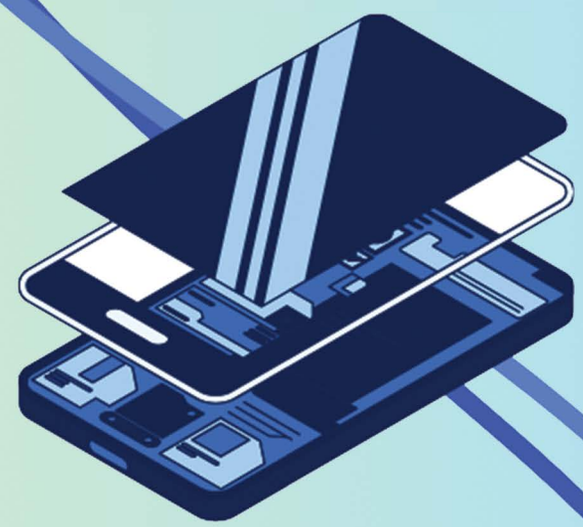
Sardar Vallabhbhai Patel
National Police Academy,
Hyderabad

Cyber Crime Investigation Manual

Volume - II



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

Mobile Phone Investigation

Mobile phones also called as Cell phones take an exceptionally essential part in people's way of life these days. Cell phone is currently a consistently on among young people. Although mobile phones have only been around for last 20 years but still the cover a major aspect of today's lifestyle.

Since the use of mobile phone in one's life is very vast so the crimes related to mobile devices also got increased. In present scenario in almost every criminal activity is somehow relate with mobile device. So, for an investigator mobile phone is a crucial evidence for any kind of criminal activity. In this document we will discuss about the various mobile device technologies and their investigation process in detail.

1. Introduction to Mobile Device & Technology

A cell phone is a remotely handheld gadget that permits clients to make and get calls and to send instant messages, among different features. The most beginner age of cell phones could just make and get calls. The present cell phones, be that as it may, are pressed with numerous extra highlights, for example, internet browsers, games, cameras, video players and even navigational frameworks.

1.1. Generations of Mobile Phones

With the time mobile phone devices have passed through various technological changes, which are known as generations of mobile phones. The very first mobile phone generation is called 0G, which has become available after world war- II. It generally refers to pre-cellular technology in which were actually two-way radios used by specific people like taxi drivers or emergency services for the purpose of communication.[1]

After 0G phones, Motorola introduced first handheld mobile phone in 1973, which was known as phone of first generation or 1G.

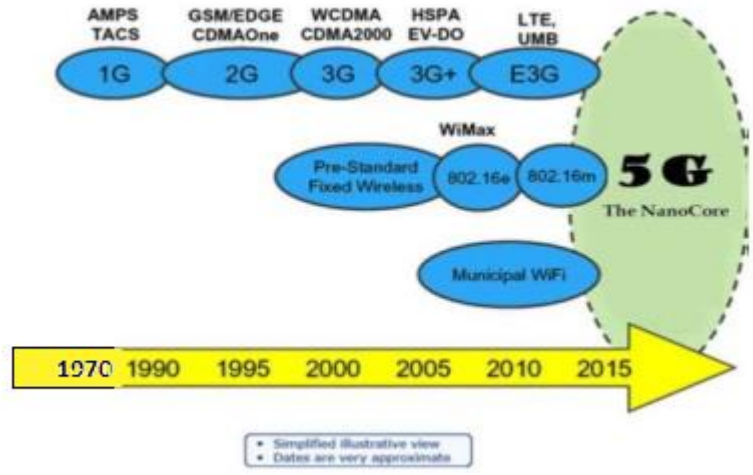


Figure 1: Mobile Technology Evolution (Mohammad Meraj ud in Mir, 2015)

[1] (Mohammad Meraj ud in Mir, 2015)

Generation	Speed	Technology	Time period	Features
1G	14.4 Kbps	AMPS,NMT, TACS	1970 – 1980	During 1G Wireless phones are used for voice only.
2G	9.6/ 14.4 Kbps	TDMA,CDMA	1990 to 2000	2G capabilities are achieved by allowing multiple users on a single channel via multiplexing. During 2G Cellular phones are used for data also along with voice.
2.5G	171.2 Kbps 20-40 Kbps	GPRS	2001-2004	2.5G the internet becomes popular and data becomes more relevant.2.5G Multimedia services and streaming starts to show growth. Phones start supporting web browsing though limited and very few phones have that.
3G	3.1 Mbps 500-700 Kbps	CDMA 200 (1xRTT, EVDO) UMTS, EDGE	2004-2005	3G has Multimedia services support along with streaming are more popular. In 3G, Universal access and portability across different device types are made possible. (Telephones, PDA's, etc.)
3.5G	14.4 Mbps 1-3 Mbps	HSPA	2006 – 2010	3.5G supports higher throughput and speeds to support higher data needs of the consumers
4G	100-300 Mbps. 3-5 Mbps 100 Mbps (Wi-Fi)	WiMax LTE Wi-Fi	Now (Read more on Transitioning to 4G)	Speeds for 4G are further increased to keep up with data access demand used by various services. High definition streaming is now supported in 4G. New phones with HD capabilities surface. It gets pretty cool. In 4G, Portability is increased further. World-wide roaming is not a distant dream.
5G	Probably gigabits	Not Yet	Soon (probably 2020)	Currently there is no 5G technology deployed. When this becomes available it will provide very high speeds to the consumers. It would also provide efficient use of available bandwidth

Table1: Various Mobile Technology Generations (Mohammad Meraj ud in Mir, 2015)

1.2. Working of Mobile Phone & Mobile Communication System

Basically, a cellphone works on radio communication technology. It consists of a radio transmitter and a radio receiver the voice signals passed through transmitter are converted into electrical signal and then passes in form of radio waves to the nearest cell tower. There is a huge network of cell towers by which the above radio wave goes to the receiver's phone, which again convert those radio signals again into voice signals.

A cell phone ordinarily works on a cellular network, which is made out of cell destinations dissipated all through urban communities, wide open spaces and even uneven districts. In the event that a client happens to be situated in a territory where there is no sign from any phone site having a place with the phone network supplier the individual in question is bought in to, calls can't be set or gotten in that area.

The phone framework associates mobile radios (called mobile stations) through radio channels to base stations. A portion of the radio channels (or parts of a computerized radio channel) are utilized for control

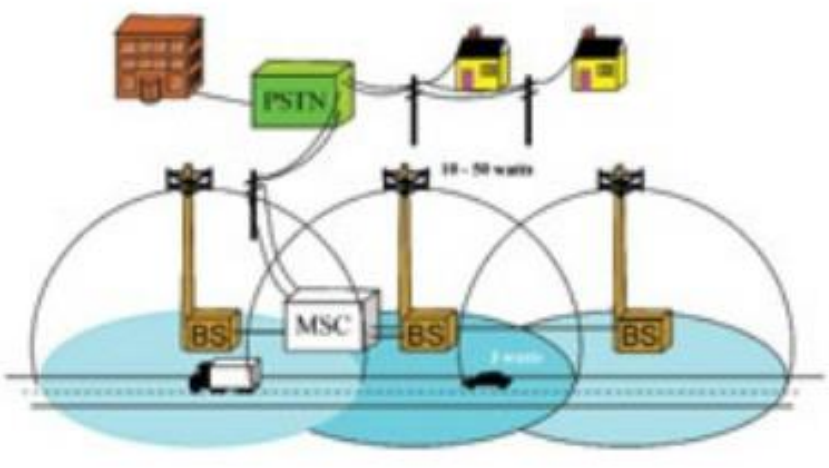


Figure.2: Basic Mobile Phone Network System (Bowler, 2004)

purposes (arrangement and detachment of calls) and some are utilized to move voice or client information signals. Each base station contains transmitters and beneficiaries that convert the radio signals to electrical signals that can be sent to and from the Mobile Switching Center (MSC). The MSC contains correspondence controllers that adjust signals from base stations into a structure that can be associated (exchanged) between other base stations or to lines that interface with the public phone network. The switching framework is associated with databases that contain dynamic (clients dynamic in its framework). The switching framework in the MSC is composed by consider preparing programming that gets demands for administration and procedures the means to arrangement and keep up associations through the MSC to goal specialized gadgets, for example, to other mobile phones or to phones that are associated with the public phone network.

1.2.1. Mobile Phone Working Procedure

To take into consideration the change from simple (analog) frameworks to advanced (digital) frameworks, some cell advances take into account the utilization of double mode or multi-mode cell phones. These handsets are equipped for working on a simple (analog) or computerized (digital)radio channel, contingent upon whichever is accessible. Most double mode telephones like to utilize computerized (digital) radio stations, in the occasion both are accessible. This permits them to exploit the extra limit and new highlights, for example, short messaging and digital voice quality, just as offering more noteworthy limit.

Cellular systems have several key differences that include the radio channel bandwidth, access technology type (FDMA, TDMA, and CDMA), data signalling rates of their control channel(s) and power levels.

Access technologies determine how mobile telephones obtain service and how they share each radio channel.

The data signalling rates determine how fast messages can be sent on control channels. The RF power level of mobile telephones and how the power level is controlled ordinarily determines how far away the mobile telephone can operate from the base station (radio tower).

Notwithstanding the size and kind of radio channels, all cell and PCS frameworks permit for full duplex activity. Full duplex activity is the capacity to have synchronous interchanges between the guest and the called individual. This implies a versatile phone must be prepared to do all the while transmitting and getting to the radio tower. The radio station from the cell phone to the radio tower is known as the uplink and the radio transmission station from the base station to the cell phone is known as the downlink. The uplink and downlink radio channels are ordinarily isolated by 45 MHz to 80 MHz.

Most cellular systems use two types of radio channels, control channels and voice channels. Control channels only carry control information such as paging (alert) and channel assignment messages. Voice channels are primarily used to transfer voice information. However, voice channels must also be capable of sending and receive some digital control messages to allow for necessary frequency and power changes during a call.

When a mobile telephone is first powered on, it initializes itself by searching (scanning) a predetermined set of control channels and then tuning to the strongest one. During the initialization mode, it listens to messages on the control channel to retrieve system identification and setup information.

After initialization, the mobile telephone enters the idle mode and waits to be paged for an incoming call and senses if the user has initiated (dialled) a call (access). When a call begins to be received or initiated, the mobile telephone enters system access mode to try to access the system via a control channel. When it gains access, the control channel sends an initial voice channel designation message indicating an open voice channel. The mobile telephone then tunes to the designated voice channel and enters the conversation mode.

1.3. Modes of Mobile Communication

On the basis of operation modes, services and multiple access schemes mobile networks can be differentiated into following parts with the aim of assigning the maximum number of users to an available radio frequency segment. There are various protocols of multiple access.

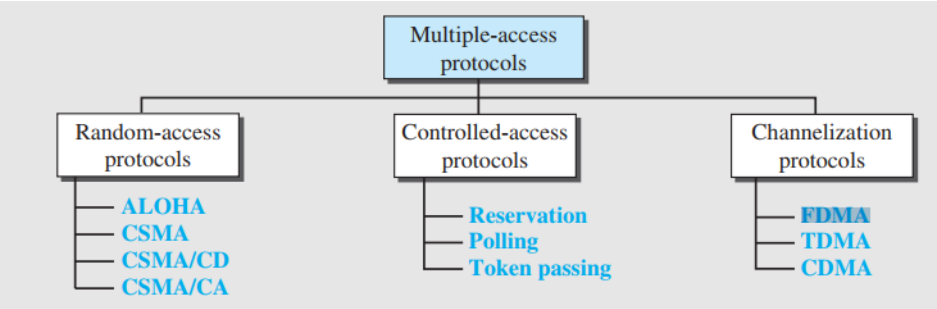


Figure 3: Various Multiple Access Protocols (Forouzan, 2013)

In mobile communication to achieve the above aim various multiple access schemes are being used. The most common access schemes are – [2]

- Frequency Division Multiple Access (FDMA)
- Time Division Multiple Access (TDMA)
- Code Division Multiple Access (CDMA)
- Orthogonal Frequency Division Multiple Access (OFDMA)

In **Frequency-Division Multiple Access (FDMA)**, the accessible data transfer capacity is separated into frequency groups. Each station is allotted a band to send its information. At the end of the day, each band is saved for a particular station, and it has a place with the station constantly. Each station additionally utilizes a bandpass filter to keep the transmitter frequencies. To prevent station interferences, the allocated bands are separated from one another by small guard bands.

In **Time-Division Multiple Access (TDMA)**, the stations share the transfer speed of the channel in time. Each station is provided a time slot during which it can send information. Each station transmits its information in its given time slot.

Code Division multiple access (CDMA). CDMA differs from FDMA in that only one channel occupies the entire bandwidth of the link. It differs from TDMA in that all stations can send data simultaneously; there is no timesharing.

In OFDMA, a large spectrum segment is allocated as a channel pool available to one or many simultaneous users.

[2] (Kukushkin, 2018)

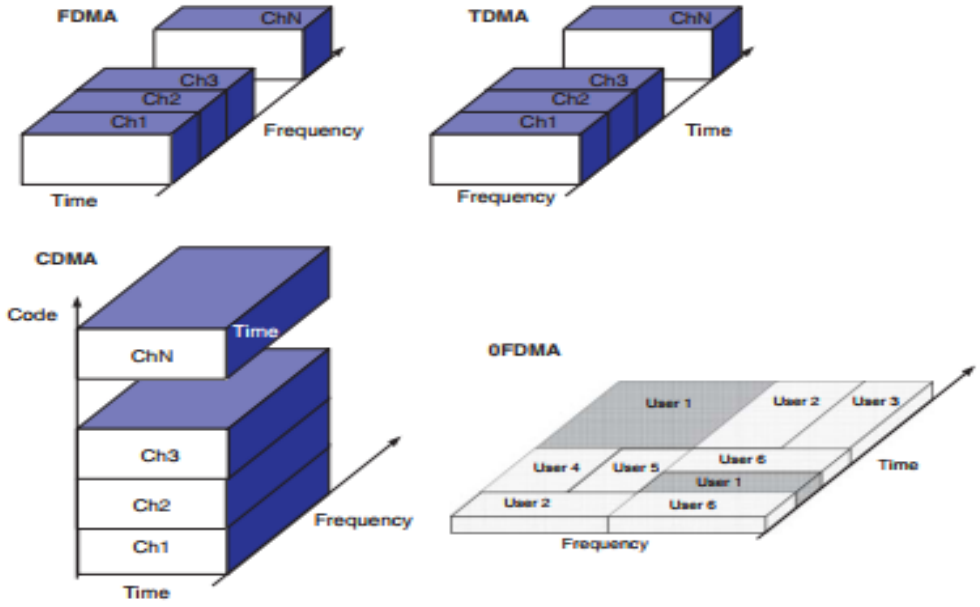


Figure 4: Common Multiple Access Protocols (Kukushkin, 2018)

1.4. Technologies Used in Mobile Communication

The important technologies used in mobile communication are as follows –

1.4.1. Cellular Frequency Reuse

Initially, in mobile radio systems number of radio channels were limited, (even though one high power transmitter is used to serve a large geographical area) due to limited availability of radio spectrum. To save the constrained measure of radio range (most extreme number of accessible radio channels), the cell framework idea was created. Cell frameworks permit reuse of a similar channel frequencies commonly inside a geographic inclusion zone. The strategy, called frequency reuse, makes it workable for a framework to offer support to more clients (called framework limit) by reusing the channels that are accessible in a geographic territory. As frameworks begin to get over-burden with numerous clients, to expand limit, the framework can extend by just adding progressively radio channels to the base station or by including more cell sites to with littler coverage regions.[3]

Some characteristics of cellular network principle are as follows –

- The territory to be secured is subdivided into cells (radio zones). These cells are frequently displayed in a rearranged manner as hexagons with a base station situated at the focal point of every cell. Accept that the administrator has a permit on a lot of channels, called, for instance, set S.
- To every cell I a subset of the frequencies S_i is allotted from the all-out set (bundle), which is allotted to the individual versatile radio system. In the GSM framework, the set of frequencies allotted to a phone is known as the Cell Allocation (CA). Under ordinary conditions the quantity of diverts in a subset S_i is driven by traffic limit prerequisites.

[3] (Bowler, 2004)

- Neighbouring cells do not normally use the same frequencies since this would lead to severe co-channel interference from the adjacent cells
- Just at separation D (the frequency reuse separation) can a frequency from the set Si be reused; that is, cells with separation D to cell i can be doled out one or all of the frequencies from the set having a place with cell i. When planning a portable radio system, D must be picked to be adequately enormous, with the end goal that the co-channel impedance stays little enough not to influence speech quality.
- At the point when a portable station moves starting with one cell then onto the next during a progressing discussion, a programmed channel/frequency change may happen (handover), which keeps up a functioning speech association over cell limits.
- The spatial redundancy of frequencies is done in an ordinary precise manner; that is, each cell with the cell designation sees its neighbours with similar frequencies again at a separation D. Along these lines, precisely six such neighbour cells exist. The primary ring in the frequency set consistently contains six co-direct cells in frequency reuse framework autonomous of the structure and size of cells, not simply in the hexagon model.[4]

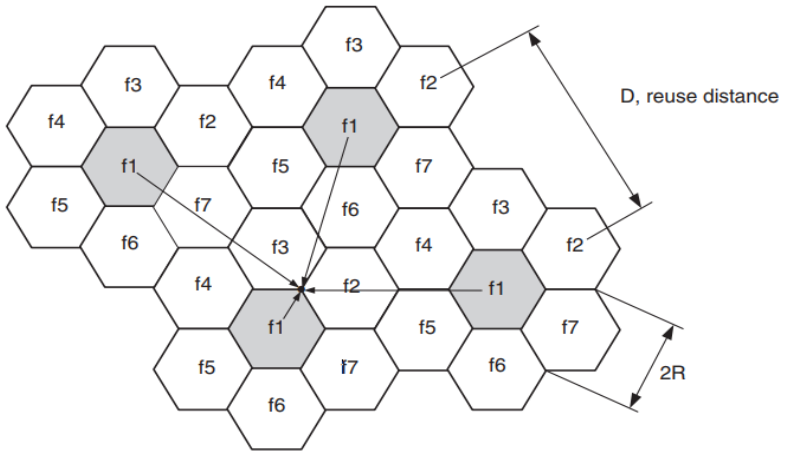


Figure 5 : Model of a cellular network with frequency reuse. Shadowed hexagons represent cells with the same set of allocated frequencies (Kukushkin, 2018)

The normal spatial redundancy of frequencies brings about a grouping of cells. these groups are known as clusters. The cells inside a cluster should each be relegated various arrangements of channels, while cells having a place to neighbouring clusters can reuse the diverts in the equivalent spatial example. The size of a cluster is portrayed by the quantity of cells per bunch k, which decides the recurrence reuse separation D when the cell radius R is given.

A cluster can contain all of the frequencies of the mobile radio system. and within a cluster, no frequency can be reused i.e. the frequencies of a set *Si* may be reused at the earliest in the neighbouring cluster. Therefore, to enhance the number of active subscribers per call it is necessary to reduce the size of a cluster.

One way to reduce cluster size, and hence increase capacity, is to use sectorization. The group of channels available at each cell is split into three cells (sectors), each of which is confined in coverage to one-third of the cell area by the use of directional antennas.

[4] (Kukushkin, 2018)

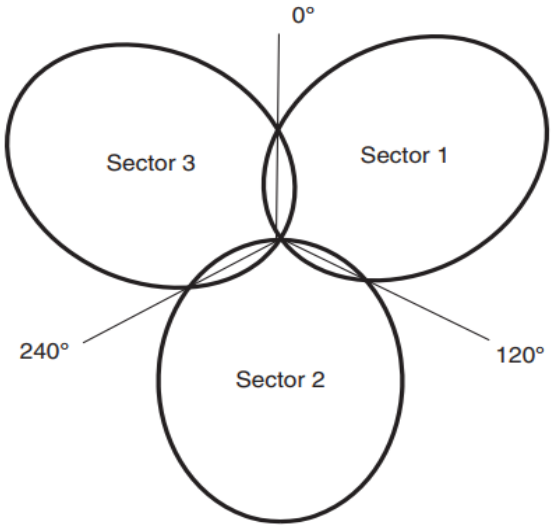


Figure 6: Antenna patterns for a cell site with three 120◦ sectors

1.4.2. Analog Cellular (1st Generation)

There are numerous sorts of analog and digital cell frameworks being used all through the world. Analog frameworks incorporate AMPS, TACS, JTACS, NMT, MCS and CNET.

1.4.2.1. AMPS (Advance Mobile Phone Services)

Advance Mobile Phone Service (AMPS) is a standard framework for analog signal cellular telephone utility. It depends on the underlying electromagnetic radiation range portion for cell administration by the Federal Communications Commission (FCC) in 1970. Presented by AT&T in 1983, AMPS got one of the most generally sent cell framework in the United States. AMPS assign frequency runs inside the 800 and 900-Megahertz (MHz) range to cell phone. Each specialist organization can utilize half of the 824-849 MHz extend for getting signals from PDAs and a large portion of the 869-894 MHz go for transmitting to mobile phones. The groups are separated into 30 kHz sub-groups, called channels. The accepting channels are called turn around channels and the sending channels are called forward channels. The division of the range into sub-band channels is accomplished by utilizing frequency division multiple access (FDMA).

The signals got from a transmitter spread a territory called a phone. As a client moves out of the phone's region into a neighbouring cell, the client starts to get the new cell's signals with no recognizable change. The signals in the contiguous cell are sent and gotten on unexpected diverts in comparison to the past cell's signals to so the signals don't meddle with one another.

The analog assistance of AMPS has been refreshed with digital cell administration by adding to FDMA a further subdivision of each channel utilizing time division multiple access (TDMA). This administration is known as digital AMPS (D-AMPS). In spite of the fact that AMPS and D-AMPS began for the North American cell phone advertise, they are presently utilized worldwide with more than 74 million endorsers, as indicated by Ericsson, one of the major PDA makers.

1.4.2.2. Total Access Communication System (TACS)

It is an analogue mobile communications system used in the U.K. and a number of other countries. TACS is an analogue FM system operating in the 890-915 MHz / 935-960 MHz

band; the band in which GSM was introduced later. The radio channel bandwidth was 25 kHz, offering 1000 duplex channels in the 900 MHz band. Because TACS used a reduced radio channel bandwidth compared to AMPS, which has a bandwidth of 30 kHz, the data signalling rate had to be reduced. A modified version of TACS has been in use in Japan. The Japanese version was called JTACS. The main differences are another radio frequency band in which it operated.

Some Other analog cellular systems are – [5]

- Nordic Mobile Telephone (NMT)
- Narrowband AMPS (NAMPS)
- Mobile Cellular System (MCS)
- CNET etc.

1.4.3. Digital Cellular Systems (2nd Generation)

The 2nd generation cellular system includes technologies like GSM, TDMA & CDMA.

1.4.3.1. Global System for Mobile Communication

The Global System for Mobile Communications (GSM) system is a global digital radio system that uses Time Division Multiple Access (TDMA) technology. A GSM system is made up of different components. A GSM architecture is shown below.

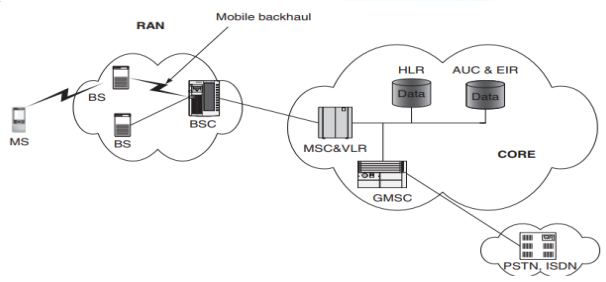


Figure 7 : GSM Architecture

MS – Mobile Station (mobile phone)	HLR – Home Location Register
BS – Base Station (site)	VLR – Visited Location Register
BSC – Base-Station Controller	AuC – Authentication Centre
MSC – Mobile Switching Centre	EIR – Equipment Identity Register
GMSC – Gateway MSC	PSTN – Public Switching Telephone Network

1.4.3.1.1. Mobile Station (MS)

The Mobile Station (MS) comprises of the types of equipment and the software that are utilized to discuss the client with the assistance of versatile system. It transmits the data and alters it to the transmission conventions of the air interface to speak with the BSS. The client data speaks with the MS through a mouthpiece and speaker for the discourse, console and show for short

[5] (Bowler, 2004)

informing and the link association for other information terminals. The versatile station has two components Mobile Equipment (ME) and Subscriber Identity Module (SIM).

1.4.3.1.2. Mobile Equipment (ME)

It is the hardware which customer gets from the equipment manufacturer. This hardware piece consists of all the components required for the implementation of the protocols to interface with the user and the air-interface to the base stations. Every Mobile equipment has a unique identifying number called IMEI.

International Mobile Equipment Identity (IMEI)

It is a unique 15 (14+ 1 Checksum digit) (or 16 (14+2 Checksum) for IMEISV) digit long number which is used to identify mobile equipments. For every transceiver present in the device it has a different IMEI number.

Structure of IMEI Number

The general format to represent an IMEI Number is AA – BBBBBB – CCCCCC -D.

Here first 8-digits AA-BBBBBB shows the TAC (Type Allocation code) in which first two digit shows RBI (Reporting Body Identifier) and remaining 6-digits show FAC(Final Assembly Code)

Next 6-digit 'CCCCCC' shows SNR(Serial Sequence of the Model) and last one digit 'D' shows the checksum digit according to Lunh Algorithm.

1.4.3.1.3. Base Station

A base station helps in transmitting and receiving user data. When the user's data transmission and data receiving is only permitted to mobile network, the base stations helps to handle the calls of several subscribers simultaneously.

1.4.3.1.4. Base Transceiver Station (BTS)

The base transceiver station helps the client in information transmission between the cell phone and the base station. A transceiver is a circuit which transmits and receives, i.e., performs the two functions.

1.4.3.1.5. Base Station Controller (BSC)

A number of BSs are controlled by one BSC. The BSC manages radio resources on in base stations, it is responsible for RF channel allocation and takes part in call setup, manages handovers. The base stations and BSC are connected by fixed lines or point-to-point radio links, this part of system infrastructure is named Mobile Backhaul. The BSs, BSCs and mobile backhaul together form the radio access network, RAN.

1.4.3.1.6. Mobile Switching Centre (MSC)

The MSC performs all of the switching functions including path search, data forwarding and service feature processing. The main difference between an ISDN switch and the MSC is that the MSC also has to consider mobility of users. The MSC has to provide additional functions for location registration of users as well as manage the handover of a connection when a user moves from cell to cell. A cellular network may have several MSCs with each being responsible for some part of the network called the Location Area (LA).

Calls originating from or terminating in the fixed network are handled by a dedicated Gateway MSC (GMSC). The interworking of a cellular network and a fixed network (e.g. PSTN, ISDN) is performed by the Interworking Function (IWF). It is needed to map the protocols of the

cellular network onto those of the respective fixed network. Either GMSC or IWF can be implemented as a standalone node or as a SW functionality with some HW interfaces in the MSC.

1.4.3.1.7. Home Location Register (HLR)

The HLR is the subscriber database of a GSM network. It contains a record for each subscriber, with information about the individually available services.

IMSI (International Mobile Subscriber Identity)

It is maximum 15-digit long number which is unique internationally and it is used to identify a subscriber. It is stored in SIM (Subscriber Identity Module) of Subscriber. It can be divided into three parts.

- Mobile Country Code (MCC): three digits, internationally standardized;
- Mobile Network Code (MNC): two digits, for unique identification of mobile networks within a country;
- Mobile Subscriber Identification Number (MSIN): a maximum of 10 digits, identification number of the subscriber in their mobile home network.

A three-digit MCC has been assigned to each of the GSM countries and two-digit MNCs have been assigned within countries (e.g. 404 is the MCC for India and MNC 01, 02 and 03 for the networks of Vodafone (Haryana), Airtel (Punjab) and Airtel (Himachal Pradesh) respectively).

When the mobile device is switched on, the IMSI is retrieved from the SIM card and sent to the MSC. There, the MCC and MNC of the IMSI are analysed and the MSC is able to request the subscriber's record from the HLR of the subscriber's home network.

MSISDN

The phone number of the user, which is called the Mobile Subscriber Integrated Services Digital Network Number (MSISDN) in the GSM standards, has a length of up to 15 digits and consists of the following parts:

CC (Country Code) – Two-digit code to identify the country (+91 for India)

NDC (National Destination Code)

SN (Subscriber Number)

Mobile Equipment Identifier (MEID)

It is globally unique 56 bit long number used to identify a CDMA mobile station.

Regional code		Manufacturer code						Serial number						CD
R	R	X	X	X	X	X	X	Z	Z	Z	Z	Z	Z	C

1.4.3.1.8. Visitor Location Register

VLR is a logical node implemented in MSC. HLR and VLR databases store the profiles of users, which are required for charging and billing and other administrative issues.

Each MSC has an associated Visitor Location Register (VLR), which holds the record of each subscriber that is currently served by the MSC (Figure 1.12). These records are only copies of the original records, which are stored in the HLR (see Section 1.6.3). The VLR is mainly used to reduce signalling between the MSC and the HLR. If a subscriber roams into the area of an MSC, the data are copied to the VLR of the MSC and are thus locally available for every connection establishment. Verification of the subscriber's record at every connection establishment is necessary as the record contains information about the services that are active and the services from which the subscriber is barred. Thus, it is possible, for example, to bar outgoing calls while allowing incoming calls, to prevent abuse of the system.

1.4.3.1.9. Equipment Identity Register (EIR)

It is a kind of database to perform security functions. It stores the record of all the mobile stations that are allowed in a network. IMEI number of all equipments are stored in this register.

1.4.3.1.10. Authentication Centre (AUC)

It stores all data related to security like the keys for authentication and various encryption.

The whole GSM network can be divided into three subsystems. These are –

- **Base Station Subsystems (BSS)** : It is also known as 'radio network' and contains all nodes and functionalities required to connect mobile subscribers over radio interface to the network wirelessly.
- **Network Subsystem (NSS)** : It is also known as 'core network' and contains all nodes and functionalities required to switching a call, subscriber management and mobility management.
- **Intelligent Network Subsystem (IN) :** It comprises SCP databases that add optional functionality to the network. One of the most important optional IN functionalities of a mobile network is the prepaid service, which allows subscribers to first fund an account with a certain amount of money which can then be used for network services like phone calls, Short Messaging Service (SMS) messages and, data services via GPRS and UMTS.

Subscriber Identity Module (SIM)

A SIM card is a small removable chip that identifies a mobile device on a cellular network. It contains an integrated circuit that stores a unique identifier called an "international mobile subscriber identity" (IMSI) number and other information specific to the mobile carrier.

The SIM card turns a handset into a mobile station (MS) with a set of network services allowed for use by subscription. The SIM concept allows to distinguish between equipment mobility and subscriber mobility. In general, a subscriber can register to the locally available network with their SIM card using different handsets. This enables international roaming independent of mobile equipment and network technology, provided that the air-interface standard in visited network is supported by mobile terminal.

Figure 8 : SIM Card

Every sim card contains a unique 20 digit serial number written over it which is known as ICCID (Integrated Circuit Card Identifier) .

The format of the ICCID is: MMCC IINN NNNN NNNN NN C x
MM = Constant (ISO 7812 Major Industry Identifier)
CC = Country Code
II= Issuer Identifier
N{12} = Account ID ("SIM number")
C = Checksum calculated from the other 19 digits using the Luhn algorithm.
x= An extra 20th digit is returned by the 'AT!ICCID?' command, but it is not officially part of the ICCID.

Handover Mechanism

Handover is the mechanism which initiates when a mobile move from its current network cell to another network cell while call on progress.

There are 4 types of handovers in GSM networks –

- **Intra Cell Handover:** Performed to optimise the traffic load in the cell.
- **Inter Cell Handover :** Mobile moves from one cell to another in same BSC.

