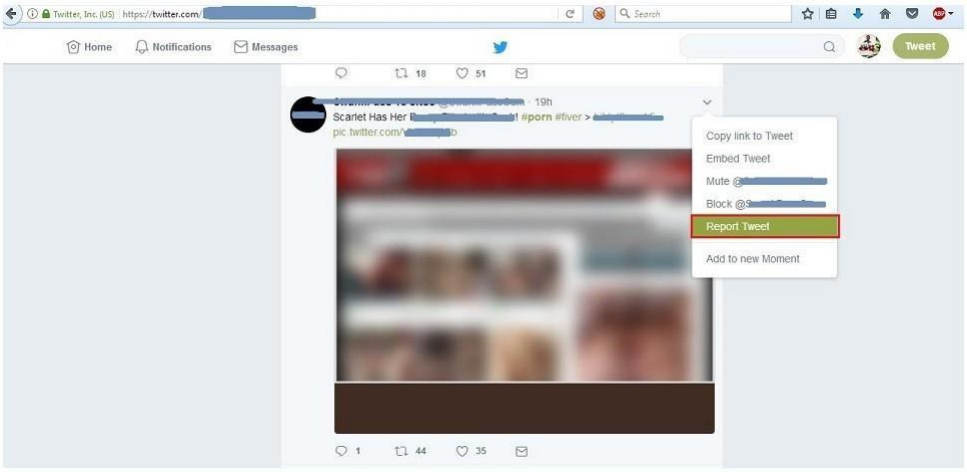
Step5:
Click on "Submit to Facebook for Review".

Screenshot of example of objectionable content in social media with pop up dialog for 'Submit to Facebook for Review'

7.4.2 Twitter Reporting

Step1:
Click or Tap the icon
Step2:

From the drop down menu, Click on **Report Tweet**



Screenshot of Twitter showing drop down window 'report tweet'

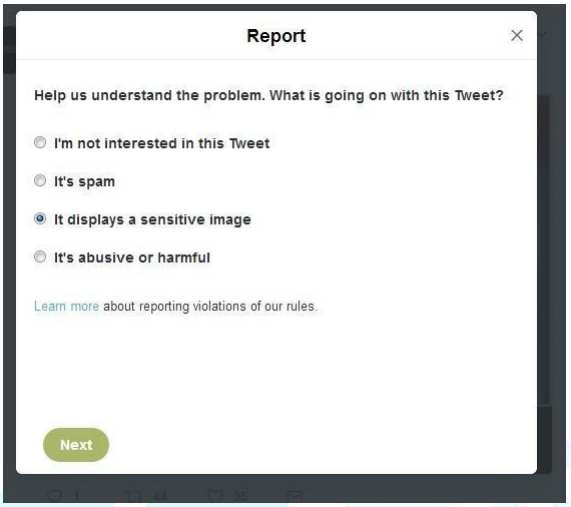
In Twitter the pornographic content tweeted by the user is possible, but re- porting a user for sharing pornographic content is not possible.

a) Reporting content shared by a user

Once you login, go to the tweet which you find to be objectionable.

Step3:

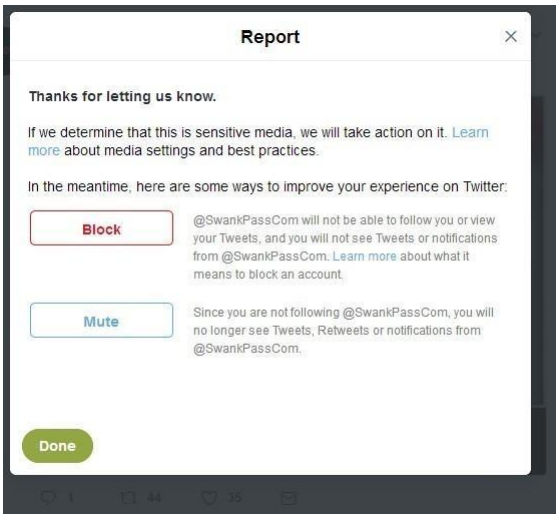
Choose the type of issue you'd like to report



Screenshot of Twitter showing drop down window 'what to report'

Step4:

You receive an acknowledgement upon submission.



Screenshot of acknowledgement upon submission

b) Reporting a user

Step1:

Open the profile you'd like to report.

Step2:

Select the overflow icon (on web and Twitter for Android) or tap the gear icon (on Twitter for iOS).

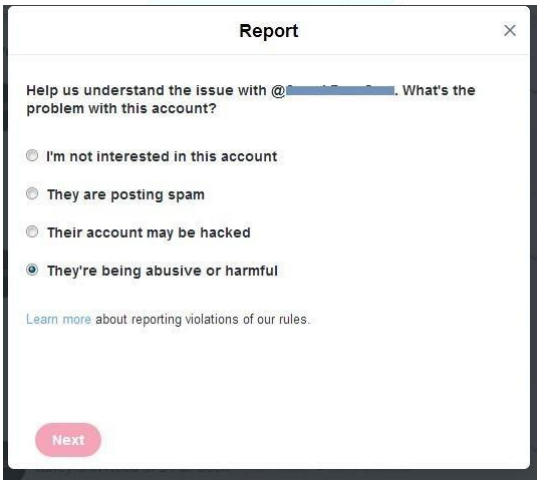
Step3:

Select Report and then select the type of issue you'd like to report.

Screenshot of Twitter profile page

Step4:

If you select They're being abusive or harmful, they'll ask you to provide additional information about the issue you're reporting.



Screenshot of window to choose on 'what issue to report'

Step5:

They may also ask you to select additional Tweets from the account you're reporting so they have better context to evaluate your report.

Screenshot of additional Tweets from the account being reported

7.4.3 Reporting in Tagged

Step1:

Login, find the profile which is objectionable. (Here its pornographic content in the profile picture) Then click on "Report Abuse".

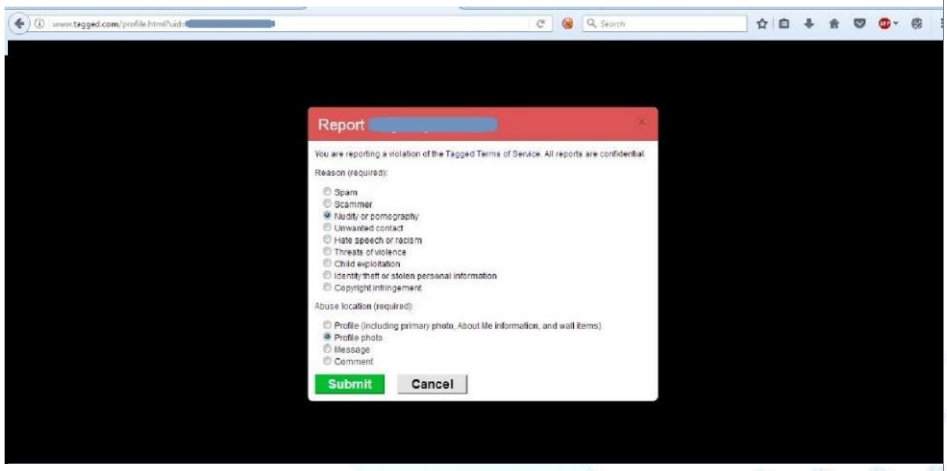
Screenshot of a profile with objectionable content

Step2:

Select reason as "Nudity or Pornography"

Step3:

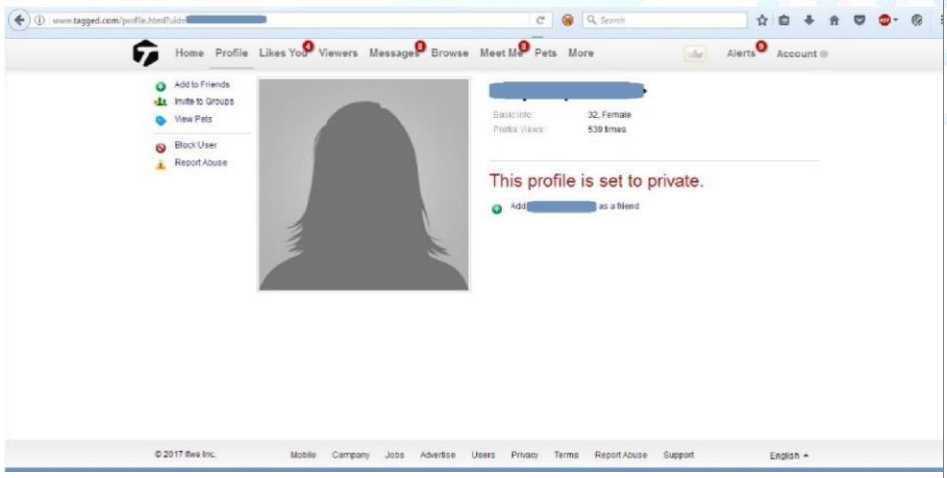
Select abuse location as "Profile photo". (Note: If the complete profile is sharing content projecting nudity or any sexual acts, select "Profile")and click on "Submit"



Screenshot illustrating Step 3 and 4 for reporting objectionable content in social media

Step4 :

The concerned team at Tagged will analyze and review the profile & content and will remove the content accordingly and will set the profile to be private.



Screenshot showing profile made private after reporting Objectionable content by another user

7.5 **Use of Social Media to Creating Awareness among People**

From Facebook to Twitter to LinkedIn, social media is changing the way people communicate across the globe. This is particularly evident in the areas of criminology and criminal justice, where law enforcement officers and researchers alike are finding new and unique ways to put social networking to use, both to solve crimes and to aware the public.

Fig 7.1: Mumbai police Facebook page

Many police organization use social media platforms such as Facebook, twitter, YouTube etc for many reasons like creating awareness among people, posting traffic updates, receiving complaints etc.

7.6 **Open Source Intelligence**

Open Source Intelligence can be defined as the retrieval, extraction and analysis of information from publicly available sources. Each of these three processes is the subject of ongoing research resulting in specialized techniques. Today the largest source of open source information is the Internet.

Most newspapers and news agencies have web sites with live updates on unfolding events, opinions and perspectives on world events are published. Most governments monitor news reports to feel the pulse of public opinion, and for early warning and current awareness of emerging crises.

The phenomenal growth in knowledge, data and opinions published on the Internet requires advanced software tools which allow analysts to cope with the overflow of information. Malicious use of the Internet has also grown rapidly particularly on-line fraud, illegal content, virtual stalking, and various scams. These are all creating major challenges to security and law enforcement agencies. The alarming increase in the use of the Internet by extremist and Terrorist groups has emerged. The number of terrorist linked websites has grown from about 15 in 1998 to some 4500 today.

These sites use slick multimedia to distil propaganda whose main purpose is to 1) enthuse and stir up rebellion in embedded communities 2) instill fear in the “enemy” and fight

psychological warfare. Anonymous communication between terrorist cells via bulletin boards, chat rooms and email is also prevalent.

The Joint Research Centre has developed significant experience in Internet content monitoring through its work on media monitoring (EMM) for the European Commission. EMM forms the core of the Commissions daily press monitoring service, and has also been adopted by the European Council Situation Centre for their ODIN system. A new research topic at the JRC is Web mining and open source intelligence. This applies EMM technology to the wider Internet and not just to news sites. This applies advanced multi-lingual search techniques to identify potential web resources and the extraction and download of all the textual content. This is then followed by automatic change detection, the recognition of places, names and relationships, and further analysis of the resultant large bodies of text. These tools help analysts to process large amounts of documents and derive structured data easier to analyse.

This talk will review 4 main topics:

- Internet trends and the rapid rise of Web 2.0 user generated content
- Information retrieval: Live content monitoring of multilingual news reports. Web scraping & RSS feed generation, Web Mining and content monitoring
- Information Extraction: Topic filtering, Topic Clustering, multilingual named entity extraction, geocoding and geolocation text, event extraction, opinion mining.
- Information Analysis: Social Network derivation, geospatial indexing and analysis, incident tracking databases, statistical trend analysis, threat monitoring and assessment.

7.6.1 Various kinds of intelligence:

There are five main ways of collecting intelligence that are often collectively referred to as “intelligence collection disciplines”.

- **Human Intelligence** (HUMINT) is the collection of information from human sources. The collection may be done openly, as when FBI agents interview witnesses or suspects, or it may be done through clandestine or covert means (espionage). Within the United States, HUMINT collection is the FBI’s responsibility. Beyond U.S. borders, HUMINT is generally collected by the CIA, but also by other U.S. components abroad. Although HUMINT is an important collection discipline for the FBI, we also collect intelligence through other methods, including SIGINT, MASINT, and OSINT.
- **Signals Intelligence** (SIGINT) refers to electronic transmissions that can be collected by ships, planes, ground sites, or satellites. Communications Intelligence (COMINT) is a type of SIGINT and refers to the interception of communications between two parties. U.S. SIGINT satellites are designed and built by the National Reconnaissance Office, although conducting U.S. signals intelligence activities is primarily the responsibility of the National Security Agency (NSA).

- **Imagery Intelligence** (IMINT) is sometimes also referred to as photo intelligence (PHOTINT). One of the earliest forms of IMINT took place during the Civil War, when soldiers were sent up in balloons to gather intelligence about their surroundings. IMINT was practiced to a greater extent in World Wars I and II when both sides took photographs from airplanes. Today, the National Reconnaissance Office designs, builds, and operates imagery satellites, while the National Geospatial-Intelligence Agency is largely responsible for processing and using the imagery.
- **Measurement and Signatures Intelligence** (MASINT) is a relatively littleknown collection discipline that concerns weapons capabilities and industrial activities. MASINT includes the advanced processing and use of data gathered from overhead and airborne IMINT and SIGINT collection systems. Telemetry Intelligence (TELINT) is sometimes used to indicate data relayed by weapons during tests, while electronic intelligence (ELINT) can indicate electronic emissions picked up from modern weapons and tracking systems. Both TELINT and ELINT can be types of SIGINT and contribute to MASINT.
- **The Defense Intelligence Agency's Central MASINT Office** (CMO), is the principal user of MASINT data. Measurement and Signatures Intelligence has become increasingly important due to growing concern about the existence and spread of weapons of mass destruction. MASINT can be used, for example, to help identify chemical weapons or pinpoint the specific features of unknown weapons systems. The FBI's extensive forensic work is a type of MASINT. The FBI Laboratory's Chem-Bio Sciences Unit, for example, provides analysis to detect traces of chemical, biological, or nuclear materials to support the prevention, investigation, and prosecution of terrorist activities.
- **Open-Source Intelligence** (OSINT) refers to a broad array of information and sources that are generally available, including information obtained from the media (newspapers, radio, television, etc.), professional and academic records (papers, conferences, professional associations, etc.), and public data (government reports, demographics, hearings, speeches, etc.).

Case 1: Open Source Intelligence and Crime Prevention

According to the report, top intelligence officials in the New York City Police Department met on Thursday to explore ways to identify "deranged" shooters before any attack. One of these tactics would involve "creating an algorithm" to identify keywords in online public sources indicative of an impending incident. In other words, they seek to build an algorithm to constantly monitor Facebook and Twitter for terms like "shoot" or "kill."

This is not a new idea. Its part of what the defense and intelligence communities call "open source intelligence" or OSINT. And it can raise serious First Amendment concerns, especially when it's used domestically and when it involves automated data mining by law enforcement agencies like the NYPD.

At the outset, it's important to understand exactly what we're talking about here. This is not tracking when police receive a tip that someone is posting public threats. Nor is it even a police officer taking it upon herself to scour for leads. Here, we're talking about a computer at the NYPD automatically reading every post on a social networking site and flagging entries with certain words for police scrutiny. This raises numerous constitutional concerns, many obvious and some less so.

First, even when you're talking about relatively sophisticated algorithms that, for instance, are able to distinguish between homonyms or polysemes (like "shoot" with a basketball versus a gun), you're going to get a vast universe of false positives. Additionally, you're also going to get true-false positives—people making dumb threats on their Facebook page as, for instance, a joke. To the extent these are "true threats" directed at an individual, they receive lesser First Amendment protection, but "true threats" are going to be a small subset of the vast amount of idiotic trolling that happens on social media on a daily basis. This problem presents an insurmountable administrative burden, not to mention the fact the digital dragnet will ensnare numerous innocent people.

Second, and aside from these practical concerns, we have a First Amendment right to be free from government monitoring, even when engaged in public activity.
Just because an anti-war group meets in a church that is open to the public doesn't mean the FBI should be able to spy on them. The same principle applies in the digital ether. The government should need a good reason—specific to a person—before it can go and monitor that person's activity. Why? Because if we fear that one peaceful protest is being monitored, we fear they all will be. And, people who would otherwise engage in lawful protest won't. It puts a big wet blanket on political discourse.

Third—and my colleague Mike German gets credit for this insight—when somebody gets snagged by these dragnets, it's very difficult to clear the "cloud of suspicion." Consider the case of Richard Jewell, the late security guard who was initially praised as a hero in the 1996 Atlanta Olympics bombing and then became the prime suspect based, in part, on statements he made to the press. FBI agents, working under the profile of a "lone bomber" who planted the device only in order to heroically find it, reviewed Jewell's television appearances and believed they matched. Although the investigation smacks of confirmation bias—agents seeing what they wanted to see—Jewell had great trouble escaping the cloud of suspicion.
With an algorithm tracking everyone's public statements on social media, take that problem and multiply it many-fold.

Finally, there is the very obvious problem that authorities are unlikely to uncover legitimately probative evidence of an impending shooting through automated OSINT. Put another way, it's exceedingly rare—and I'm not aware of a case—where a mass murderer *clearly* announced his or her intention beforehand on YouTube, Facebook or Twitter. Rather, automated OSINT will likely start zeroing in, as indicative of dangerous intent, on indications of mental instability, extreme political views or just weird thoughts. These all qualify as constitutionally protected speech, and, indeed, political

speech is often said to receive the highest level of First Amendment protection. (I would say that to the extent that an individual does take to a Facebook wall to issue a credible threat, that should of course be reported.)

All of this is to say that automated OSINT, in addition to being constitutionally problematic, just won't work. It will divert limited law enforcement resources; focus investigative activity on quacks more than dangerous individuals; and increase the risk that police will miss the true threat, made in private to a trusted confidante, which does deserves swift action to protect the public. It's a bad idea.

7.6.2 Why Open Source Intelligence is Important?

Although open sources of information have always been important to intelligence activities throughout the ages, there are a number of technological drivers that have now greatly expanded the utility, availability and breadth of OSINT. The advent of the WWW in 1990 has led to an exponential growth in information in digital form. The information age has resulted in the general public having the ability to publish information or multimedia quickly and cheaply worldwide audience. The explosion in readily accessible data has greatly increased the availability of OSINT from a wide variety of sources. During the same period, that has been an accompanying explosion in computer power. The PC user now has the ability to store and instantaneously retrieve massive amounts of data inexpensively. As a result, a laptop computer equipped with two Terabytes of hard drive storage can store the entire contents of a large university library and retrieve the information based on keyword query in a fraction of a second.

Globalization has also played an important role in increasing the utility of OSINT. The increased importance of OSINT has come as a result of the realization that it can provide information on a broad range of topics that was previously only available through the other INTs. OSINT's ability to provide global coverage at significantly less cost and lower risk has meant that the more limited, expensive and dangerous collection technology, globalization and communication tools such as social networking continue to redefine how we live our lives, the OSINT discipline will increasingly redefine the business of Intelligence.

7.7 Conclusion

Social media is a huge part of the internet, and on each site, there is a tremendous amount of things to learn about how to use it, reporting illicit content, requesting for the data related to any activity from the social media platforms. Police organizations today getting cases like fake profiles, fake news etc. That it is the reason why investigating the case related to social media has become challenge for law enforcement agency.

Social media platforms also help law enforcement agencies in performing the various kinds of analysis (crime, sentiment and behavior).It also helps in locating the suspect location based on the IP address. Most of the police organizations are making

social media sites as a platform to create awareness among the people regarding various crimes happening in the locality, traffic updates, emergency messages etc.

8. WINDOWS & NETWORK FORENSICS

8.1 Windows Forensics & Its Importance

Microsoft Windows is a graphical user interface (GUI) operating system that has been distributed in various forms since 1985. Overtime, windows became the most common operating system that was installed on a computer system. Each version has brought changes to the user interface, though not all have been popular. Each version has had different ways of storing data that is of forensics value to the examiner.

An artifact refers to anything man-made – a Windows artifact, for the purpose of computer forensics, is evidential data that is automatically saved by the windows operating system as a result of a person interacting with or using the computer. It does not refer to the default files that saved to the computer on install – most of which may have no bearing on an investigation.