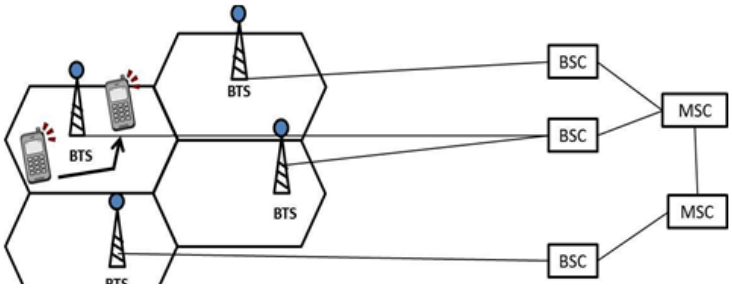


Figure 9: Intra Cell Handover

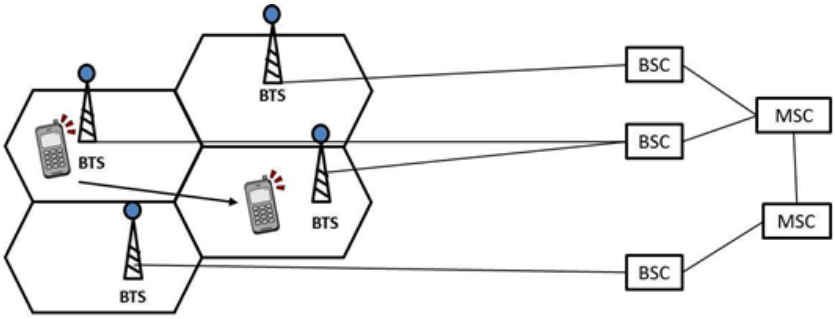


Figure 10 : Intra BSC or Inter Cell Handover

- **Inter BSC Handover:** Performed when mobile moves from one BSC to another BSC under one MSC.

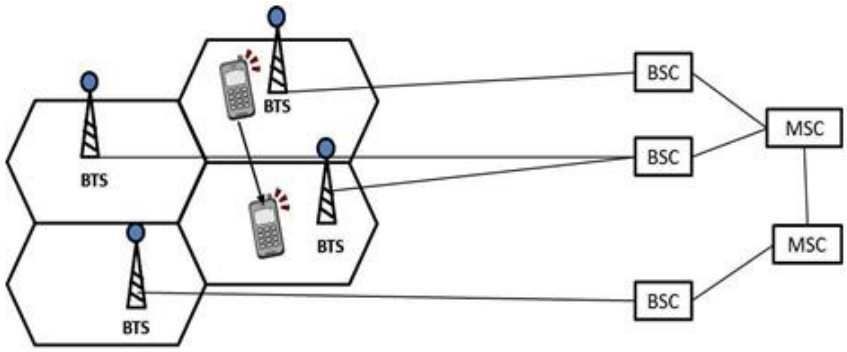


Figure 11: Inter BSC Handover

- **Inter MSC Handover:** Performed when mobile moves from one MSC to another MSC.

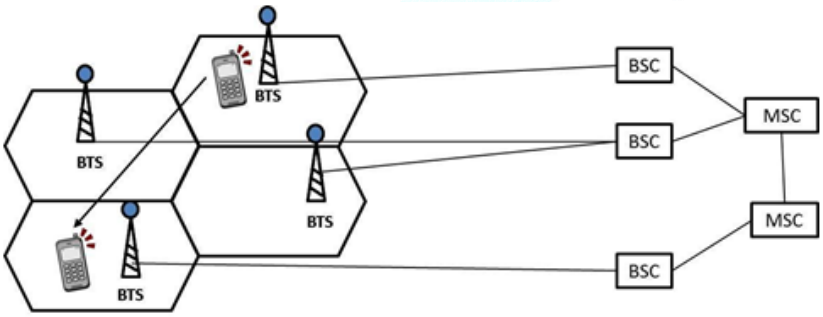


Figure 12 : Inter MSC Handover

1.4.4. Advance Digital Cellular Systems (Generation 2.5)

It includes technologies like GPRS, EDGE etc.

1.4.4.1. General Packet Radio Service (GPRS)

General Packet Radio Service (GPRS) is a part of the GSM particular that permits bundle radio help on the GSM framework. The GPRS framework includes (characterizes) new bundle channels and exchanging hubs inside the GSM framework. The GPRS framework accommodates hypothetical information transmission rates up to 172 kbps.

1.4.4.2. Enhanced Data Rates for Global Evolution (EDGE)

Enhanced Data Rates for Global Evolution (EDGE) is a developed adaptation of the Global System for Mobile (GSM) radio channel that utilizes new stage adjustment and bundle transmission to accommodate propelled fast information administrations. The EDGE framework employments 8 levels Phase Shift Keying (8PSK) to permit one image change to speak to 3 bits of data. This is multiple times the measure of data that is moved by a standard 2 level Gaussian Minimum Shift Keying (GMSK) signal utilized by the original of GSM framework. This outcomes in a radio channel information transmission pace of 604.8 kbps and a net most extreme conveyed hypothetical information transmission pace of 384 kbps. The progressed bundle transmission control framework takes into consideration continually fluctuating information transmission rates in either bearing between portable radios.

1.4.5. 3rd Generation Cellular Systems (3G)

It generally works on UMTS and HSPA technology.

1.4.5.1. Universal Mobile Telecommunication Systems (UMTS)

It is 3rd generation wireless telecommunication system with advancement in GSM and GPRS. C3G mobile network can be divided into three parts. These are –

- A Radio Access Network (RAN). This is a hierarchical arrangement of cell towers and base stations. The base stations are called base transceiver stations (BTSs) or NobeBs in 3G. In some versions, there are also Radio Network Controllers (RNCs) that link to the BTSs to form a Radio Network Subsystem (RNS). A collection of RNSs using the Wideband CDMA (WCDMA) air interface option form the UMTS Terrestrial Radio Access Network (UTRAN). All of these are referred to as "network devices
- A core network (usually IP) tying the RAN to the 3G service network. The core network consists of all the switches, routers, and other network components required to transport mobile traffic.
- A service network reached through the core network. Some of the services reached are specific to the service provider, such as accounting information (current balance), short message service (SMS) texting, paging, and voice mail. Other services are reached through the GGSN (which is not properly part of the 3G service network), such as the Internet, other Internet service providers (ISPs), or corporate network virtual private networks (VPNs). The MobileNext Broadband Gateway can be configured as a GGSN.

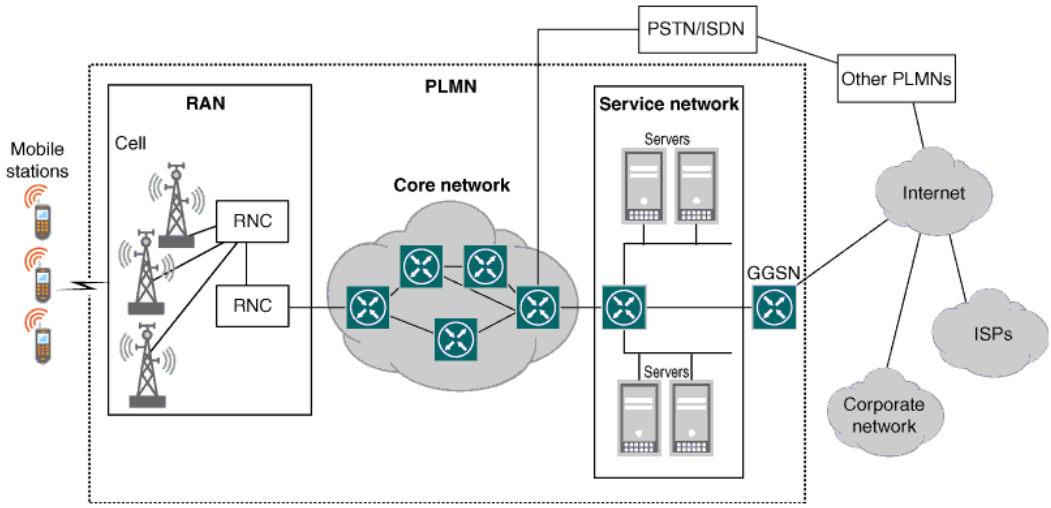


Figure 13 : 3G Architecture

The major parts of UTMS network are as follows –

1.4.5.1.1. User Equipment (UE)

The USER Equipment or UE is a significant component of the general 3G UMTS netwrok architecture. It shapes the last interface with the client. Considering the far more noteworthy number of uses and offices that it can play out, the choice was made to consider it a client hardware as opposed to a portable. Anyway, it is basically the handset (in the broadest wording), in spite of the fact that approaching a lot higher speed information interchanges, it very well may be considerably more adaptable, containing a lot more applications. It comprises of a wide range of components including RF hardware, preparing, recieving wire, battery, and so on.

1.4.5.1.2. Radio Network Subsystem (UTRAN)

This is the section of the 3G UMTS / WCDMA network that interfaces to both the UE and the core network. The overall radio access network, i.e. collectively all the Radio Network Subsystem is known as the UTRAN UMTS Radio Access Network.

The radio network subsystem is also known as the UMTS Radio Access Network or UTRAN

Radio Network Controller

The RNC owns and controls the radio resources in its domain. It is an intermediate component between NodeB and the CN. RNC performs three main functions and on the basis of these functions RNC can be of three types –

Controlling RNC (CRNC) : To control Each NodeB in architecture.

Serving RNC (SRNC) : Mobile UE is controlled by this RNC. It acts as a sole point of contact with the core network for the device.

Drift RNC (DRNC) : A drift RNC uses the Iur interface to carry UE specific signalling information between the NodeBa and the SRNC.

1.4.5.1.3. Serving GPRS Support Node (SGSN)

As the name implies, this entity was first developed when GPRS was introduced, and its use has been carried over into the UMTS network architecture. The SGSN provides a number of functions within the UMTS network architecture. The major functions of SGSN are –

- Mobility Management
- Session Management
- Interaction with other areas of network
- Billing

1.4.5.1.4. Gateway GPRS Support Node (GGSN)

Like the SGSN, this entity was also first introduced into the GPRS network. The Gateway GPRS Support Node (GGSN) is the central element within the UMTS packet switched network. It handles inter-working between the UMTS packet switched network and external packet switched networks, and can be considered as a very sophisticated router. In operation, when the GGSN receives data addressed to a specific user, it checks if the user is active and then forwards the data to the SGSN serving the particular UE.

1.4.5.1.5. Gateway MSC (GMSC)

This is a switch used to connect UTMS PLMN to external network.

1.4.6. 4th Generation Cellular Systems (4G)

It includes technologies like LTE, Wimax etc. It is the evolution of 3G contains various technologies like GSM, CDMA, GPRS, Wireless LAN etc.. The data rate in 4G systems are in range 20-100 MBPS.

4G Architecture

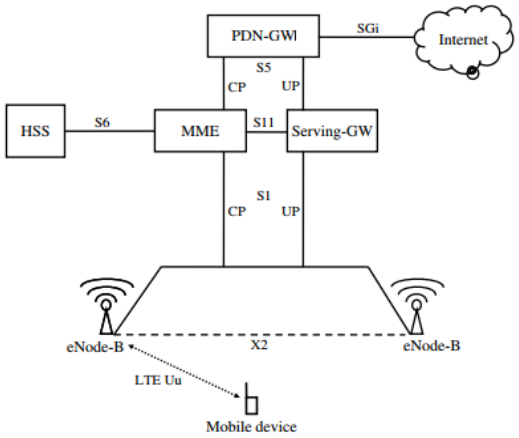


Figure 14 : LTE Network Overview

The major components of 4G network architecture are –

1.4.6.1. User Equipment (UE)

As in UMTS, the LTE mobile station is called User Equipment (UE). It is constructed using a modular architecture that consists of three main components.

- ***Mobile Termination*:** The MT represents termination of the radio interface. In this entity the RRC signalling is terminated and RRC messages are sent/received.
- ***Terminal Adapter*:** The terminal adapter represents the termination of the application-specific service protocols; for example, SIP signalling for VoIP. The terminal adapter could be in fact an external device, such as a modem with a USB interface to connect to a laptop.
- ***Terminal Equipment*:** The TE represents termination of the service. In case of USB, the laptop acts as a TE. Otherwise, a smart phone is the TE where the service is terminated in application on mobile device.

1.4.6.2. eNB

An eNB provides users with the radio interfaces and performs Radio Resource management (RRM) functions such as dynamic resource allocation, eNB measurement configuration and provisionetc.

1.4.6.3. Evolved Packet Core Network (EPC)

Entity	Description
MME	An MME is the main control entity for the E-UTRAN. It communicates with an HSS for user authentication and user profile download, and provides UEs with EPS Mobility Management (EMM) and EPS Session Management (ESM) functions using NAS signaling. The main functions supported by a MME are as follows: • NAS signaling (EMM, ESM and NAS Security) • User authentication and roaming with HSS over the S6a interface • Mobility management (paging, Tracking Area List (TAI) management and handover management) • EPS bearer management
S-GW	An S-GW terminates the interface towards an E-UTRAN. It serves as the local mobility anchor point of data connections for inter-eNB handover and inter-3GPP handover.
P-GW	A P-GW provides a UE with access to a PDN by assigning an IP address from the address space of the PDN. The P-GW serves as the mobility anchor point for handover between 3GPP and non-3GPP. It also performs policy enforcement, packet filtering and charging based on the PCC rules provided by a PCRF. The main functions supported by a P-GW are as follows: • IP routing and forwarding • Per-SDF/Per-User based packet filtering • UE IP address allocation • Mobility anchoring between 3GPP and non-3GPP • PCEF functions • Charging per-SDF/per-User
HSS	An HSS is the central DB where user profiles are stored. It provides user authentication information and user profiles to the MME.
PCRF	A PCRF is the policy and charging control entity. It makes policy decisions for SDFs and provides the PCC rules (QoS and charging rules) to the PCEF (P-GW).
SPR	A SPR provides subscription information (access profile per subscriber) to the PCRF. Receiving the information, the PCRF performs subscriber-based policy and creates PCC rules.
OCS	An OCS provides (i) real-time credit control and (ii) charging functions based on volume, time and event.
OFCS	An OFCS provides CDR-based charging information.

Figure 15 : LTE Entities

2. Mobile Phone Forensics

2.1. Introduction

Mobile devices are very common in today's society, used by many individuals for both personal and professional purposes. Mobile devices vary in design and are continually undergoing changes as existing technologies are getting and new technologies are

introduced (software as well as hardware). When a mobile device is found during an investigation, many questions arise:

- What is the best method to preserve the evidence?
- How should the device be handled?
- How should valuable or potentially relevant data present in the device be extracted?

The key to answering these questions begins with a firm understanding of the hardware and software characteristics of mobile devices. The digital forensic community faces a constant challenge to stay abreast of the latest technologies that may be used to expose relevant clues in an investigation. Many vendors and forensic examiners have not specified any standard operating procedures for acquisition in mobile forensics. But, they will guide to set appropriate policies and procedures for dealing with mobile devices.

2.1.1. Important Key Terms

TERMS	ACRONYM
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
SIM	Subscriber Identity Module
ESN	Electronic Serial Number (CDMA)
ICCID	Integrated Circuit Card ID (20-bit) or unique serial number printed on SIM
CGI	Cell Global Identity
PIN	Personal Identification Number (For SIM)
PUK	Personal Unblocking code
GSM	Global system for Mobiles
CDMA	Code division multiple access
TDMA	Time division multiple Access
iDEN	Integrated Digital Enhanced Network
GPRS(2.5 G)	General Packet Radio Service
EDGE(2.75G)	Enhanced Data rates for GSM Evolution

UMTS(3G)	Universal Mobile Telecommunication System
HSDPA(3.5G)	High Speed Downlink Packet Access
LTE (4G)	Long Term Evolution

2.1.2. Definition

Mobile Forensics is a sub-discipline of Digital Forensic Science dealing with forensic analysis of cell phone / mobile phone & its accessories and core network. Or
Mobile device forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods given by (National institute of standards and technology).

2.1.3. Scope of Work

The scope of work mainly focuses on various characteristics of mobile devices such as:

1. Cell Phone
2. SIM Cards
3. GPS Navigation Devices
4. Satellite Phones
5. Memory Card (Expandable Memory) 6. Logs from Service Provider (For Correlation)

2.2. Mobile Forensics –Principles:

Mobile devices perform an array of functions ranging from a simple telephony device to those of a personal computer. Designed for mobility, they are compact in size, battery powered, and lightweight. Most of the mobile phones have more features and capabilities (we call them Smartphone's) just like today's modern computers have almost same forensic properties and principles.

i) Forensically sound

The science of retrieving data from a "handheld device" under forensically sound conditions.

ii) Acquisition from multiple sources Includes full data retrieval/ examination of data found on the SIM, the phone body itself and the optional memory cards.

iii) Variety of data

Data retrieved and examined can include images, videos, text or SMS messages, call times and contact numbers etc.

iv) Legal admissibility

Data retrieved “may be” admissible as an evidence in the court of law.

Acceptable Operating Procedures:

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

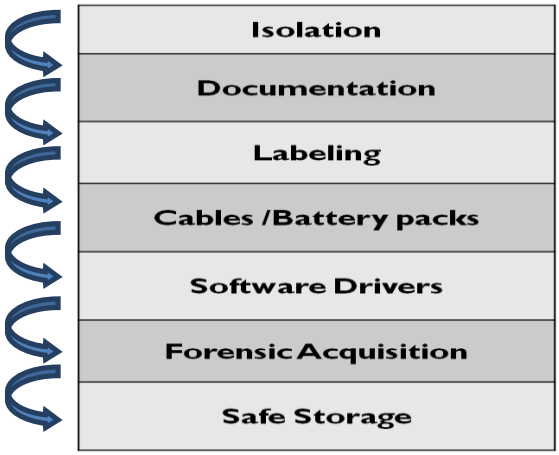


Figure 16 Mobile Seizure

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 acquisition 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.

Documentation: Documenting every piece of electronic evidence with its serial number, make and model number properly in "seizure punchnama" 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.

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.

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 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: For all devices that uses SIM cards like GSM handsets, the IMEI (International Mobile equipment Identifier) which can be obtained from any mobile phone just by keying in *#06#. For CDMA mobiles we have to get the ESN (electronic serial number) from the handset.

  IMEI is a 15-digit number that indicates the manufacturer, model and country of approval for GSM phones. The structure of IMEI is divided into three parts.

  1. TAC (Type approval code) – 6 digit
  2. FAC (Final Assembly code) – 2 digits
  3. Serial Number- 7 digit (Unique)

  Collectively called TAC (Type allocation code).

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

Figure 17: IMEI 1

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

Figure 18: IMEI 2

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/ 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.

Forensic 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. Now a days all forensic tools support extraction either wired (USB, RS-232) 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.

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.

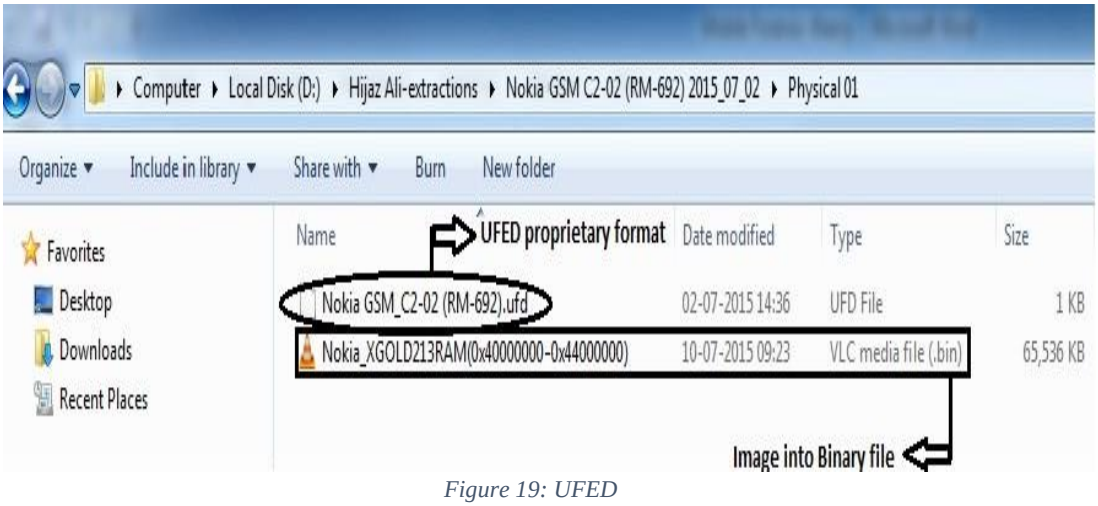


Figure 19: UFED

3. 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.

What if your Device (SIM & Handset) is Damaged:

If 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 perform methods like MicroRead 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.

Difference between Computer Forensics & Mobile Forensics

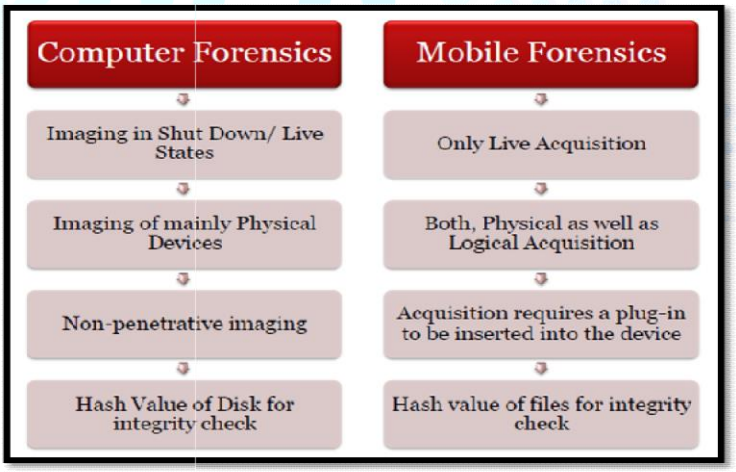


Figure 20: Computer Forensics Vs Mobile Forensics

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 non-volatile 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.

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.

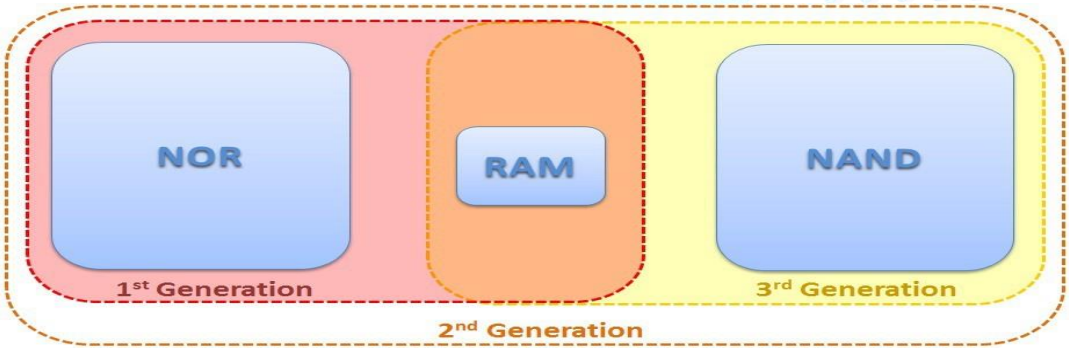


Figure 21: Mobile Generations

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 leveling 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 leveling 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.

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 artifacts found totally dependable on the type of case. We will see a different type of artifacts from different memory modules belongs to the mobile device.

Figure 21: Mobile components

Artifacts 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 8 digit 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).

Artifacts 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

Artifacts Collected from Network provider:

- Subscriber name and address
- Phone number associated with SIM
- Billing account details
- Telephone number (MSISDN)
- IMSI
- SIM number
- PIN (Personal Identification Number) /PUK (PIN Unlock key) for the SIM.
- 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.

Figure 21: mobile forensic tools

Reporting:

- Simple language (Use less technical terminology and explain in easy way)
- Date and time when the examination was started
- Physical condition of the phone
- 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

3. SIM (Subscriber Identity Module)

A subscriber identity module or subscriber identification module (SIM) is an integrated circuit chip that is intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contacts on many SIM cards. SIM cards are always used on GSM phones; for CDMA phones, they are only needed for newer LTE-capable handsets. SIM cards can also be used in satellite phones.

Service Providers that use SIM Cards in India

- Bharti Airtel
- Vodafone Idea
- Reliance Communications (RCOM) or JIO
- BSNL

The SIM circuit is part of the function of a Universal Integrated Circuit Card (UICC) physical smart card, which is usually made of PVC with embedded contacts and semiconductors. "SIM cards" are designed to be transferable between different mobile devices. The first UICC smart cards were the size of credit and bank cards; the development of physically smaller mobile devices has prompted the development of smaller SIM cards, where the size of the plastic carrier is reduced while keeping electrical contacts the same.

A SIM card contains its unique serial number (ICCID), international mobile subscriber identity (IMSI) number, security authentication and ciphering information, temporary information related to the local network, a list of the services the user has access to, and two passwords: a personal identification number (PIN) for ordinary use, and a personal unblocking code (PUK) for PIN unlocking.

A PIN locks the SIM card until correct code is entered. Each phone network sets the PIN of SIM to a standard default number (this can be changed via handset). If PIN protection is enabled, the PIN will need to be entered each time phone is switched on. If the PIN is entered incorrectly 3 times in a row, the SIM card will be blocked requiring a PUK from the network/service provider.

A PUK is needed if the PIN is entered incorrectly 3 times and the SIM is blocked (phone is unable to make and receive calls/texts). The PUK can be received from the network provider, or possibly the GSM cell phone manual. Caution: if PUK is entered 10 times incorrectly, the SIM card is permanently disabled and must be exchanged.

3.1. Integrated Circuit Card ID (ICCID)

Each SIM is internationally identified by its ICC-ID (Integrated Circuit Card ID). ICC-IDs are stored in the SIM card and can also be engraved or printed on the SIM card's body during a process called personalization. The number is up to 18 digits long with an addition of a single "check digit" that is used for error detection. This single digit allows us to detect an input error of digits, mistyped digits or a permutation of two successive digits. This digit was calculated using the Luhn algorithm.

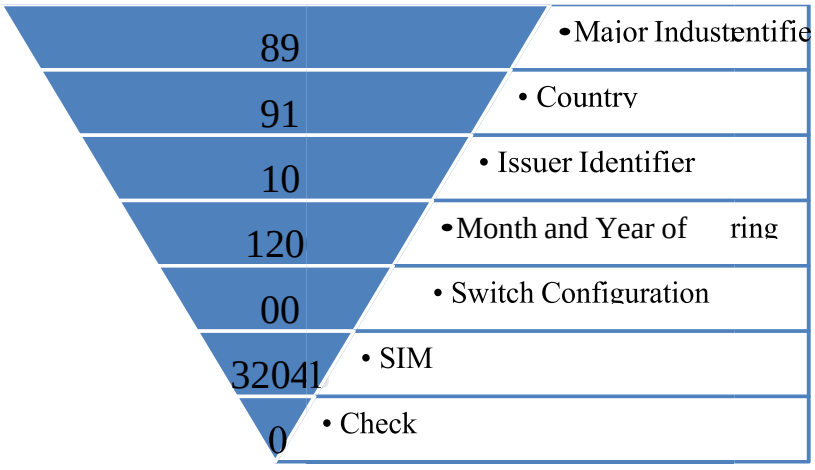


Figure 22 : ICCID

A typical SIM (19 digits) example 89 91 10 1200 00 320451 0, provide several details as follows:

- The first two digits (89 in the example) refers to the Major Industry Identifier.
- The next two digits (91 in the example) refers to the country code (91-India).
- The next two digits (10 in the example) refers to the issuer identifier number.
- The next four digits (1200 in the example) refers to the month and year of manufacturing.
- The next two digits (00 in the example) refers to the switch configuration code.
- The next six digits (320451 in the example) refers to the SIM number.
- The last digit which is separated from the rest is called the checksum digit.

These digits can be further grouped for additional information:

- The major Industry Identifier, Country Code, and Issuer Identifier Number make up the Issuer Identification Number (IIN) which is a maximum of 7 digits.
- The next several digits (variable length) represent the Individual Account Identification Number The final digit is a checksum digit

3.2. Location Area Identify

Operation networks for cell phone devices are divided into area locations called Location Areas. Each location is identified with its own unique identification number creating the LAI (Location Area Identity). A phone will store this number 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. This way if a phone is powered down, when it boots back up, it can search its list of LAIs it has stored until it finds the one it's in and can start to receive service again. This is much quicker than scanning the whole list of frequencies that a telephone can have access on. This is a real plus for forensic investigators because when a SIM card is reviewed, they can get a general idea of where the SIM card has been geographically. In turn this tells them where the phone has been and can then relate back to where the individual who owns the phone has been.

3.3. SIM Structure

SIM contains both a processor (CPU) and an operating system which is either native (proprietary, vendor specific) or Java Card (a subset of the Java programming language). SIMs also have Electrically Erasable Programmable Read Only Memory (EEPROM), Random Access Memory (RAM) for controlling program execution, and persistent Read Only Memory (ROM) which stores user authentication, data encryption algorithms, the operating system, and other applications. Communication between the SIM card and the handset is via a serial interface.

A SIM card also contains a hierarchical file system which resides in EEPROM. The file structure consists of a Master File (MF), which is the root of the file system, Dedicated Files (DFs), and Elementary Files (EFs). Dedicated Files are subordinate directories under the MF, their contents and functions being defined by the GSM11.11 standards. Three are usually present: DF (DCS1800), DF (GSM), and DF (Telecom). Also present under the MF is EF

(ICCID). Subordinate to each of the DFs are supporting EFs which contain the actual data. The EFs under DF (DCS1800) and DF (GSM) contain network related information and the EFs under DF (Telecom) contain the service related information. A typical SIM card file system is shown in Figure

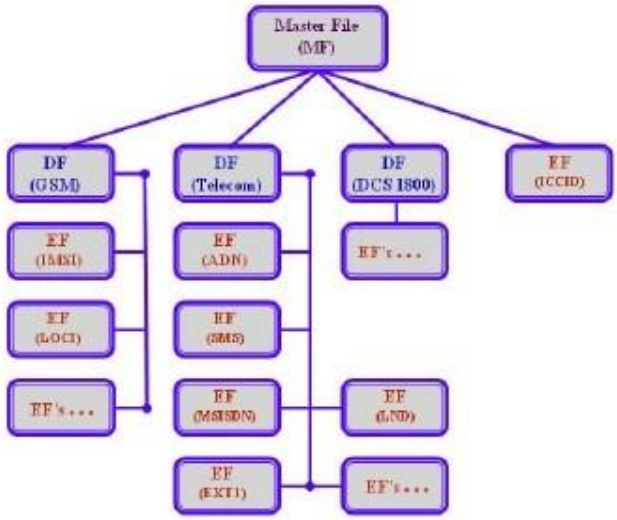


Figure 23: SIM Hierarchy

While all the files have headers, only the EFs contain data. The first byte of the header identifies the file type. Headers contain the security and meta-information related to the structure and attributes of the file, such as length of record. The body of the EFs contains information related to the application(s). Files can be either administrative or application specific and access to stored data is controlled by the operating system.

3.4. SIM SECURITY

SIM cards have built in security features that are designed to make them tamper resistant, thereby ensuring data security. A SIM card's MF, DFs, and EFs all contain security attributes. One security attribute, the access conditions, are constraints upon the execution of commands. They filter every execution attempt, thus ensuring that only those with the proper authorization can access the requested functionality controlled by the DFs or EFs. Access conditions can be thought of as somewhat analogous to the user rights associated with the file/directory attributes found in computer operating systems. There are different levels of access conditions associated with DF and EF files:

Always (ALW): file access is allowed without restrictions and the command is executable upon the file.

- Card Holder Verification 1 (CHV1): file access is allowed with the valid verification of the users PIN1 (or PIN1 verification is disabled) and the command is executable upon the file.
- Card Holder Verification 2 (CHV2): file access is allowed with a valid verification of the user's PIN2 (or PIN2 verification is disabled) and the command is executable upon the file.
- Administrative (ADM): the administrative authority (i.e. the card issuer who provides the SIM card to subscribers), is responsible for the allocation of these levels.

- Never (NEV): file access is prohibited and the command is never executable upon the file.

3.5. Data of Forensic Value

Depending upon the phone's technology and access scheme, the same data, such as a contact list, may be stored on the SIM, in the handset, or on the phone's memory card. SIM cards themselves contain a repository of data and information, some of which is listed below:

- Integrated Circuit Card Identifier (ICCID)
- International Mobile Subscriber Identity (IMSI)
- Service Provider Name (SPN)
- Mobile Country Code (MCC)
- Mobile Network Code (MNC)
- Mobile Subscriber Identification Number (MSIN)
- Mobile Station International Subscriber Directory Number (MSISDN)
- Abbreviated Dialing Numbers (ADN)
- Last Dialed Numbers (LDN)
- Short Message Service (SMS)
- Language Preference (LP)
- Card Holder Verification (CHV1) and (CHV2)
- Ciphering Key (Kc)
- Ciphering Key Sequence Number
- Emergency Call Code
- Fixed Dialing Numbers (FDN)
- Local Area Identity (LAI)
- Own Dialing Number
- Temporary Mobile Subscriber Identity (TMSI)
- Routing Area Identifier (RIA) network code
- Service Dialing Numbers (SDNs)

Digital evidence is scattered throughout the Elementary Files (EF). Although a thorough discussion of all the potential evidence that could be on a SIM card

3.6. Service-Related Information

3.6.1. ICCID

Every SIM card is uniquely identified by its Integrated Circuit Card ID (ICCID) which is comprised of either nineteen or twenty digits. It is normally printed on the SIM card itself. The numbering of ICCIDs is based upon ITU-T recommendation E.118. A nineteen digit ICCID includes the Issuer Identification Number (IIN), the Individual Account Identification, and a single "Check Digit" that is used for error detection. Twenty digit ICCIDs have an additional "Checksum" digit.

3.6.2. IMSI

The International Mobile Subscriber Identity (IMSI) is a fifteen digit code that is used to uniquely identify an individual subscriber on a GSM network. It is stored in the EF(IMSI). IMSI conforms to ITU E.212 and consists of three components, the Mobile Country Code (MCC), the Mobile Network Code (MNC), and the Mobile Subscriber Identity Number (MSIN)

3.6.3. MSISDN

More than one definition exists for MSISDN. The most common is Mobile Subscriber Integrated Services

Digital Network Number. Another definition is Mobile Station International Subscriber Directory Number. The MSISDN can be thought of as a SIM card's unique telephone number (i.e., the telephone number of the GSM phone). It is stored in the EF(MSISDN). The MSISDN numbering format conforms to ITU-T E.164 and consists of three components, a Country Code (CC), the National Destination Code (NDC), and the Subscriber Number (SN).

Together, the MSISDN and IMSI are used to identify the mobile subscriber. While an IMSI is uniquely associated with a SIM, a SIM can have different MSISDNs associated with it. Also, the MSISDN is an optional EF and it can be updated by the subscriber.

3.7. Call Information

3.7.1. AND: Abbreviated Dialling Numbers

Abbreviated Dialling Numbers (ADNs) are stored in the EF(ADN) and are usually generated by the subscriber. Essentially, they are shortcuts for the subscriber's commonly called numbers. Since ADNs cannot be changed or viewed by the provider, they can be attributed to the user of the phone. How these are described could be helpful in an investigation to link the phone to a suspect.

3.7.2. LND: Last Number Dialled

The Last Number Dialled (LND) is stored in EF(LND). What is generally maintained is a listing of the most recent calls. However, SIMs are normally limited in the number of entries they can maintain. If necessary, to store additional digits from ADN and LDN, the EF(EXT1) may be used. Depending upon the phone, it is also conceivable that the information may be stored in the handset and not on the SIM. Any numbers that may be present can provide valuable information to an investigator.

3.8. Messaging Information

Text messaging or Short Message Service (SMS) is an extremely popular method of communication between individuals. Not surprisingly, there are many instances of SMS providing probative information for investigators in criminal proceedings. The maximum size of an SMS is limited to either 160 characters (Latin alphabet) or 70 characters (for other alphabets). Longer messages are broken down by the sending phone and reassembled by the receiving phone. Normally when one user sends a message to another, it is temporarily stored in the Short Message Service Center (SMSC) which handles the SMS for the network. The SMSC provides a "store and forward" functionality. If the recipient's phone is active, the message is forwarded. If it is not active (switched off), the message is temporarily stored and is only forwarded when the phone becomes active again. In addition to sending an SMS from

phone to phone, they can also be sent via a VoIP application such as Skype, from an instant messaging client such as ICQ, or from a Web based application running within a browser.

A SIM's capacity to store SMS varies. They can also be stored in the phone's internal memory. The EF(SMS) stores not only the text message, but other useful investigative information about the message, such as the time it was sent, the sender's phone number, and so forth. Although text messages can be deleted, initially they will still reside on the SIM. The space occupied by the deleted message is marked as free space and becomes available for another message. This is somewhat analogous to what occurs when a file is deleted on a computer. When a new text message is received, it takes the available free space, overwriting the previously deleted message and any unused portion of that free space.

3.9. Location Information

A SIM card contains the LOCI (Location Information) Elemental File which can be found under the GSM

Dedicated File (see April/May 2011 Digital Forensic Insider column for information regarding the SIM Card File System). This file contains the Temporary Mobile Subscriber Identity (TMSI), TMSI TIME, Location Area Information/Local Area Identifier (LAI), and the Location Update Status.

3.9.1. Temporary Mobile Subscriber Identity (TMSI):

In addition to allowing mobile phones to communicate with each other, the Network Switching Subsystem (NSS) also acts somewhat as a telephone exchange. However, it has additional functionality to deal with the roaming ability of cell phones. A key component of the NSS is the Mobile services Switching Centre (MSC) which provides functionality such as registration, location updating, and call routing. When a subscriber roams into the jurisdiction of an MSC, information about the cell phone is stored in a temporary database called the Visitor Location Register (VLR). Since each Base Station in the GSM network is served by one VLR, a subscriber cannot be present in more than one VLR at a time. The VLR assigns the TMSI which ensures privacy since it prohibits tracing of the identity of the subscriber should anyone attempt to intercept the link. The TMSI is assigned for the duration that the subscriber is within the jurisdiction of a particular MSC and combined with the current location area, allows a subscriber to be uniquely identified.

3.9.2. Location Area Information/Local Area Identifier (LAI)

The LAI for voice communications is structured hierarchically and uniquely identifies a Location Area (LA) in a GSM network. It consists of three components:

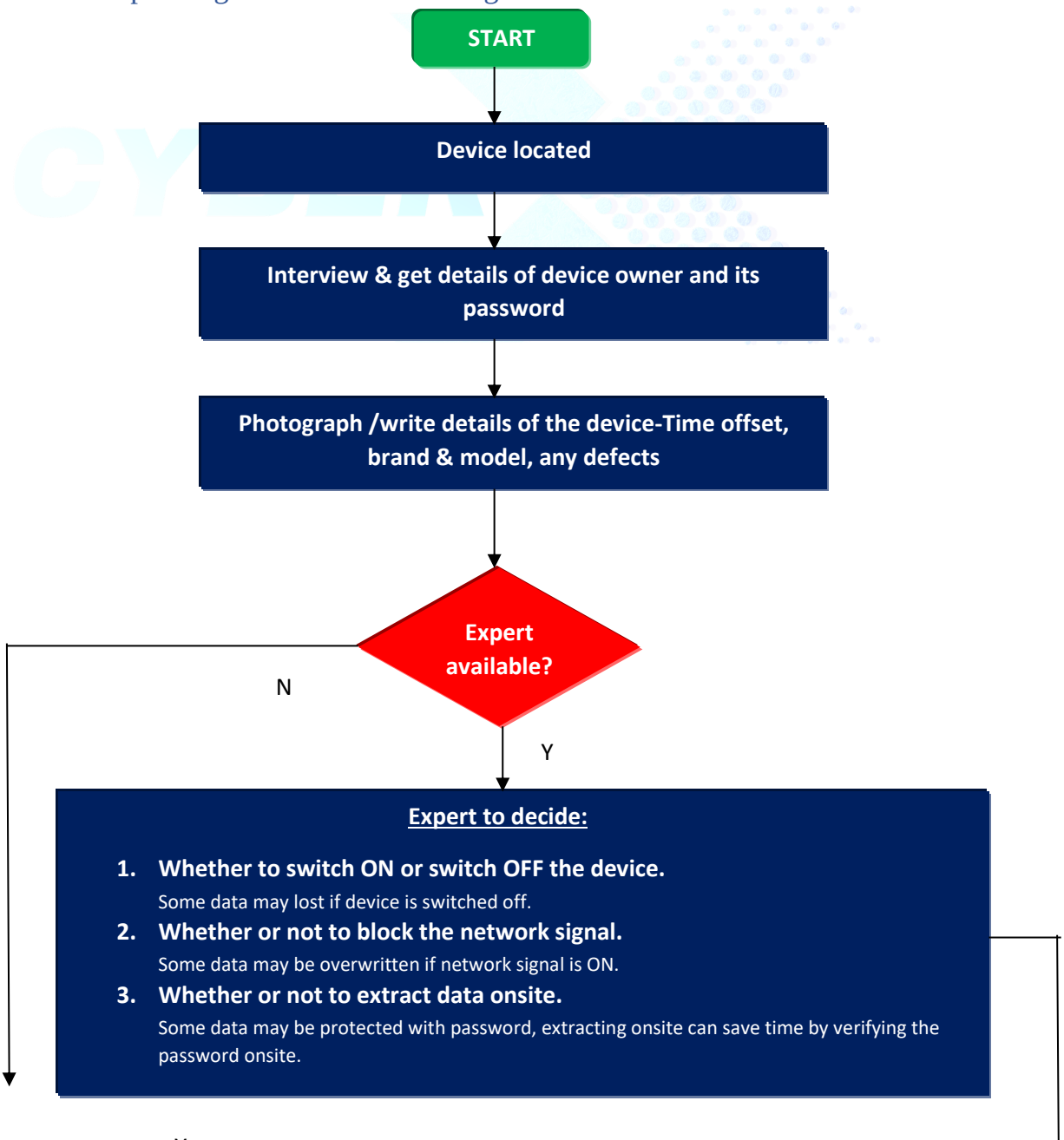
- Mobile Country Code (MCC): consists of three decimal places and is used to identify the country of origin of the SIM card.
- Mobile Network Code (MNC): consists of two decimal places and is used in conjunction with the MCC to identify the SIM card's network provider.
- Location Area Code (LAC): consists of a maximum of five decimal places.

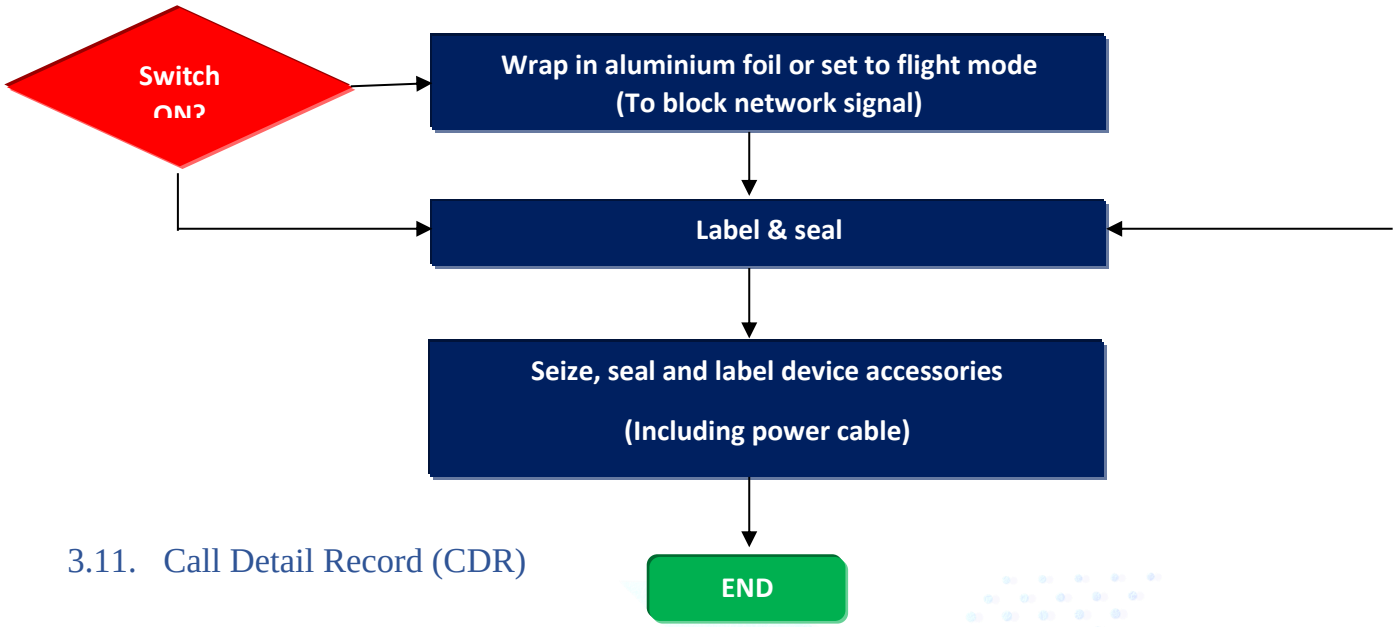
GSM networks are divided into LAs which are comprised of one or more radio cells. Each of the LAs is uniquely identified within the network by its Location Area Code (LAC). These numbers are stored on the SIM card, thus providing the handset with its location. This also serves as a unique reference for the location of the subscriber as well since the LAI is required before the handset can receive an incoming call. When the subscriber roams into a new LA,

the handset also stores the new LAI on the SIM card, adding it to a list of the previous LAIs. After being powered off and then powered back on, the handset will search the list of its stored LAIs until it finds the one it is currently located in, thereby allowing service to resume. Analysing the SIM card can provide the geographical location(s) where the SIM card, the phone, and the owner of the phone (suspect) may have been.

* To analyse a SIM card, it is normally removed from the handset and inserted into an appropriate reader. Command directives, called Application Protocol Data Units (APDUs), are sent to the SIM by the tool to extract potential probative evidence that may be present in the SIM file system. The original data on the SIM card is normally preserved by the elimination of write requests to the SIM during its analysis. Extracted data integrity can be maintained by the tool calculating the hash value(s) of the data from the files created and re-verifying as necessary to demonstrate that they remain unchanged. Some SIM tools extract and preserve data better than others. As with any forensic tool, examiners need to thoroughly research those that are available to determine which one(s) meet their needs. Most examiners are aware (or should be) that no one tool will be able to extract all the data from every different type of cell phone or SIM card.

3.10. Standard Operating Procedure for Seizing a Mobile Device & Tablets





3.11. Call Detail Record (CDR)

A **call detail record** (**CDR**) is a data record produced by a telephone exchange or other telecommunications equipment that documents the details of a telephone call or other communications transaction (e.g., text message) that passes through that facility or device. The record contains various attributes of the call, such as time, duration, completion status, source number, and destination number. It is the automated equivalent of the paper toll tickets that were written and timed by operators for long-distance calls in a manual telephone exchange.

3.11.1. Importance of CDR

- CDR comes very handy 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 holder which help police investigating the crime in a systematic fashion.
    - ❖ e.g; if someone is absconding after committing a crime, following information can be obtained from CDR about him which will prove handy for investigating the case:
    - ❖ The current location of SIM user
    - ❖ Night locations of SIM user
    - ❖ Person(s) he is talking to (via incoming/outgoing calls) most frequently.

3.11.2. Current Telecom Providers in India

Figure2 3 : Major Telecom providers in India

The list of telecom service providers and the associated details can be downloaded using the link http://www.trai.gov.in/ConsumerGroupUser.aspx

3.11.3. Guidelines for Requesting CDR

- 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.

3.11.4. Relevant Legal Sections & Compliances to Acquire CDR

- Call data records (CORs) can be sought under the statutory provisions contained in Section 92 of the Code of Criminal Procedure, 1973 or Section 5(2) of Indian Telegraph Act, 1885 read with Rule 419 A of Indian Telegraph (Amendment) Rules, 2007
- The authority seeking the COR in accordance with para (a), should first ascertain the identity of the subscriber and ensure that the person in question is not someone whose call details maybe of a sensitive nature.
- Any proposal for seeking COR of a telephone, subscribed in the name of a sitting Member of Parliament or a Member of State Legislature, should contain a clear indication to that effect. In case the telephone belongs to sitting Member of Parliament, the Police or Investigating Authority concerned should obtain prior approval of the Commissioner of Police / Director General of Police, as the case may be.
- The SOPs for LEA and TSP for lawful interception and monitoring, in so far as they pertain to COR, should be followed. In addition to that, following safeguards should be complied while handling COR related records electronically:
    - The officials, handling the COR related records, are required to maintain the sanctity and confidentiality of their password. The password shall be changed frequently, at least once a month. The password shall not be shared with any unauthorized person and if the authorization is found to be misused, it is the authorized official, who will be held responsible.
    - Any storage/communication made in respect of COR should be done through a designated computer (I.P. address and MAC address) having biometric authorization (Finger print) and kept in the office of officer concerned.
- The nodal officer of LEA shall reconcile the COR requests sent by them with the TSP on a fortnightly basis.
- A register should be maintained of all numbers whose CDRs have been sought. Supervisory officers must inspect the register containing details of the COR sought once a month It should be impressed upon all the officers that obtaining the CDRs of any individual is an intrusion into his/her privacy and cannot be resorted to in a casual and cavalier manner.

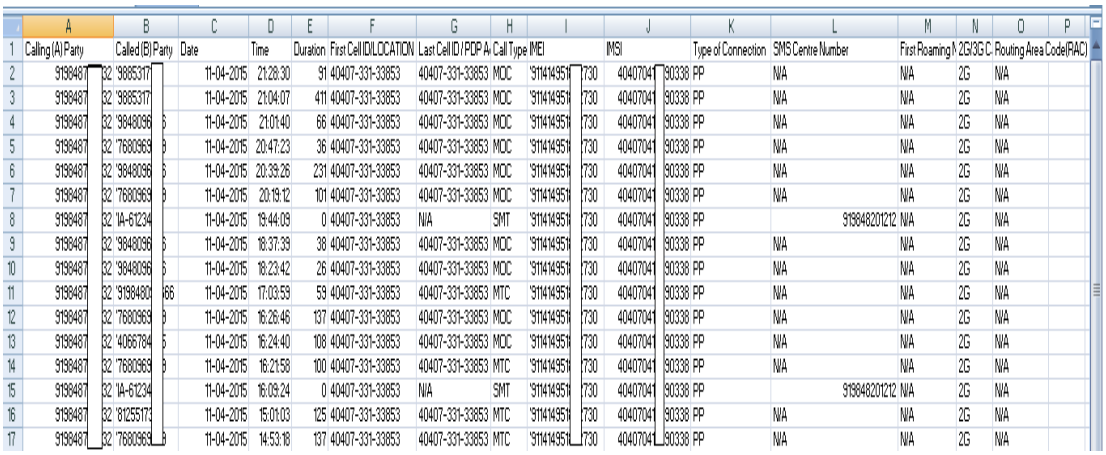
3.12. Types of CDR

a) Normal CDR – Details of Incoming, Outgoing call SMS & MMS

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. 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												**Period: DD/MM/YYYY to DD/MM/YYYY**
Calling Party	Called Party	Call Date	Time	Dur	First Cell ID of A Party	Last Cell ID of A Party	Call Type	IMEI	IMSI	Type of Connection (Pre/ Post paid)	SMSC	Roaming Circle
1	2	3	4	5	6	7	8	9	10	11	12	13

Figure2 4 : Format of 13 field column CDR required from Telecom Service Provider



Calling (A) Party	Called (B) Party	Date	Time	Duration	First Cell ID/LOCATION	Last Cell ID / PDP Ad	Call Type	IMEI	IMSI	Type of Connection	SMS Centre Number	First Roaming N	2G/3G C	Routing Area Code(RAC)
9198487	32 '9885317	11-04-2015	21:28:30	91	40407-331-33853	40407-331-33853	MOC	'911414951	730 4040704	90338 PP	N/A	N/A	2G	N/A
9198487	32 '9885317	11-04-2015	21:04:07	411	40407-331-33853	40407-331-33853	MOC	'911414951	730 4040704	90338 PP	N/A	N/A	2G	N/A
9198487	32 '9848096	11-04-2015	21:01:40	66	40407-331-33853	40407-331-33853	MOC	'911414951	730 4040704	90338 PP	N/A	N/A	2G	N/A
9198487	32 '7680969	11-04-2015	20:47:23	36	40407-331-33853	40407-331-33853	MOC	'911414951	730 4040704	90338 PP	N/A	N/A	2G	N/A
9198487	32 '9848096	11-04-2015	20:39:26	231	40407-331-33853	40407-331-33853	MOC	'911414951	730 4040704	90338 PP	N/A	N/A	2G	N/A
9198487	32 '7680969	11-04-2015	20:19:12	101	40407-331-33853	40407-331-33853	MOC	'911414951	730 4040704	90338 PP	N/A	N/A	2G	N/A
9198487	32 'IA-61234	11-04-2015	19:44:09	0	40407-331-33853	N/A	SMT	'911414951	730 4040704	90338 PP	919848201212	N/A	2G	N/A
9198487	32 '9848096	11-04-2015	18:37:39	38	40407-331-33853	40407-331-33853	MOC	'911414951	730 4040704	90338 PP	N/A	N/A	2G	N/A
9198487	32 '9848096	11-04-2015	18:23:42	26	40407-331-33853	40407-331-33853	MOC	'911414951	730 4040704	90338 PP	N/A	N/A	2G	N/A
9198487	32 '9198480	11-04-2015	17:03:59	59	40407-331-33853	40407-331-33853	MTC	'911414951	730 4040704	90338 PP	N/A	N/A	2G	N/A
9198487	32 '7680969	11-04-2015	16:26:46	137	40407-331-33853	40407-331-33853	MOC	'911414951	730 4040704	90338 PP	N/A	N/A	2G	N/A
9198487	32 '4066784	11-04-2015	16:24:40	108	40407-331-33853	40407-331-33853	MOC	'911414951	730 4040704	90338 PP	N/A	N/A	2G	N/A
9198487	32 '7680969	11-04-2015	16:21:58	100	40407-331-33853	40407-331-33853	MTC	'911414951	730 4040704	90338 PP	N/A	N/A	2G	N/A
9198487	32 'IA-61234	11-04-2015	16:09:24	0	40407-331-33853	N/A	SMT	'911414951	730 4040704	90338 PP	919848201212	N/A	2G	N/A
9198487	32 '8125517	11-04-2015	15:01:03	125	40407-331-33853	40407-331-33853	MTC	'911414951	730 4040704	90338 PP	N/A	N/A	2G	N/A
9198487	32 '7680969	11-04-2015	14:53:18	137	40407-331-33853	40407-331-33853	MTC	'911414951	730 4040704	90338 PP	N/A	N/A	2G	N/A

Figure 25 : Normal CDR

b) GPRS CDR –Details of Internet Uses & Its Location

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.

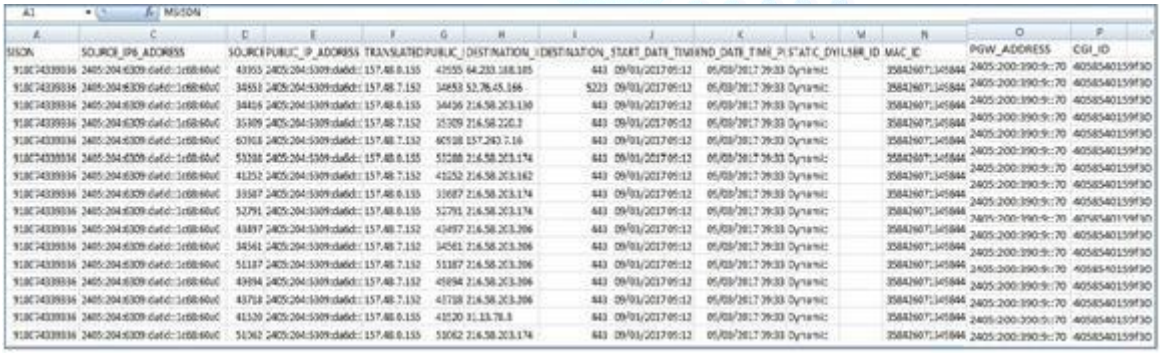


Figure 26 : Internet Sessions & Their Corresponding Locations in gprs cdr

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

Figure 27 : GPRS CDR Format

c) Cell ID Chart – Information about BTS Tower

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	K
1	Cell ID	Site Name	Town name	District	Latitude	Longitude	Azimuth	Address	MCC	MNC	LAC
2	10721	Achampet	Achampet (Gntr)	Guntur	16.62799	80.12449	80	Sy.NO. 123/1B, Chigurupadu Village, Achampet Mandal, Guntur	405	025	12017
3	10722	Achampet	Achampet (Gntr)	Guntur	16.62799	80.12449	220	Sy.NO. 123/1B, Chigurupadu Village, Achampet Mandal, Guntur	405	025	12017
4	10723	Achampet	Achampet (Gntr)	Guntur	16.62799	80.12449	320	Sy.NO. 123/1B, Chigurupadu Village, Achampet Mandal, Guntur	405	025	12017
5	10191	Dharmapuri	Dharmapuri	Karimnagar	18.9432	79.0901	0	Sri.Chukka Shankar S/o Pedda Narasaiah,Survey No.650/1, Dharmapuri Vill	405	025	17167
6	10192	Dharmapuri	Dharmapuri	Karimnagar	18.9432	79.0901	120	Sri.Chukka Shankar S/o Pedda Narasaiah,Survey No.650/1, Dharmapuri Vill	405	025	17167
7	10193	Dharmapuri	Dharmapuri	Karimnagar	18.9432	79.0901	280	Sri.Chukka Shankar S/o Pedda Narasaiah,Survey No.650/1, Dharmapuri Vill	405	025	17167
8	49951	Duvvur	Duvvur	Cuddapah	14.83991	78.65628	130	Sy.No. 651/B, Duvvur village & mandal, Kadapa dist.9908548943	405	025	17133
9	49952	Duvvur	Duvvur	Cuddapah	14.83991	78.65628	240	Sy.No. 651/B, Duvvur village & mandal, Kadapa dist.9908548943	405	025	17133
10	49953	Duvvur	Duvvur	Cuddapah	14.83991	78.65628	330	Sy.No. 651/B, Duvvur village & mandal, Kadapa dist.9908548943	405	025	17133
11	49371	IEEJ	Ieej	Mahbubnagar	16.0165	77.6654	30	SRI KATKESHWAR RICE MILL,IEEJA VILL+MANDAL,MAHBUB NAGAR DISTRICT	405	025	12023
12	49372	IEEJ	Ieej	Mahbubnagar	16.0165	77.6654	120	SRI KATKESHWAR RICE MILL,IEEJA VILL+MANDAL,MAHBUB NAGAR DISTRICT	405	025	12023
13	49373	IEEJ	Ieej	Mahbubnagar	16.0165	77.6654	250	SRI KATKESHWAR RICE MILL,IEEJA VILL+MANDAL,MAHBUB NAGAR DISTRICT	405	025	12023
14	49971	Indravelli	Indravelli	Adilabad	19.4879567	78.67749667	90	Atram Shivaji H.No. 6-30, Indravelli V & M, Adilabad 504 346, 9440747704	405	025	12013
15	49972	Indravelli	Indravelli	Adilabad	19.4879567	78.67749667	240	Atram Shivaji H.No. 6-30, Indravelli V & M, Adilabad 504 346, 9440747704	405	025	12013
16	49973	Indravelli	Indravelli	Adilabad	19.4879567	78.67749667	330	Atram Shivaji H.No. 6-30, Indravelli V & M, Adilabad 504 346, 9440747704	405	025	12013
17	12051	Jami	Jami	Vizianagaram	18.05266	83.25798	90	Sy No. 676/1A, Jami Village & Mandal, Vijayanagaram	405	025	12019
18	12052	Jami	Jami	Vizianagaram	18.05266	83.25798	180	Sy No. 676/1A, Jami Village & Mandal, Vijayanagaram	405	025	12019
19	12053	Jami	Jami	Vizianagaram	18.05266	83.25798	310	Sy No. 676/1A, Jami Village & Mandal, Vijayanagaram	405	025	12019

Figure2 8 : Cell ID Chart

d) 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

Figure 30 : Different Fields in Tower Dump CDR

e) 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

Figure 319 : Format of An IPDR

f) 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

Figure 32 : Different Fields of GPRS Dump

g) 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

Figure 33 : Format of SDR

h) IMEI Database

A collective database that cross-examine an 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.

i) 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

Figure 35 : Format of RAW CDR

j) SDR (Subscriber Data Record)/CAF (Customer Acquisition Form)

SDR are the record document collected and details filled by a consumer at the time of purchase of the SIM card. This document contains name, a passport sized photograph, location of purchase of SIM card and address details of the Subscriber as filled by him/her.

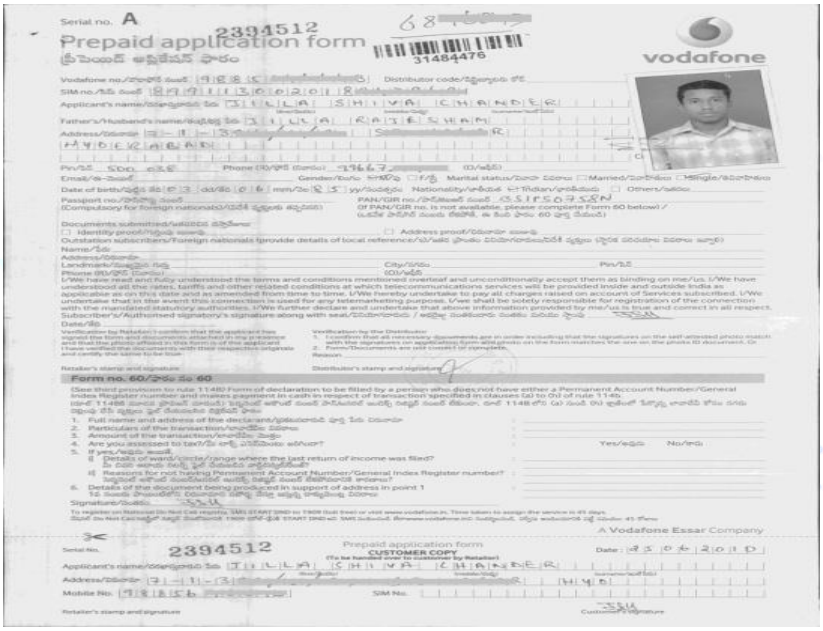


Figure 35 : Sample CAF

3.13. Different fields available in CDRs

- **Calling Number**
  - Calling number column in CDR provides details about those numbers which have made the calls (Outgoing calls)
- **Called Number**
  - Called number column in CDR provides details about those numbers which have received the calls (Incoming Calls)
  - Some MSPs provide this data under A_Number Column
  - Some MSPs provide this data under B_Number Column.
- **Date**
  - Date of Call
- **Time**
  - Time of Call
  - Sometime Data/Time is combined in Single column

- **Duration**
  - Duration in Seconds
- **Tower ID**
  - Mobile Tower from which the calls are made/received
- **Call Type**
  - Type of Call – Incoming call (INC), Outgoing Call (OUT), Incoming SMS (SMS_INC), Outgoing SMS (SMS_OUT)
  - Also known as Cell ID. The Symbols for type of call i.e. INC, OUT, SMS_INC and SMS_OUT might change with different MSPs
- **IMEI**
  - International Mobile Equipment Identity (IMEI) is a number to identify the Mobile phone device. Every Mobile phone device is having an unique IMEI. It is usually printed inside the phone. It can also be found by typing *#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 if a number is working on multiple SIMs (Number Cloning), the IMSI of each SIM will be different

- **Connection Type**
  - Prepaid (PRE) / Postpaid (PO/PP)
- **SMS Centre**
  - SMS centre is responsible for sending/receiving the text messages for a telephone network. When someone sends a SMS, it gets stored in SMS Centre from which it is delivered to the recipient.