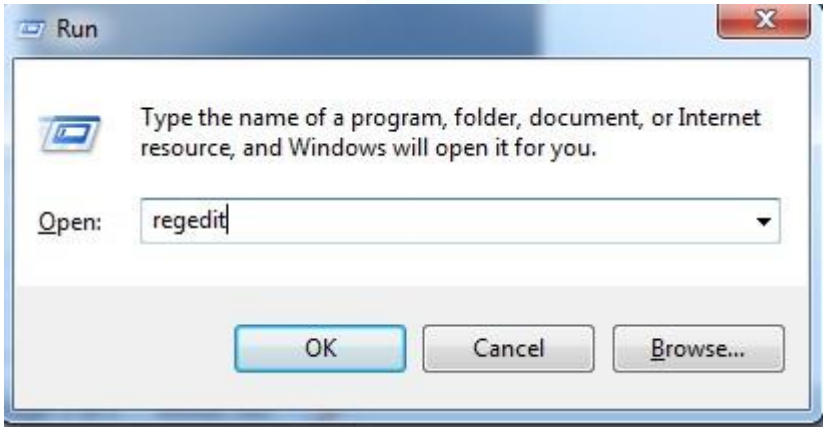
8.2 Artefacts in Windows System and Their Analysis

Windows Registry

Windows Registry is a repository for configuration and settings information for the operating system and for other software, such as applications. It can be thought of as a file system optimized for small files implemented in kernel mode and exposed to user mode.
The registry is stored on disk as several different files called "hives." One, the System hive, is loaded early in the boot sequence and provides configuration information required at that time. Additional registry hives, providing software-specific and user-specific data, are loaded during later phases of system initialization and during user login, respectively.

It is a hierarchical database which maintains configuration settings and data related to Applications, Hardware, Devices and Users of a Windows based Operating System.

To open the registry editor, goto **start > run** and type **regedit** and hit enter.

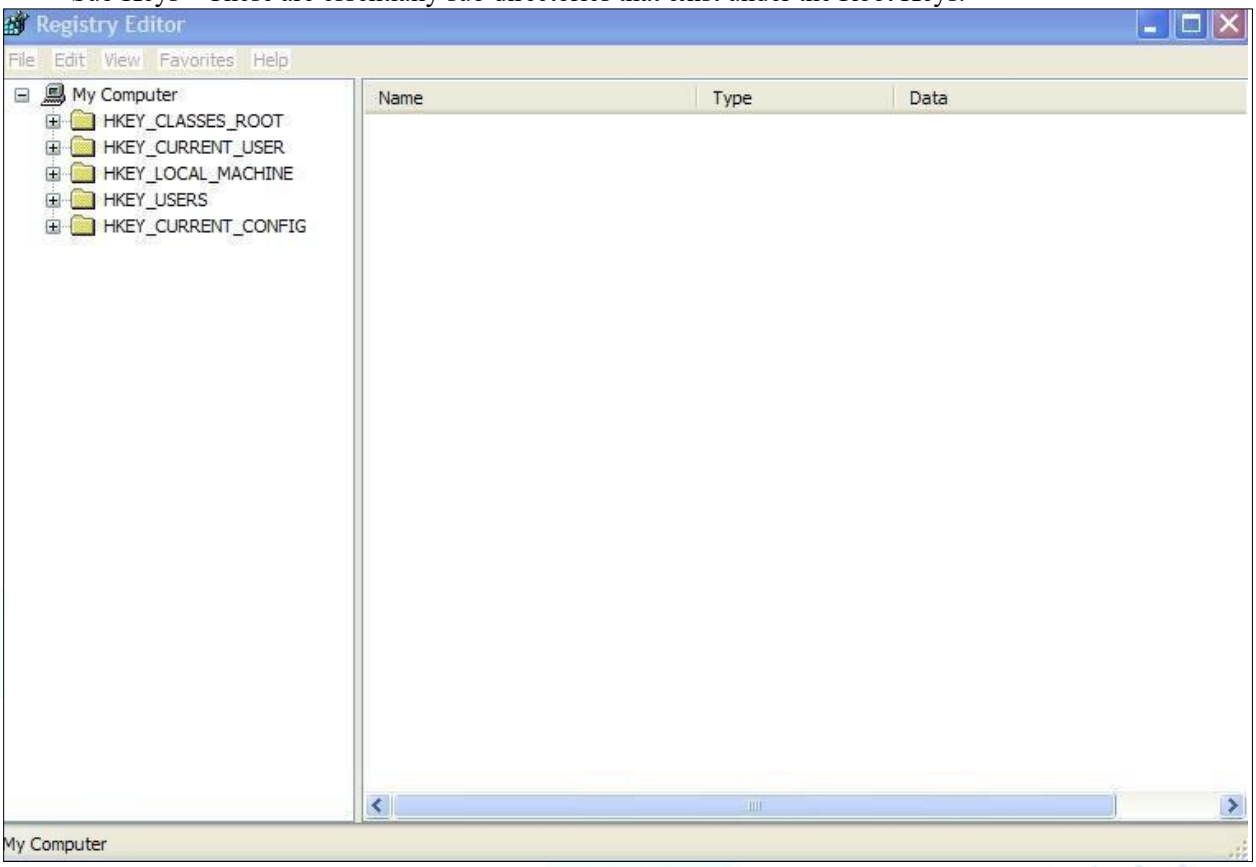


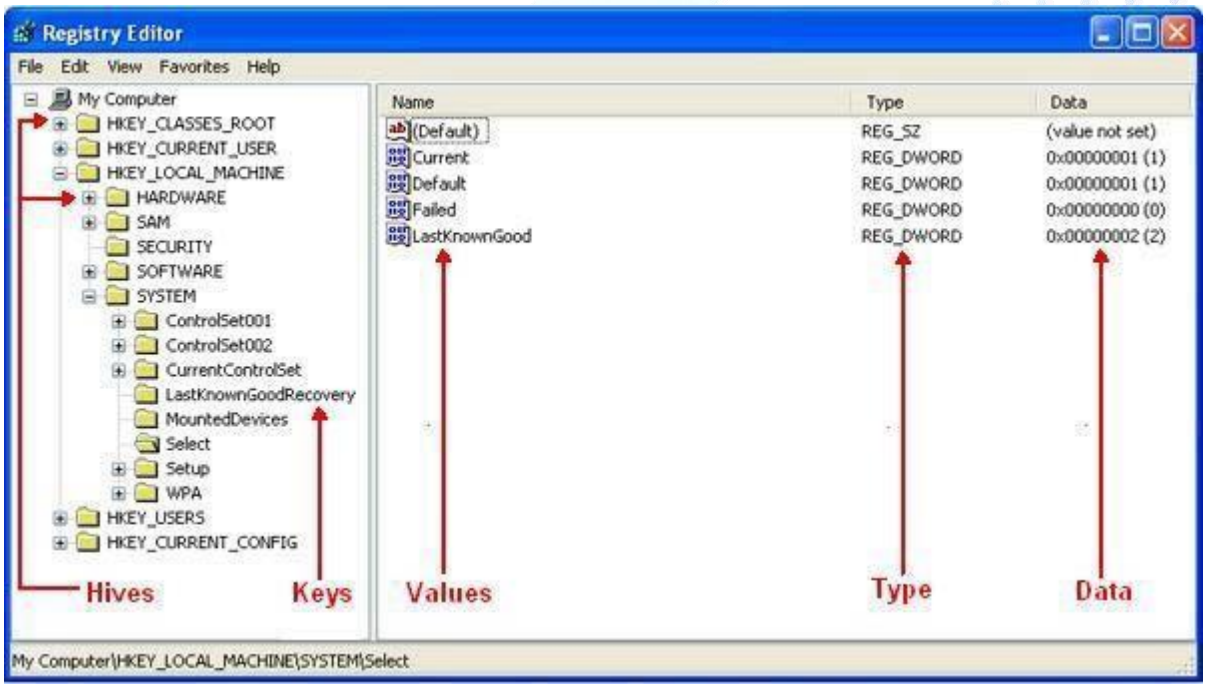
Registry Organisation

• Root Keys
– HKEY_CLASSES_ROOT (HKCR)
• Contains information in order that the correct program opens when executing a file with Windows Explorer.
– HKEY_CURRENT_USER (HKCU)

• Contains the profile (settings, etc) about the user that is logged in.
– HKEY_LOCAL_MACHINE (HKLM)
• Contains system-wide hardware settings and configuration information.
– HKEY_USERS (HKU)
• Contains the root of all user profiles that exist on the system.
– HKEY_CURRENT_CONFIG (HKCC)

- Contains information about the hardware profile used by the computer during start up.
- Sub Keys – These are essentially sub directories that exist under the Root Keys.





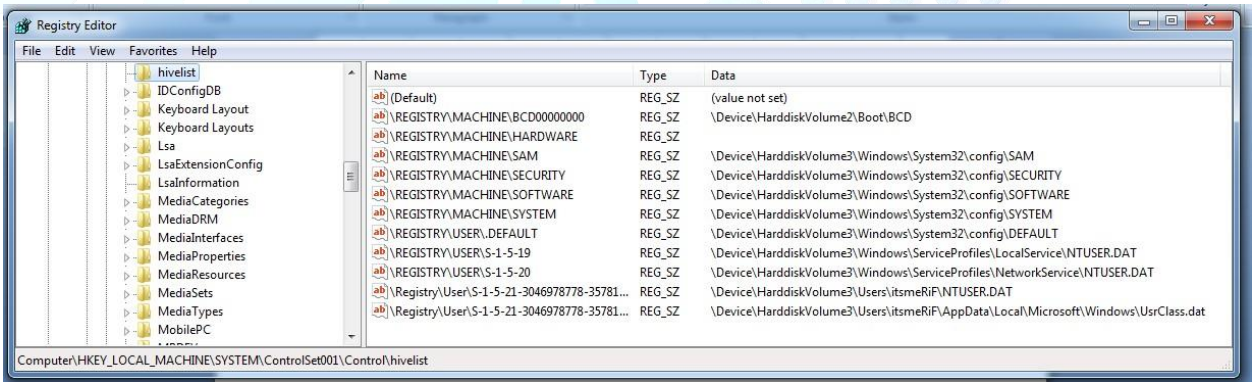
Hive properties in brief

- HKEY_USERS – all loaded user data
- HKEY_CURRENT_USER – currently logged on user
- HKEY_LOCAL_MACHINE – array of software and hardware settings
- HKEY_CURRENT_CONFIG – hardware and software settings at start-up
- HKEY_CLASSES_ROOT – contains information about application needs to be used to open files

Registry-to-File correspondence

Hive Registry Path	Hive File Path
HKEY_LOCAL_MACHINE\SYSTEM	\Windows\System32\Config\System
HKEY_LOCAL_MACHINE\SAM	\Windows\System32\Config\Sam
HKEY_LOCAL_MACHINE\SECURITY	\Windows\System32\Config\Security
HKEY_LOCAL_MACHINE\SOFTWARE	\Windows\System32\Config\Software
HKEY_LOCAL_MACHINE\HARDWARE	Volatile hive
HKEY_LOCAL_MACHINE\SYSTEM\Clone	Volatile hive (Win 2K only)
HKEY_USERS\<SID of Username>	\Documents and settings\<username>\Ntuser.dat
HKEY_USERS\<SID of Username>_Classes	\Documents and Settings\<username>\Local Settings\Application Data\Microsoft\Windows\Usrclass.dat
HKEY_USERS\.DEFAULT	\Windows\System32\Config\Default

Hive file locations



File locations and purpose

Filename and location	Purpose of file
Windows 9x/Me	
Windows\System.dat	User-protected storage area; contains installed program settings, usernames and passwords associated with installed programs, and system settings
Windows\User.dat Windows\profile*UserAccount*	Contains the most recently used (MRU) files list and desktop configuration settings; every user account created on the system has its own user data file
Windows NT, 2000, XP, and Vista	
Documents and Settings*user-account*\ Ntuser.dat (in Vista, Users*UserAccount*\ Ntuser.dat)	User-protected storage area; contains the MRU files list and desktop configuration settings
Winnt\system32\config\Default	Contains the computer's system settings
Winnt\system32\config\SAM	Contains user account management and security settings
Winnt\system32\config\Security	Contains the computer's security settings
Winnt\system32\config\Software	Contains installed programs settings and associated usernames and passwords
Winnt\system32\config\System	Contains additional computer system settings

Types of Registry Forensics and analysis

There are four types of Registry Forensics & Analysis methods which are as follows:

- Perform a GUI-based live-system analysis ➲ Easiest Method.
  - ➲ Use regedit, FTK Imager OsF, Etc.

- Perform a command-line live-system analysis
  - ➲ Use "reg" command.

- Remote live system analysis
  - ➲ regedit allows access to a remote registry
  - ➲ Superscan 3.0 from McAfee

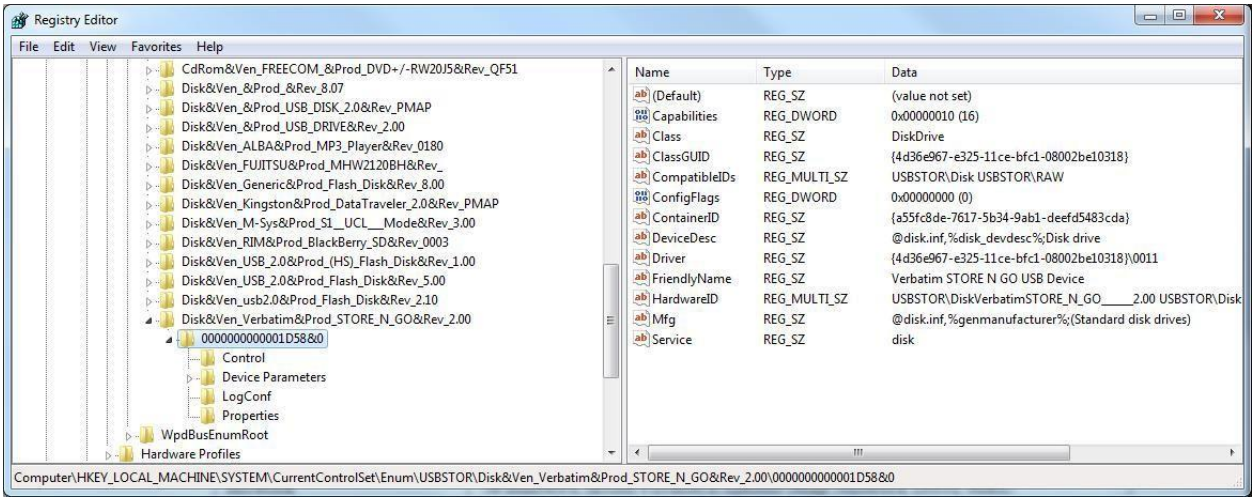
- Offline analysis on registry files.
  - ➲ Encase, FTK (Access data) have specialized tools ➲ regedit on registry dump.

How Registry can give artifacts for Forensic Analysis?

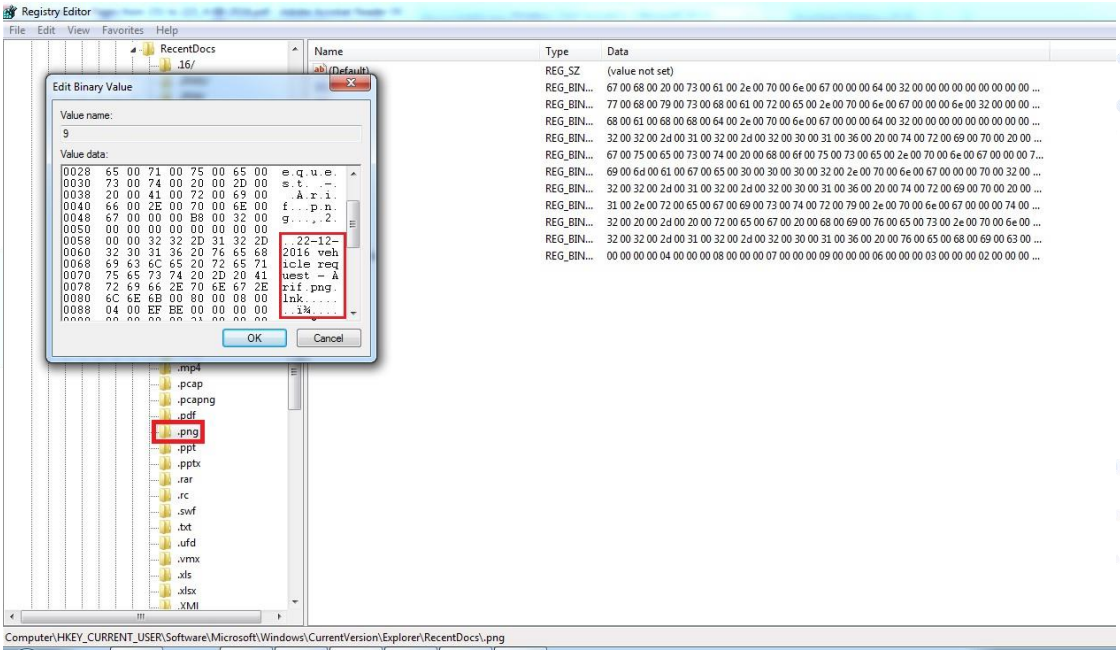
Registry Analysis can reveal a lot of information from a computer which are important artifacts for an Investigator or Analyst.

Some of the important questions framed in a questionnaire which can be answered by Registry Analysis are as follows:

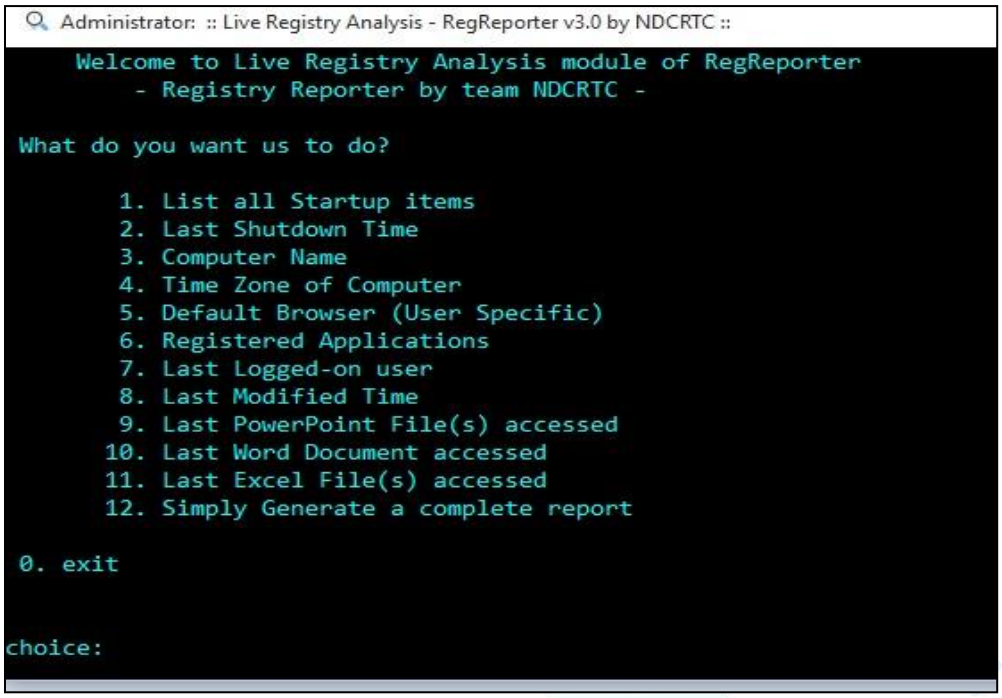
- USB devices connected
- Most Recently accessed files
- Time Zone of a computer



The image above reveals information collected from Registry about USB devices which were connected to the target computer.

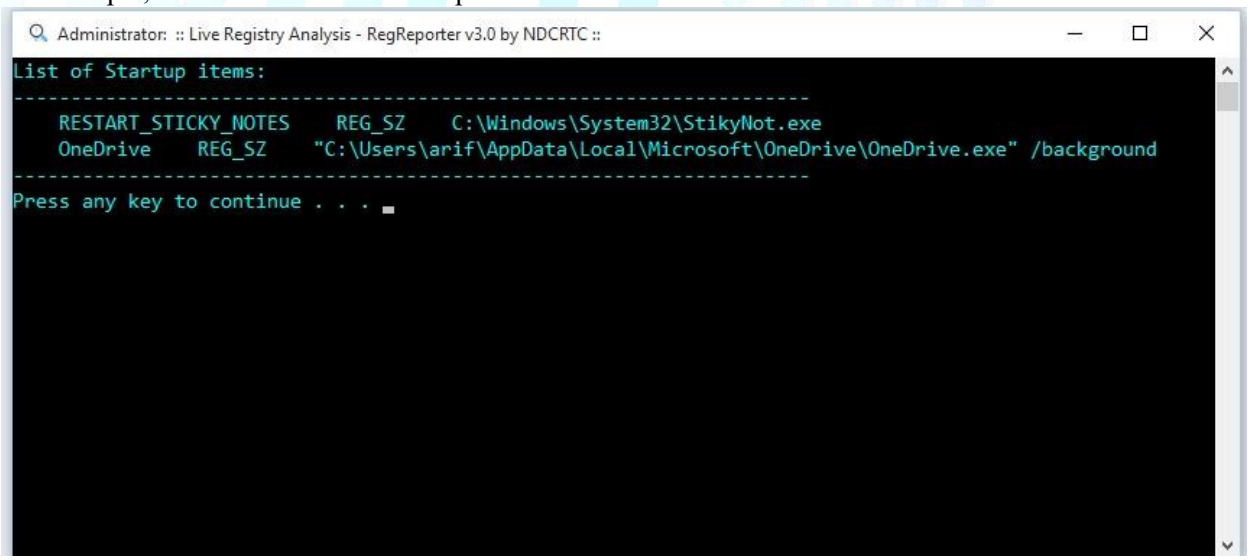


The image above reveals information about the most recently accessed files on the target computer. (Here, the recently accessed PNG files are shown). Similarly, various other artifacts can be collected from the Registry. A simple tool developed by team NDCRTC can be useful to fetch few important artifacts without having to manually search all the hives.