3.14. Different formats of CDRs

There are many MSPs in India. It has been observed that the format and type of the file in which the MSPs provide the CDRs is not same. In fact every MSP might have its own format in which it provides the CDRs.

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

3.15. Junk numbers in CDR

There are some junk numbers found in the CDR.

- In the above mentioned CDR there are some calling numbers like –
  - 1446BC65381C0613
  - 549697C8>0BCC56
- These numbers are nothing but some automatically generated SMSs from various entities like Companies, promotional SMS, Alerts etc
- To find details on those seemingly gibberish numbers, you may contact nodal officer of respective service provider and request for additional details regarding the same.

3.16. Misuse of CDR

- CDR can easily be used to harass and inflict privacy violation
- Many Private Detectives ask for help from police to retrieve CDRs in name of character verification or background verification resulting in fake cases
- Employees of Telecom Companies that have access to customer and billing database

3.17. 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

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.

Creating a Pivot Table

After the CDR to be analyzed is converted into MS Excel or CSV format, a pivot table needs to be created. Pivot table is a data analysis and summarization tool found in MS Excel. In order to analyze the data, a pivot table is created consisting of data which is to be analyzed.

1. Arrange the data in proper order (ascending) based on the time,date and in serial number and make sure the 1st column (or) the "Calling Number" or "A party" consists of only the number whose CDR we are analysing. The "Called Number" or "B Party" consists of all other numbers.
2. Now goto **Insert** tab and click on pivot table. We get a prompt showing "create pivot table". Click OK. It will create a new pivot table in a new worksheet.
3. i) Drag the "Called No." field into the left most bottom box named as row labels.
   ii) Drag the "CallType" field into the right most upper box named as column labels.
   iii) Drag the "Calling No." field into 'Σ' (summation) Values column and click on it & select "value field settings" and select 'count' and say OK.
4. Select the grand total column until the last row, go to **Options** and click sort largest to smallest. Here we will get the number to whom the accused has called maximum number of times.

3.18. Analysis of CDR

The CDR may consist of hundreds, thousands or even lakhs of call records. Analysis of a CDR is compulsory process to get useful information out of it. CDR Analysis is usually performed to get following information (but not limited to) from a CDR[6] -

1. Top few numbers on which to which a mobile number user is calling frequently(Out going calls)
2. Top few numbers from which a mobile number user is getting calls frequently (incoming calls)
3. Top few maximum duration calls
4. 1-5 seconds calls
5. Night location of mobile number user
6. How many SIM cards mobile number user has changed

[6]The information required from CDR might vary from case to case

7. How many Mobile sets mobile number user has used
8. Calls made during a particular time period (e.g. 10 AM – 6 PM), etc.

3.18.1. Vlookup

- Vlookup is a function in MS Excel.It is used to work with more than one excel file.In CDR Analysis, it is generally used to map the CELL/Tower IDs in CDR to Tower Locations in another file – Example in next slide.
- It is a great tool to look for similar values in another excel sheets/workbook**Vlookup function can be used to map Cell ID in one workbook to Site name in another**

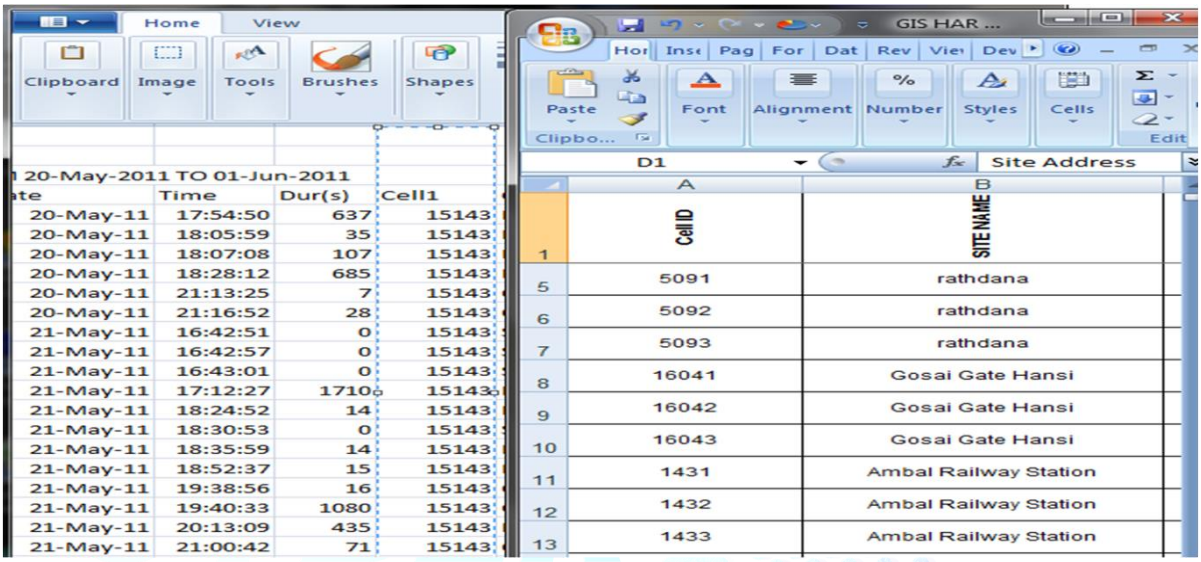


Figure 36: Vlookup

Creating a Pivot Table

After the CDR to be analyzed is converted into MS Excel or CSV format, a pivot table needs to be created. Pivot table is a data analysis and summarization tool found in MS Excel. In order to analyze the data, a pivot table consisting of all ‘to be analyzed data’ is created.

Pivot table

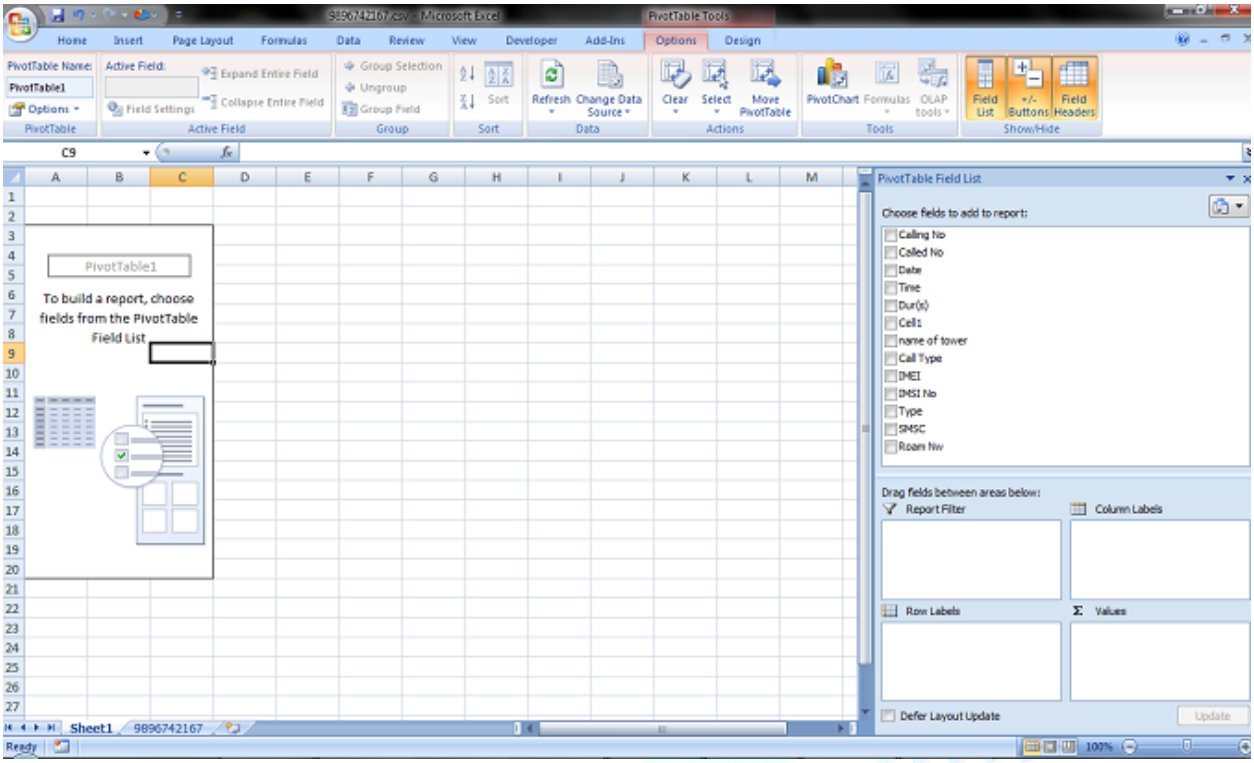


Figure 37 pviot table

3.18.2. Analysis using Pivot Table

As discussed above, CDR analysis using pivot table provides us various information which are useful in solving a case. Let's see how CDR can be analyzed using Pivot table to get above discussed details –

- Top few numbers on which a mobile number user is calling frequently (outgoing calls)

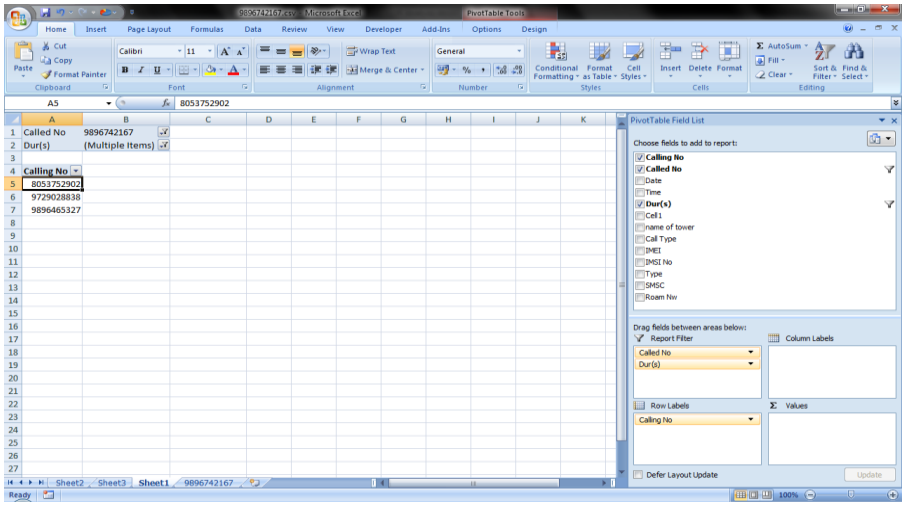


Figure 38 : Top Incoming Calls

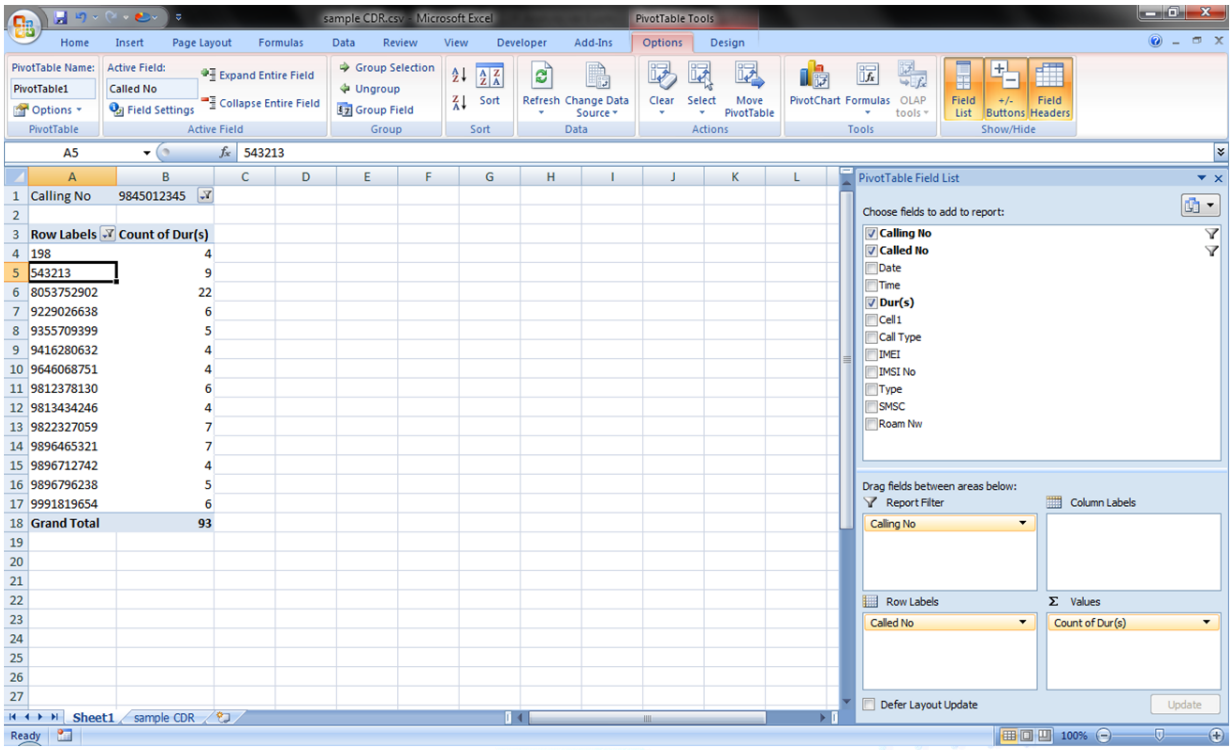


Figure 39 : Outgoing Call Analysis Using Pivot Table

- Top few numbers from which a mobile number user is getting calls frequently (incoming calls)

- Top few maximum duration calls

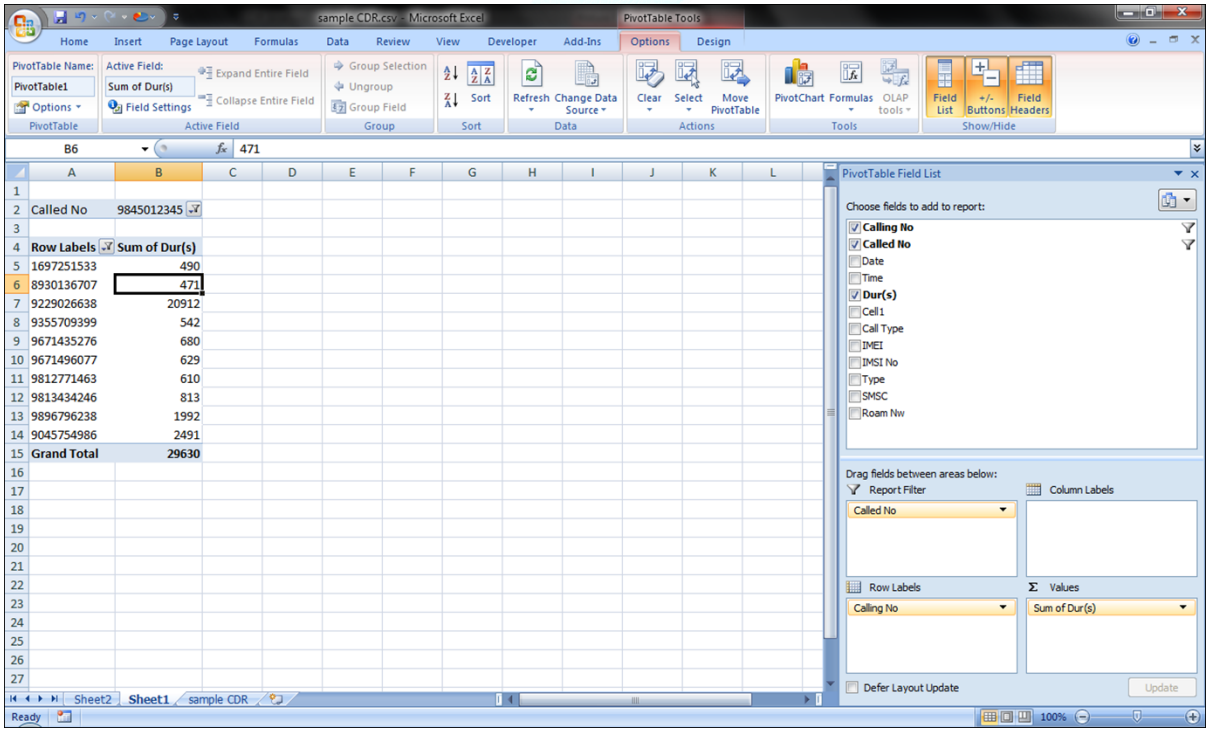


Figure 40 : Maximum Duration Call

- Night location of a mobile number user

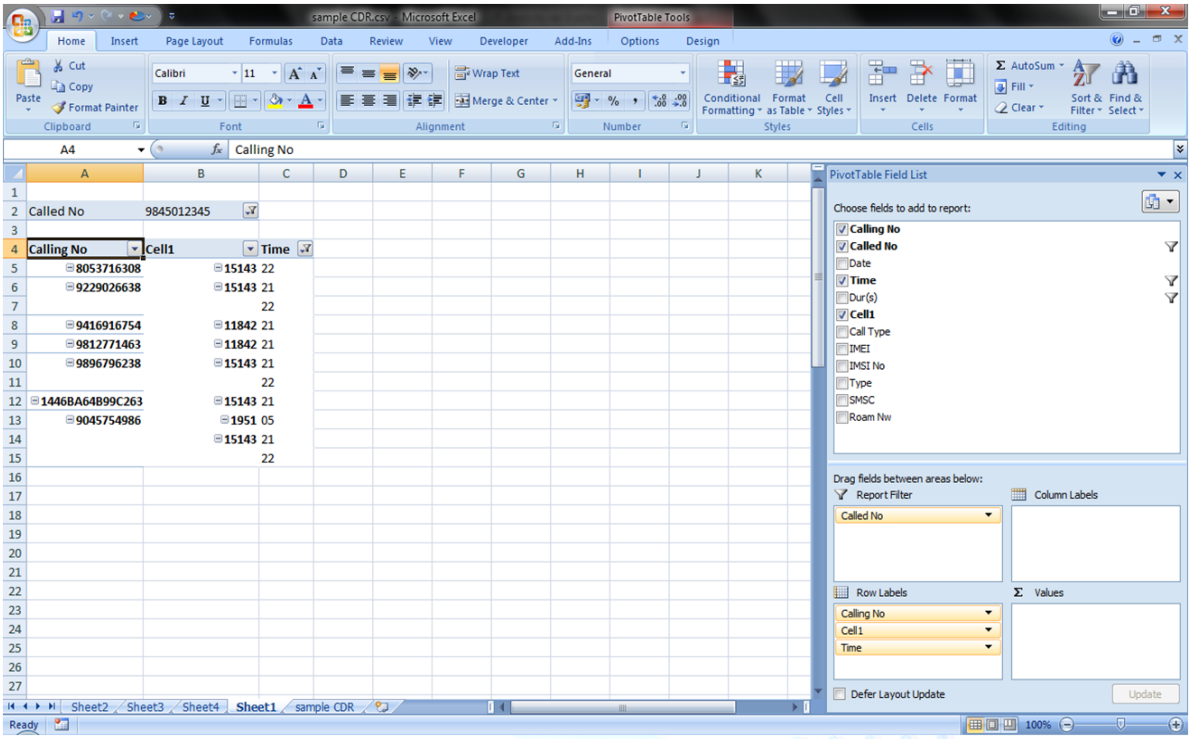


Figure 41 : Night Location of a User

- How many SIM cards a mobile number user has changed?

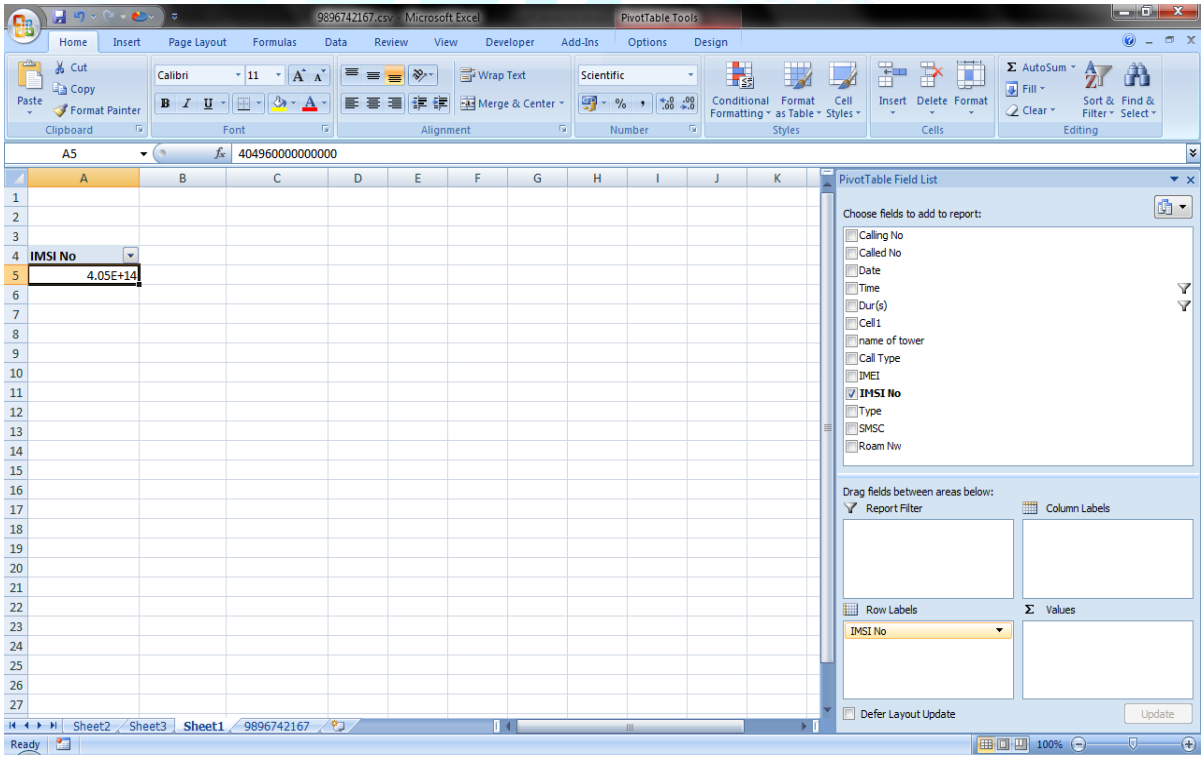


Figure 42 : Number of Sim Cards Used

- Calls made during a particular period (such as 9PM to 06AM)

Step 1: Display the time by dragging Time into Row Label

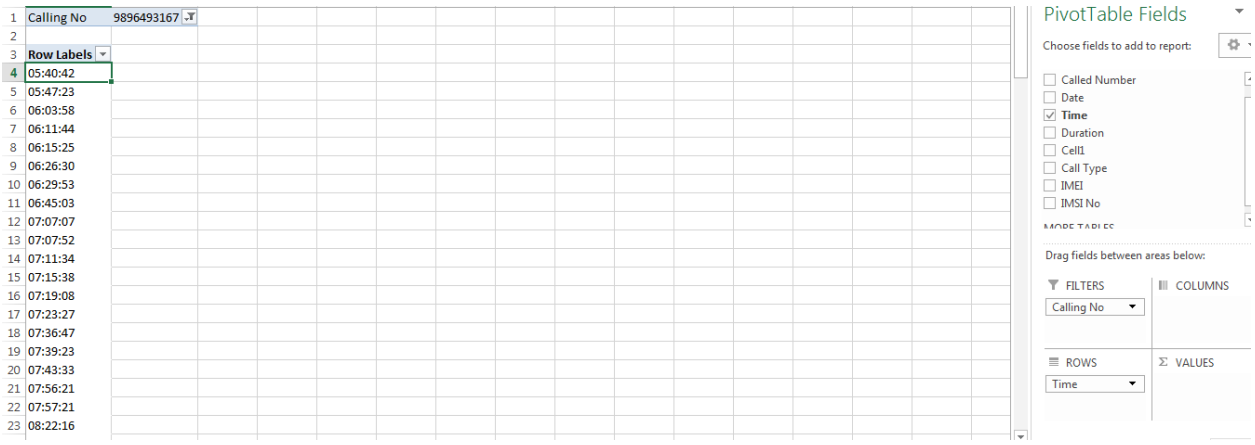


Figure 43 : step -1

Step 2: 'Group the time' into hours

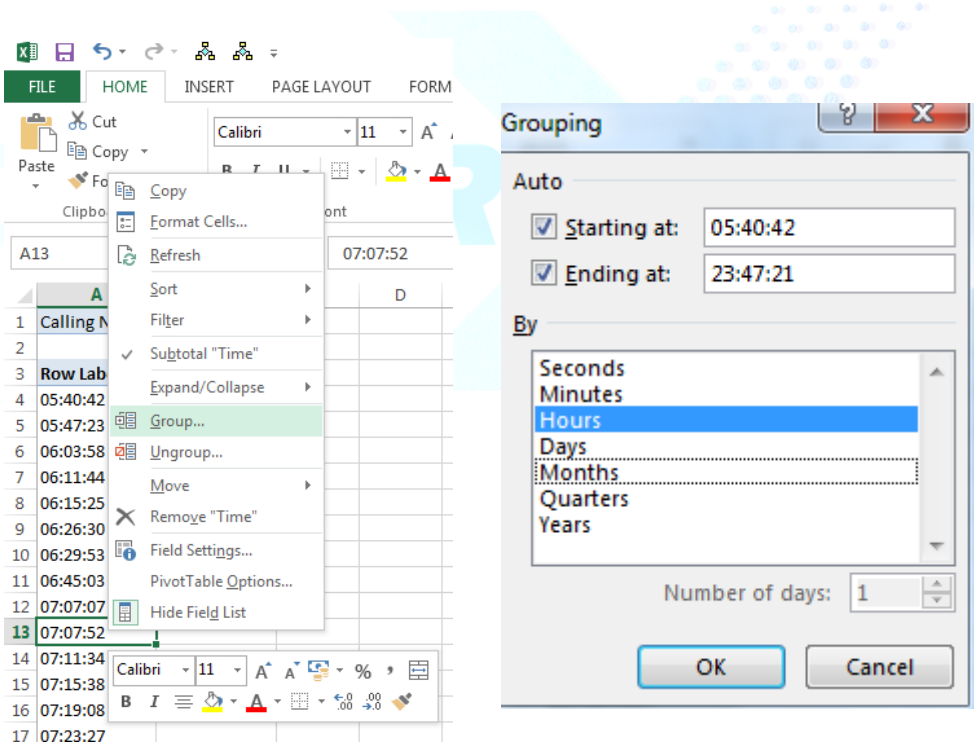


Figure 44 : Step - 2

Step 3:
Drag Time into Filters and select the hours from 21hrs (i.e. 9PM) to 05hrs (i.e. till 5:59:55 AM)

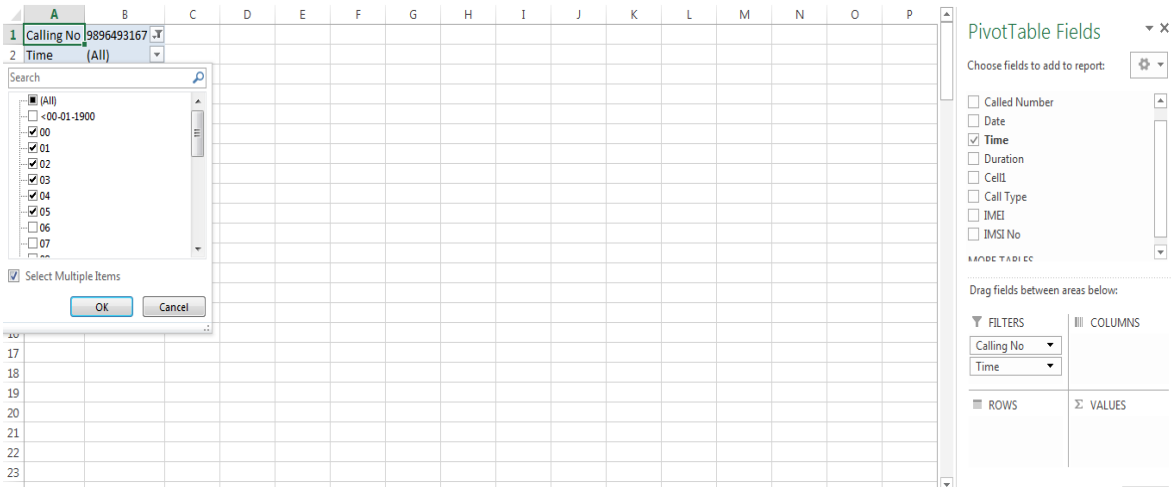


Figure 45 : Step - 3

Step 4: Lastly, drag the called number to know to whom the mobile number user called during a particular period (9PM to 06AM in this case)

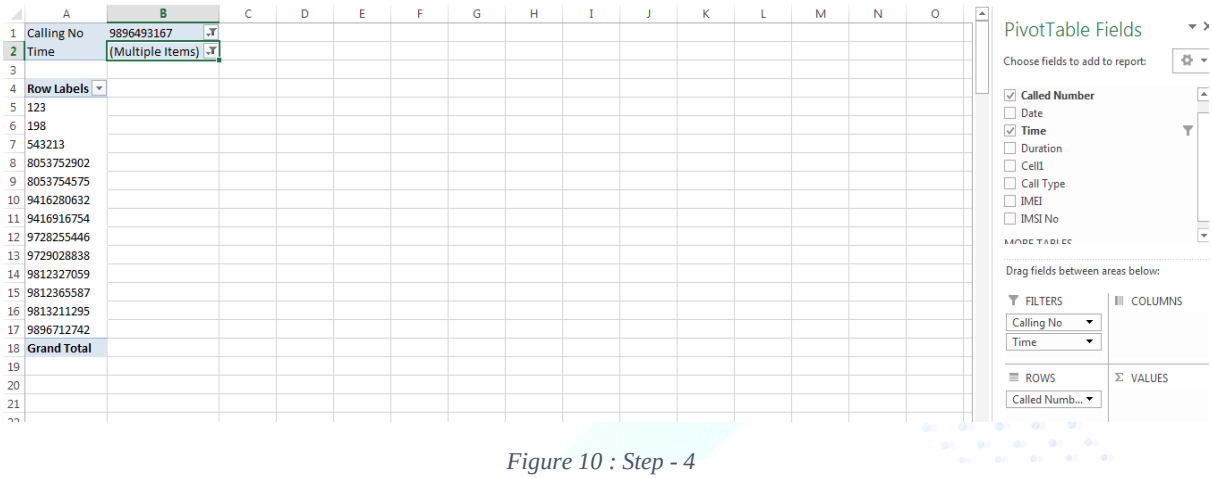


Figure 10 : Step - 4

- Calls made during a particular time period (e.g. 10 AM – 6 PM)

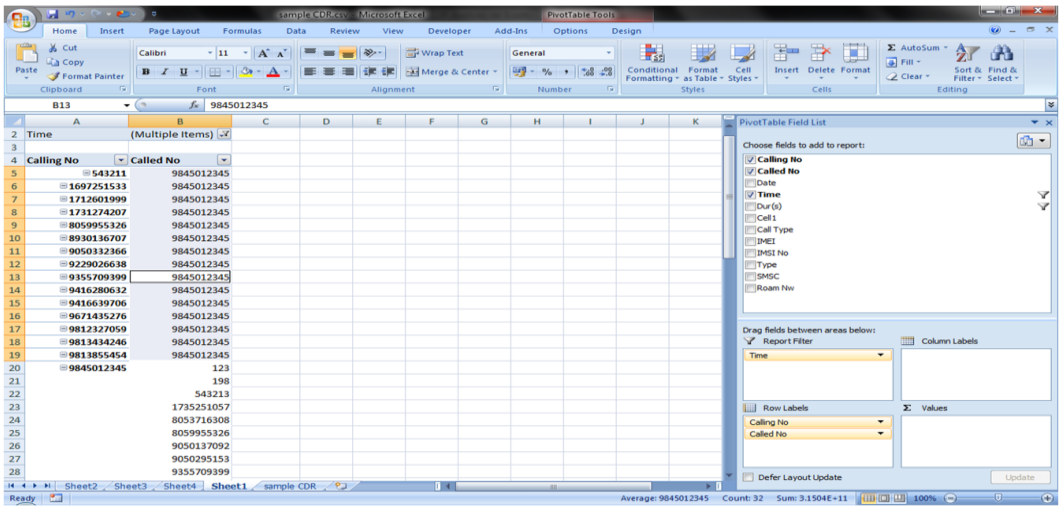


Figure 47 : Outgoing Calls between time period

8. Calls received during a particular period (such as 9PM to 06AM)

Follow the same procedure as what is described in Query 9, except the last step where instead of calling number, called number should be put into filters and called number should be put into the row label.