The tool provides options to perform Live / Online Registry Analysis and as well as Offline Registry Analysis The picture shows the menu of Live Registry Analysis. Here, the most common questions from a questionnaire can be answered from Registry.

For example, let's see a list of all startup items.



Thus, registry can help the forensic analyst in ascertaining the facts which can be more important in the cases.

LOG ANALYSIS

What is log?

Log is a systematic daily or hourly record of activities, events, and/or occurrences in a computer. Logging is the act of keeping a log. In the simplest case, messages are written to a single log file.

Types of logs:

Computer or System Logs : Detailed list of an application information, system performance, or user activities. A log can be useful for keeping track of computer use, emergency recovery, and application improvement.

Computer Log file is a file that records either events that occur in an operating system or other software runs, or messages between different users of a communication software.

Why do we perform Log Analysis?

• Compliance with security policies

• Compliance with audit or regulation

• System troubleshooting

• Forensics (during investigations, or in response to Summons)

• Security incident response

Benefits of Logs

– Logs provide clues about performance issues, application function problems, intrusion and attack attempts etc.

– The logs provide vital inputs for managing the computer security incidents, both for Incident Prevention and Incident Response Benefits

– When responding to computer security incident, logs provide leads to the activities performed over the system

– Facilitates cyber crime investigation

- Determine the activity
- Determine the origin of attack **What are the sources of Logs?**

- System Logs
- Web Server Logs • Firewall logs
- Mail Server Logs
- Database Server Logs
- FTP Logs

Windows Event Logs

The windows operating system is built on a complex architecture with which to handle events like logging on requires proper security measures. The system logs and application logs can be used in a number of ways of writing specific events to the log. Windows also has a specific type of logging, the security logging system, which can only be written by the Local Security Authority Sub-system Service or LSASS. The windows event logging system logs events like account logon, account management, directory service access, object access, policy change, privilege use, process tracking, and system events.

Windows Operating System maintains primarily three types of logs, which are as follows:

- Security Logs

– valid and invalid login attempts

– resource use such as creating, opening, or deleting files or other objects

- Application Logs
  – events logged by applications or programs
  – Depends on developer
- System Logs

  – events logged by system components

  Example: Functioning of drivers

How do we view the logs of a Windows Operating System?

Event Viewer, a component of Microsoft's Windows NT line of operating systems, lets administrators and users view the event logs on a local or remote machine.

To access Event viewer, follow these steps:

Goto **Start** > **Control Panel** > **Administrative Tools**

(or)
Goto **Start** > **Run** and type "**eventvwr.msc**"

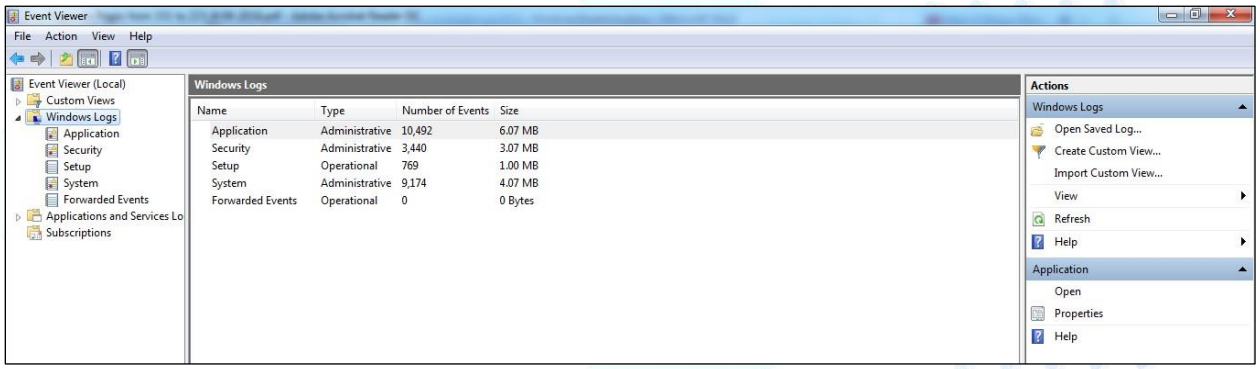


Image: Windows Event Viewer

You can find all the events in the Event Viewer window. You can also access them manually from the following location: C:\Windows\system32\Winevt

They are stored with these file extensions : *.evt, *.evtx

Some important Events which can be found in Logs, are as follows:

Local logon attempt failures

- Event IDs 529, 530, 531, 532, 533, 534, and 537

Account Misuse

- Events IDs 530, 531, 532, and 533

Account Lockouts

- Event ID 539

Terminal Services attacks

- Terminal Services sessions can be left in a connected state that allows processes to continue running after the session is ended. Event ID 683 indicates when a user does not log out from the Terminal Services session, and Event ID 682 indicates when a connection to a previously disconnected session has occurred.

Policy Change

- Event ID 608: User right assigned
- Event ID 609: User right removed

Application Server Logs

• Web Server logs –

Error Logs

– Access Logs

• Mail Server logs

– Connection Status

– SMTP queues

– Protocol Status (IMAP, POP3, SMTP)

• FTP Server Logs

– Current logins

– Commands executed

– File uploaded and downloaded

• Database Server Logs –

User activity

– Objects accessed

– Creation of new tables, databases, etc..

Note: Windows Operating System has a default firewall of its own and the logs generated by that even can be very helpful in analysis.

• Firewall logs

– Firewall logs provide useful information about

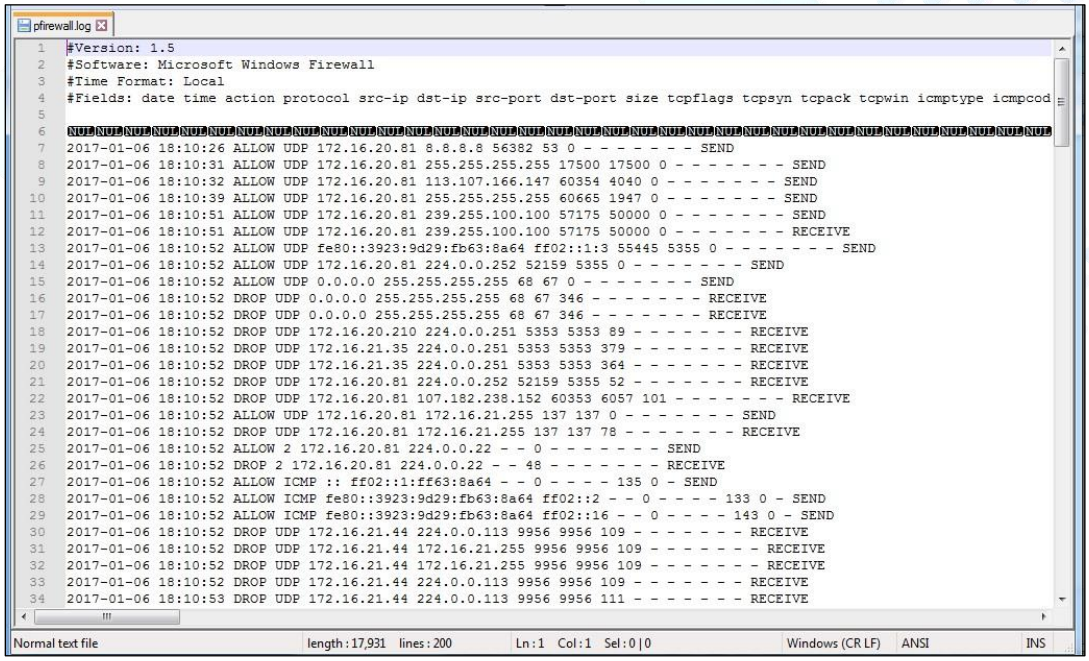
- The inbound and outbound packets
- Information about particular servers e.g. Web Server
- Packets which have been dropped
- Alerts to the System Administrator
- Probing the system

By default, the Windows Firewall Logs are stored at: C:\Windows\System32\LogFiles\pfirewall.log (if 'C:' is your drive where Windows is installed)

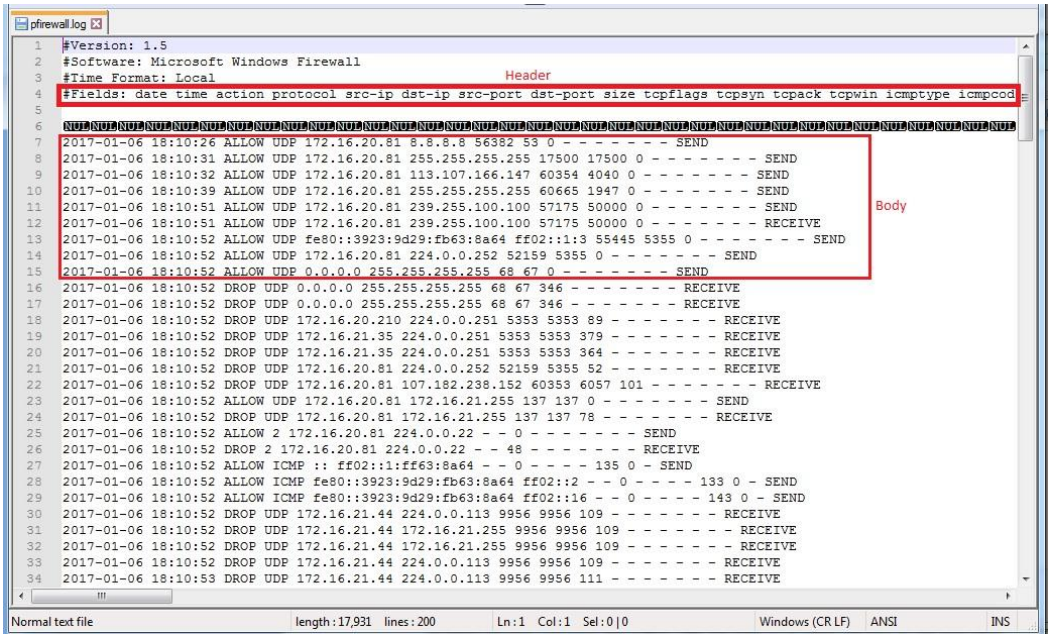
Why and when is Firewall Logging useful?

- To verify if newly added firewall rules work properly or to debug them if they do not work as expected.
- To determine if Windows Firewall is the cause of application failures — With the Firewall logging feature you can check for disabled port openings, dynamic port openings, analyze dropped packets with push and urgent flags and analyze dropped packets on the send path.
- To help and identify malicious activity — With the Firewall logging feature you can check if any malicious activity is occurring within your network or not, although you must remember it does not provide the information needed to track down the source of the activity.
- If you notice repeated unsuccessful attempts to access your firewall and/or other high profile systems from one IP address (or group of IP addresses), then you might want to write a rule to drop all connections from that IP space (making sure that the IP address isn't being spoofed).
- Outgoing connections coming from internal servers such as Web servers could be an indication that someone is using your system to launch attacks against computers located on other networks.

A Windows Firewall log looks as following:



It can be explained as follows:



While dealing with Logs, there are a few problems associated with it too, such as:

- Non availability of proper logs

– No auditing

– Insufficient security

– Poor management of Logs

- With logs available

– Volume

– Storage space, portability

– Skills

8.3 Overview of Network Forensics

Network Forensics is a process of collecting and analysing 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, there's more focus on this field and increasing demand for skilled technicians. Labour forecasts predict a shortfall of 50,000 network forensics specialists in Law Enforcement, Legal firms, corporations, and universities.

You might hear the terms Cyber Forensics or Digital Forensics; they usually refer to network forensics, not computer forensics.

When intruders break into a network, they leave a trail behind. Being able to spot variations in network traffic can help you track intrusions, so knowing your 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 a.m. to 6:30 p.m. because that is the duration of 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 unusual activity and could take steps to investigate it.

Network forensics can also help you determine whether a network is truly under attack or a user has unknowingly installed a custom program.

Network forensics examiners must establish standard procedures for how to acquire data after an attack or intrusion incident. Typically, network administrators want to find compromised machines, get them offline, and restore them as quickly as possible to minimize downtime.

However, taking the time to follow standard procedures is essential to ensure that all compromised systems have been found and to ascertain attack methods in an effort to prevent them from happening again.

Securing a Network

Network Forensics is used to determine how a security breach occurred; however, steps must be taken to harden networks before a security breach happens, particularly with recent increase in network attacks, viruses, and other security incidents. Hardening includes a range of tasks, from applying the latest patches to using a layered network defence strategy, which sets up layers of protection to hide the most valuable data at the innermost part of the network. It also ensures that the deeper into the network an attacker gets, the more difficult access becomes and the more safeguards are in the place.

Testing networks is as important as testing servers. You need to be up to date on the latest methods intruders use to infiltrate networks as well as methods internal employees use to sabotage networks. In the early and mid-1990s, approximately 70% of network attacks were caused by internal employees. Since then, this problem has been compounded by contract employees, who often have the same level of network privileges as full-time employees.

In addition, small companies of fewer than 10 employees often don't consider security precautions against internal threats necessary, so the can be more susceptible to problems caused by employees revealing proprietary information to competitors. However, increasing use of the internet has caused a sharp rise in external threats, so internal and external threats are currently about 50-50.

8.4 Scope of Network Forensics

Network forensics plays a critical role in the cloud computing environment but with limitations that tie the network forensics deeply to systems and computer forensics. Network forensics is best applied where the network is owned by the company at the boundary and into the desktops or systems that access cloud resources. Network forensics works in the cloud environment when the company has addressed many of the limitations of network forensics in the cloud when the company is still building out their cloud infrastructure. It is possible to go back and retrofit an in-built forensics capability, and it should be done if the capability to conduct forensics was not part of the original business plan of moving information and systems into the cloud.

Network forensics can also have an influence on the outcome of an investigation into an event as long as data was collected at the box and at the entry and exit points of the company network. The use of inbuilt firewall logs, system logs, and other logs will generally point to an entry time, place, and IP address that can be used to help determine how the event was propagated through the network and what steps can be taken to help 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 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 your network or facilities team has maintained a good database of these associations, then you can find the physical location of the suspected computer. Otherwise, you will need 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, you are left to pulling on wires and following the cable, which may or may not be possible with walls and floors in place.

8.5 Standard Operating Procedure of Network Data

Search and seizure of Network Data basically includes collection of data from Network devices such as Routers, Firewall, Modems, and computers which are connected with the network.

Criminals now a days are heavily using Network based servers in committing their crimes apart from using Computer, Mobile and Laptops etc.

For example – If a death threat email is sent by using an email server which is hosted by the criminal, then the email server will essentially have to be seized in order to preserve the evidence.

Similarly, in a case of Denial of Service (DoS) attack on an organization or network, the traces are found on the network devices.

The recent case of "Bangladesh Bank heist" further emphasizes the importance of having an ability to investigate network device in order to find relevant evidences of the crime.

Hence, it becomes pertinent to have a Standard Operating Procedure (SOP) to seize such Network devices. Electronic records such as Network Logs, Firewall logs, FTP logs and File Server Logs etc. play an important role in gathering the evidences in network-based crimes.

• *Search & Seizure of Digital Evidence from Network* ***Step1:***

Before You Twitch

- ★ Consent search or Search warrant
  - ✞ Understand the nature of the crime
  - ✞ Read the search warrant
- ★ Concerns
  - ✞ Safety – It is a crime scene
  - ✞ Destruction of potential evidence
- ★ Plan, Plan, Plan
  - ✞ The seizure
  - ✞ The collection techniques
  - ✞ The order of events

Step2:- What to Take Along

1) Evidence Tape
2) Chain of Custody forms
3) Reading Glasses

4) Inventory forms
5) Camera (battery, memory)
6) Backup disposable camera
7) Tool kit. Jewelers set. Needle nose pliers.
8) Sharpies, pens
9) Adhesive tape
10) New, wiped and verified Hard Drives in Pelican, w/lock
11) Gloves
12) Static wrist bands
13) Tableau Pelican (ATA, SCSI, eSATA, Firefly) with power supplies and line cords. Firewire I/F cables, laptop adaptor. Small laptop adaptor.
14) Firewire I/F board.
15) Several USB mouse. Two PS mouse.
16) Laptop with X-Ways and FTK (crossover tested)
17) eSATA interface
18) USB-small USB cable
19) PS2/USB converter
20) Small flatscreen monitor
21) UPS
22) Extension cord
23) Power strip (2)
24) Digital Media Flash reader
25) DOS Boot w/Firewire USB.
26) DOS Boot with utilities
27) 1GB NIC
28) ATA interface with cable
29) CDs with WinHex, FTK, Linen,
30) Boot CD with Helix/Lenin, Boot USB
31) F-Response CD
32) Dongles – FTK, X-Ways, F-Response
33) Flashlight
34) Powered USB Hub
35) Magnifying Glass

36) Blank Labels
37) Bottle water
38) RFID readers/writers
39) Credit card readers/writers
40) Smart card readers/writers
41) Bar code readers/writers

Step3: Think About Potential Evidence

- ✞ Probable cause to seize HW?
- ✞ Probable cause to seize SW?
- ✞ Probable cause to seize Data? Such as – network logs, firewall logs, Pcap Files, FTP logs, File system logs
- ✞ Where will the search of the seized evidence be conducted?
- ✞ Careful of business interruption issues and proprietary information.
- ✞ Depends on the role of the computers in the crime.

Step4: Prior to Serving the Warrant

- ✞ Start your investigation report
- ✞ Understand the nature of the crime
- ✞ Describe the role of the computer/digital device in the crime
- ✞ Describe the limits of your investigation
- ✞ Probable cause for seizure
- ✞ What can be seized
- ✞ What can be looked at
- ✞ Where is the search to be conducted?

Step5: Seize what ?

- ✞ HW
- ✞ SW
- ✞ Data - Such as – network logs, firewall logs, Pcap Files, FTP logs, File system logs ✞ All things digital
- ✞ All things related to digital
- ✞ Media, notes, documentation
- ✞ Stay within the bounds of the search warrant

Step 6: Search or Seizure Where -

- ✞ Secure the scene, restrict access
- ✞ Preserve the area, no more fingerprints ✞ Ensure the safety of all concerned ✞ Nobody touches nothing!
- ✞ Usually, the forensic specialist will not be a first responder. However, often they are.
- ✞ On site, in the field office, in a lab
- ✞ Disposal of seized items ✞ Consider the size of the seizure ✞ Suspects:

- Interview
- Passwords
- Location of data
- Installed software
- Network

Step 7: Tag & Bag

- Tape every drive slot shut
- Photograph, diagram and label all components
- Photograph, diagram and label all connections
- Photograph, diagram and label all cables – both ends
  You will have to reconstruct
- Pack it for transport
- Keep it away from EM
- Collect all printed material
  Docs, records, notes

Step8: Seizure

- If the network is active
  Do not power down any networking gear
  They have no hard drives
  All evidence is volatile
  If no significant network traffic disconnects from the ISP
- Using the USB device harvest the routers and switches
- Then disassemble the network
  Seize the servers and work stations
- Get the network admin to help
  They could corrupt the data, SO be careful
  - If OFF leave it off.
    Tag and bag
- If ON
  Photograph and document especially comm connections
  An attempt may be made to access memory and capture the most recently printed document.
  If the device is a scan first and then dispatch, everything is stored on the hard drive.
  Disconnect the comms interfaces
  Tag and bag
- Determine phone connections
  Subpoena service provider ***Step9:***

Other Stuff

- Docs, notes, documentation, etc.
- Credit cards, smart cards, RFIDs, etc
- CDs, DVDs – all media

Step 10: Security Systems

- Ingress/egress logs – time line, IDs

- Service provider
- System info
- Photograph and document location of all devices
- Text, video
- Tag and bag all stored data and recorded data.
- Detailed documentation – you can't tag and bag

Step11: After Pictures are taken from a "switched on" Network Device

- If the computer is a standalone PC
  - pull the plug
  - Vista is different
  - Do not turn it off
- If it is a laptop
  - Pull the plug
  - If it is still on, it has a functioning battery
  - Pull the battery
  - Keep the battery separate ***Step12: Photos Method***
- Items and placement
- Each Item
  - Placement
  - Model numbers, Serial numbers
  - Front
  - Back
  - Cables
  - Anything that might be of interest.
- You only get one chance to record the original evidence
- Floor plan
  - Locate all equipment
  - Number all equipment on the floor plan
  - You will have to reconstruct
- Photograph/Video graph
  - The entire area containing HW & cables
  - The screen of each computer that is on.

Steps14: Notes

- Keep a very detailed log of every operation action
  - Details
  - Time
  - Order
- They can cover a lot of mistakes during the seizure and search What did you do?
- What reasons for doing it.
- Itemize potential harm versus another way of doing it.

• *Crime Scene Scenarios (Network based Server)*

A. When Network Server is in Power ON condition –

Step I

- Isolating the accused working on the Computer if any and his/her Interrogation without allowing him/her to touch the Computer

– Step II

- Visible inspection of Scene of Crime in front of technically qualified independent witnesses without touching anything – Step III
- 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**
  - System in power on condition (Contd..) – Step IV
- Collection of finger print if required

– Step V

- Search for any kind of external memory devices like Pen Drive, Hard Disk, etc.

– Step VI

- **Collection of RAM dump and system information, encrypted files if any by the IO/ Cyber Forensic Expert**

– Step VII

- **Remove the power plug without shutting down the system**

– Step VIII

- Open the CPU and take a photograph of the inside view **showing all peripherals like Hard Disk, RAM, Motherboard** etc.
- Remove the Hard Disk

– Step IX

- Photography of the Hard Disk showing:
- Unique S. No. of the Hard Disk
- Connector Ports
- Jumper Position
- Logic Board

– Step X

- **Creation of 3 Images of Hard Disk and other external memory devices seized with Write Blocker**
- **Hash calculation**

– Step XI

- 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 XII

- Dispatching of HardDisk:
- 1st image to be sent to the Forensic Lab along with seizure list and questionnaire with permission of the court as per regular procedure
- 2nd image to be kept with IO for analysis
- 3rd image to be handed over to the accused party
- **Original Hard Disk and external memory devices along with seizure list to be sent to the Court along with other original documents at the time of submission of Final Report.**

- *Crime Scene Scenarios (MODEM)*

- Step I ○ Take Photographs of MODEM indicating its make and model along with serial numbers
- Step II ○ IF the MODEM is ON, then browse into the MODEM through any of the computer devices which is 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 III ○ IF the MODEM is switched off, then seize the Modem with proper chain of custody

- *If the IO is not technically qualified to handle Digital Evidence*

If System in Network Based environment –

Step I

- Visible inspection of Scene of Crime in front of technically qualified independent witnesses – Step II

- 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 III

- Collection of fingerprints if required

– Step IV

- Search for any kind of external memory devices like Pen Drive, Hard Disk, etc.

– Step V

- **Remove the power plug of the CPU without shutting down the system.**

– Step VI

– Open the CPU and take a photograph of the inside view **showing all peripherals like Hard Disk, RAM, Motherboard** etc.
- Remove the Hard Disk

– Step VII

- Photography of the Hard Disk showing :
- Unique S.No. of the Hard Disk
- Connector Ports
- Jumper Position
- Logic Board

– Step VIII

- 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 IX

- Dispatching of HardDisk:
- Original Hard Disk and external memory devices along with seizure list to be sent to the Forensic Lab with permission of the Court along with questionnaire

8.6 Packet Level Analysis in Network

Next, we are moving to packet level analysis. Select Analyze pane. Each Packet is represented in this as an entry with a short-detailed description. When we select each entry in the packet list the bottom windows (Packet tree and Packet hex view) are updated. Packet tree helps us to see the packet in a very detailed manner. It lists each protocol present in the packet including its fields. When we select each field in the packet tree that area is marked in the packet hex view with a blue color. This is applicable only to the protocols known to NeSA. In this too we can perform the search using the search dialog. The search hits are marked as in the Packet hex view. Packet filtering is also supported in this, but the filtering language is different from the session filter. The filtering language used in this is the well-known language used by tcpdump. For example, if you want to filter out only UDP packets enter the filter text “udp” in filter combo and press enter. It will filter out all the UDP packets present in the dump file. In this tool you can select multiple packets from Packet list and export it to view in other packet

analysis tools. The combined use of these features should help a person to analyse and extract evidence from a dump file.

- Wireshark

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.

You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, all that has changed.

Wireshark is perhaps one of the best open source packet analyzers available today.

Features

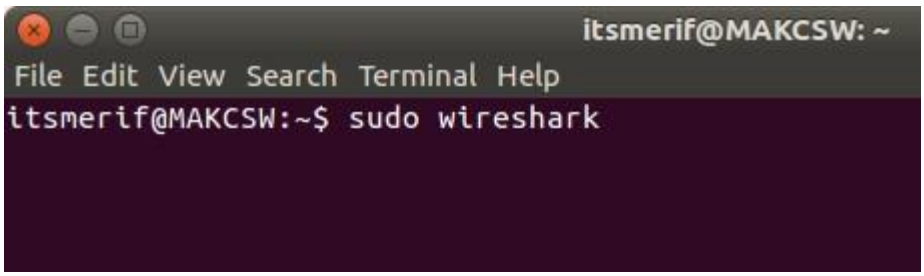
The following are some of the many features Wireshark provides:

- Available for *UNIX* and *Windows*.
- *Capture* live packet data from a network interface.
- *Open* files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.
- *Import* packets from text files containing hex dumps of packet data.
- Display packets with *very detailed protocol information*.
- *Save* packet data captured.
- *Export* some or all packets in a number of capture file formats.
- *Filter packets* on many criteria.
- *Search* for packets on many criteria.
- *Colorize* packet display based on filters.
- Create various *statistics*.

- *Using Wireshark*

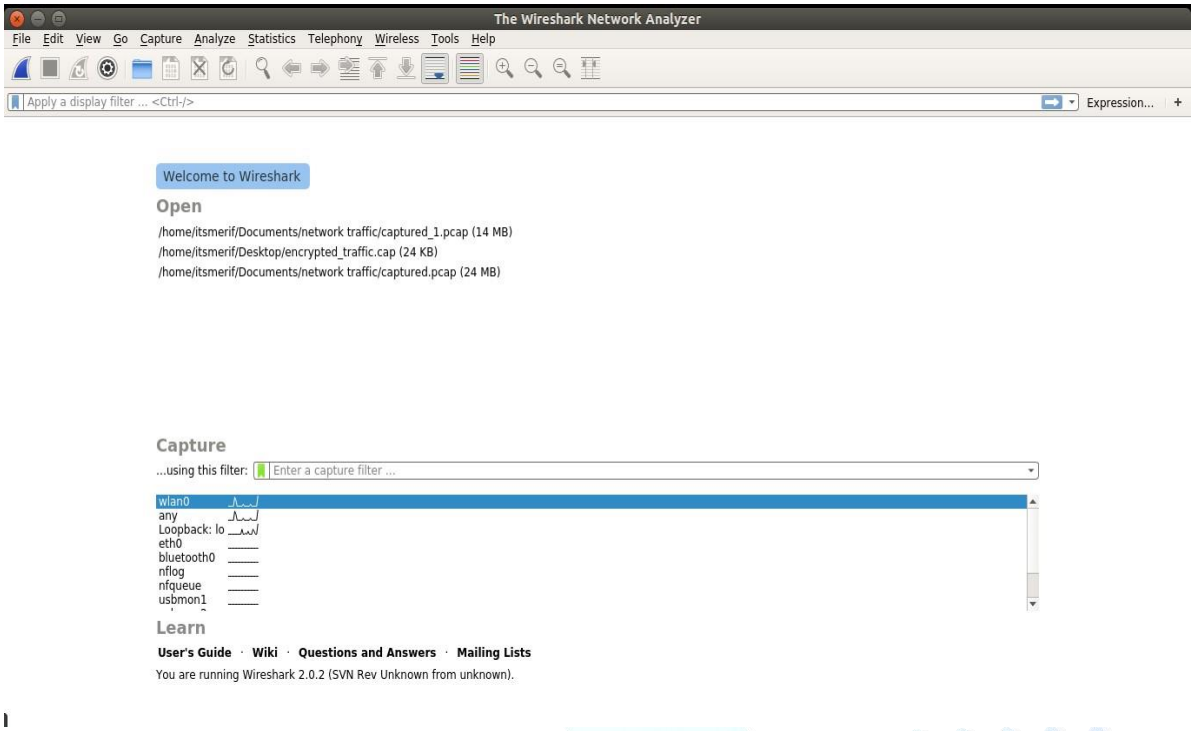
1. To run Wireshark in Linux, in monitor mode, we need to be a super user and Run Wireshark with the following command:

sudo wireshark

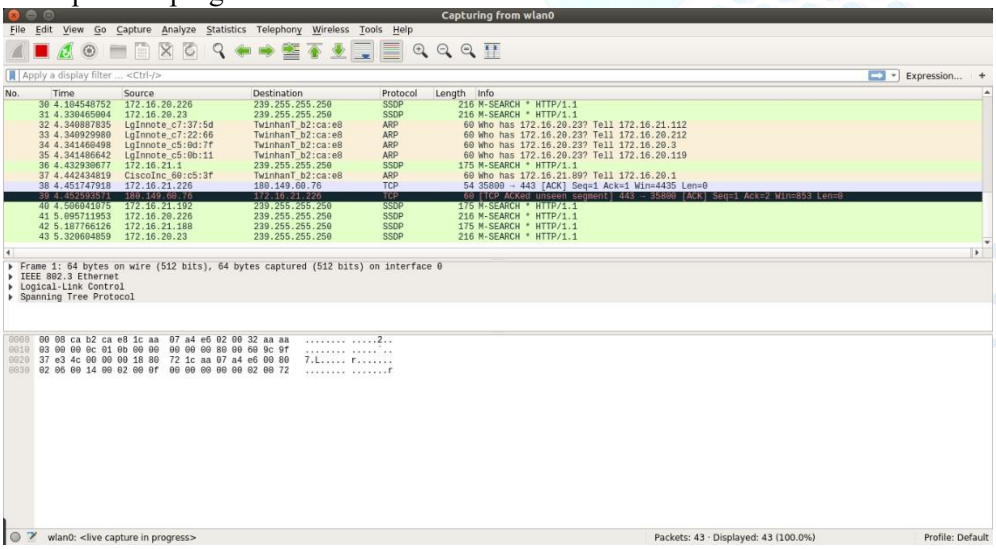


Microsoft Windows' Users can simply right-click on the Wireshark executable file and select "Run as Admin"

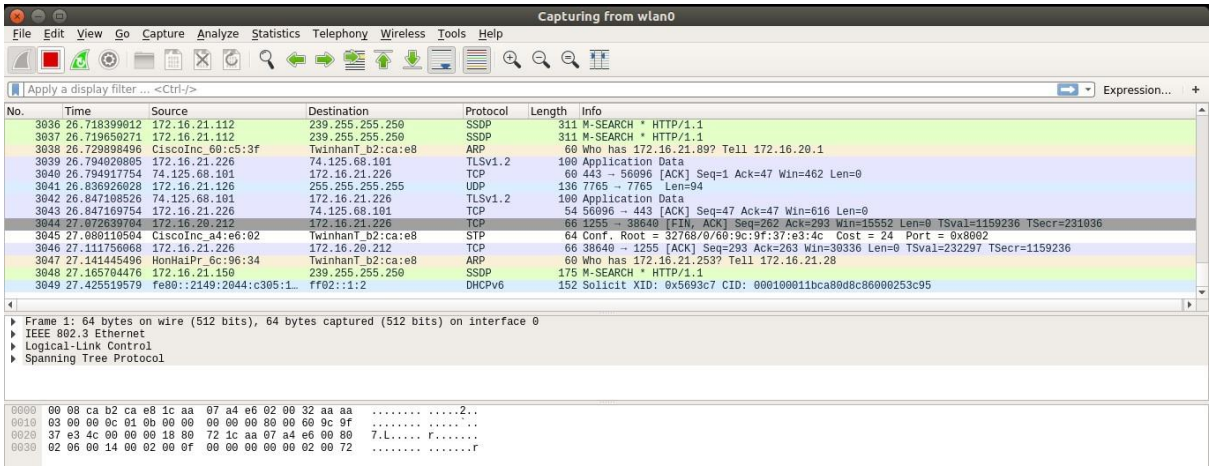
2. Select interface to start monitoring on; Here we are selecting our Wireless interface (wlan0)



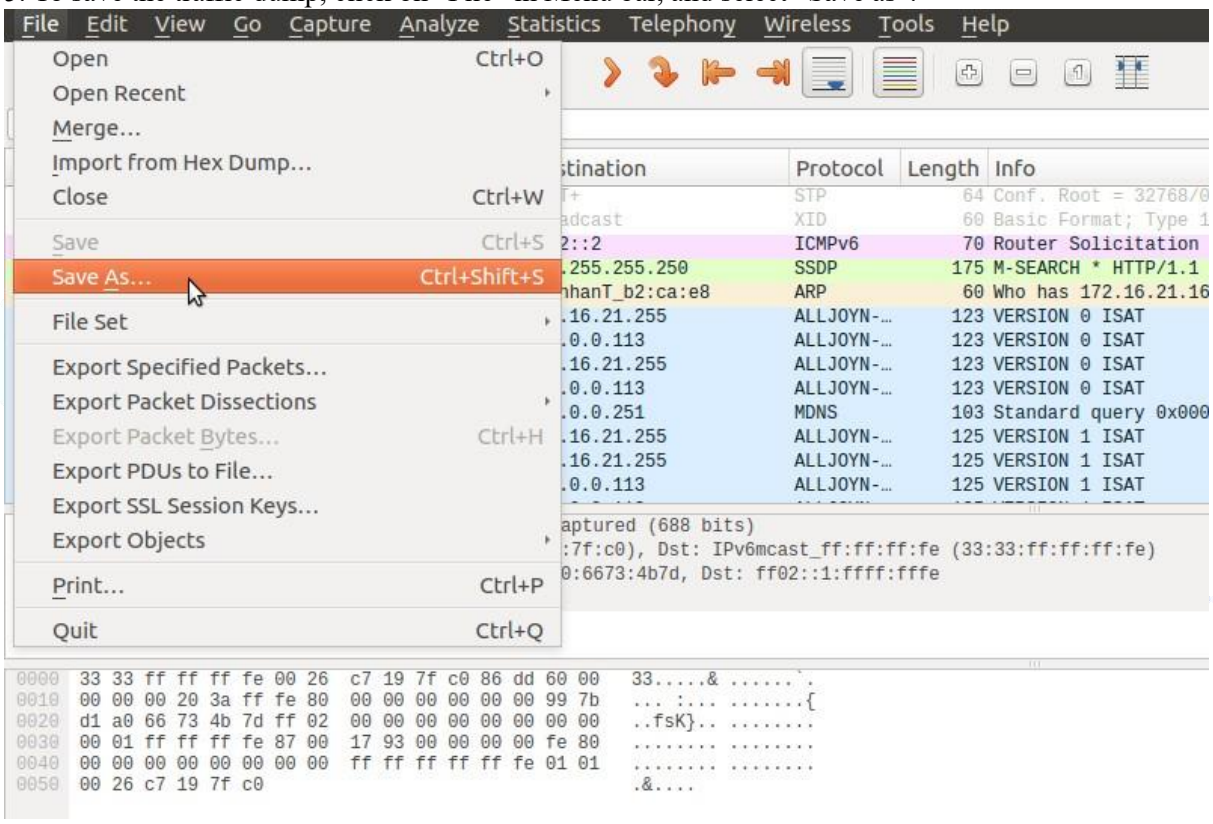
3. We can see capture in progress



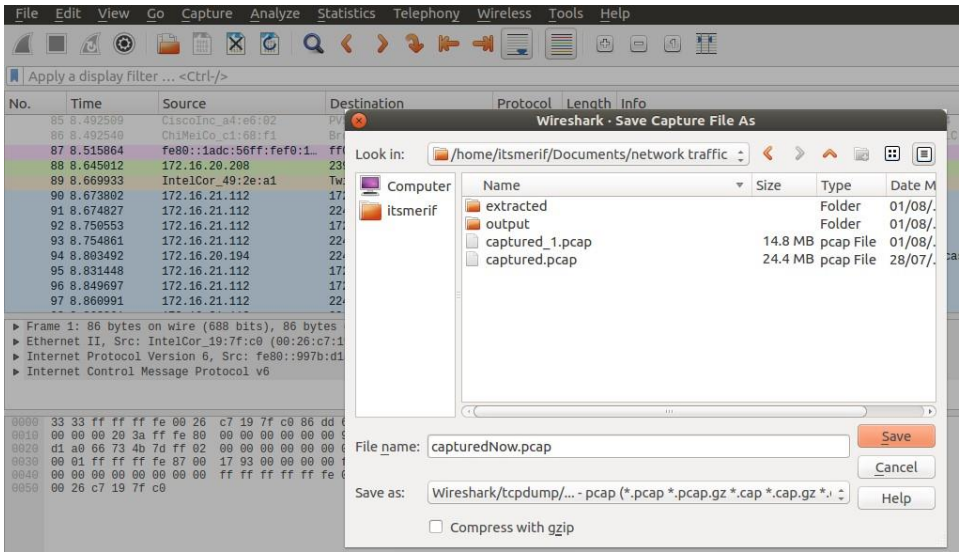
4. To stop capturing traffic, click on the stop button (in red).



5. To save the traffic dump, click on “File” in Menu bar, and select “Save as”.



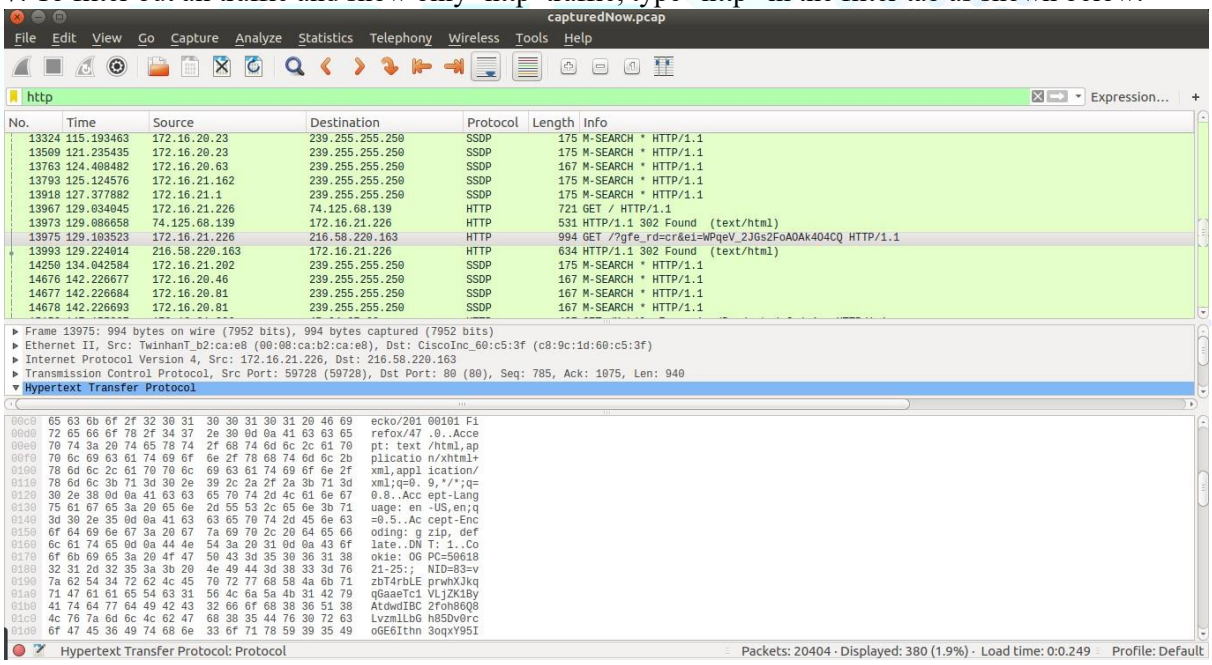
6. Save the file with any name, and in any available formats shown below:



Now, we can also use these pcap file(s) to analyse using various other tools as this format is supported by almost all the network forensics tools.