Figure 48 : incoming Calls between time period

- Locations from where the calls were made during a particular period

Follow the same procedure as what is described in Query 9, except the last step where instead of called number, cell ID or Tower ID or CELL1 in this case would be dragged to the row label.

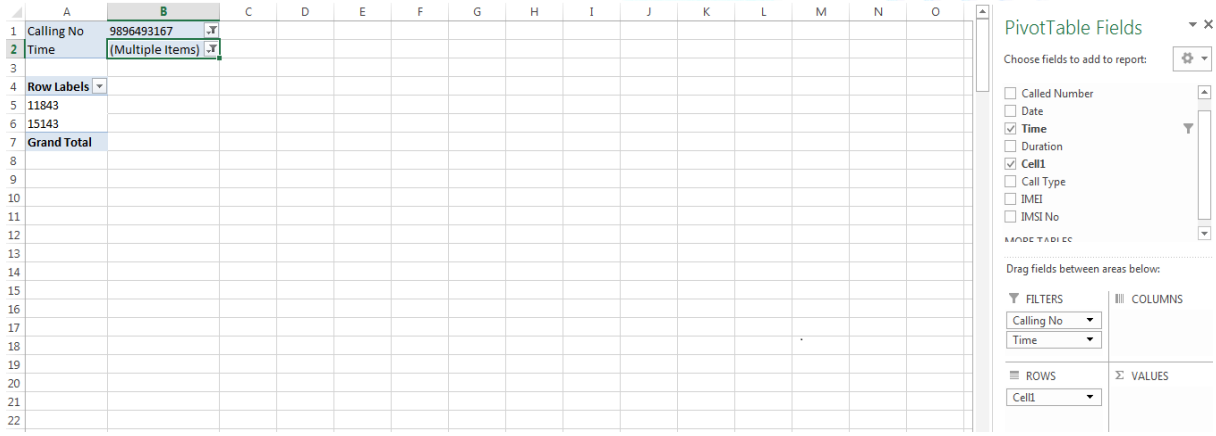


Figure 49 : Call Location between a time period (outgoing calls)

- Locations from where the calls were received during a particular period

Follow the same procedure as what is described in Query 11, except the last step where instead of calling number, called number would be dragged to the filter.

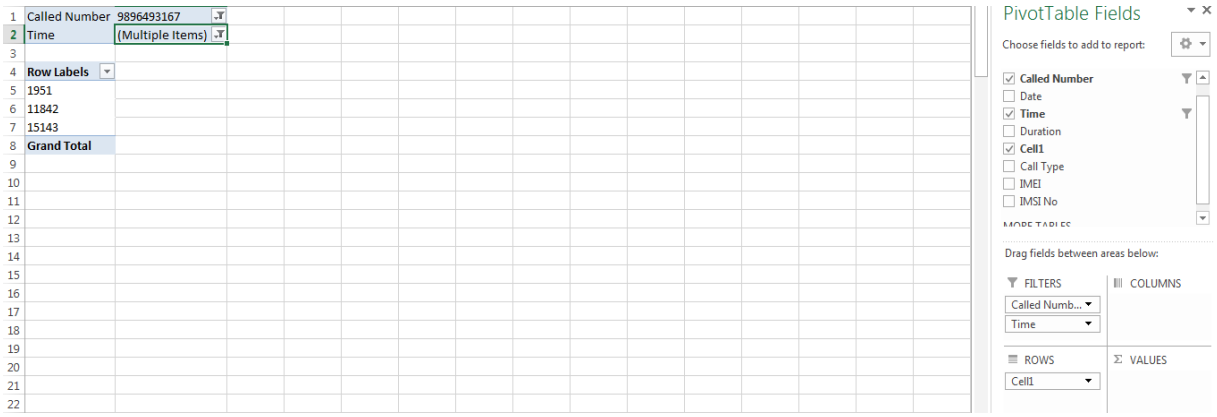


Figure 50 : Location of Call between a time period (Received Calls)

- Numbers from whom SMSs have been received

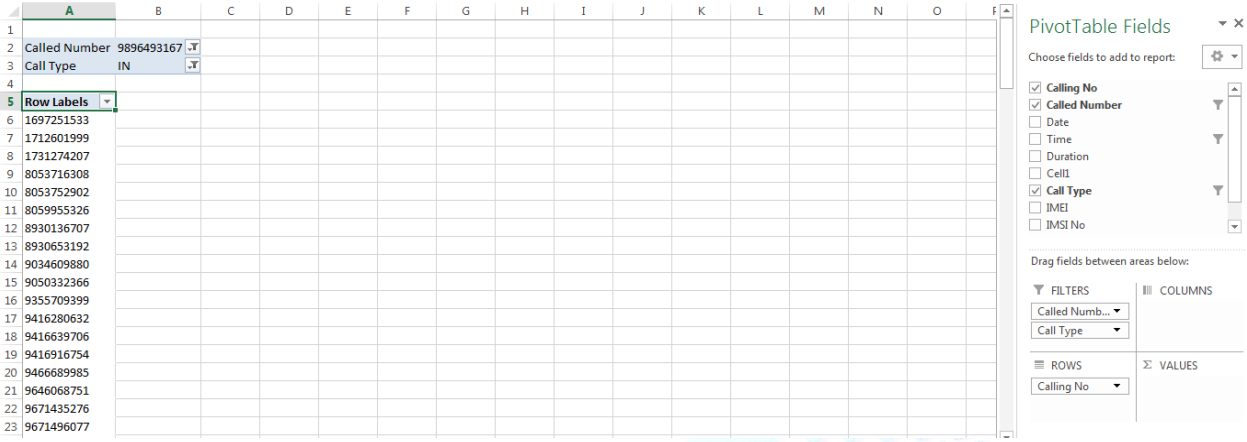


Figure 51 : SMS Numbers

IF we want to check about how many SMSs each number as sent, then we should drag any field into the 'Values' and take a count of it.

Figure 52 frequent location

- Numbers to whom SMSes have been sent

Just exchange the calling number and called number in query 13, and select call type as 'SMO' i.e. SMS Outgoing.

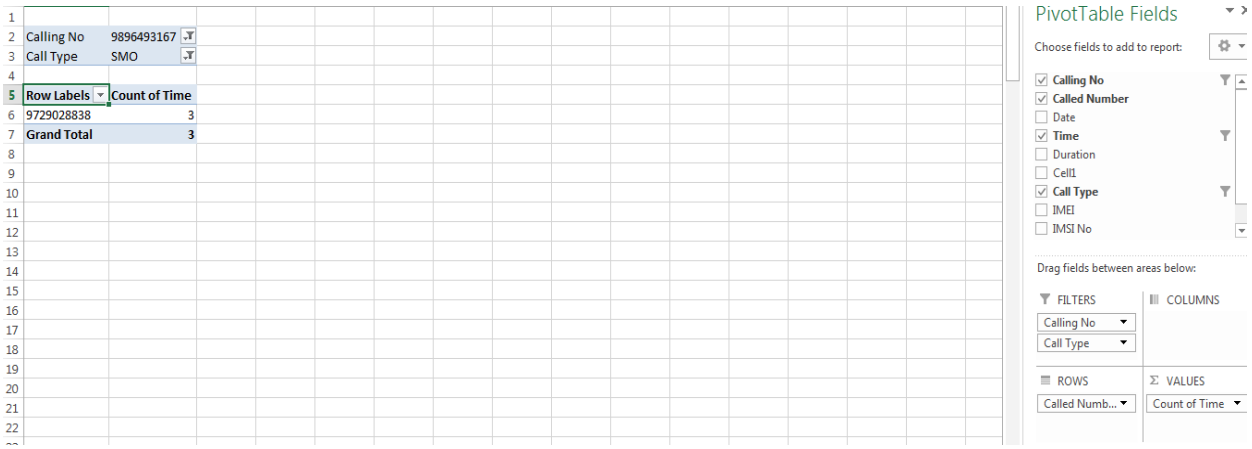


Figure 11 : Sent SMS Numbers

- Numbers from whom maximum SMSs have been received

Follow the procedure detailed in Query 13. Then, right click on any of the number in the 'count of Time' column and select Sort -> Largest to Smallest

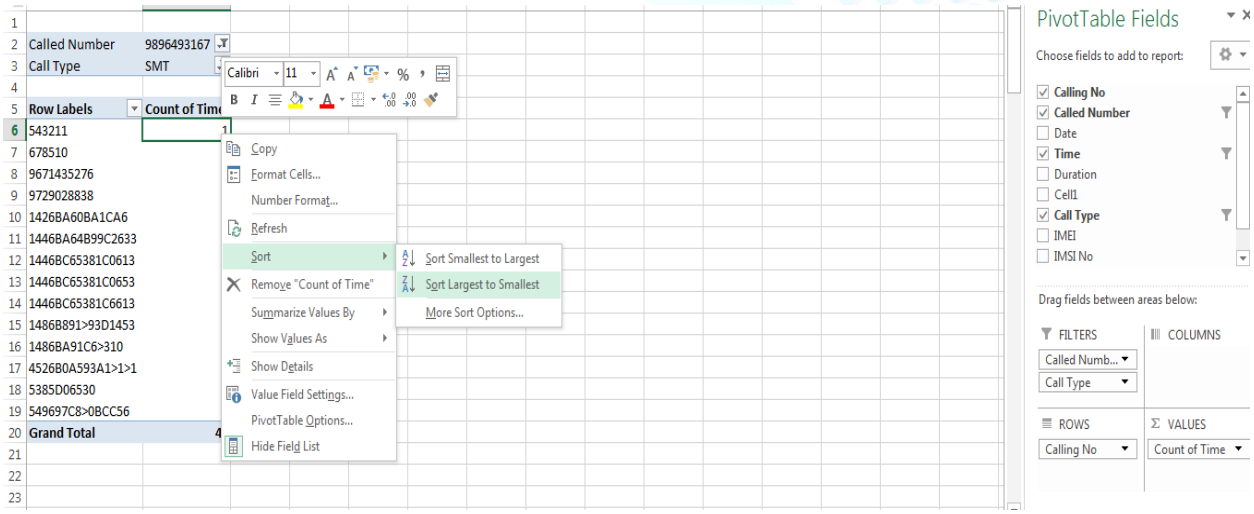
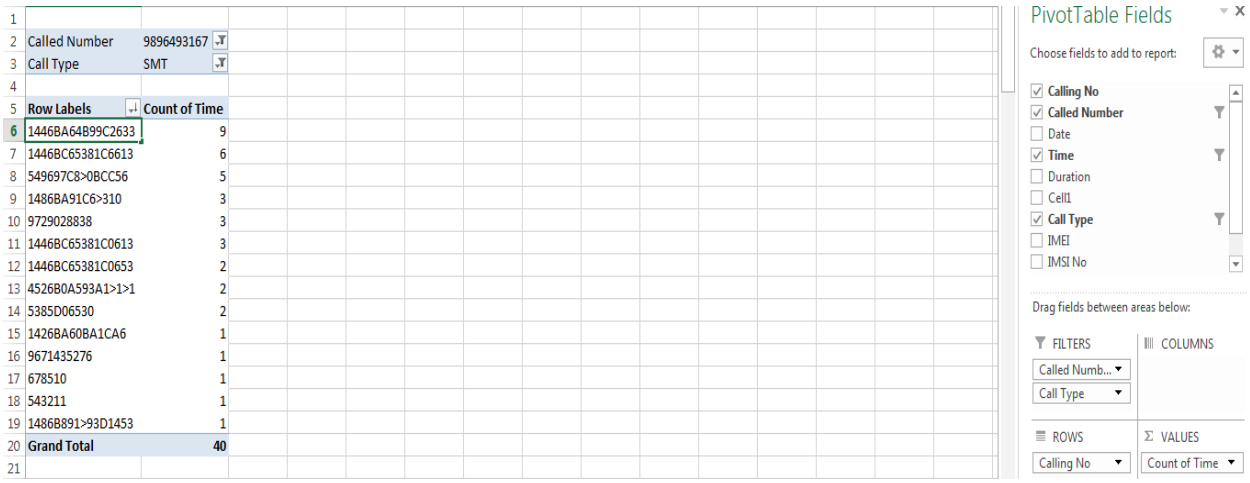


Figure 54 : Number from which maximum SMS are received

As we can see below, Total 40 SMSs have been received, out of which Maximum SMSs have been received from 1446BA64B99C2633 which appears to be company SMS (which we received once we shop online or reserve our tickets and so on)



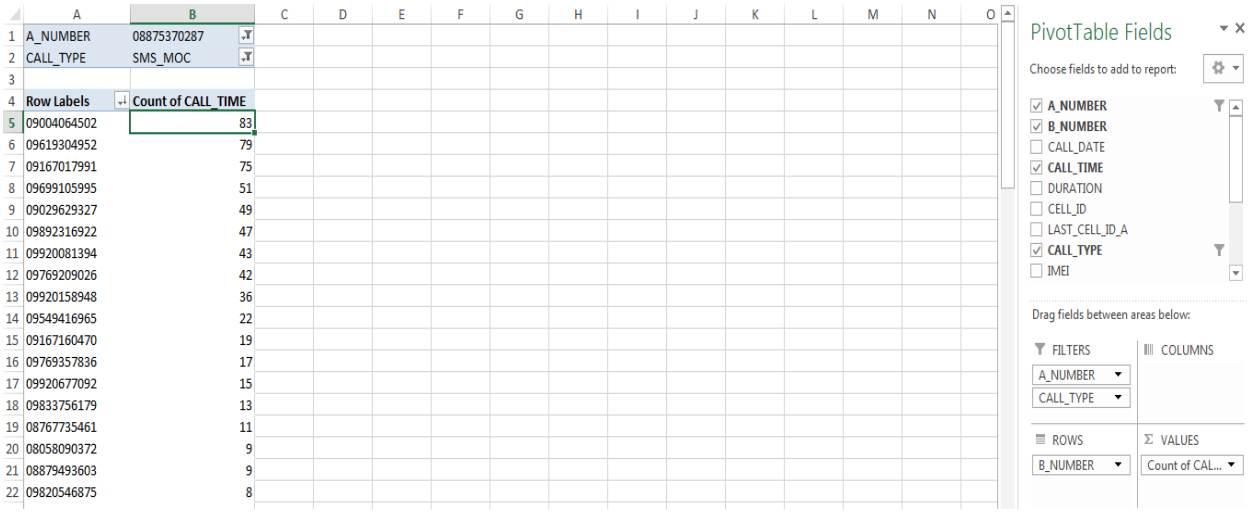
Called Number	9896493167
Call Type	SMT

Row Labels	Count of Time
1446BA64B99C2633	9
1446BC65381C6613	6
549697C8>0BCC56	5
1486BA91C6>310	3
9729028838	3
1446BC65381C0613	3
1446BC65381C0653	2
4526B0A593A1>1>1	2
5385D06530	2
1426BA60BA1CA6	1
9671435276	1
678510	1
543211	1
1486B891>93D1453	1
Grand Total	40

Figure 12 Maximum SMS received

- Numbers to whom maximum SMSs have been sent.

Follow the same procedure as query 14, and right click on any of the values in Count of Time column and select Sort -> largest to smallest



A_NUMBER	08875370287
CALL_TYPE	SMS_MOC

Row Labels	Count of CALL_TIME
09004064502	83
09619304952	79
09167017991	75
09699105995	51
09029629327	49
09892316922	47
09920081394	43
09769209026	42
09920158948	36
09549416965	22
09167160470	19
09769357836	17
09920677092	15
09833756179	13
08767735461	11
08058090372	9
08879493603	9
09820546875	8

Figure 56 : Number at Which Maximum SMS has Sent

- All locations visited by the mobile number user- It's a simple query, where we have just drag the CELL ID field into Row Label.

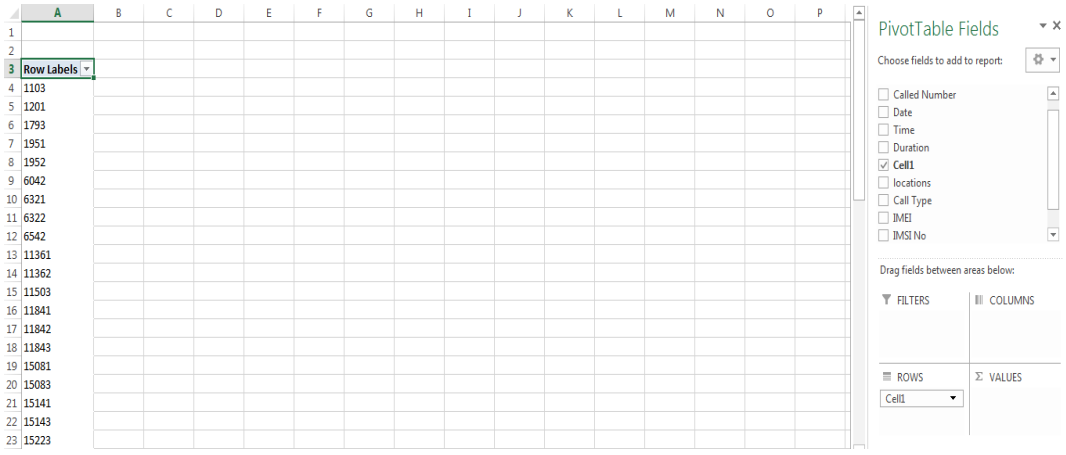


Figure 57 : Locations Visited by Mobile User

However, if we also want the places where these cell IDs are placed, we should drag the location part into Row label and format it in Table format.

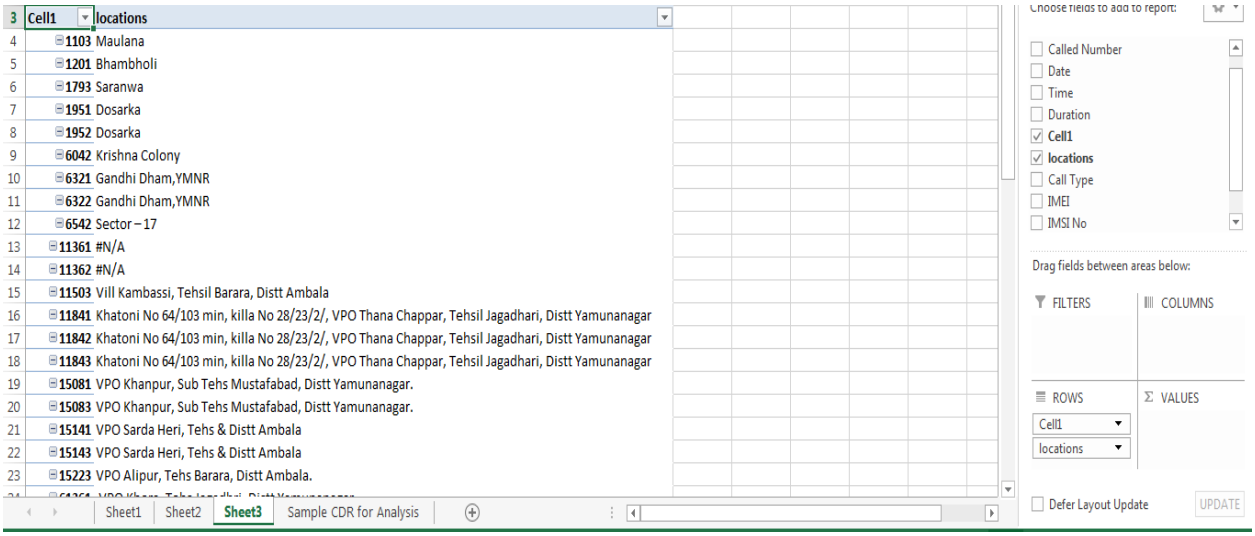
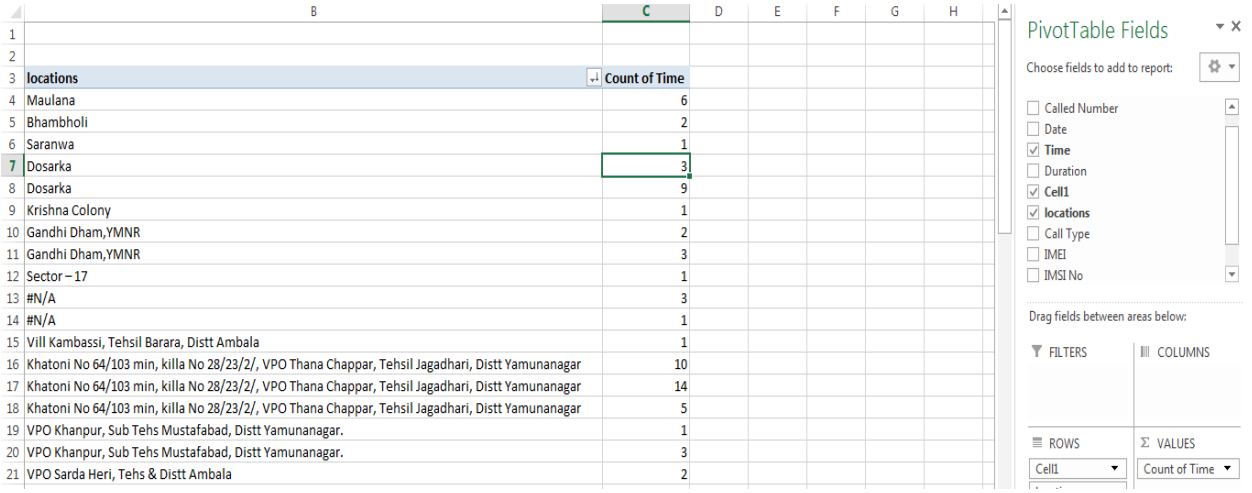


Figure 58: Cell to location

PS: Please refer to the vlookup description to fetch the locations of the Tower IDs if they are not already available in the CDR.

- Locations most frequently visited

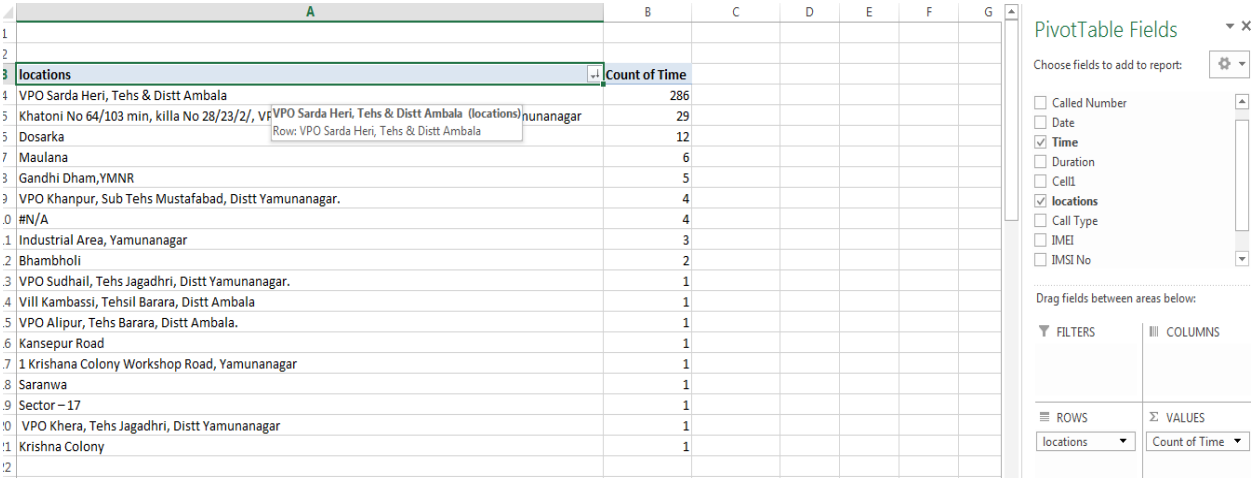
Follow the same procedure as in query 17. In addition, drag time field into ‘values’ and select count of time.



locations	Count of Time
Maulana	6
Bhambholi	2
Saranwa	1
Dosarka	3
Dosarka	9
Krishna Colony	1
Gandhi Dham,YMNR	2
Gandhi Dham,YMNR	3
Sector – 17	1
#N/A	3
#N/A	1
Vill Kambassi, Tehsil Barara, Distt Ambala	1
Khatoni No 64/103 min, killa No 28/23/2/, VPO Thana Chappar, Tehsil Jagadhari, Distt Yamunanagar	10
Khatoni No 64/103 min, killa No 28/23/2/, VPO Thana Chappar, Tehsil Jagadhari, Distt Yamunanagar	14
Khatoni No 64/103 min, killa No 28/23/2/, VPO Thana Chappar, Tehsil Jagadhari, Distt Yamunanagar	5
VPO Khanpur, Sub Tehs Mustafabad, Distt Yamunanagar.	1
VPO Khanpur, Sub Tehs Mustafabad, Distt Yamunanagar.	3
VPO Sarda Heri, Tehs & Distt Ambala	2

Figure 59 : Most Frequent Visited Locations

Then, sort the values in Count of Time column from largest to smallest (as demonstrated earlier)



locations	Count of Time
VPO Sarda Heri, Tehs & Distt Ambala	286
Khatoni No 64/103 min, killa No 28/23/2/, VPO Sarda Heri, Tehs & Distt Ambala (locations)	29
Dosarka	12
Maulana	6
Gandhi Dham,YMNR	5
VPO Khanpur, Sub Tehs Mustafabad, Distt Yamunanagar.	4
#N/A	4
Industrial Area, Yamunanagar	3
Bhambholi	2
VPO Sudhail, Tehs Jagadhri, Distt Yamunanagar.	1
Vill Kambassi, Tehsil Barara, Distt Ambala	1
VPO Alipur, Tehs Barara, Distt Ambala.	1
Kansepur Road	1
1 Krishana Colony Workshop Road, Yamunanagar	1
Saranwa	1
Sector – 17	1
VPO Khera, Tehs Jagadhri, Distt Yamunanagar	1
Krishna Colony	1

Figure 60: frequent address

Here we can see that VPO SardaHeri, Tehs & District Ambala seems to be the most frequently visited location of the mobile number user. It also conveys that the mobile number user might be staying at this place.

- Locations visited during a particular period

Same as Query 11. However, just change the time according to the requirement.

- Route chart for a day

Route chart is extremely helpful in the investigations. Route chart of the mobile number user for a day would invariably inform about his/her whereabouts throughout the day.

In order to find the route chart for one day, we can sort out the CELL IDs or Locations according to the time of any particular day (for e.g. 25 may 2011 in this CDR).

STEPS

1. Create a filter on Date field

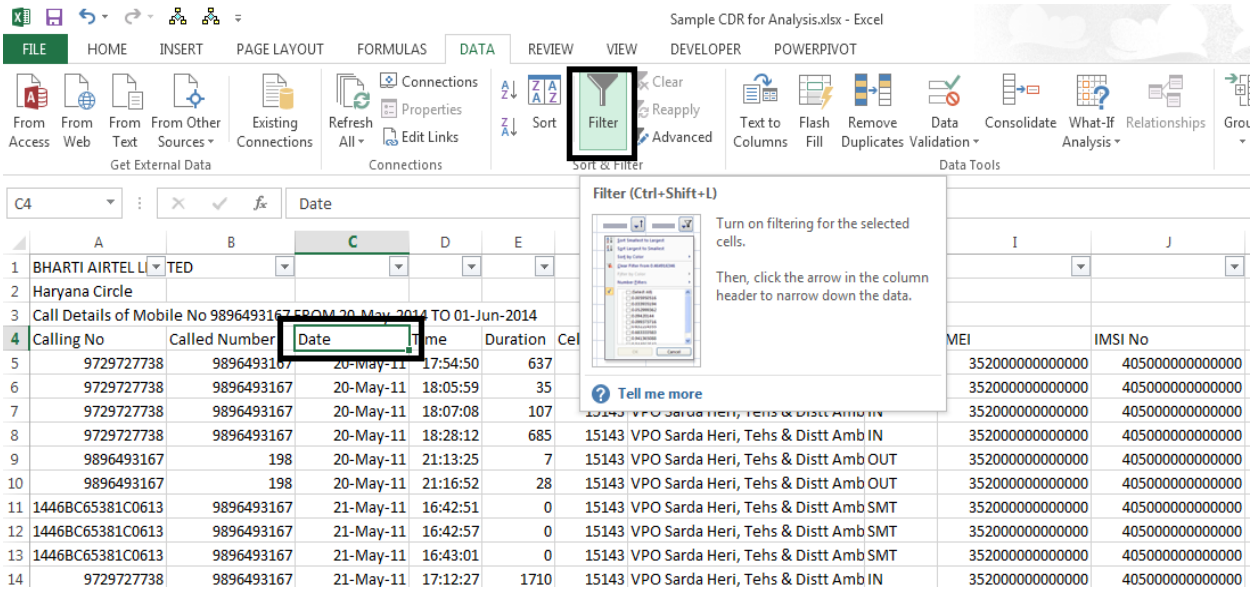


Figure 61: Date filter

2. Select 25 may

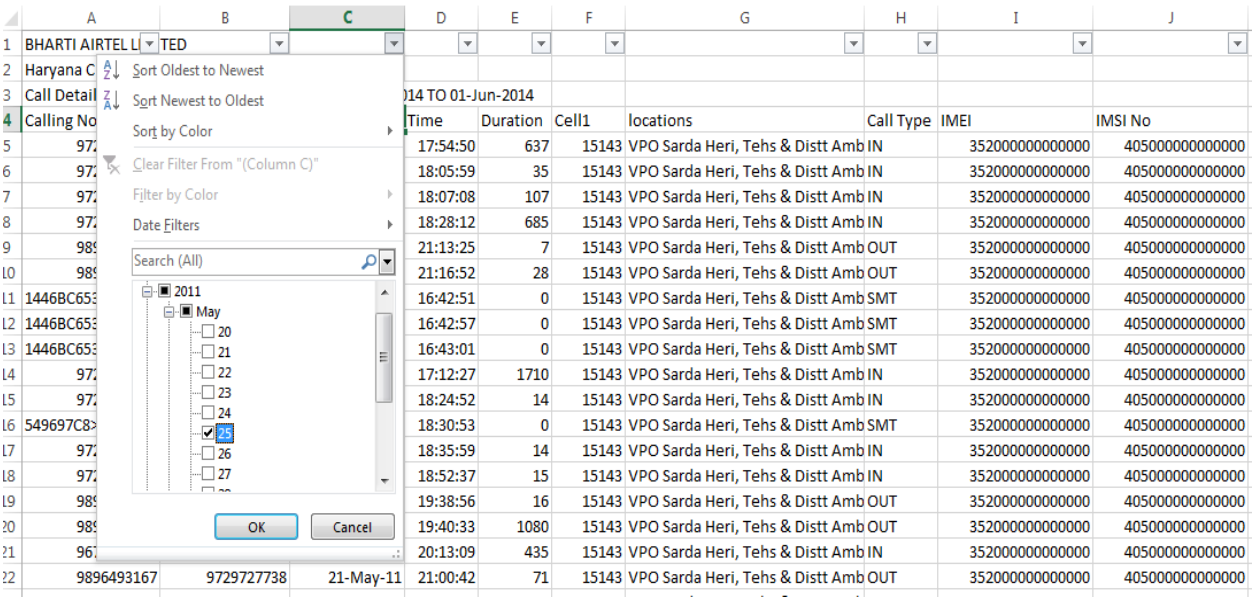


Figure 62: Filtering date

It is now seen that only those calls which were made or received dated 25th may 2011 are listed in time sorted manner.