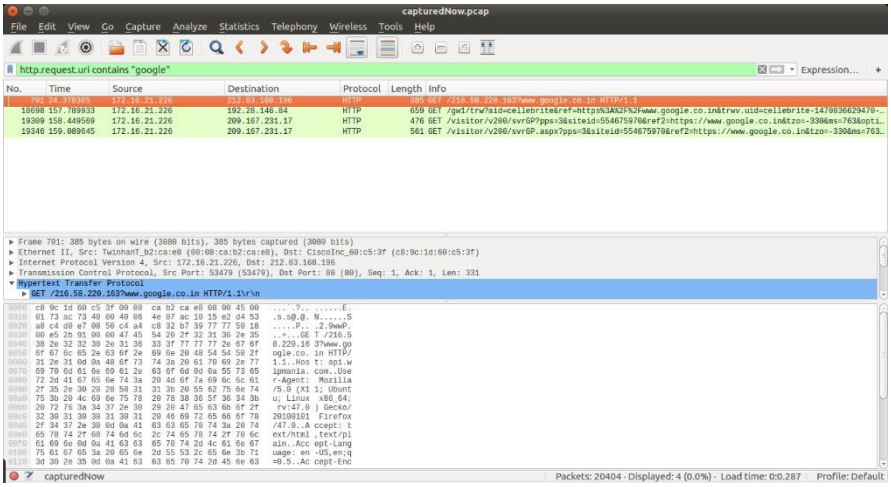
Let us try some basic filters in Wireshark.

7. To filter out all traffic and show only ‘http’ traffic, type “http” in the filter tab as shown below:

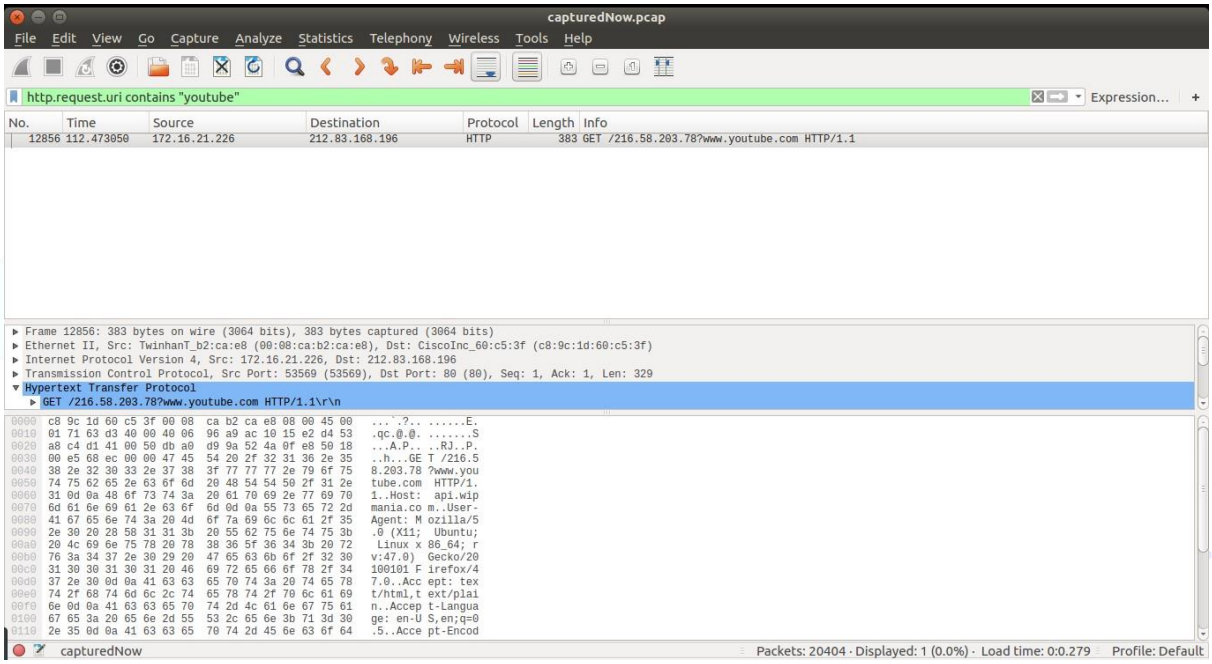


Similarly, we can also use ftp,smtp,smb,telnet,..etc to display respective traffic.

8. To find out if any user in the network had visited a website containing the keyword “google” in the domain, use the filter as follows: http.request.uri contains "google"

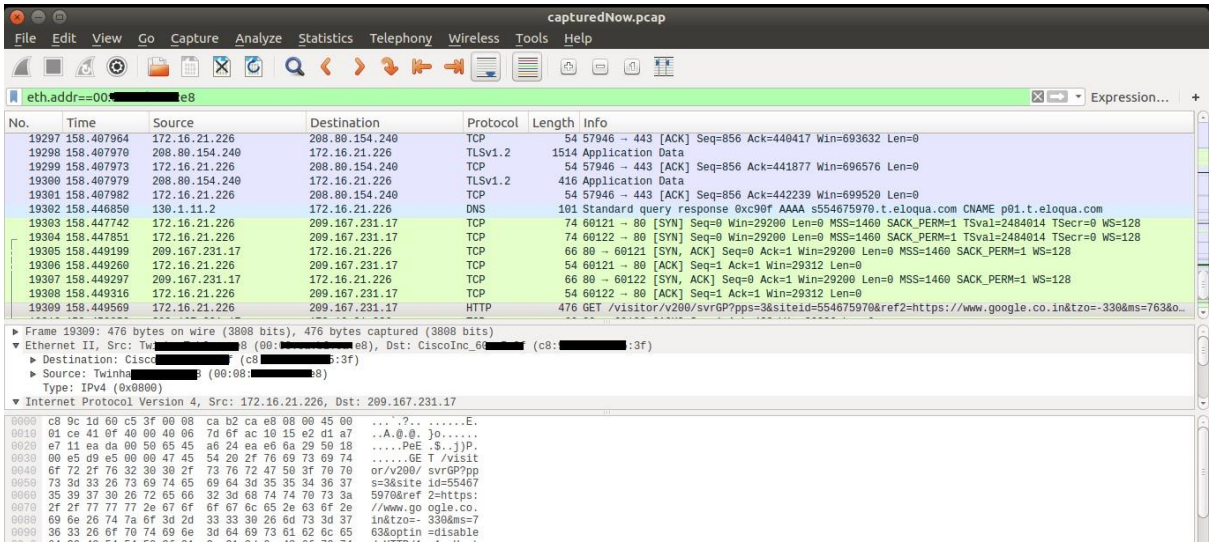


9. Similarly, to find out if any user in the network had visited YouTube website, or any website containing the keyword “youtube”, apply the following filter: http.request.uri contains "youtube"



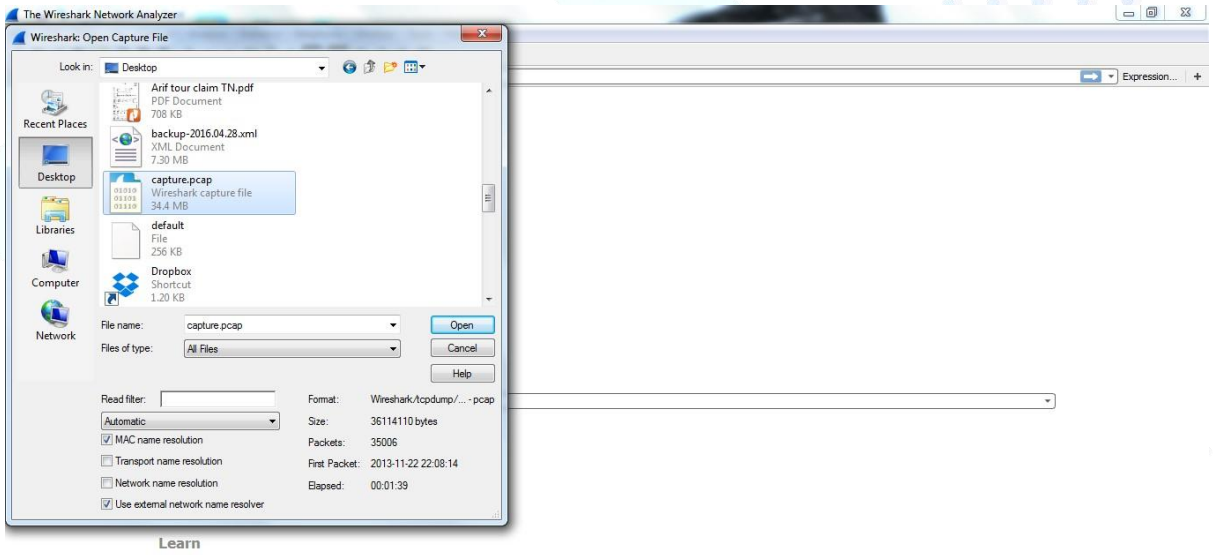
10.To find out if any network activity was done from a device having a specific MAC address, apply the following filter:

eth.addr==<MAC address of target device>

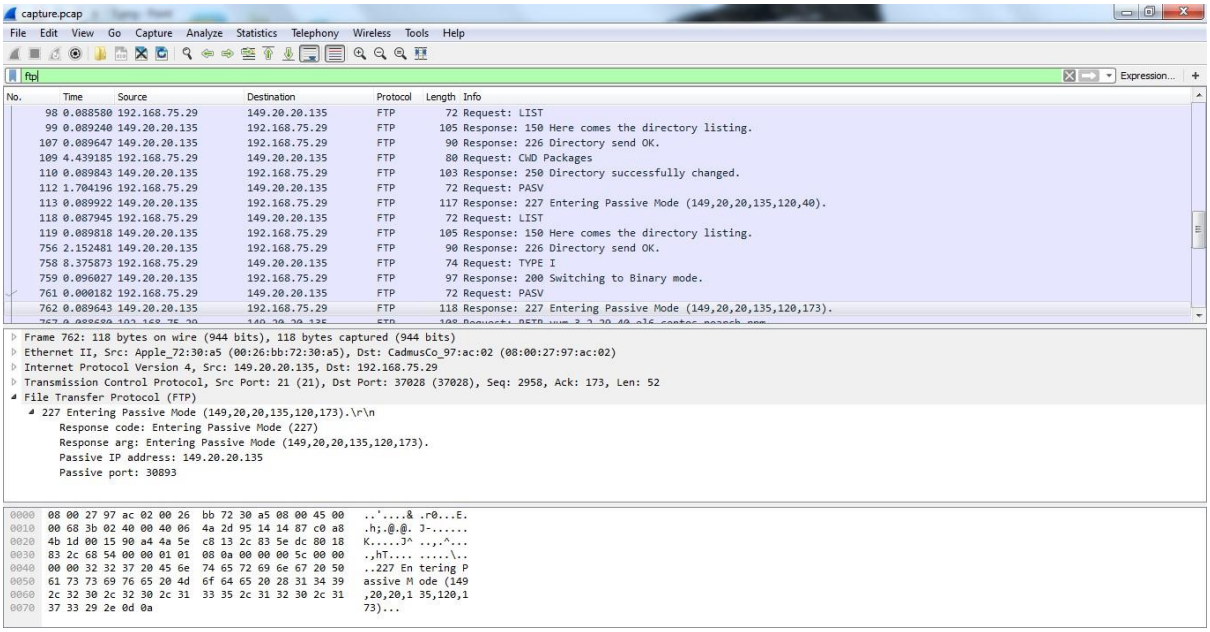


• *FTP Analysis using Wireshark*

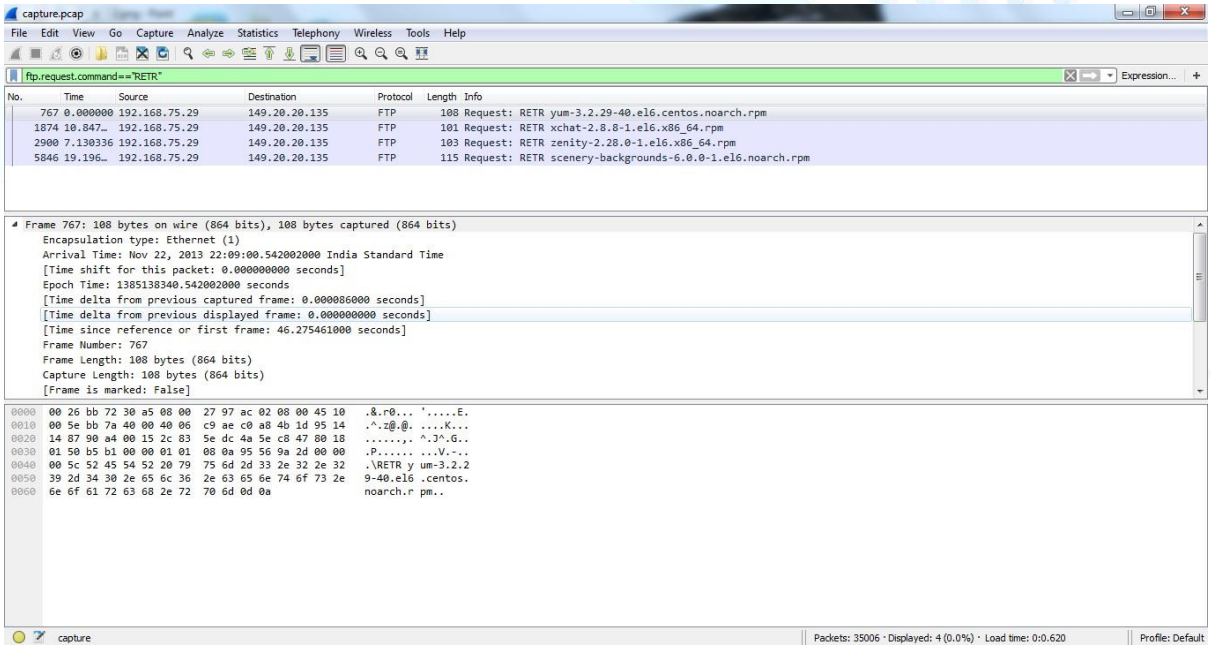
1. Open the pcap file in Wireshark



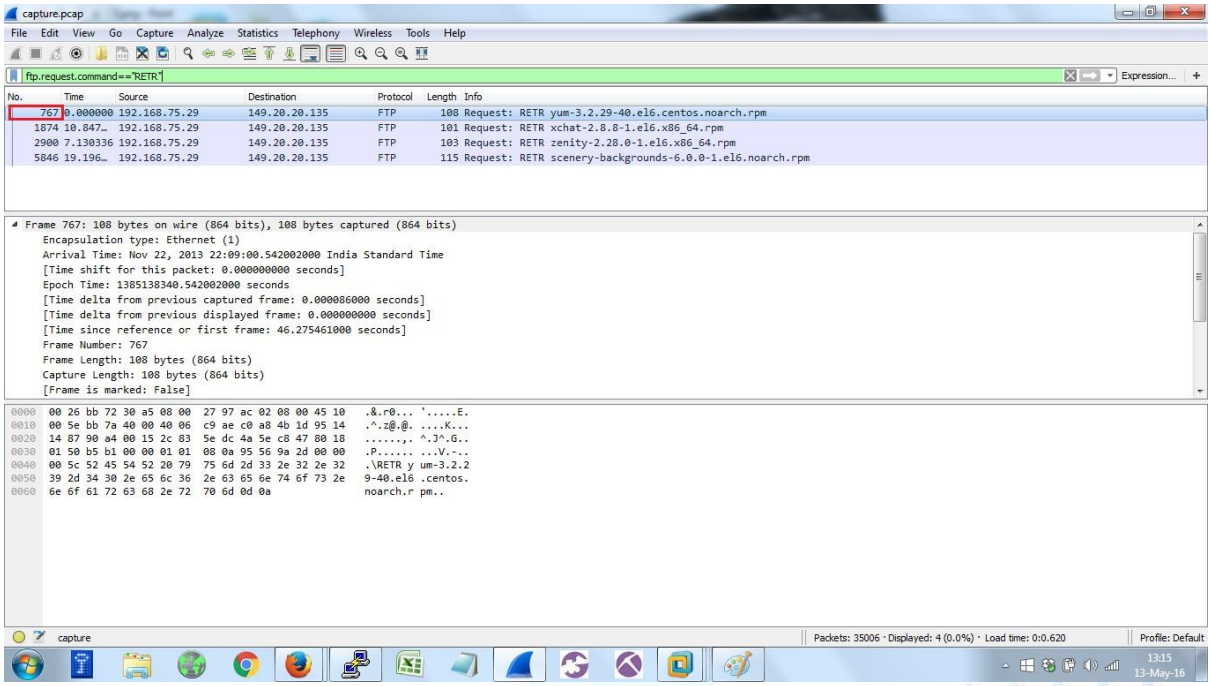
2. To find out if there is any FTP traffic in it, just apply the filter '**ftp**' in the display filter.



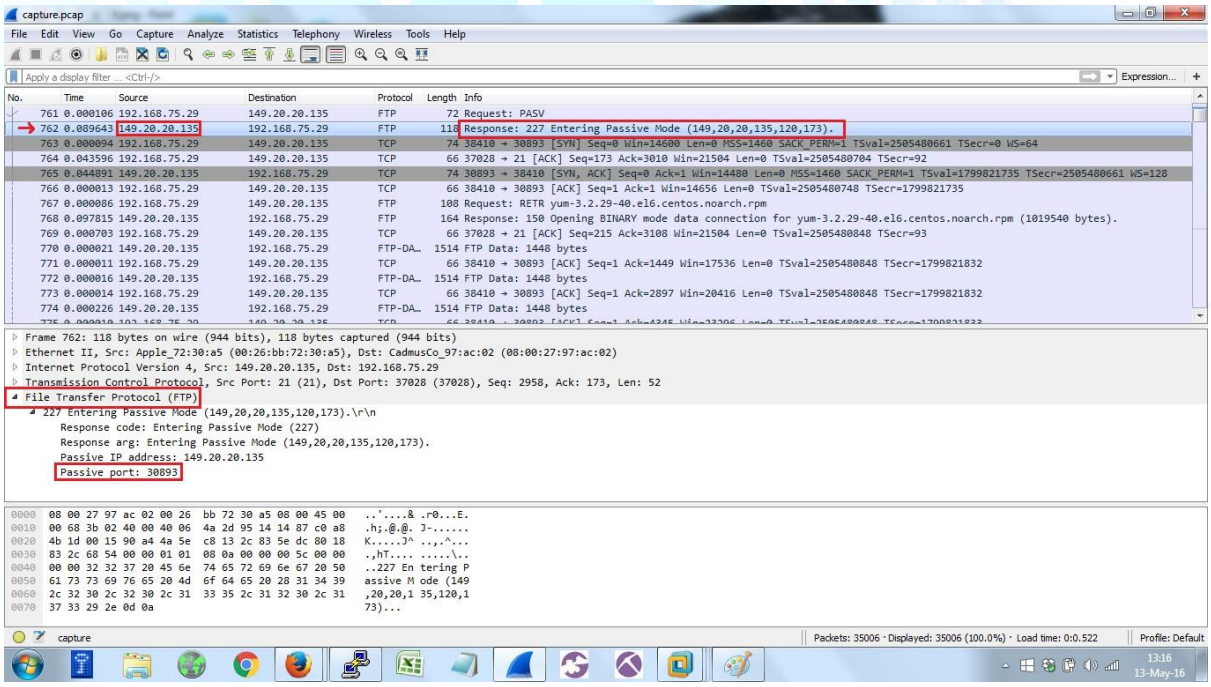
3. Now when you see FTP traffic, find out if any data was downloaded by a user. To find out, just apply the display filter **ftp.request.command=="RETR"**



4. You can see a retrieve (RETR) request by a few packets, let us see the packet number 767 which was the first instance.