	A	B	C	D	E	F	G	H	I	J
1	BHARTI AIRTEL LI	TED								
2	Haryana Circle									
3	Call Details of Mobile No 9896493167 FROM 20-May-2014 TO 01-Jun-2014									
4	Calling No	Called Number	Date	Time	Duration	Cell1	locations	Call Type	IMEI	IMSI No
182	8053752902	9896493167	25-May-11	05:59:39	133	1951	Dosarka	IN	352000000000000	405000000000000
183	9896663742	9896493167	25-May-11	07:10:53	27	1103	Maulana	IN	352000000000000	405000000000000
184	9896493167	9812378130	25-May-11	10:05:26	67	1103	Maulana	OUT	352000000000000	405000000000000
185	9896796238	9896493167	25-May-11	10:09:40	99	1103	Maulana	IN	352000000000000	405000000000000
186	9896493167	9991087188	25-May-11	10:32:44	36	1103	Maulana	OUT	352000000000000	405000000000000
187	9896493167	9813105486	25-May-11	10:36:38	229	1103	Maulana	OUT	352000000000000	405000000000000
188	9896493167	9813105486	25-May-11	10:42:08	298	1103	Maulana	OUT	352000000000000	405000000000000
189	8053752902	9896493167	25-May-11	12:10:10	128	15141	VPO Sarda Heri, Tehs & Distt Amb	IN	352000000000000	405000000000000
190	9671435276	9896493167	25-May-11	12:15:51	0	1793	Saranwa	SMT	352000000000000	405000000000000
191	1712601999	9896493167	25-May-11	12:36:47	75	15143	VPO Sarda Heri, Tehs & Distt Amb	IN	352000000000000	405000000000000
192	9896493167	8053752902	25-May-11	13:35:23	61	15143	VPO Sarda Heri, Tehs & Distt Amb	OUT	352000000000000	405000000000000
193	9416639706	9896493167	25-May-11	13:37:15	64	15143	VPO Sarda Heri, Tehs & Distt Amb	IN	352000000000000	405000000000000
194	9813434246	9896493167	25-May-11	14:04:31	81	15143	VPO Sarda Heri, Tehs & Distt Amb	IN	352000000000000	405000000000000
195	1731274207	9896493167	25-May-11	14:16:52	31	15141	VPO Sarda Heri, Tehs & Distt Amb	IN	352000000000000	405000000000000
196	9813434246	9896493167	25-May-11	14:42:27	41	15223	VPO Alipur, Tehs Barara, Distt Am	IN	352000000000000	405000000000000
197	9896493167	8053752902	25-May-11	14:55:40	90	1951	Dosarka	OUT	352000000000000	405000000000000
198	9896493167	9812378130	25-May-11	15:48:21	44	6321	Gandhi Dham,YMNR	OUT	352000000000000	405000000000000
199	9896493167	8053752902	25-May-11	15:50:14	24	6322	Gandhi Dham,YMNR	OUT	352000000000000	405000000000000
200	8053752902	9896493167	25-May-11	15:51:03	64	6322	Gandhi Dham,YMNR	IN	352000000000000	405000000000000

Figure 63: Date Filter output

- Route chart for the month

STEPS

1. Create a pivot table and drag the date into row label

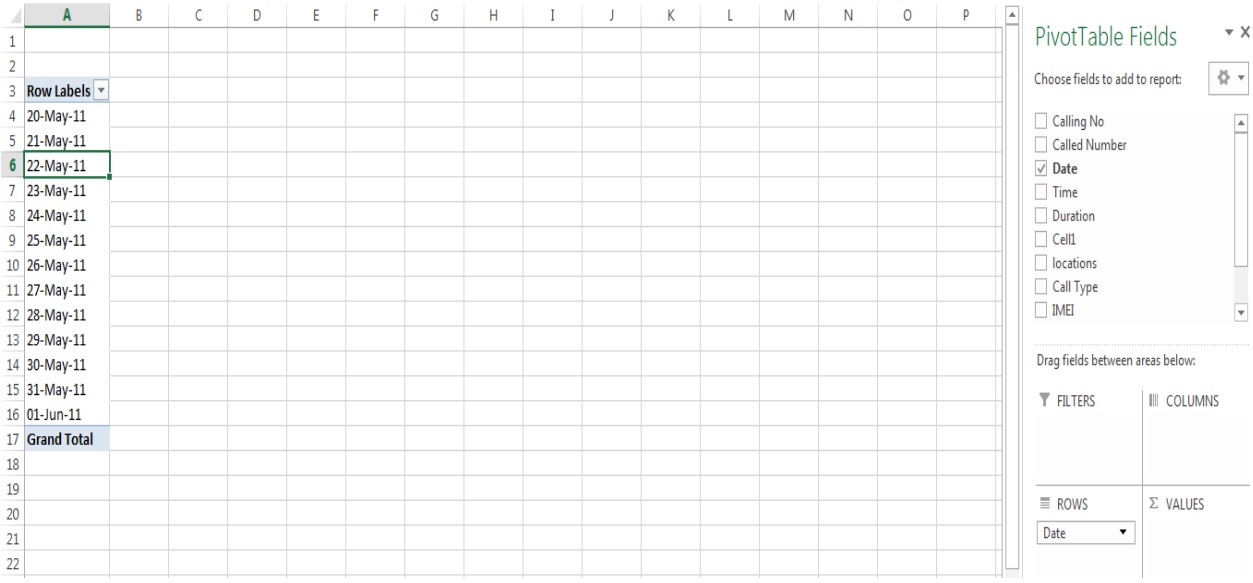


Figure 64: Maximum activity

2. Group the dates into month

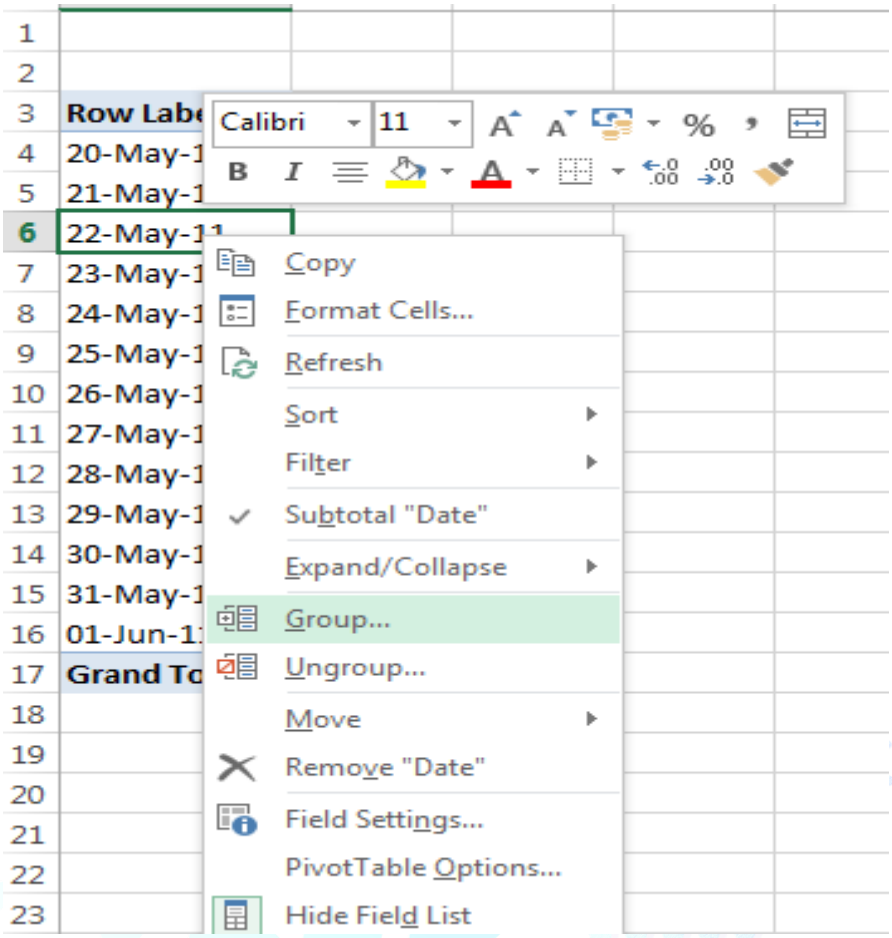


Figure 65: Grouping date

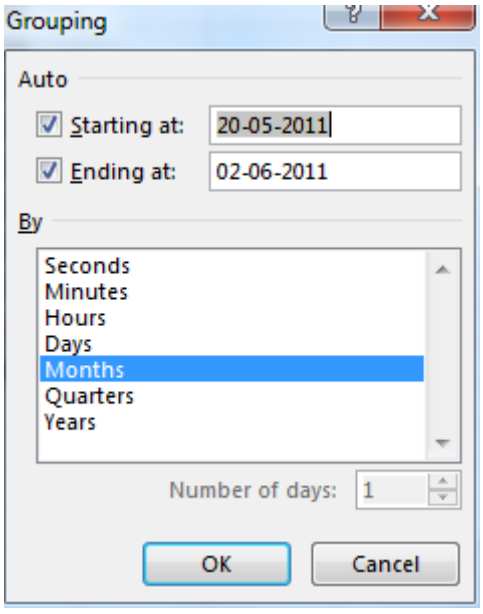


Figure 66: Monthly grouping of dates

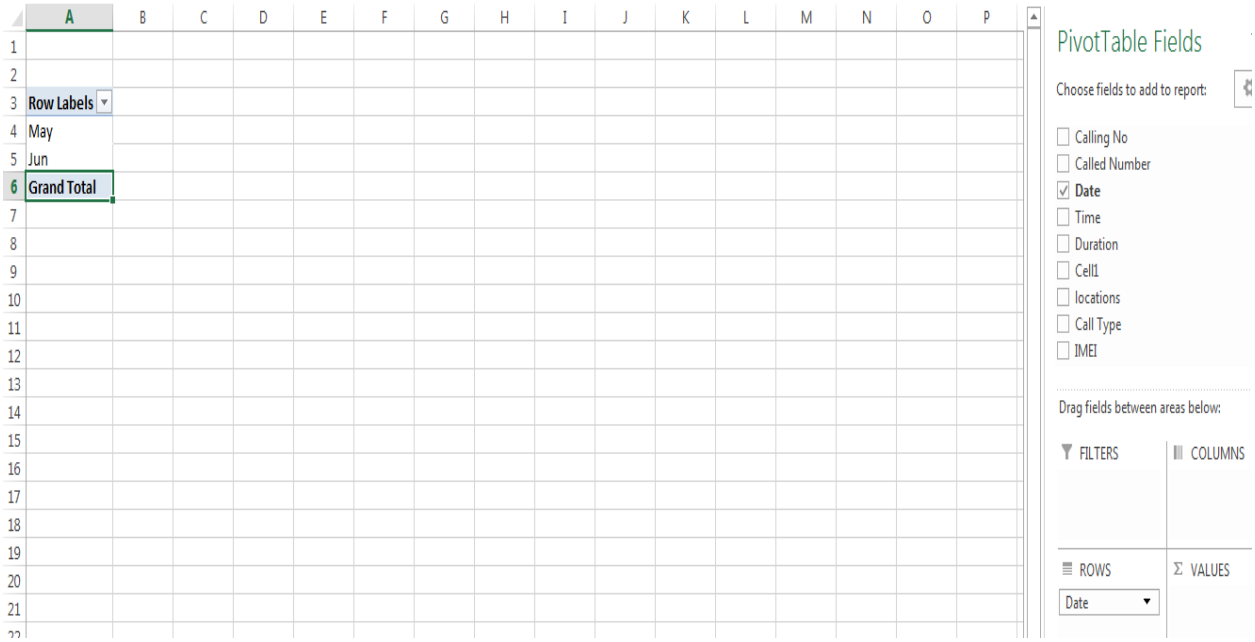


Figure 67: Date in pivot table

3. Count the number of calls made/received during a particular month (say May in this CDR)

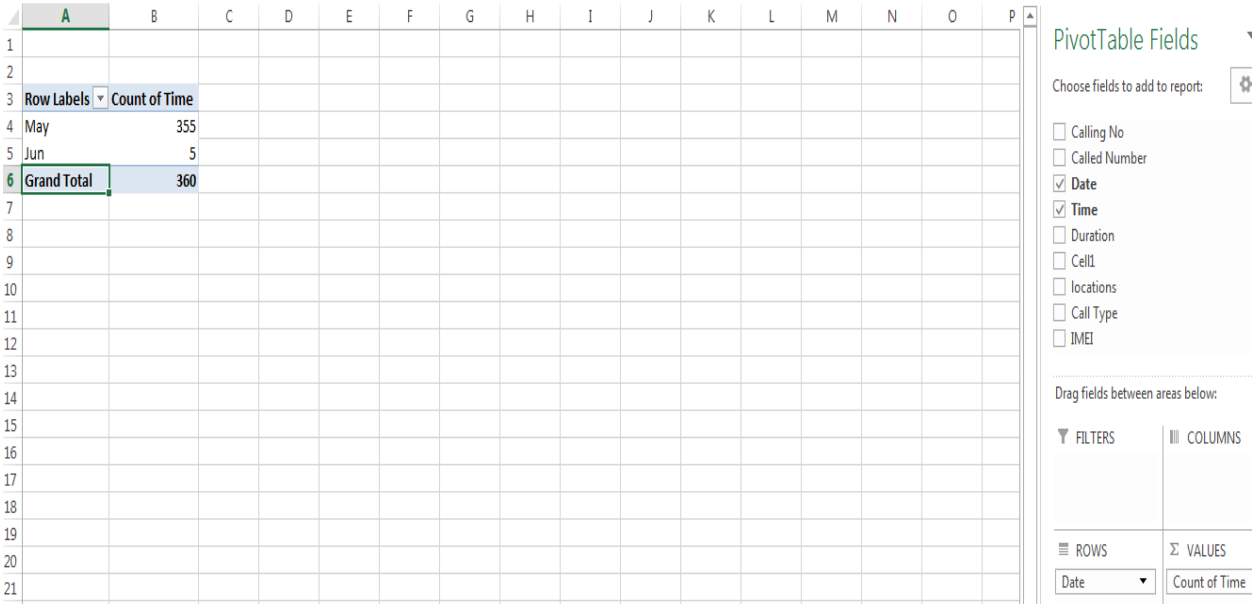


Figure 68: Pivot Filtering

4. Right click on the value against Month of May (i.e. 355) and select ‘show details’

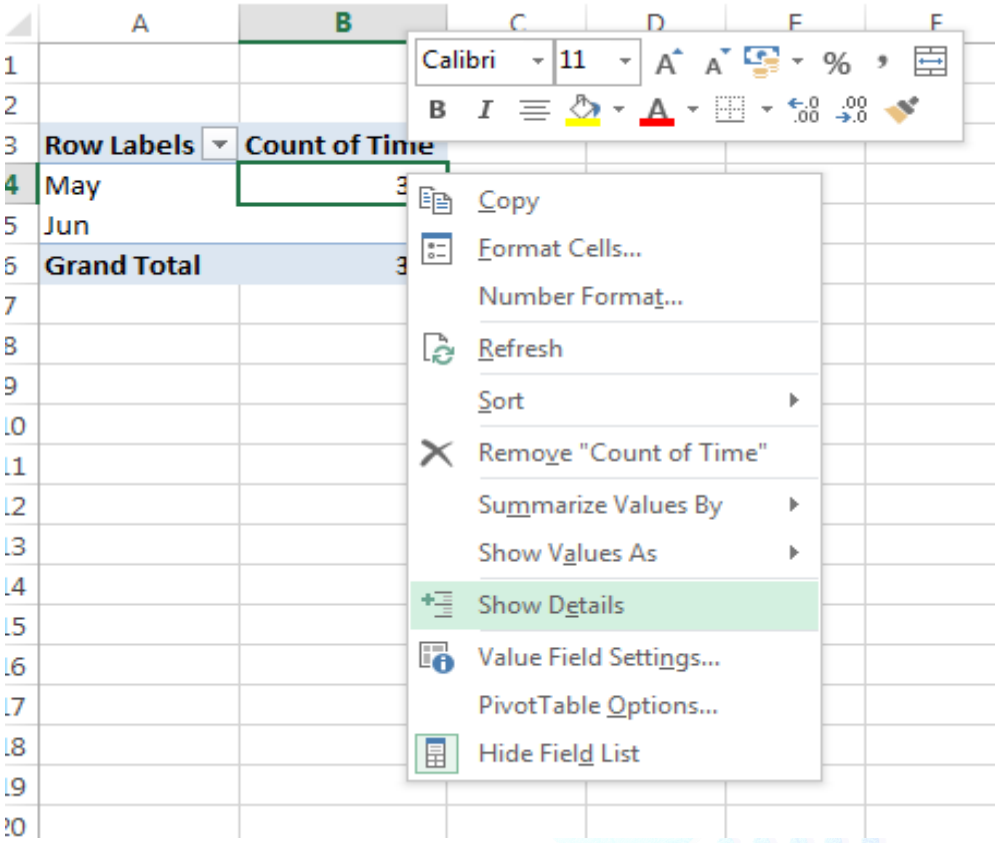


Figure 69:Counting monthly activities

It would show all the calls made/received during a month sorted with Time.

Calling No	Called Number	Date	Time	Duration	Cell1	locations	Call Type	IMEI	IMSI No
9729727738	9896493167	20-05-2011	17:54:50	637	15143	VPO Sarda H	IN	3.52E+14	4.05E+14
9729727738	9896493167	20-05-2011	18:05:59	35	15143	VPO Sarda H	IN	3.52E+14	4.05E+14
9729727738	9896493167	20-05-2011	18:07:08	107	15143	VPO Sarda H	IN	3.52E+14	4.05E+14
9729727738	9896493167	20-05-2011	18:28:12	685	15143	VPO Sarda H	IN	3.52E+14	4.05E+14
9896493167	198	20-05-2011	21:13:25	7	15143	VPO Sarda H	OUT	3.52E+14	4.05E+14
9896493167	198	20-05-2011	21:16:52	28	15143	VPO Sarda H	OUT	3.52E+14	4.05E+14
1446BC65381(	9896493167	21-05-2011	16:42:51	0	15143	VPO Sarda H	SMT	3.52E+14	4.05E+14
1446BC65381(	9896493167	21-05-2011	16:42:57	0	15143	VPO Sarda H	SMT	3.52E+14	4.05E+14
1446BC65381(	9896493167	21-05-2011	16:43:01	0	15143	VPO Sarda H	SMT	3.52E+14	4.05E+14
9729727738	9896493167	21-05-2011	17:12:27	1710	15143	VPO Sarda H	IN	3.52E+14	4.05E+14
9729727738	9896493167	21-05-2011	18:24:52	14	15143	VPO Sarda H	IN	3.52E+14	4.05E+14
549697C8>0B(	9896493167	21-05-2011	18:30:53	0	15143	VPO Sarda H	SMT	3.52E+14	4.05E+14
9729727738	9896493167	21-05-2011	18:35:59	14	15143	VPO Sarda H	IN	3.52E+14	4.05E+14
9729727738	9896493167	21-05-2011	18:52:37	15	15143	VPO Sarda H	IN	3.52E+14	4.05E+14
9896493167	9355709399	21-05-2011	19:38:56	16	15143	VPO Sarda H	OUT	3.52E+14	4.05E+14
9896493167	9355709399	21-05-2011	19:40:33	1080	15143	VPO Sarda H	OUT	3.52E+14	4.05E+14
9671792740	9896493167	21-05-2011	20:13:09	435	15143	VPO Sarda H	IN	3.52E+14	4.05E+14
9896493167	9729727738	21-05-2011	21:00:42	71	15143	VPO Sarda H	OUT	3.52E+14	4.05E+14
9896493167	543213	21-05-2011	21:06:18	30	15143	VPO Sarda H	OUT	3.52E+14	4.05E+14
9896493167	543213	21-05-2011	21:07:00	3	15143	VPO Sarda H	OUT	3.52E+14	4.05E+14

Figure 70: Pivot result

Now we can easily find out the locations during the month.

- Route chart plotting on Google Map for a particular day

Plotting the Route Chart on Google Map require the Coordinates of the Tower. The coordinates can be retrieved from the Tower ID Chart received from the Mobile Service Provider.

A normal Tower ID chart would contain the Tower ID as well as the Latitude and Longitude of the Towers.

	A	B	C
1	CELL ID Final	Lat	Long
2	2071	30.16565	76.8726
3	2072	30.16565	76.8726
4	2073	30.16565	76.8726
5	5091	28.9029	77.0588
6	5092	28.9029	77.0588
7	5093	28.9029	77.0588
8	16041	29.10745	75.95575
9	16042	29.10745	75.95575
10	16043	29.10745	75.95575
11	1431	30.34555	76.7989
12	1432	30.34555	76.7989
13	1433	30.34555	76.7989
14	22121	28.5971	76.1514
15	22122	28.5971	76.1514
16	22123	28.5971	76.1514
17	2161	30.07475	76.98225
18	2162	30.07475	76.98225
19	2163	30.07475	76.98225
20	1251	30.21205	77.0365

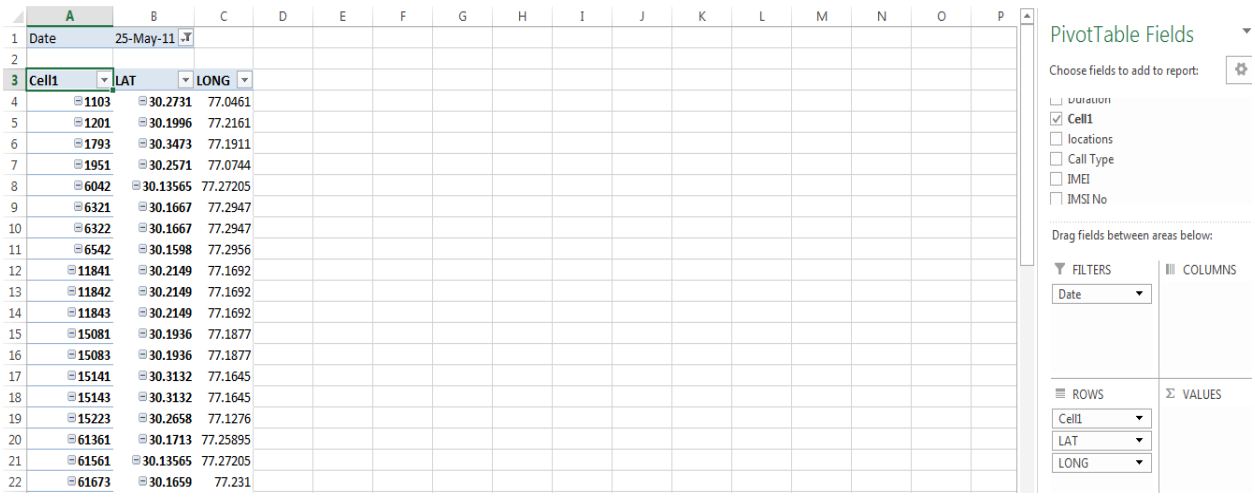
Figure 71: Cell ID chart

We can use Vlookup to fetch the Coordinates from the Tower ID Chart to the CDR file.

	A	B	C	D	E	F	G	H	I	J	K	L	M
4	Calling No	Called Number	Date	Time	Duration	Cell1	locations	Call Type	IMEI	IMSI No	LAT	LONG	
5	9729727738	9896493167	20-May-11	17:54:50	637	15143	VPO Sarda Heri, Tehs & Distt Amb	IN	352000000000000	405000000000000	30.3132	77.1645	
6	9729727738	9896493167	20-May-11	18:05:59	35	15143	VPO Sarda Heri, Tehs & Distt Amb	IN	352000000000000	405000000000000	30.3132	77.1645	
7	9729727738	9896493167	20-May-11	18:07:08	107	15143	VPO Sarda Heri, Tehs & Distt Amb	IN	352000000000000	405000000000000	30.3132	77.1645	
8	9729727738	9896493167	20-May-11	18:28:12	685	15143	VPO Sarda Heri, Tehs & Distt Amb	IN	352000000000000	405000000000000	30.3132	77.1645	
9	9896493167	198	20-May-11	21:13:25	7	15143	VPO Sarda Heri, Tehs & Distt Amb	OUT	352000000000000	405000000000000	30.3132	77.1645	
10	9896493167	198	20-May-11	21:16:52	28	15143	VPO Sarda Heri, Tehs & Distt Amb	OUT	352000000000000	405000000000000	30.3132	77.1645	
11	1446BC65381C0613	9896493167	21-May-11	16:42:51	0	15143	VPO Sarda Heri, Tehs & Distt Amb	SMT	352000000000000	405000000000000	30.3132	77.1645	
12	1446BC65381C0613	9896493167	21-May-11	16:42:57	0	15143	VPO Sarda Heri, Tehs & Distt Amb	SMT	352000000000000	405000000000000	30.3132	77.1645	
13	1446BC65381C0613	9896493167	21-May-11	16:43:01	0	15143	VPO Sarda Heri, Tehs & Distt Amb	SMT	352000000000000	405000000000000	30.3132	77.1645	
14	9729727738	9896493167	21-May-11	17:12:27	1710	15143	VPO Sarda Heri, Tehs & Distt Amb	IN	352000000000000	405000000000000	30.3132	77.1645	
15	9729727738	9896493167	21-May-11	18:24:52	14	15143	VPO Sarda Heri, Tehs & Distt Amb	IN	352000000000000	405000000000000	30.3132	77.1645	
16	549697C8>0BCC56	9896493167	21-May-11	18:30:53	0	15143	VPO Sarda Heri, Tehs & Distt Amb	SMT	352000000000000	405000000000000	30.3132	77.1645	
17	9729727738	9896493167	21-May-11	18:35:59	14	15143	VPO Sarda Heri, Tehs & Distt Amb	IN	352000000000000	405000000000000	30.3132	77.1645	
18	9729727738	9896493167	21-May-11	18:52:37	15	15143	VPO Sarda Heri, Tehs & Distt Amb	IN	352000000000000	405000000000000	30.3132	77.1645	
19	9896493167	9355709399	21-May-11	19:38:56	16	15143	VPO Sarda Heri, Tehs & Distt Amb	OUT	352000000000000	405000000000000	30.3132	77.1645	
20	9896493167	9355709399	21-May-11	19:40:33	1080	15143	VPO Sarda Heri, Tehs & Distt Amb	OUT	352000000000000	405000000000000	30.3132	77.1645	
21	9671792740	9896493167	21-May-11	20:13:09	435	15143	VPO Sarda Heri, Tehs & Distt Amb	IN	352000000000000	405000000000000	30.3132	77.1645	
22	9896493167	9729727738	21-May-11	21:00:42	71	15143	VPO Sarda Heri, Tehs & Distt Amb	OUT	352000000000000	405000000000000	30.3132	77.1645	
23	9896493167	543213	21-May-11	21:06:18	30	15143	VPO Sarda Heri, Tehs & Distt Amb	OUT	352000000000000	405000000000000	30.3132	77.1645	
24	9896493167	543213	21-May-11	21:07:00	3	15143	VPO Sarda Heri, Tehs & Distt Amb	OUT	352000000000000	405000000000000	30.3132	77.1645	
25	1446BA64B99C2633	9896493167	21-May-11	21:07:01	0	15143	VPO Sarda Heri, Tehs & Distt Amb	SMT	352000000000000	405000000000000	30.3132	77.1645	
26	1446BA64B99C2633	9896493167	21-May-11	21:07:15	0	15143	VPO Sarda Heri, Tehs & Distt Amb	SMT	352000000000000	405000000000000	30.3132	77.1645	

Figure 72: vlookup to map lat and long

Route Chart plotting for a day (e.g. 25-May 2011) hence would include all the Locations (with their Coordinates) which were visited by the CDR holder during the day.

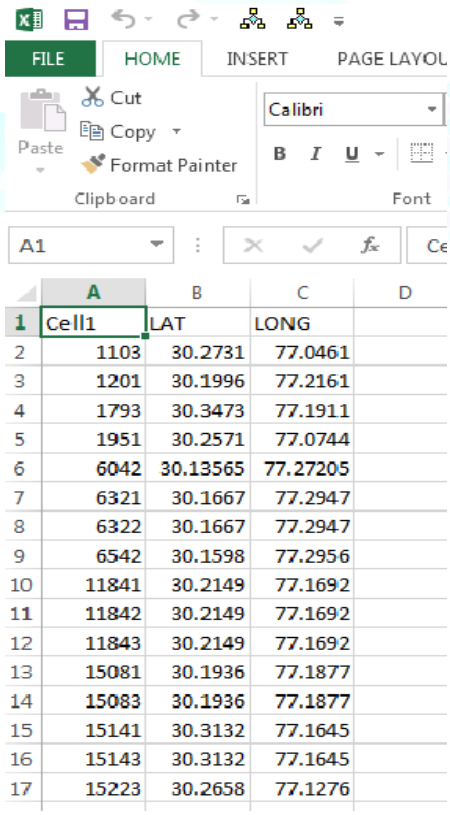


	A	B	C
1	Date	25-May-11	
2			
3	Cell1	LAT	LONG
4	1103	30.2731	77.0461
5	1201	30.1996	77.2161
6	1793	30.3473	77.1911
7	1951	30.2571	77.0744
8	6042	30.13565	77.27205
9	6321	30.1667	77.2947
10	6322	30.1667	77.2947
11	6542	30.1598	77.2956
12	11841	30.2149	77.1692
13	11842	30.2149	77.1692
14	11843	30.2149	77.1692
15	15081	30.1936	77.1877
16	15083	30.1936	77.1877
17	15141	30.3132	77.1645
18	15143	30.3132	77.1645
19	15223	30.2658	77.1276
20	61361	30.1713	77.25895
21	61561	30.13565	77.27205
22	61673	30.1659	77.231

Figure 73: vlookup on cell id

In order to plot the Tower IDs on Google Map, we would collect the above-mentioned CELL IDs along with the coordinates and prepare a .CSV file.

In order to prepare the .CSV file, the data above should be copied and paste into a new Excel Sheet, and should be saved as Comma Separated Value format.



	A	B	C	D
1	Cell1	LAT	LONG	
2	1103	30.2731	77.0461	
3	1201	30.1996	77.2161	
4	1793	30.3473	77.1911	
5	1951	30.2571	77.0744	
6	6042	30.13565	77.27205	
7	6321	30.1667	77.2947	
8	6322	30.1667	77.2947	
9	6542	30.1598	77.2956	
10	11841	30.2149	77.1692	
11	11842	30.2149	77.1692	
12	11843	30.2149	77.1692	
13	15081	30.1936	77.1877	
14	15083	30.1936	77.1877	
15	15141	30.3132	77.1645	
16	15143	30.3132	77.1645	
17	15223	30.2658	77.1276	

Figure 74: save the result

USE OF FUSION TABLE

Next, we will use the Google's Fusion Table feature to plot the coordinates onto the Map.