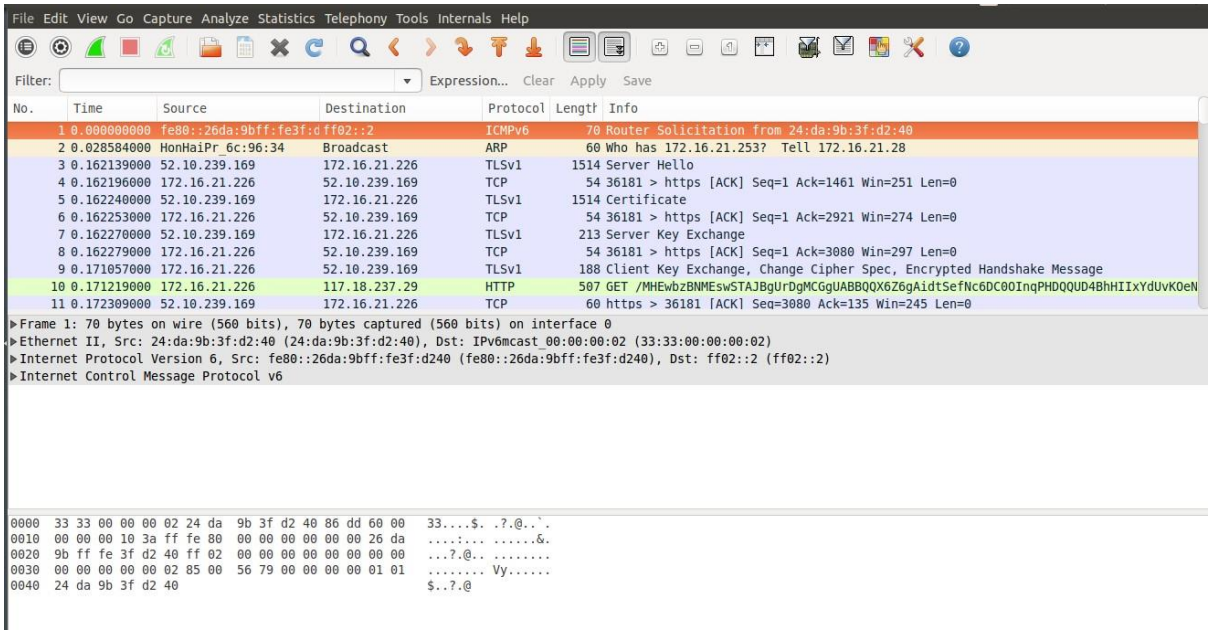


5. Now clear the filters and scroll down to a couple of packets before 767. If you look at packet number 762, the "info" tab gives some information. If you click on the "packet details" pane and on "File Transfer Protocol (FTP)" as shown in the picture below, you will find a field called "passive port". Note down the port number of that field.

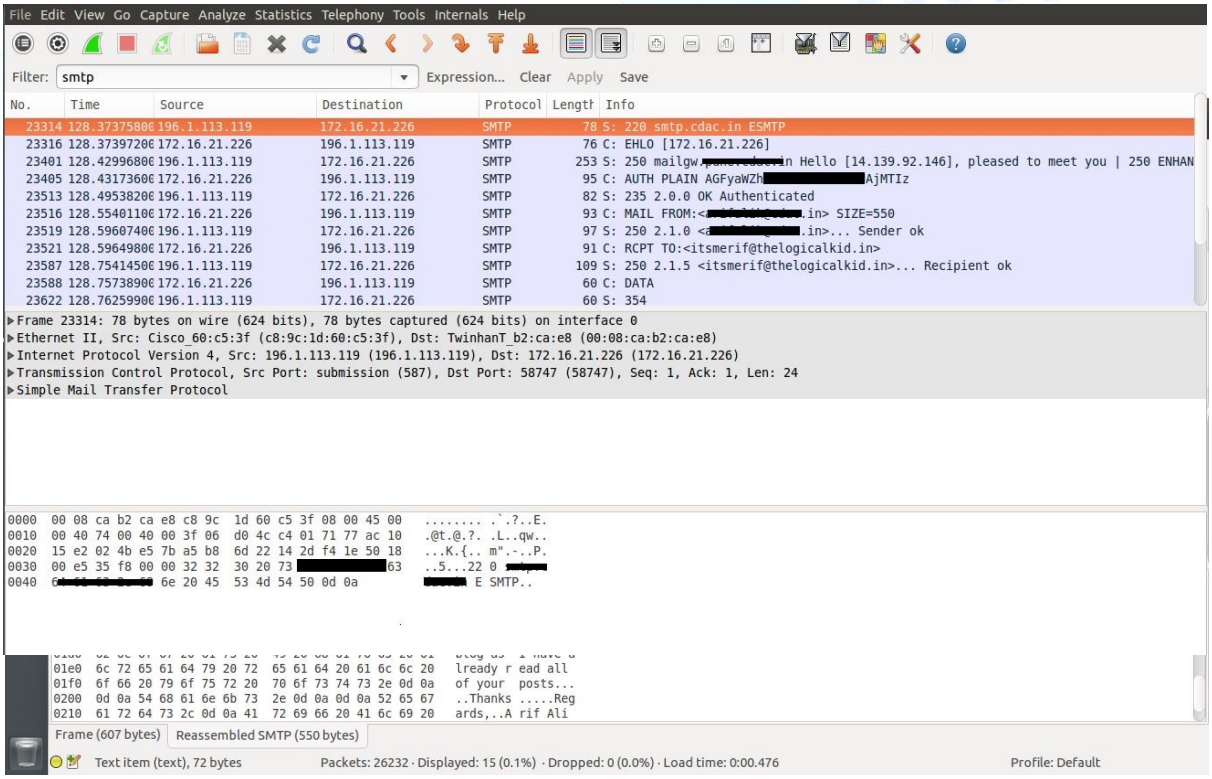


- *SMTP Analysis using Wireshark*

1. Load the captured pcap file in Wireshark.

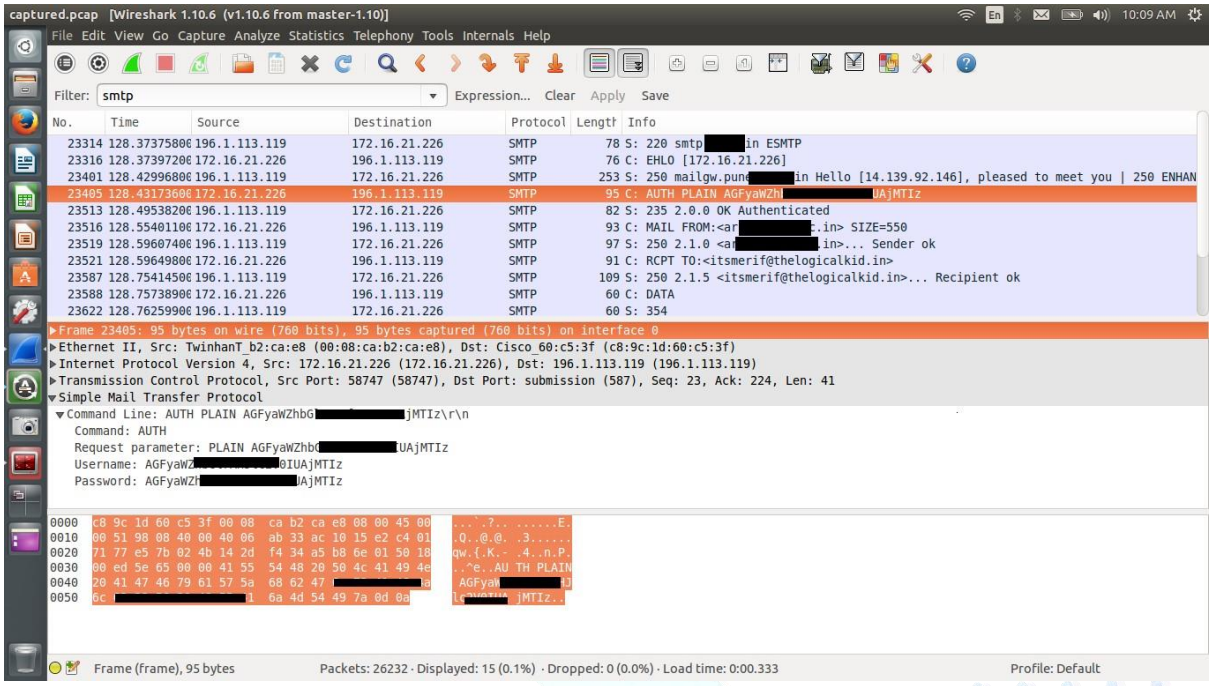


2. Type “smtp” in filter to show only SMTP traffic.

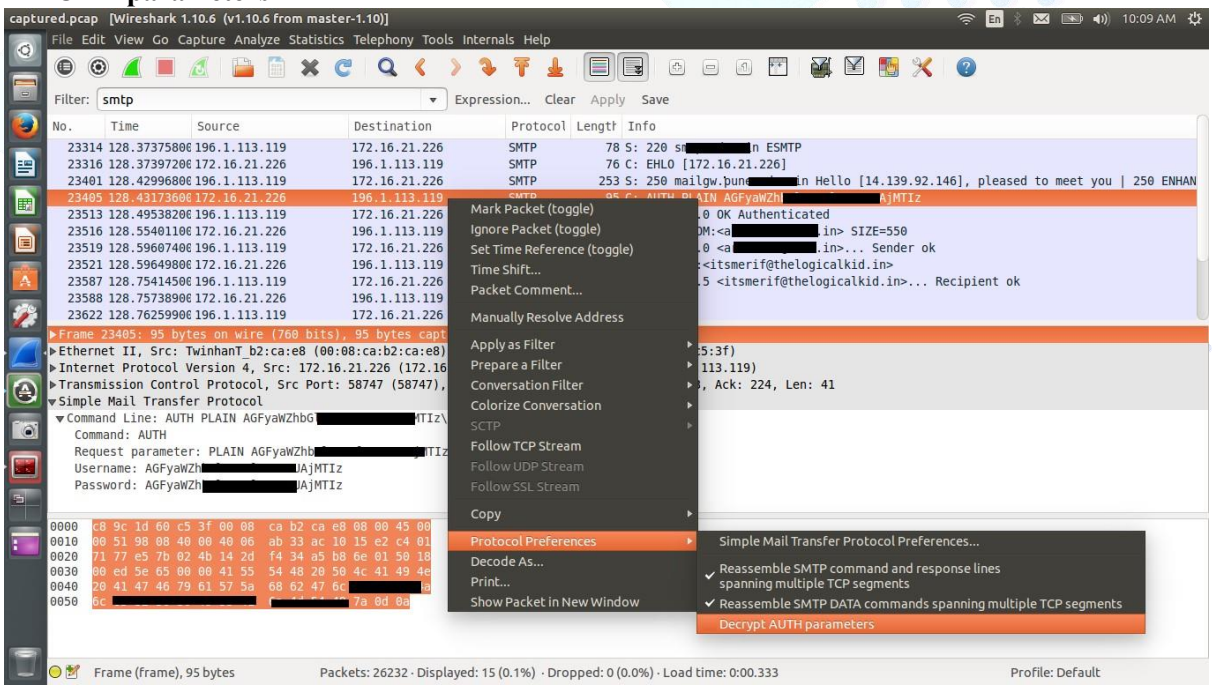


3. Click on the frame having the protocol 'Internet Message Format' (IMF) to see the content of the mail.

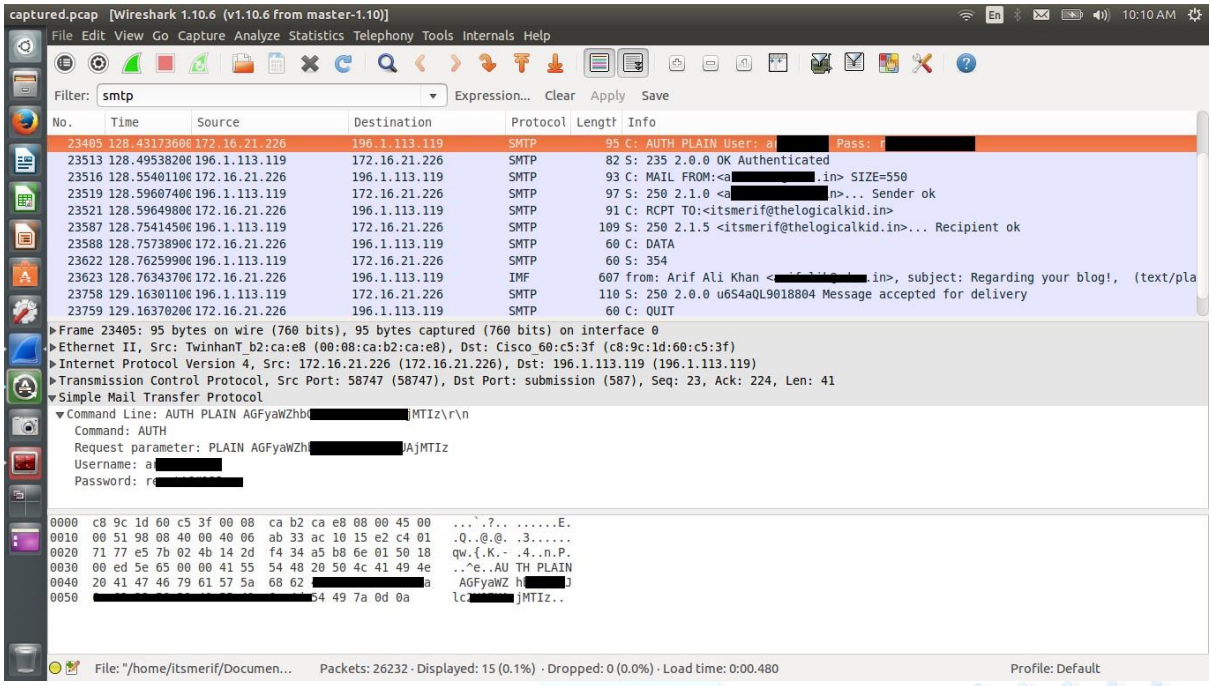
4. Notice the frames/packets which contain info as “AUTH”



5. Right click on the packet containing "AUTH" in info, and select "**Protocol Preferences**" > "**Decrypt AUTH parameters**"



6. You can now see the credentials in clear text.



8.7 Tools for retrieving content from Network Traffic

8.7.1 NetworkMiner

NetworkMiner is a Network Forensic Analysis Tool (NFAT) for Windows (but also works in Linux / Mac OS X / FreeBSD). NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. NetworkMiner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files. Ths tool makes it easy to perform advanced Network Traffic Analysis (NTA) by providing extracted artifacts in an intuitive user interface. The way data is presented not only makes the analysis simpler, it also saves valuable time for the analyst or forensic investigator.

It has, since the first release in 2007, become a popular tool among incident response teams as well as law enforcement. NetworkMiner is today used by companies and organizations all over the world.

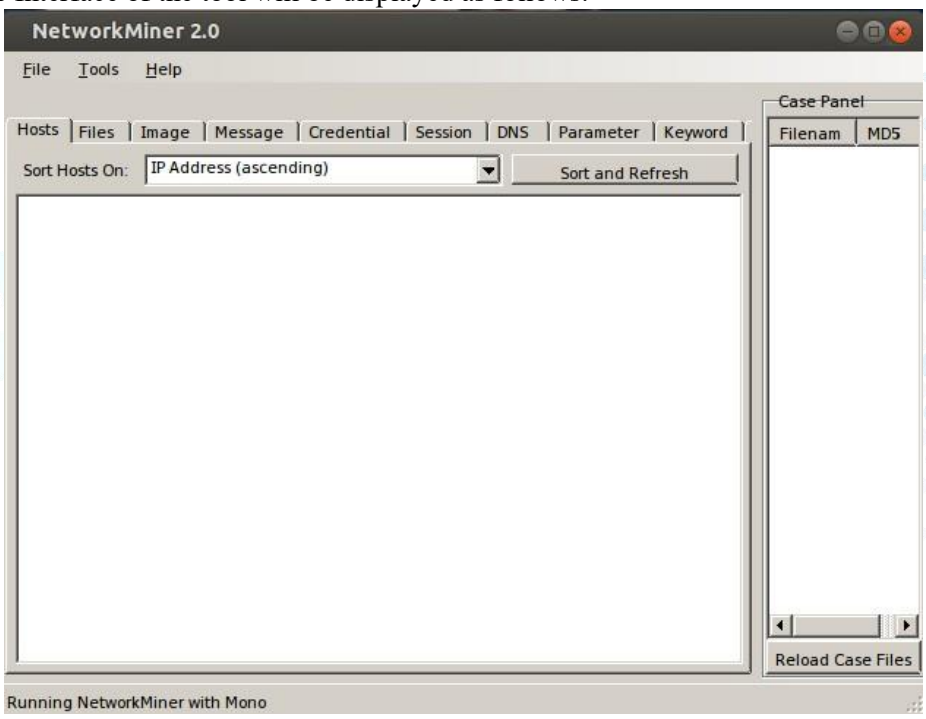
This tool can extract files and certificates transferred over the network by parsing a PCAP file or by sniffing traffic directly from the network. This functionality can be used to extract and save media files (such as audio or video files) which are streamed across a network from websites such as YouTube. Supported protocols for file extraction are FTP, TFTP, HTTP, SMB, SMB2 and SMTP.

You can download the tool from: http://www.netresec.com/?page=NetworkMiner

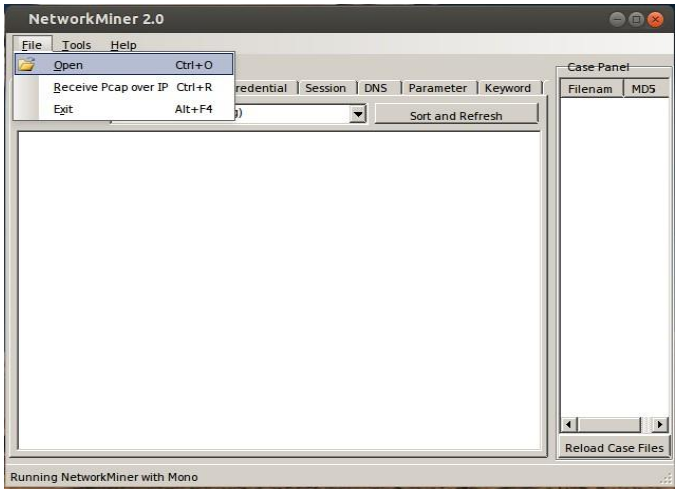
Steps for using NetworkMiner for extracting multimedia files from Network Traffic

1. Double-click on the NetworkMiner.exe file

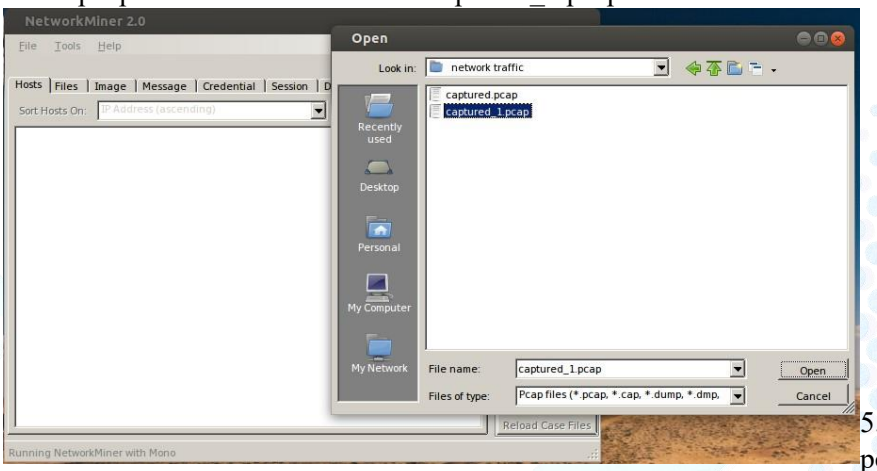
2. The Interface of the tool will be displayed as follows.



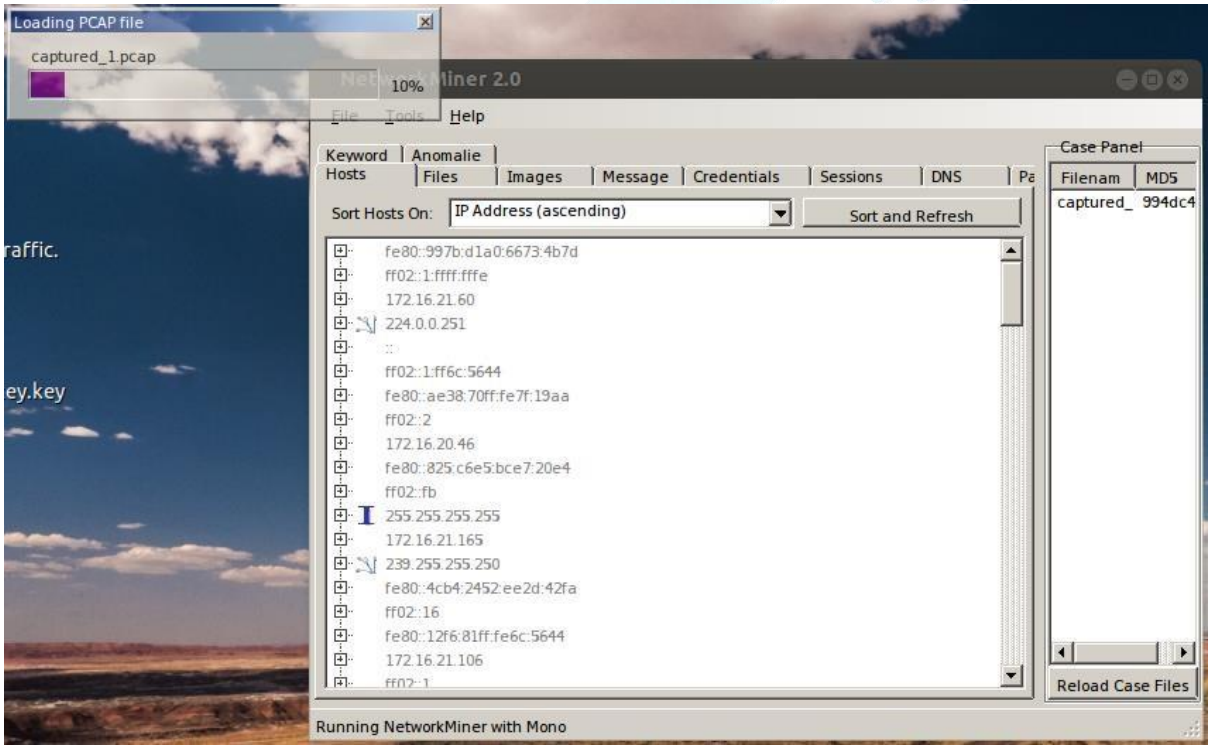
3. Click on “File” in Menu bar and select “Open”.



4. Select the appropriate file. NetworkMiner supports all popular packet capture file formats. Let us analyse the .pcap file which we have – i.e captured_1.pcap

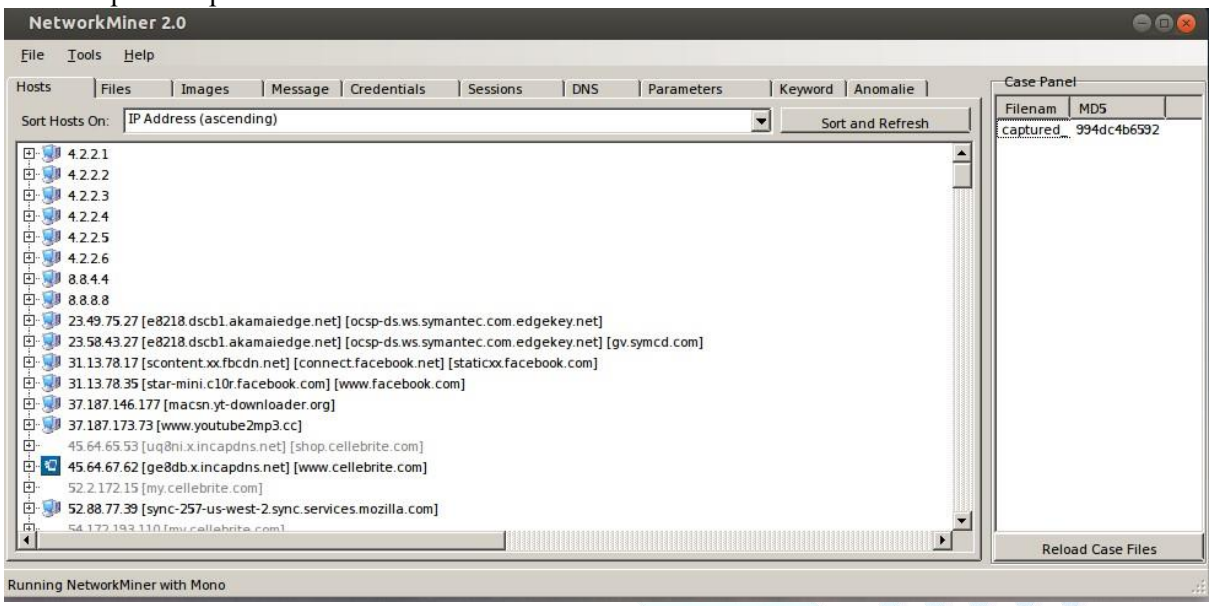


5. Wait until the pcap file gets loaded and parsed by NetworkMiner.

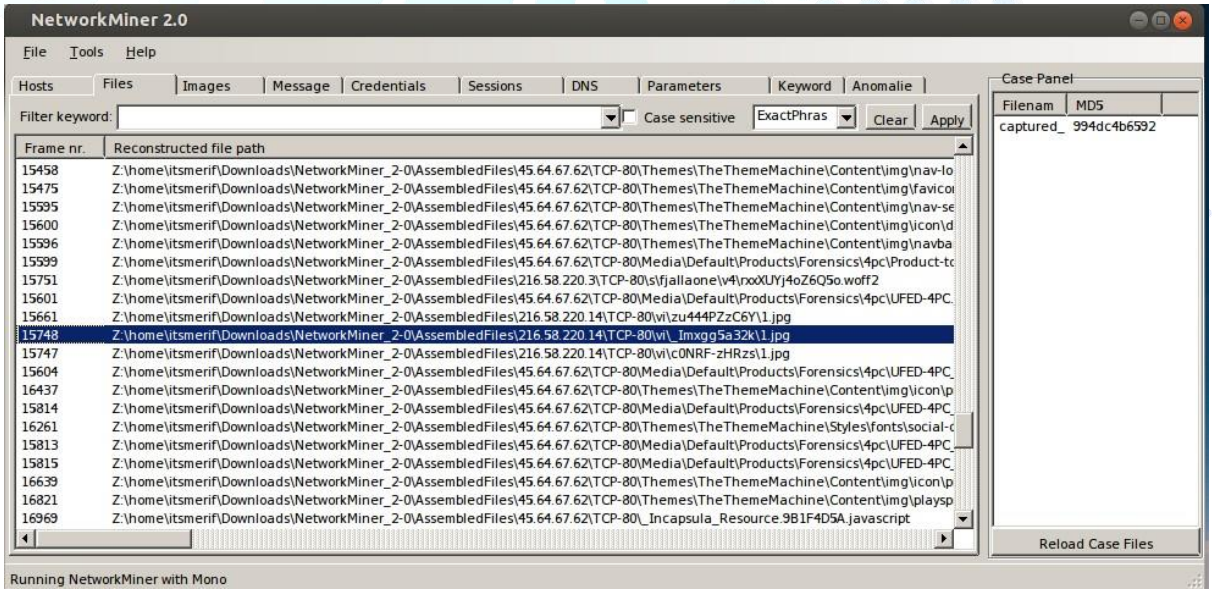


6. Once the file gets loaded, we can see a variety of data available in the various tabs of the interface, like “Hosts”, “Files”, “Images”, “Credentials”, etc.

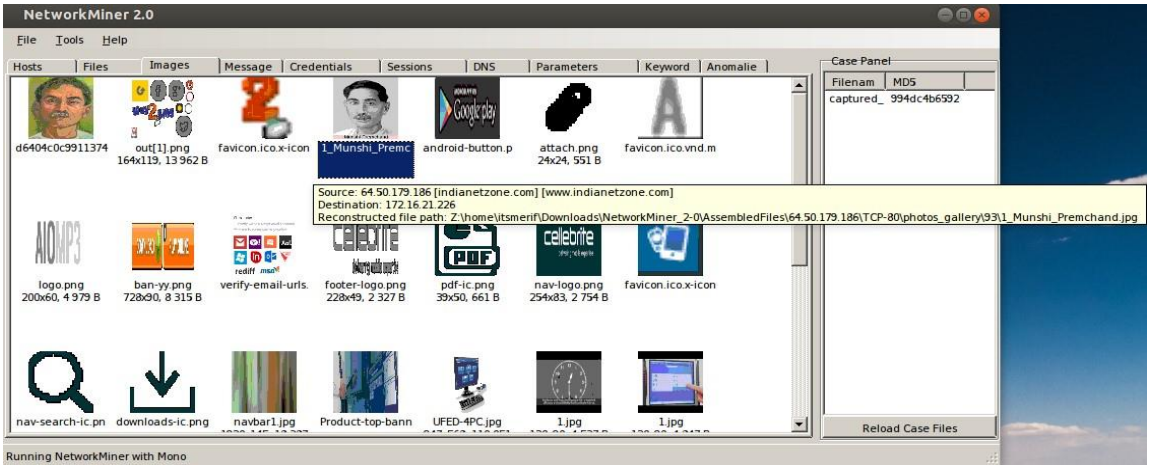
Let us explore important tabs first.



7. The “Files” tab shows us if any files were created/downloaded/uploaded during a session.

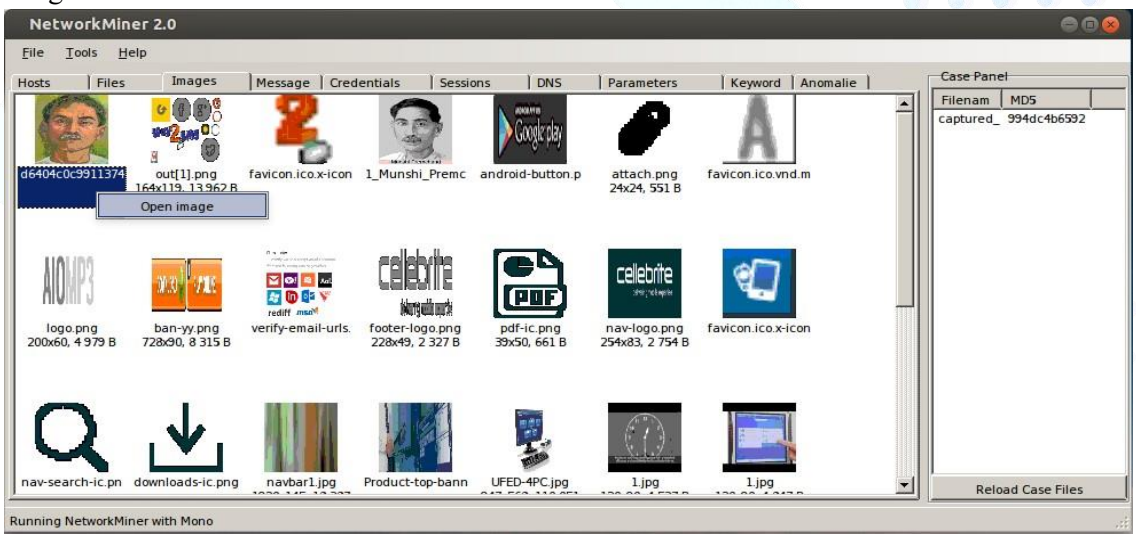


8. The “Images” tab shows the thumbnails of the images which were downloaded/uploaded during a session. When we hover our mouse over any image, it will show the source of the image from where it was downloaded, and the destination to which the image was served.

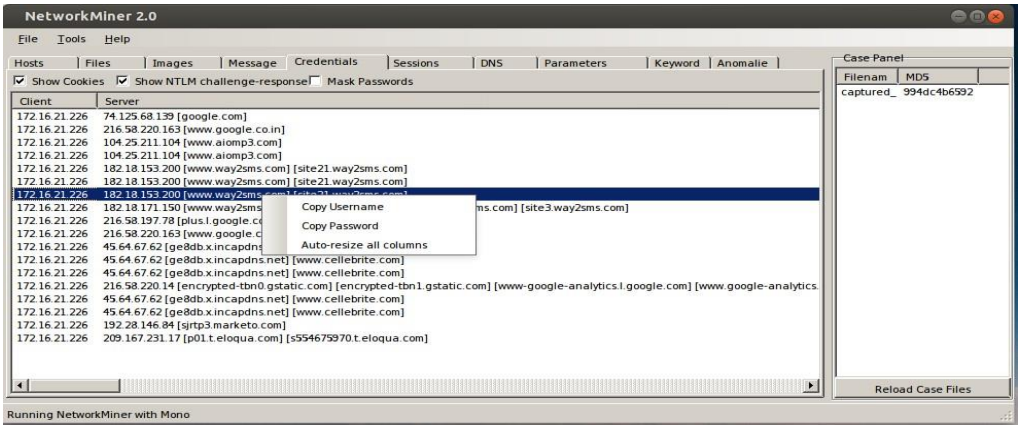


In the above screenshot, we can see that the image was fetched/downloaded from a source 64.50.179.186 which apparently belongs to a website indianetzone.com, and was requested by the destination IP 172.16.21.226 which belongs to a host within the internal network of the organisation from which the image was requested.

To view the complete image, right-click on any image and select “Open Image” to open with a default image-viewer or a web browser.



9. This tool has the ability to even identify authentication sessions and/or credentials from the pcap file. This will help us find out details of any website logins by the devices in our Network.



Although NetworkMiner is good as it quickly parses the data, but the free version is limited to analysis of a lesser size of traffic. This can be used if the network dump (pcap) is of a lesser size. We also have a better option which is also free, and has a more comprehensive approach towards analysis of data – Xplico

8.7.2 Xplico

Xplico is also a Network Forensics Analysis Tool (NFAT) for Linux based Operating Systems, which is a software that reconstructs the contents of acquisitions performed with a packet sniffer (e.g. Wireshark, tcpdump, Netsniff-ng).
Unlike the protocol analyzer, whose main characteristic is not the reconstruction of the data carried by the protocols, Xplico was born expressly with the aim to reconstruct the protocol's application data and it is able to recognize the protocols with a technique named Port Independent Protocol Identification (PIPI).
The goal of Xplico is to extract from an internet traffic capture the applications data contained. For example, from a pcap file Xplico extracts each email (POP, IMAP, and SMTP protocols), all HTTP contents, each VoIP call (SIP), FTP, TFTP, and so on. Xplico isn't a network protocol analyzer. Xplico is an open source NFAT.

Users having Ubuntu 32/64bit version between11.04 and 15.10 can download and install the software from within their terminal using the following commands:

```
sudo bash -c 'echo "deb http://repo.xplico.org/ $(lsb_release -s -c) main" >> /etc/apt/sources.list'
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 791C25CE
sudo apt-get update
sudo apt-get install xplico
```

The rest, can download from here: **http://www.xplico.org/download**

After installing, just open http://localhost:9876 in your browser, and login using the default username and password as follows:

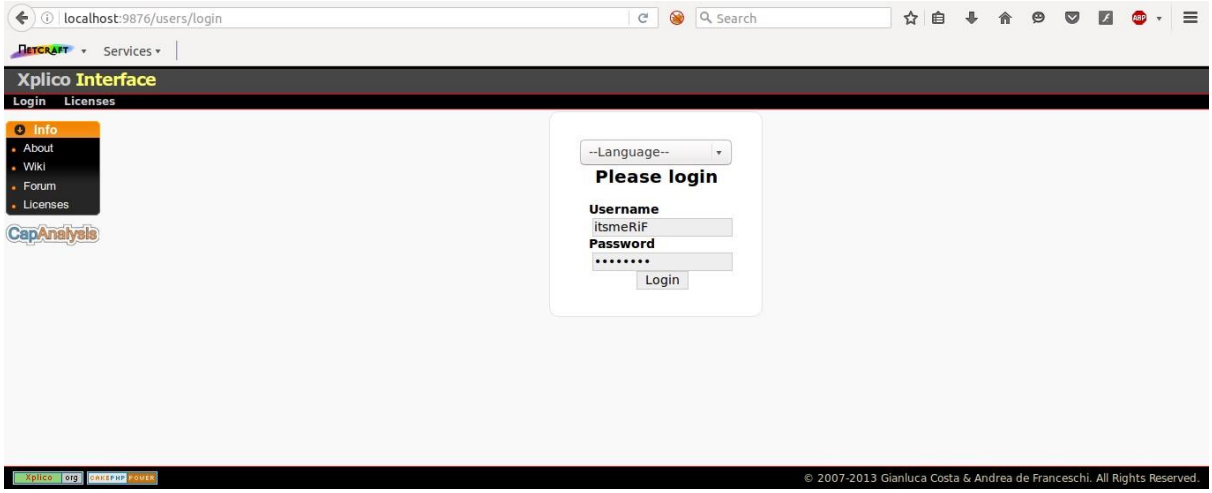
username: admin password:

xplico

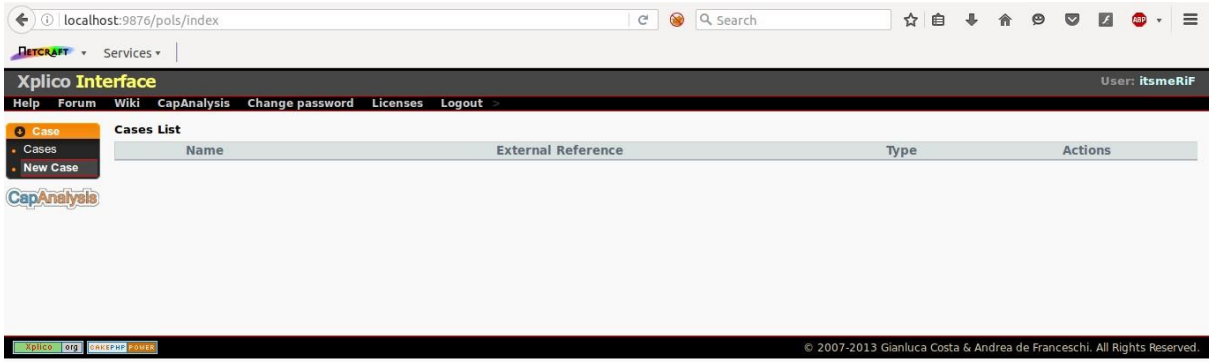
You can anyways create a separate user later. Please note that to load and parse pcap, we should not be an admin user. For the same, we have created a standard user for the demo.

- *Steps for using Xplico* 1.

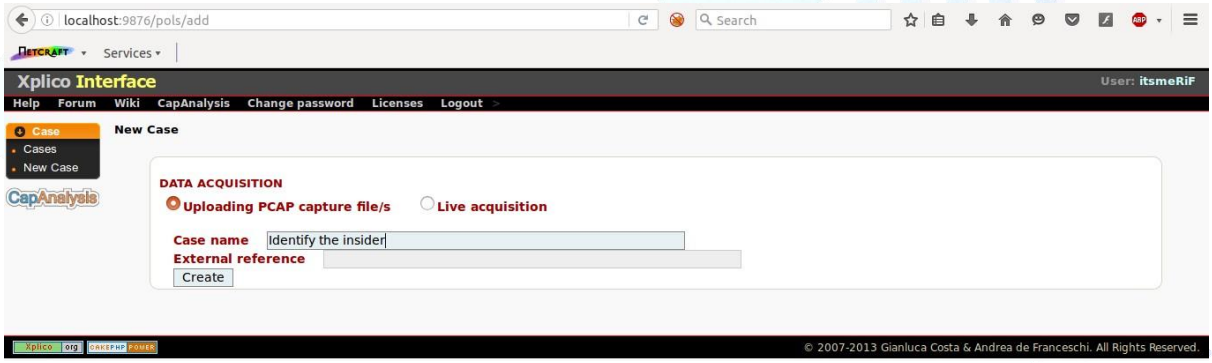
Login to your account.



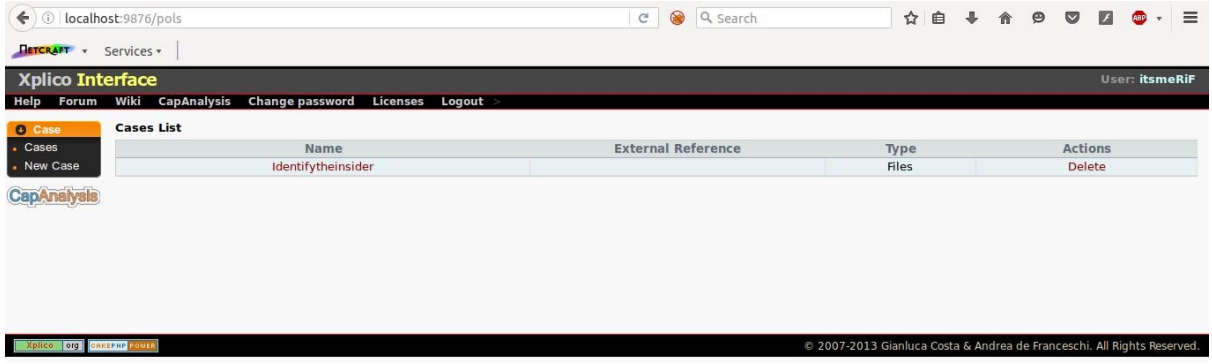
2. Click on “New Case”



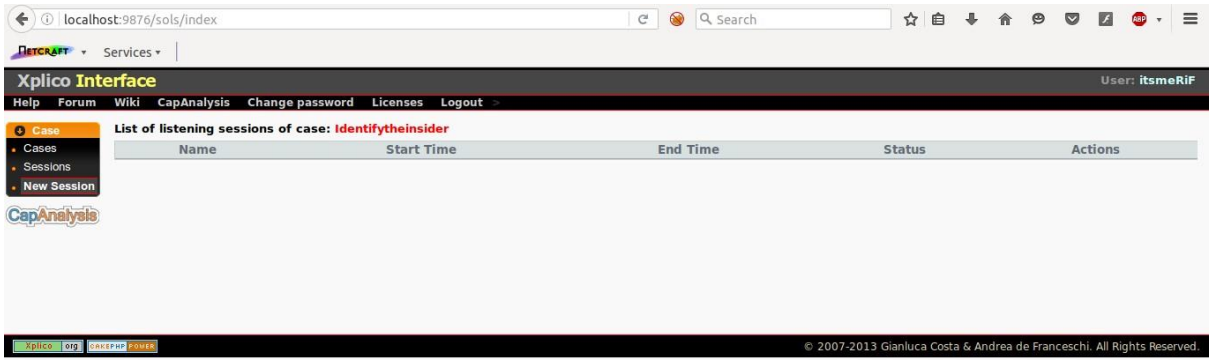
3.Provide case name, and click on “Create”



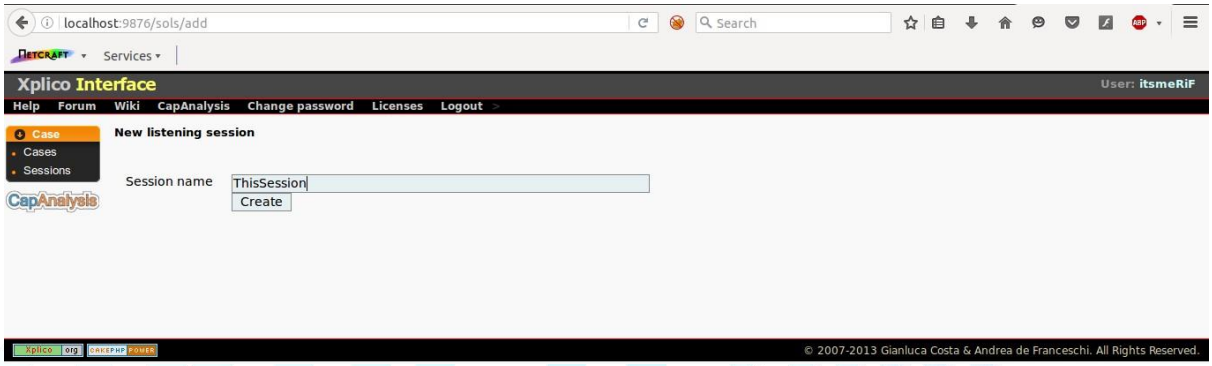
4. Click on the case name.