Fusiontables can be accessed from here –

https://support.google.com/fusiontables/answer/2571232

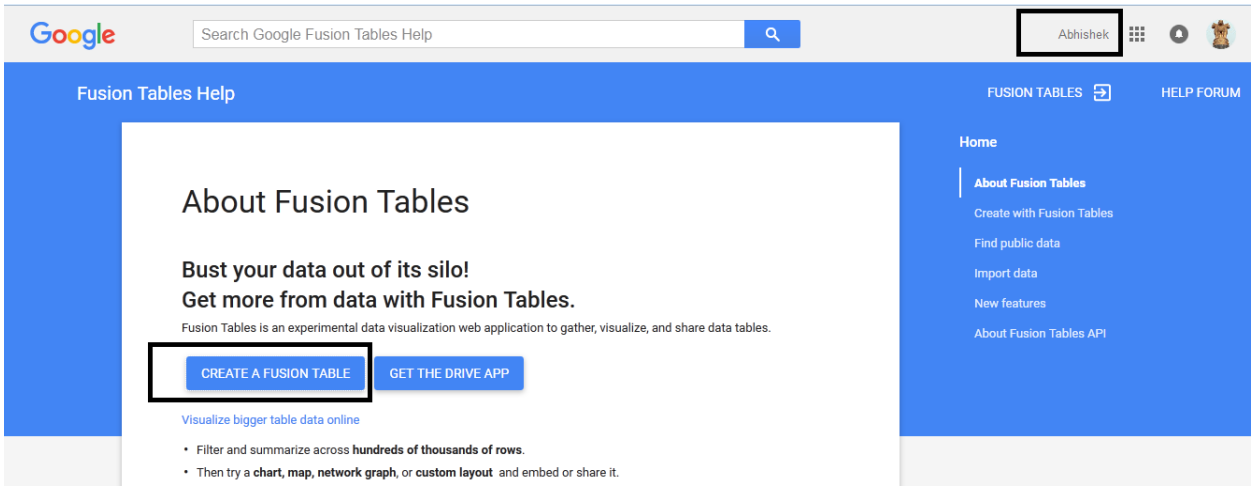


Figure 75 Fusion table

We can create a new Fusion Table by clicking on 'Create Fusion Table' button.

PS: We need to be signed in with a Google ID in order to create a fusion Table

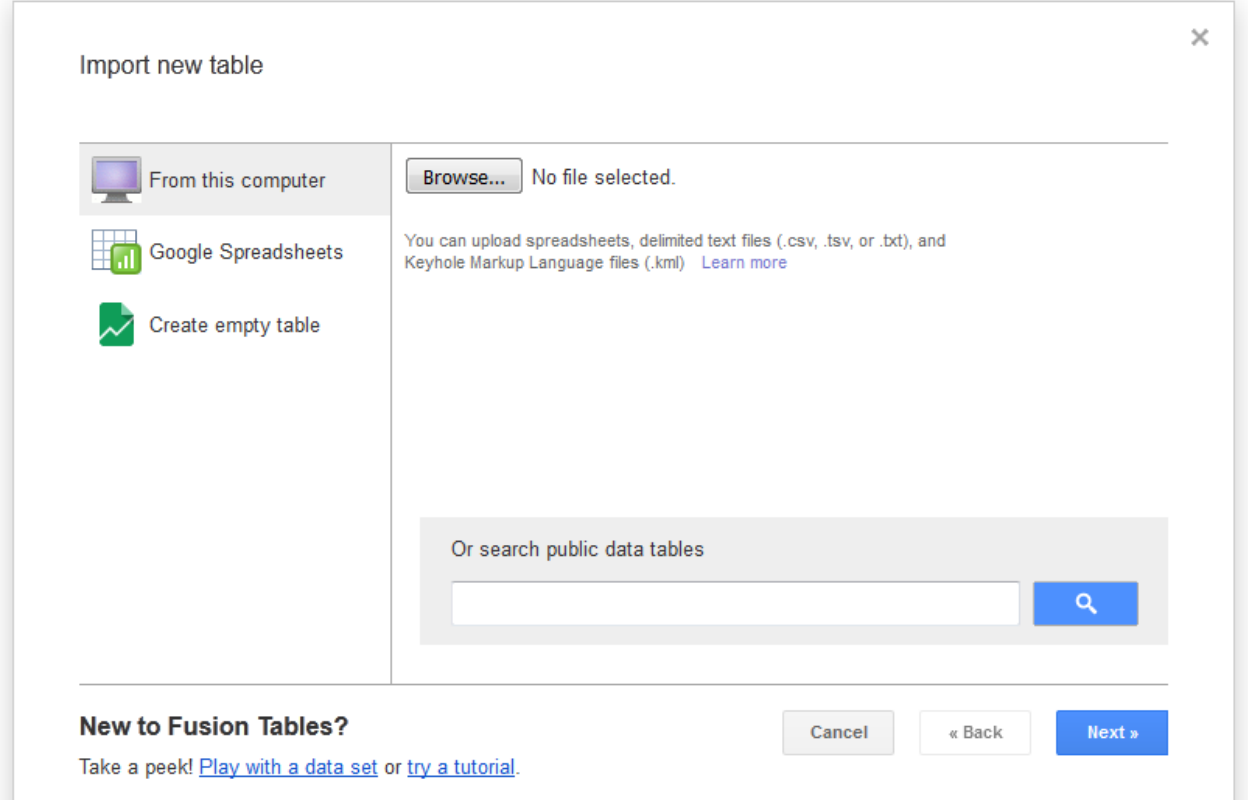


Figure 76: Add File

Now, browse the .CSV file which was created above.

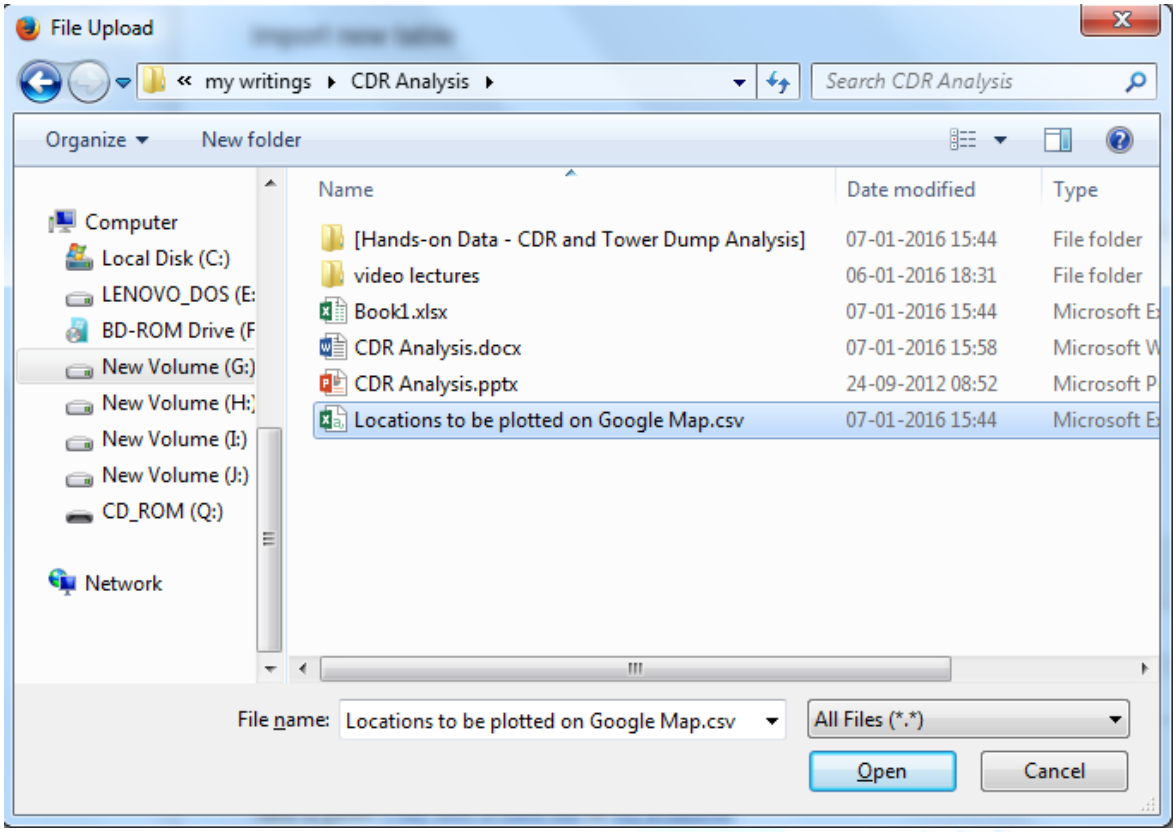


Figure 77: Select File

The file has been shown as selected. Click on Next

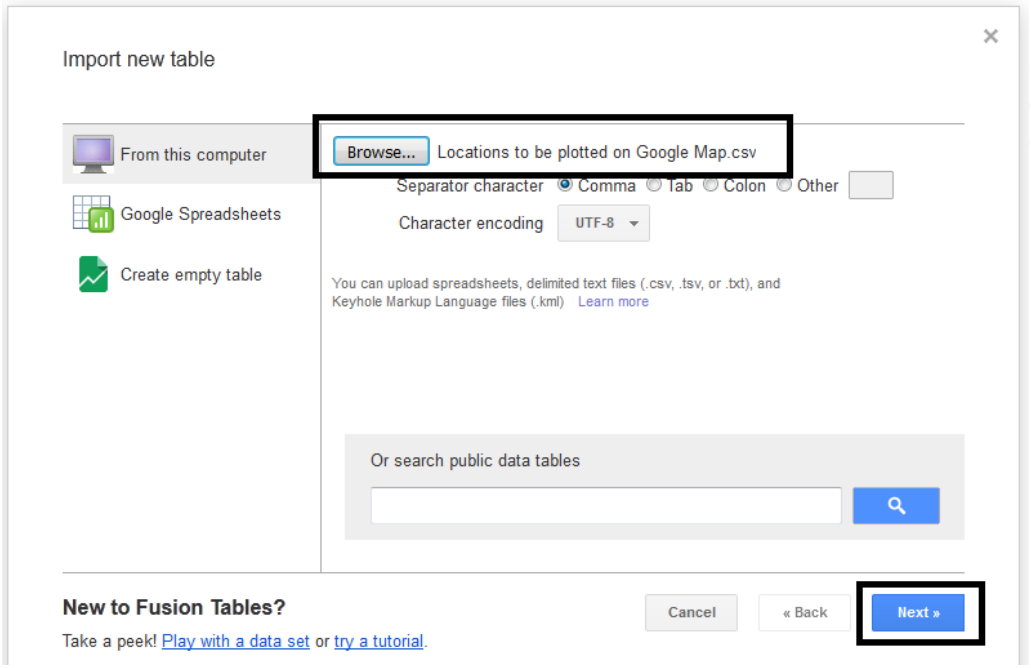


Figure78 : Using Fusion Table

The data imported is previewed here. Click on Next

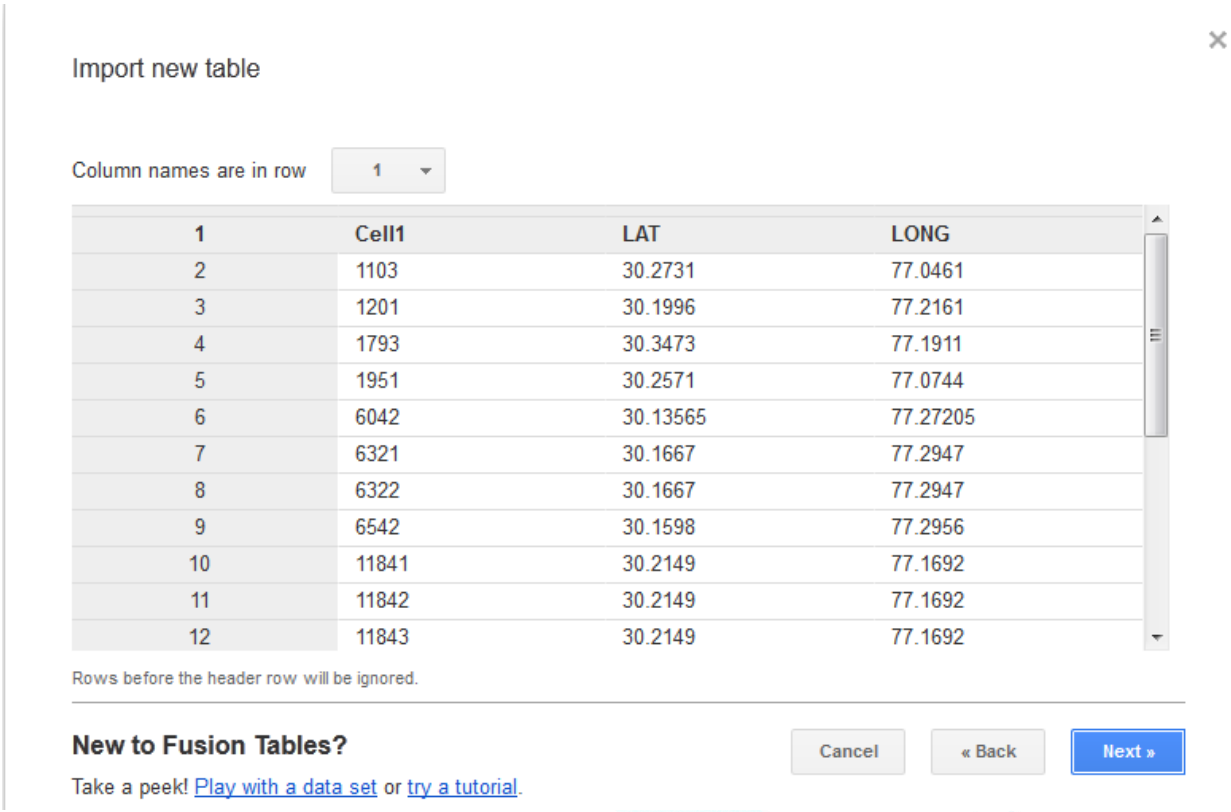


Figure 79: Fusion table

Click on Finish

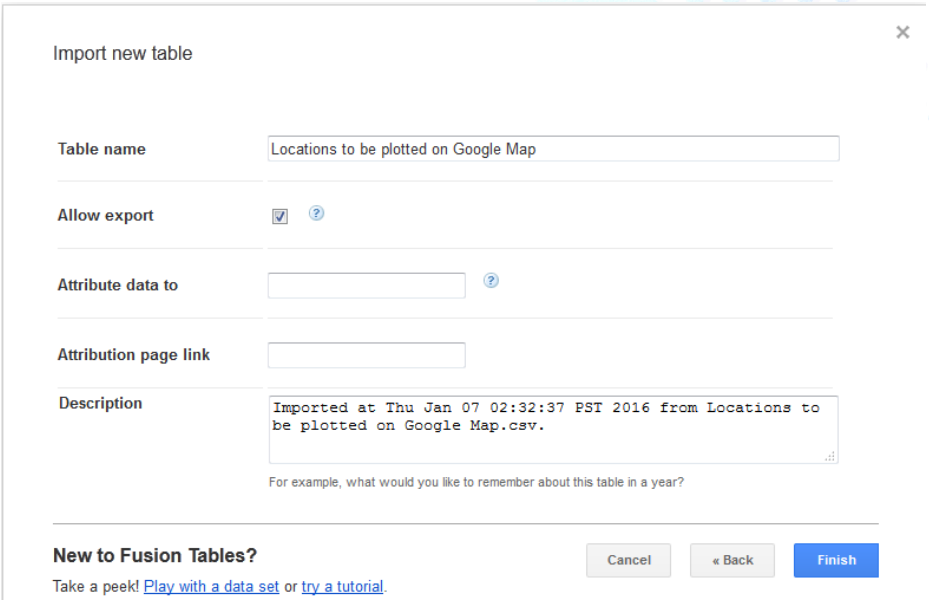


Figure 80: Fusion Table

We now see that the locations are inserted into Fusion Table. In order to plot the coordinates on Google Map, click on “Map of LAT”

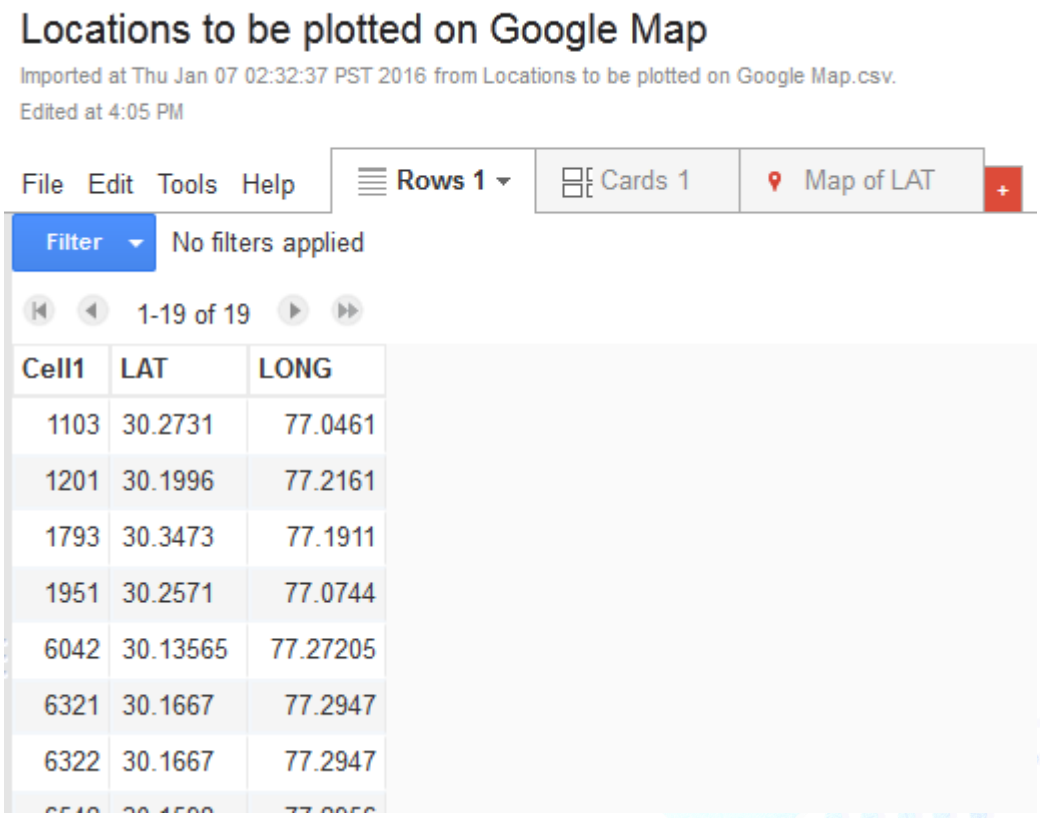


Figure 81: Google map

Here we can see that that Towers are plotted on Google Map.

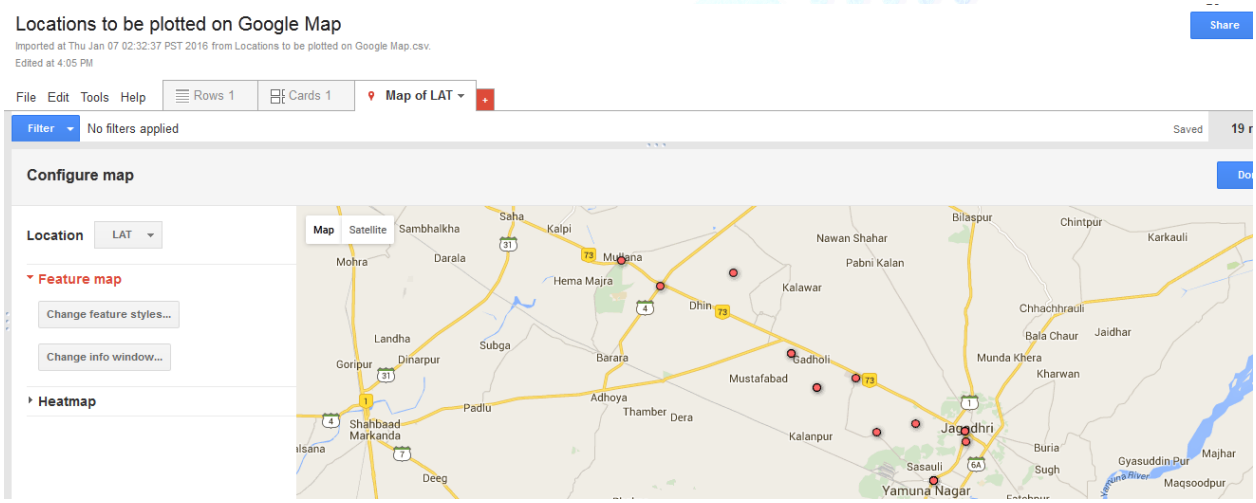


Figure 82: Google map 2

In order to plot the Coordinates on Stand alone Google Maps (i.e. Maps.Google.com), we can download the KML file of the fusion table, which can be later uploaded to the Maps.