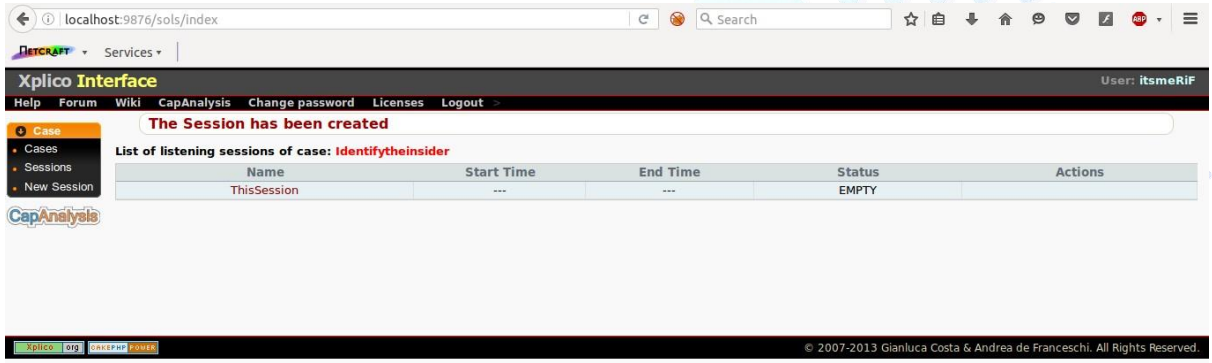
5. Click on “New Session”



6. Enter a session name.

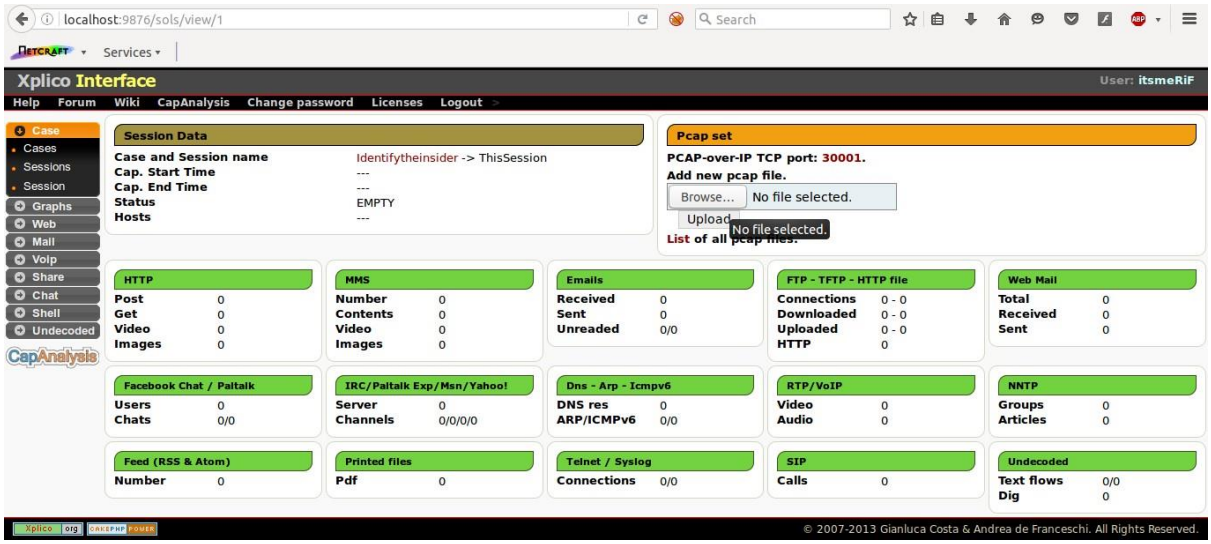


7. Click on the Session name.

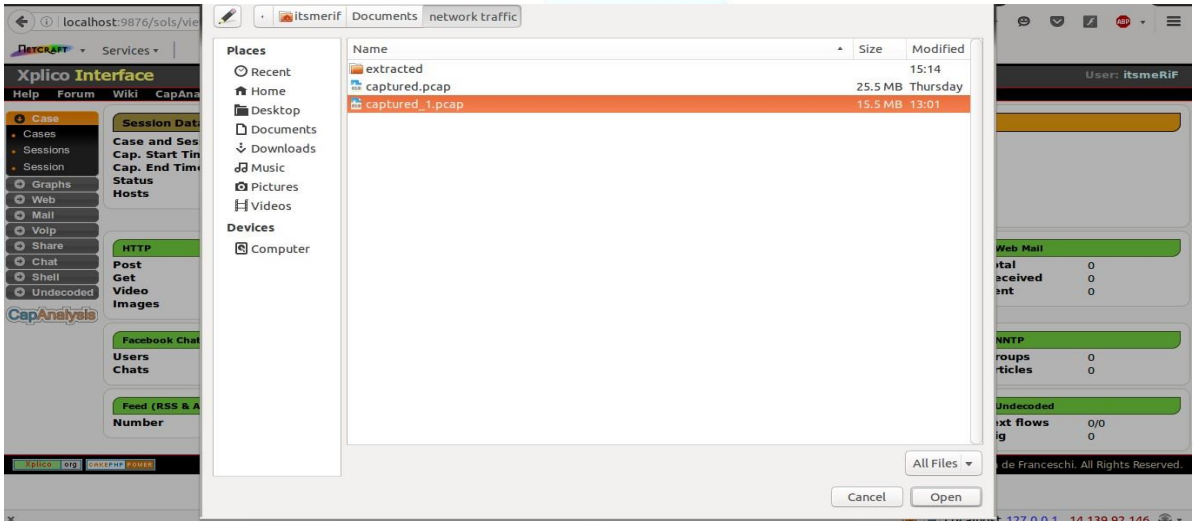


You will be displayed with a window as follows.

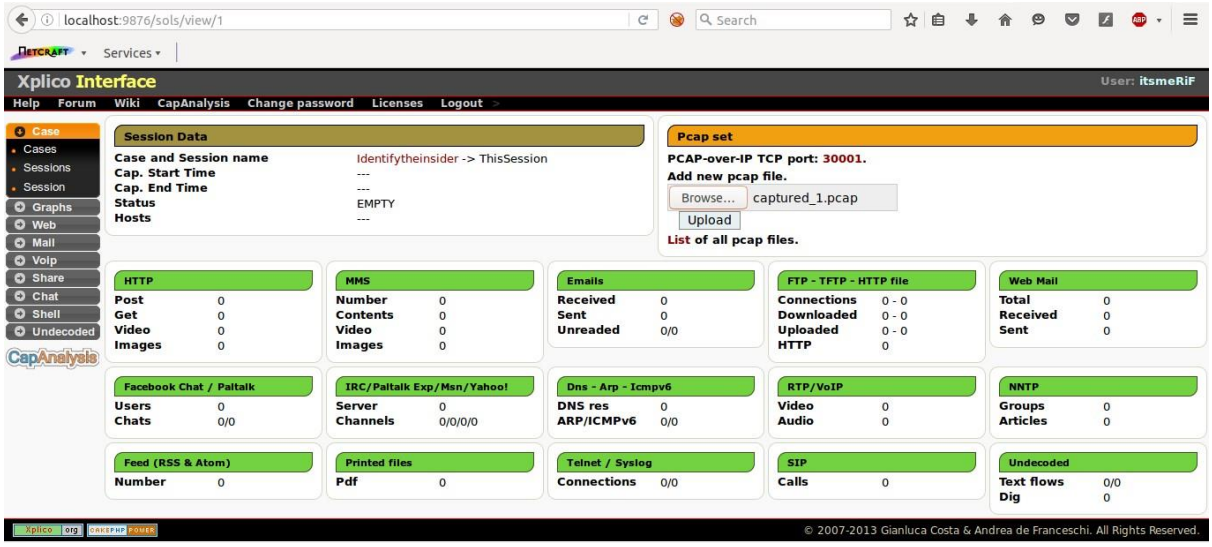
8. Click on “Browse”



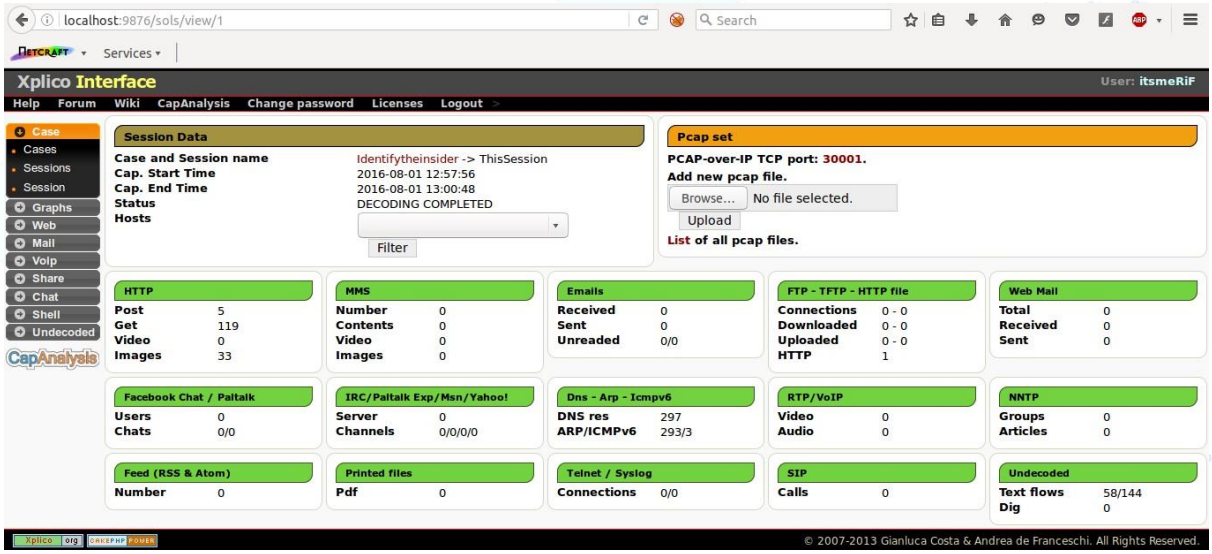
9. Select the appropriate traffic dump file. (pcap/pcapng/..and all supported pcap formats)



10. Click on “Upload”

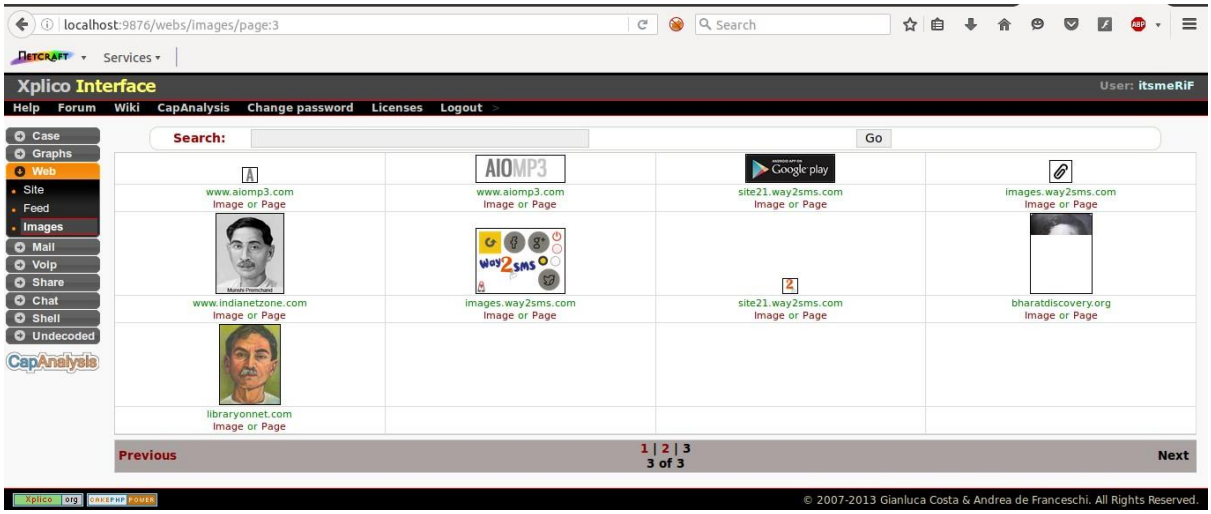


11. Wait until the data gets parsed and decoded by this tool.

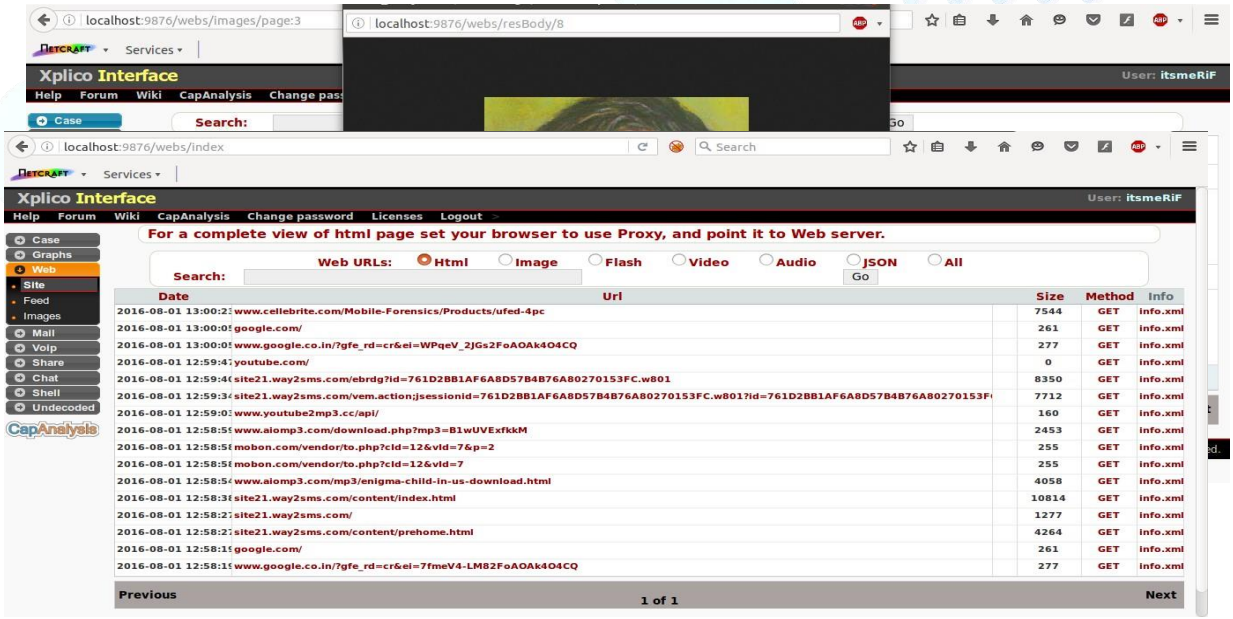


After decoding is completed, we can see a menu in the left side which contains various categories. Let us see through each of them.

12. Under “Web” menu, there is a sub-menu named “Images”, click on that. We can see all images which were accessed (uploaded/downloaded) during a session.

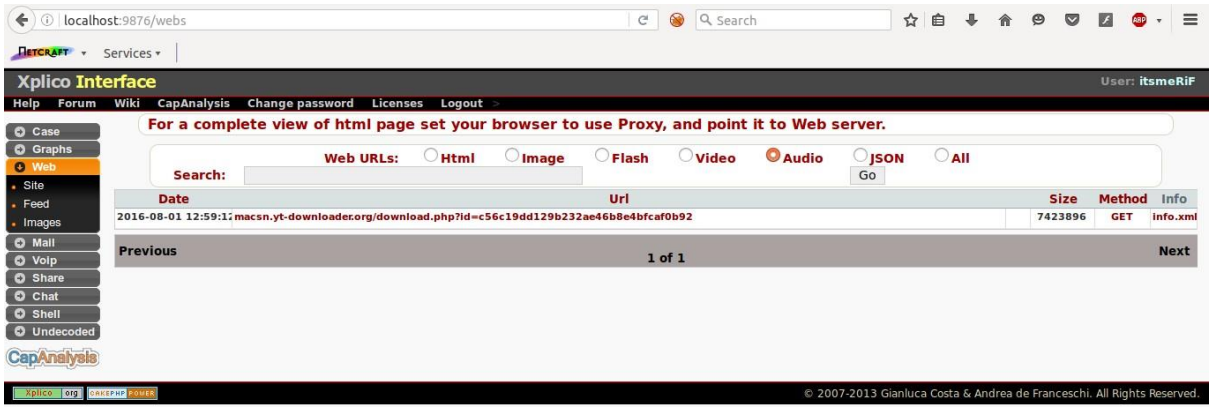


13. When we click on the "Image" link below the thumbnail of the image, we can see the original version of the image.

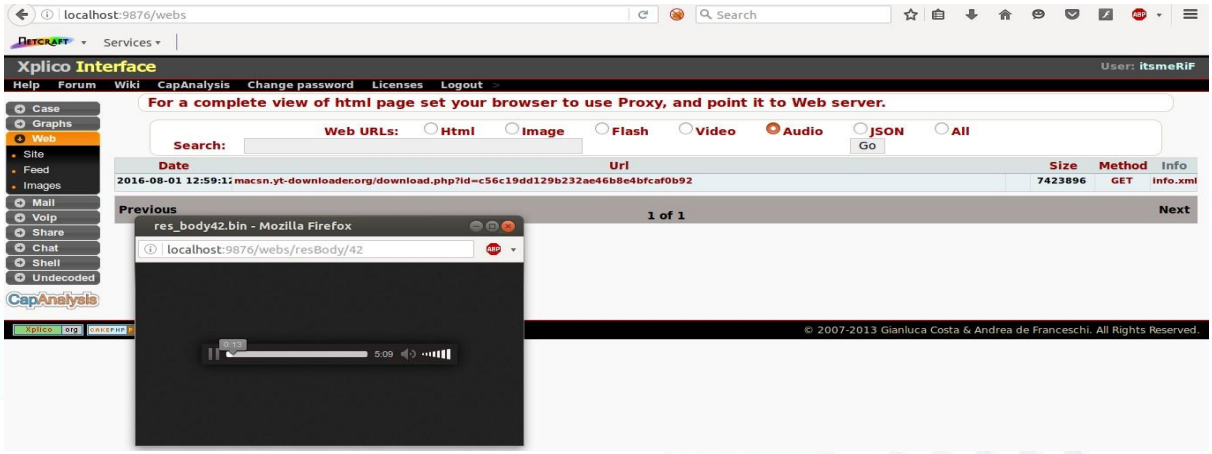


14. Click on the "Site" sub-menu under "Web" to see a list of websites which were visited by the users in the session recorded in the pcap file.

15. Click on "Web" menu and select the filter "Audio" to show any audio files were downloaded/uploaded during a session.



16. Click on the URL to play the audio file which was extracted from the pcap file.



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