STEPS to download the KML file from Fusion Table

1. Switch to the Classic look

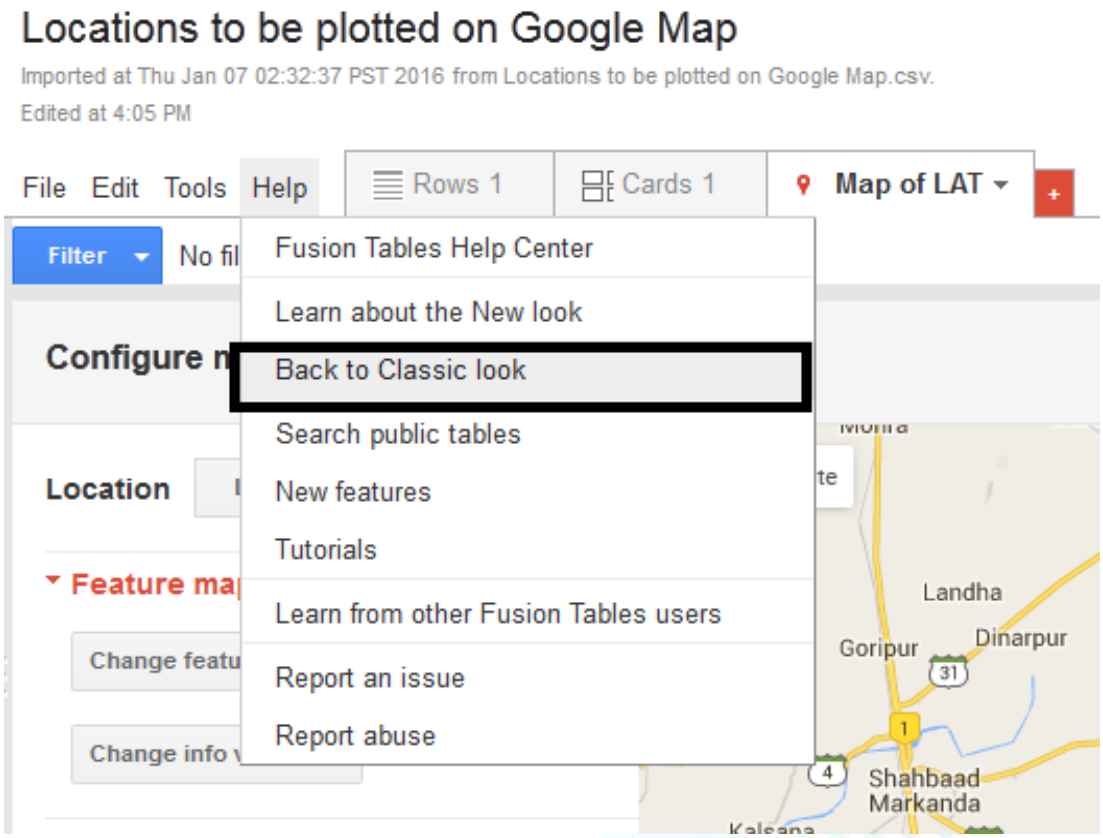


Figure 83: Plotting Google map 3

2. Select the Map

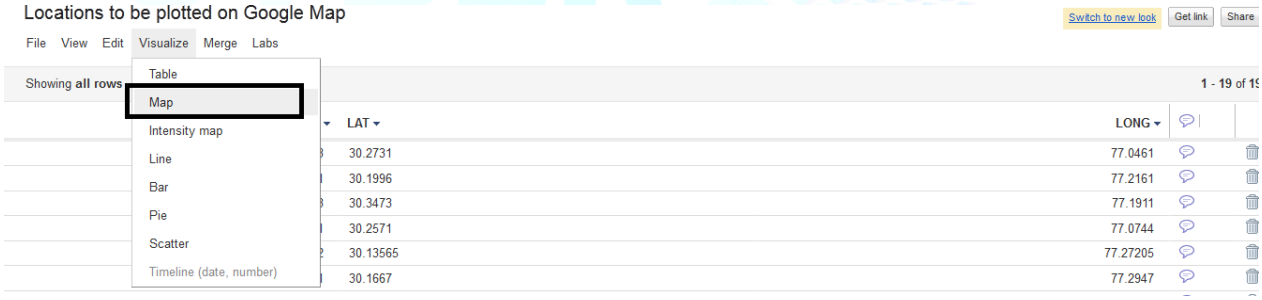


Figure 84: Map Data

3. Download KML

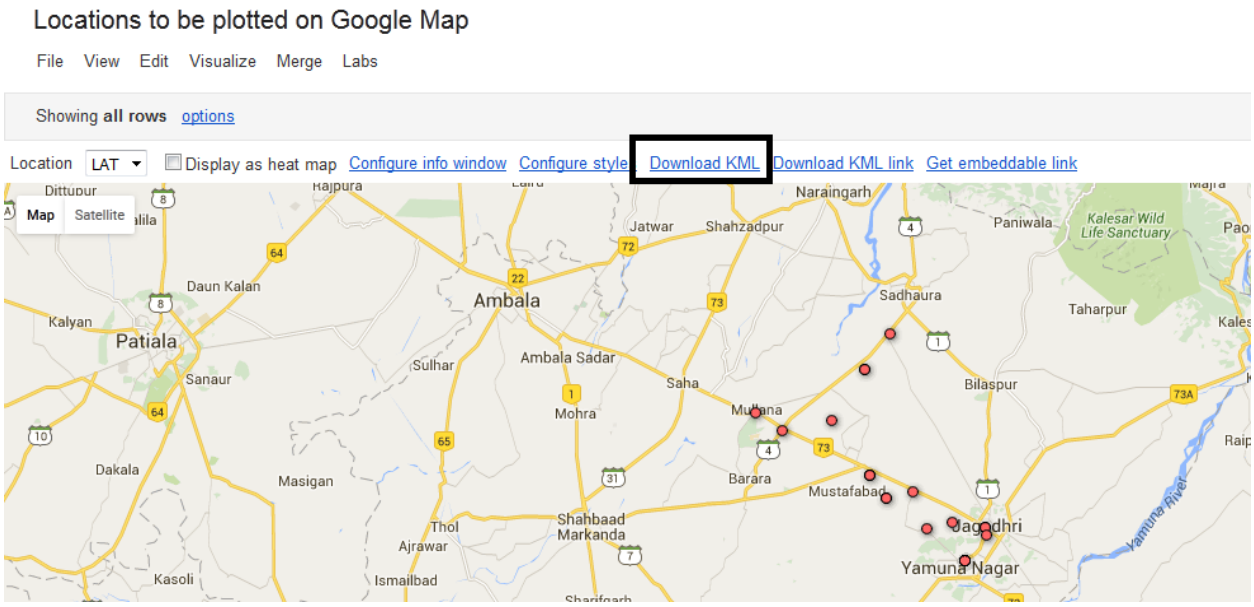


Figure 85: Download KML

STEPS to upload the KML file to Google Map

1. Open maps.google.com (after logging into the gmail account)
2. Open MyMap (https://www.google.com/maps/d/)

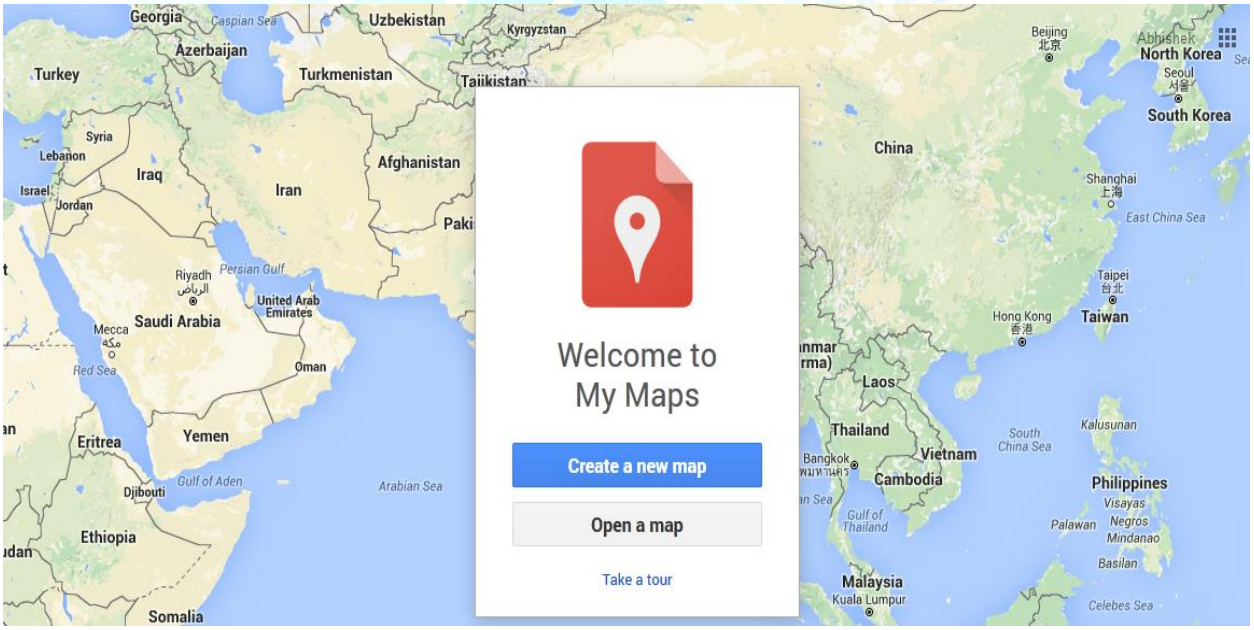


Figure 86: Map link

3. Click on “Create a New Map”

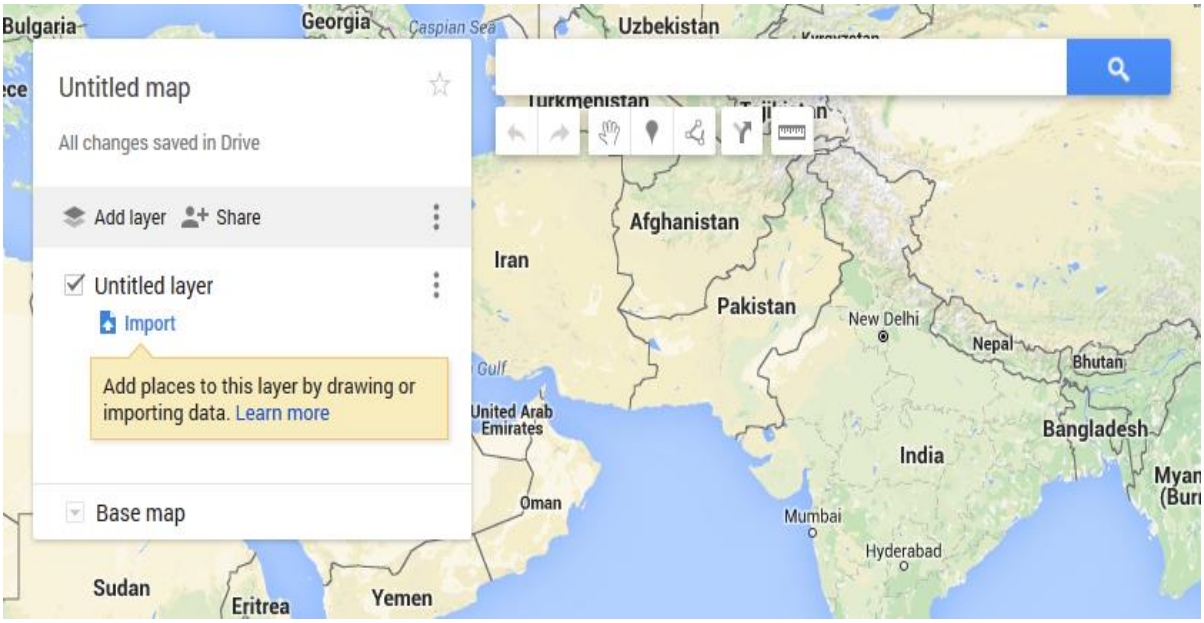


Figure 87: New Map

4. Click on Import

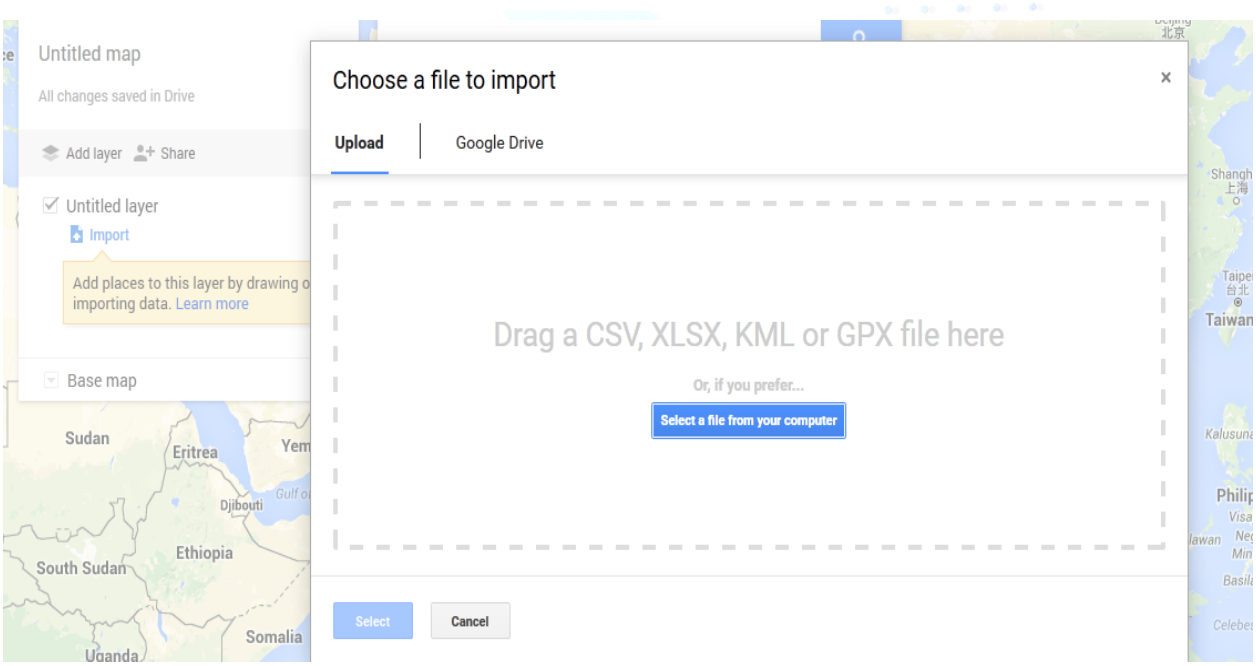


Figure 88: selecting Data

5. Upload the KML file downloaded earlier

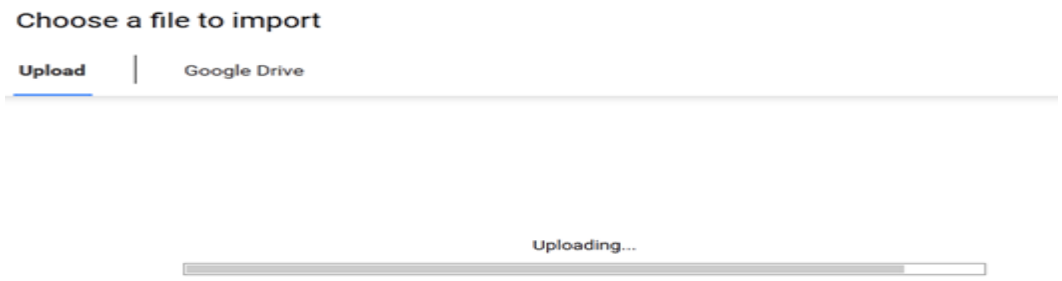


Figure 89: File upload

All the locations are now plotted on the Map

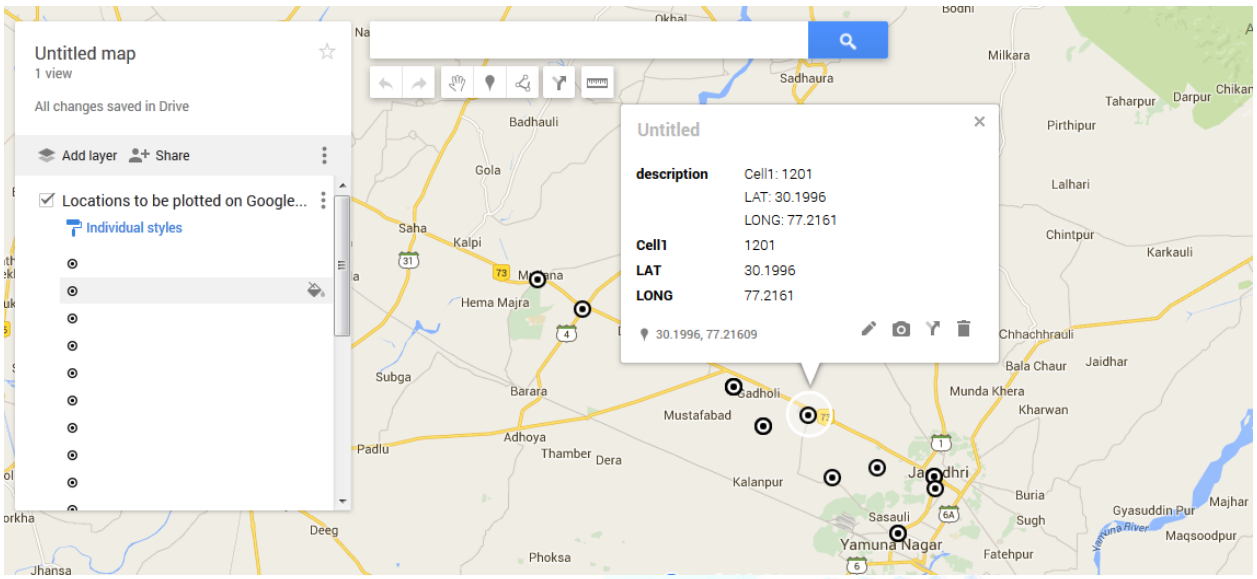


Figure 90: Result Map

3.18.3. Multiple CDRs Analysis

Multiple CDR Analysis is very useful in cases where there are more than one suspect in a case. The CDRs of the suspects can be analyzed to find out –

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

M S Excel again can be used to analyzed multiple CDRs

Steps

1. Place all the CDRs to be analyzed in one folder

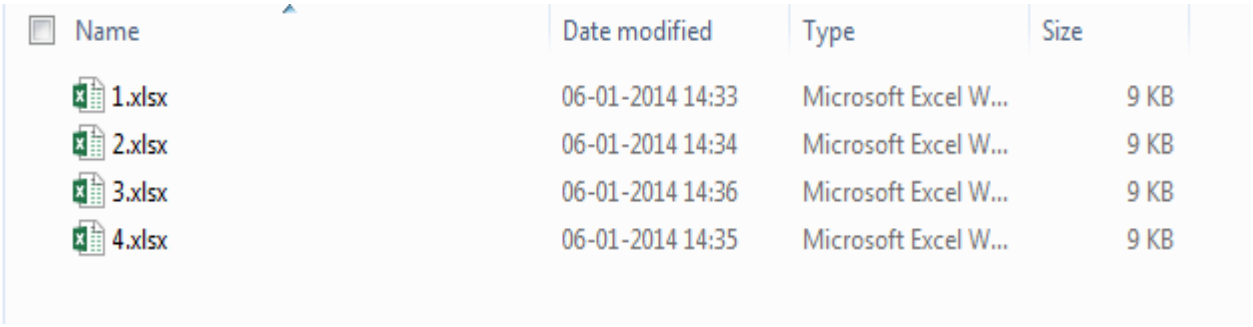


Figure 91: Multiple CDRs

2. Create a MASTER file appending all the calling numbers and called numbers of all the CDRs

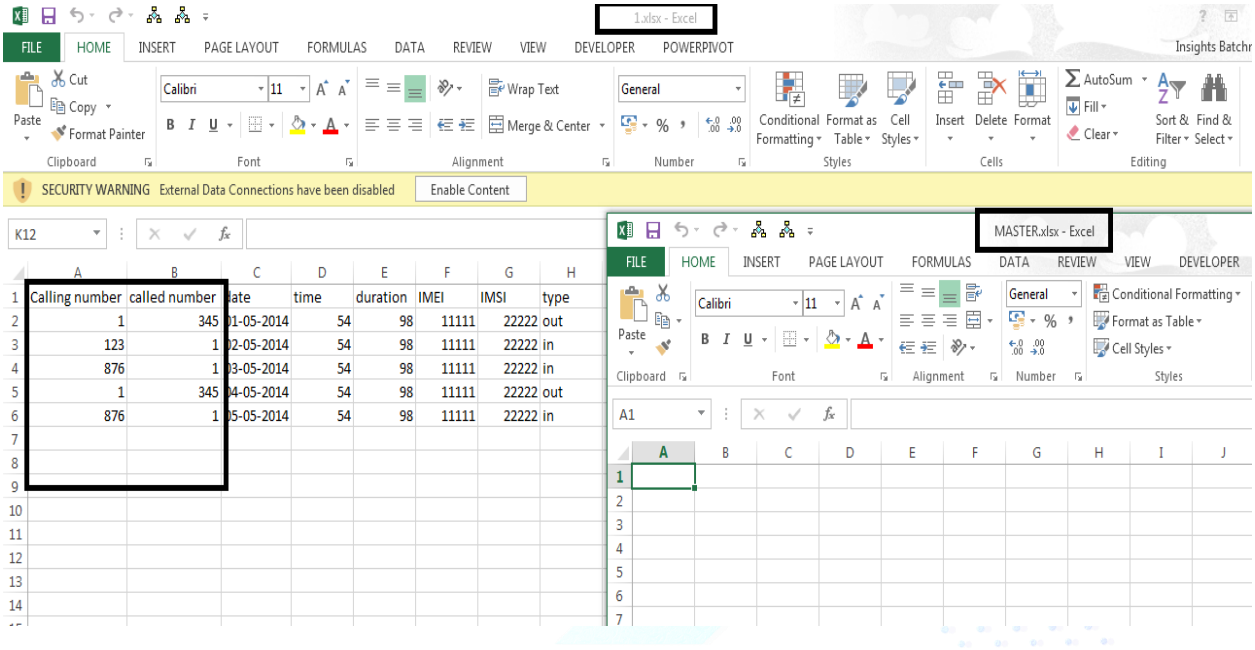


Figure 92: Creating Master file

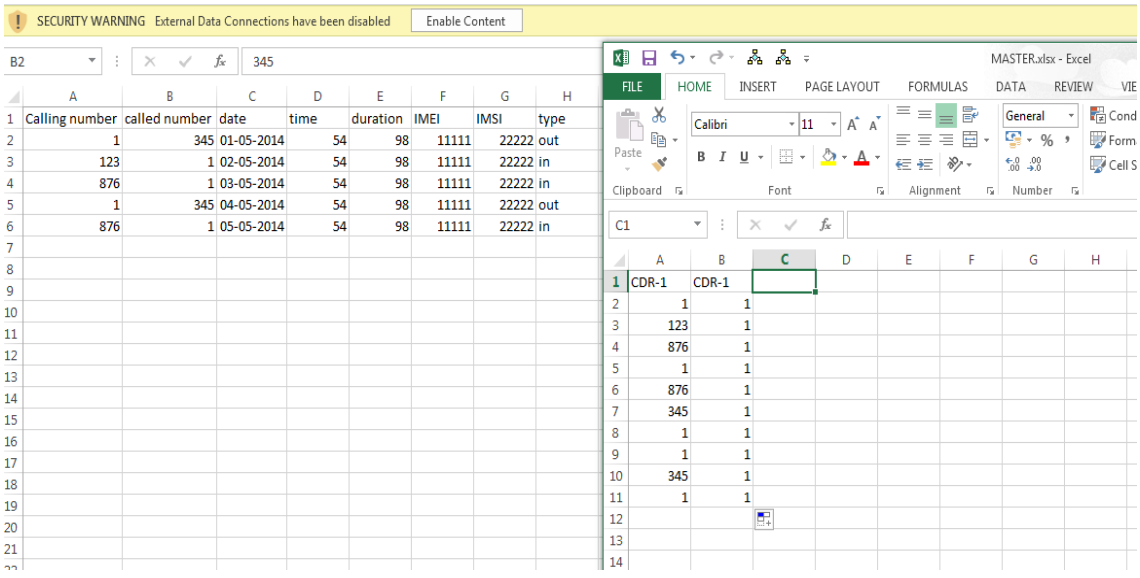
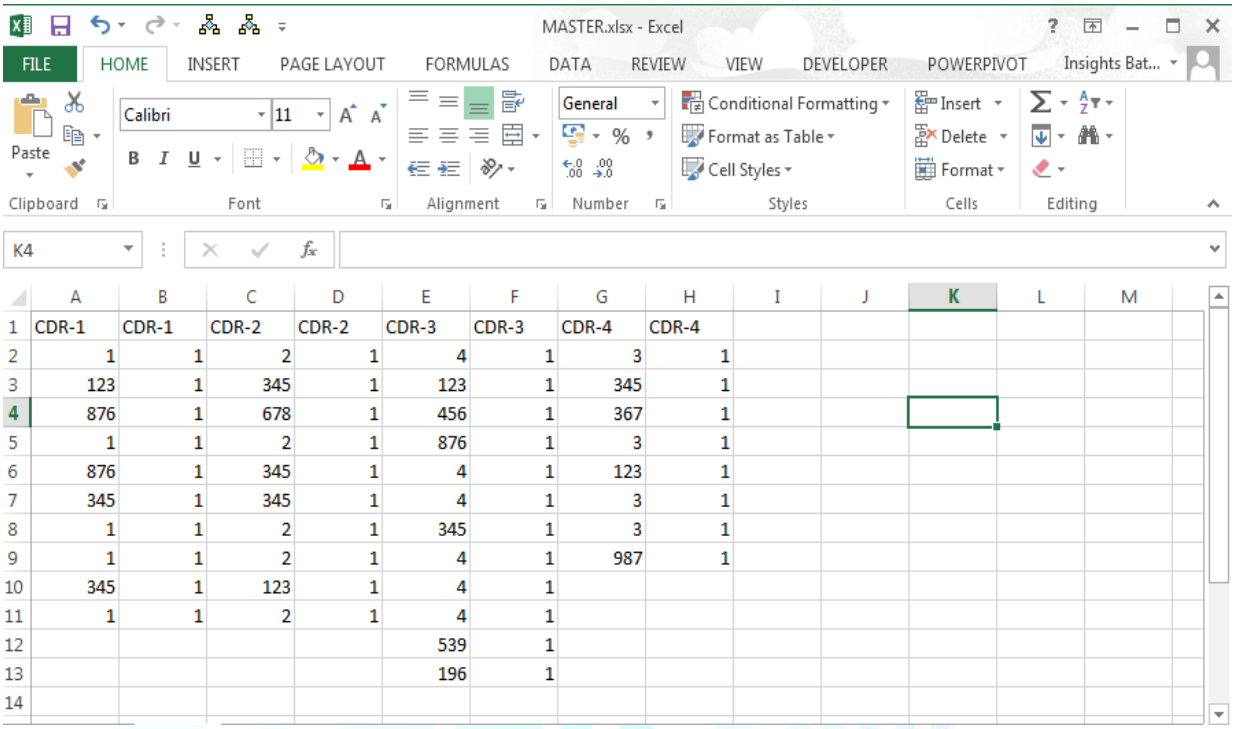


Figure 93: creating master file 2

PS: 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. 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, the MASTER.xlsx would like below screenshot after adding 4 CDR data into it.



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	CDR-1	CDR-1	CDR-2	CDR-2	CDR-3	CDR-3	CDR-4	CDR-4					
2	1	1	2	1	4	1	3	1					
3	123	1	345	1	123	1	345	1					
4	876	1	678	1	456	1	367	1					
5	1	1	2	1	876	1	3	1					
6	876	1	345	1	4	1	123	1					
7	345	1	345	1	4	1	3	1					
8	1	1	2	1	345	1	3	1					
9	1	1	2	1	4	1	987	1					
10	345	1	123	1	4	1							
11	1	1	2	1	4	1							
12					539	1							
13					196	1							
14													

Figure 94: Master file

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

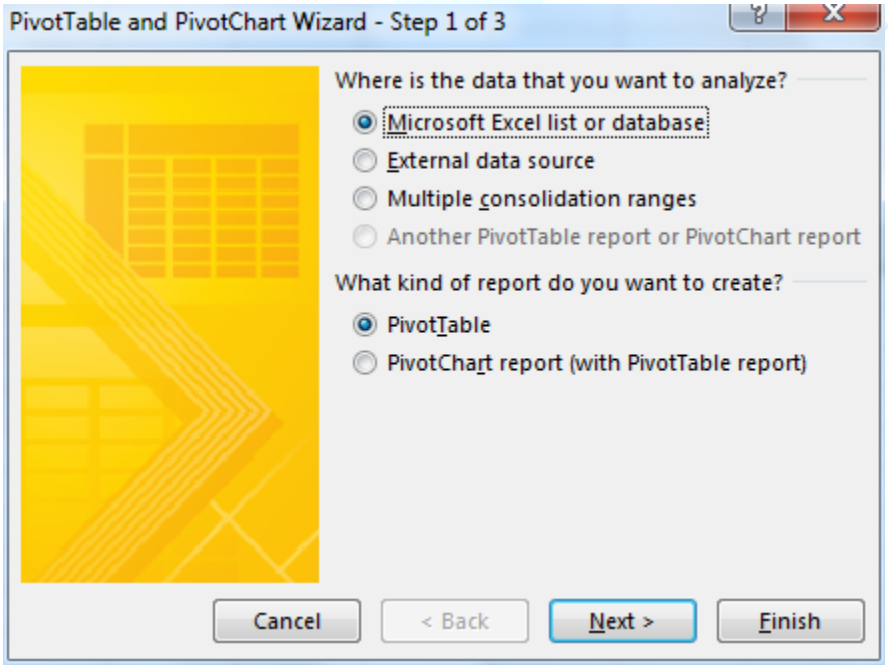


Figure 95: Pivot Wizard

4. Select Multiple Consolidation Ranges and press Next. The following window would appear

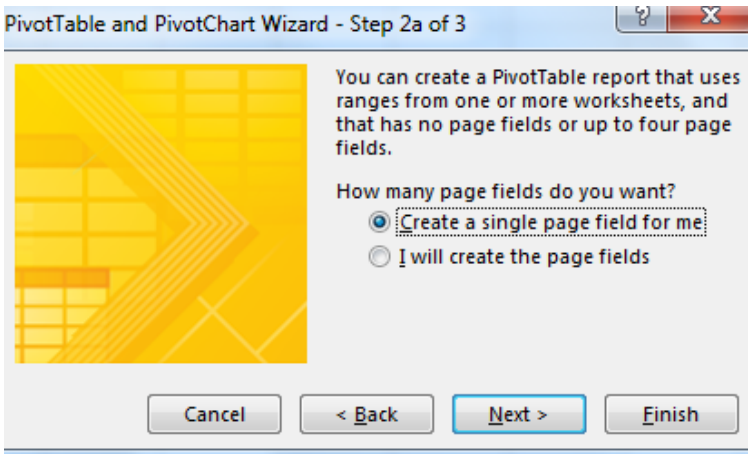


Figure 96: Pivot Wizard

5. Click on “I will create the page fields” and click on Next. Following window will appear

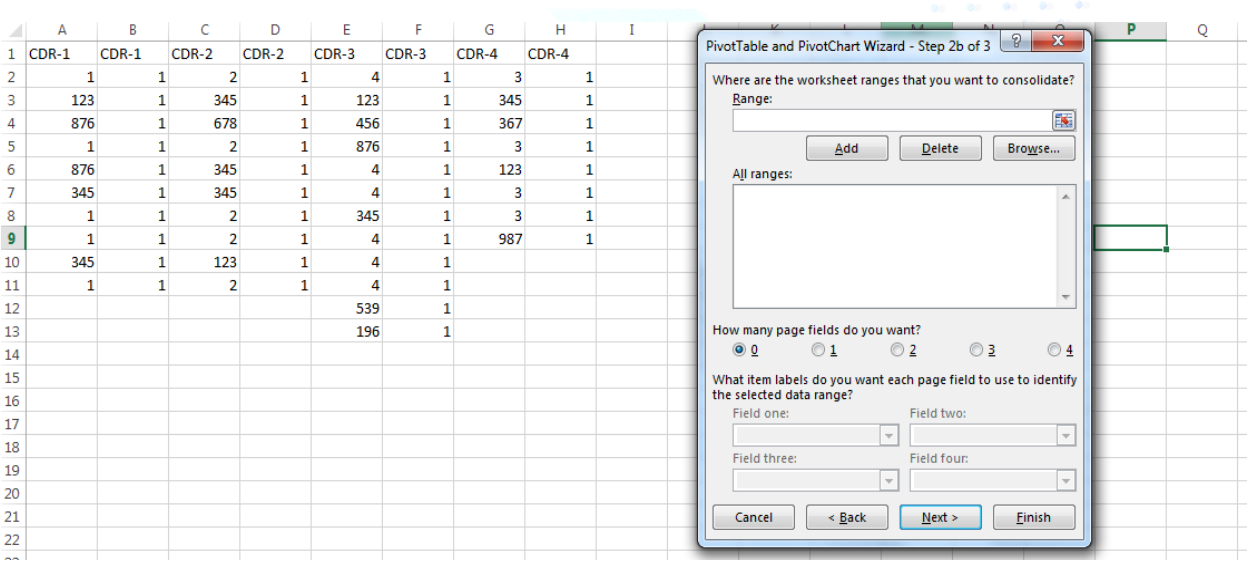


Figure 97: Pivot wizard

6. Select the range of data from the First CDR and click on Add. Then select ‘1’ as the page field, write field one as CDR-1, and click "Add"

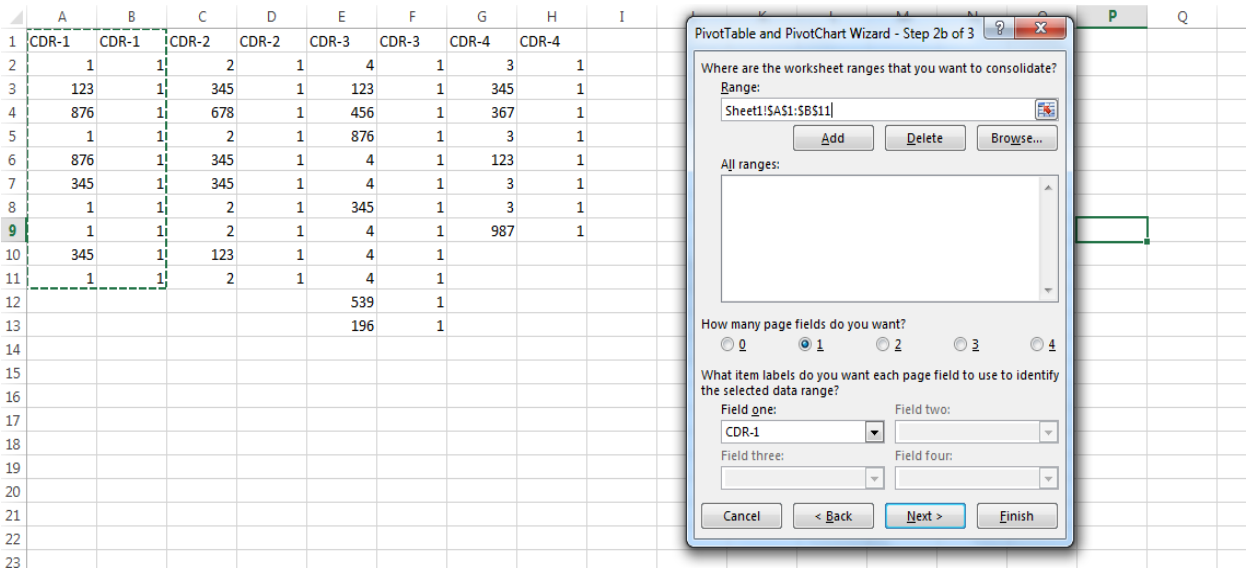


Figure 98 Pivot Wizard

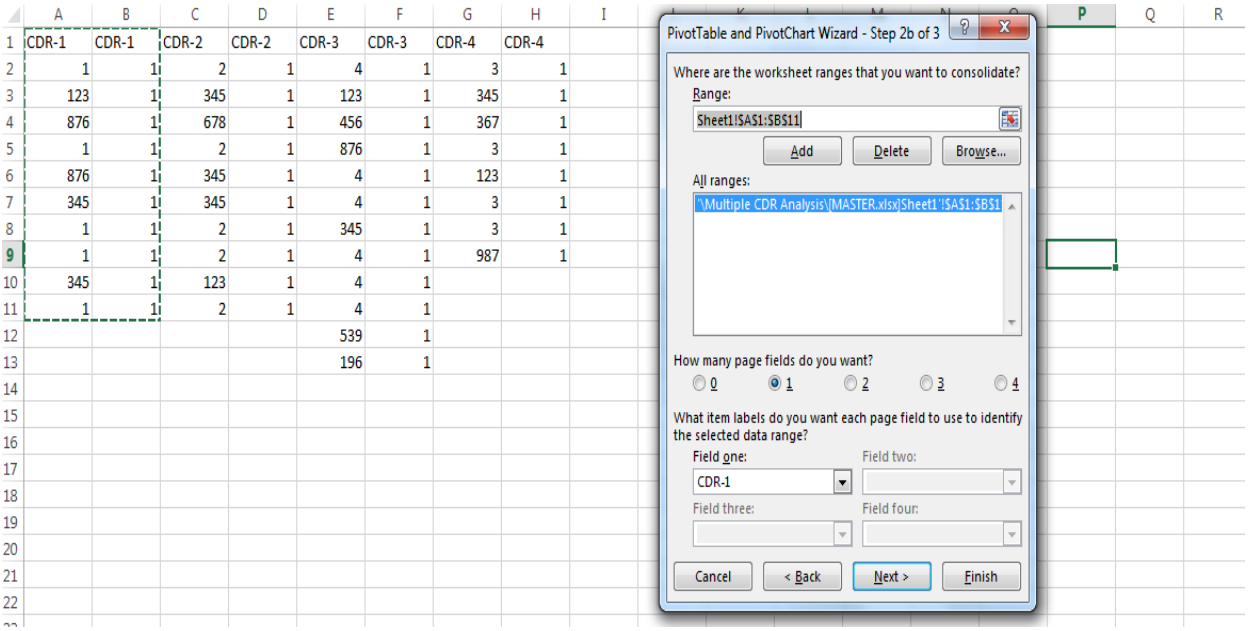
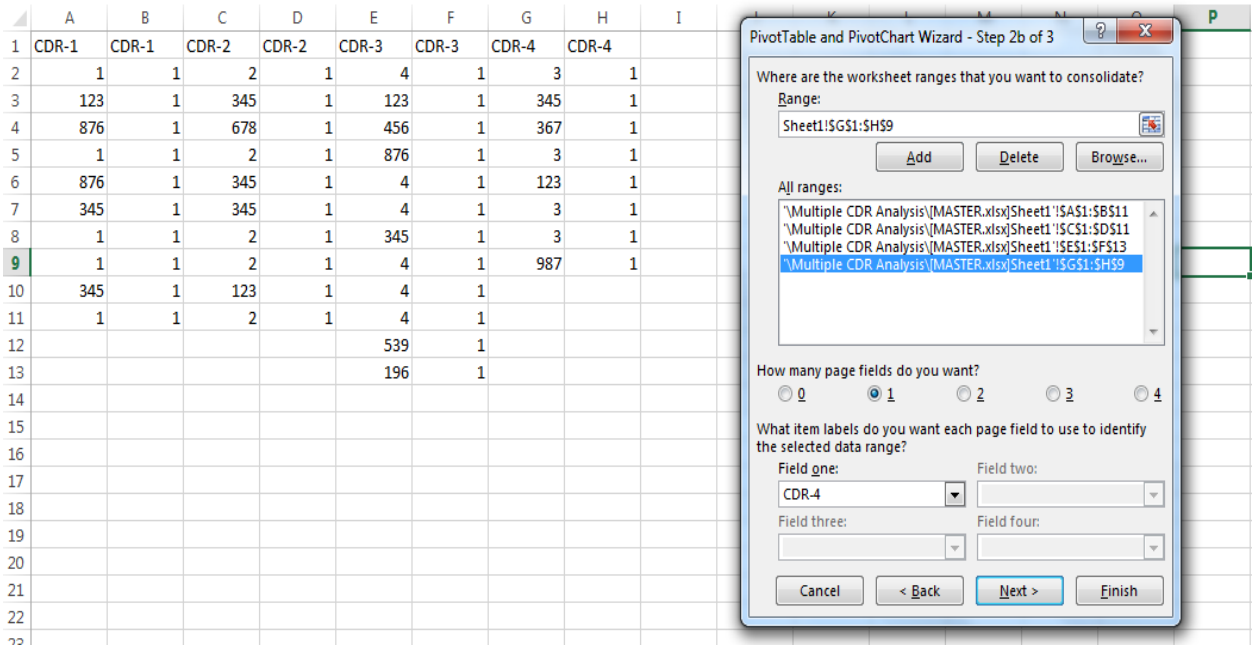


Figure 99: Pivot Wizard

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



	A	B	C	D	E	F	G	H
1	CDR-1	CDR-1	CDR-2	CDR-2	CDR-3	CDR-3	CDR-4	CDR-4
2	1	1	2	1	4	1	3	1
3	123	1	345	1	123	1	345	1
4	876	1	678	1	456	1	367	1
5	1	1	2	1	876	1	3	1
6	876	1	345	1	4	1	123	1
7	345	1	345	1	4	1	3	1
8	1	1	2	1	345	1	3	1
9	1	1	2	1	4	1	987	1
10	345	1	123	1	4	1		
11	1	1	2	1	4	1		
12					539	1		
13					196	1		

Figure 100: Pivot Wizard

Click on Next

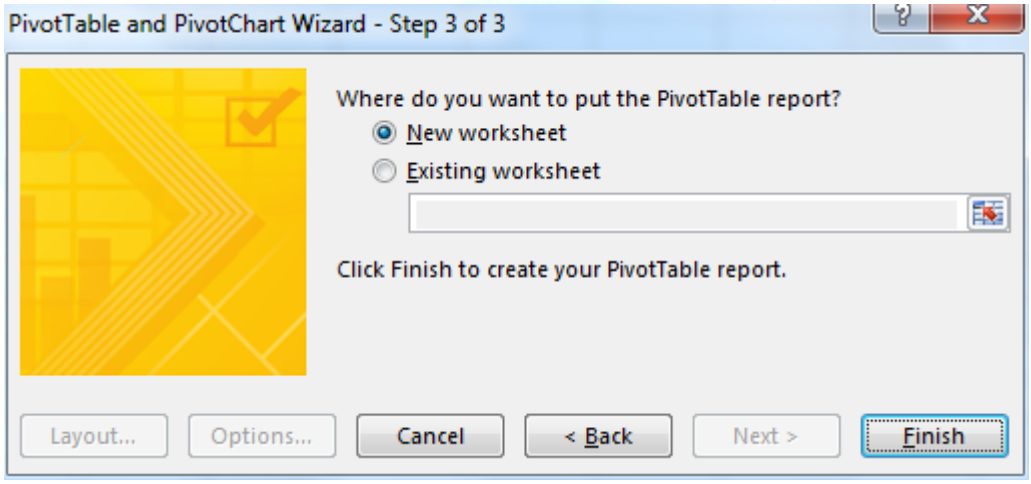


Figure 101: Pivot Wizard

Click on Finish.

The resulting screen looks like this

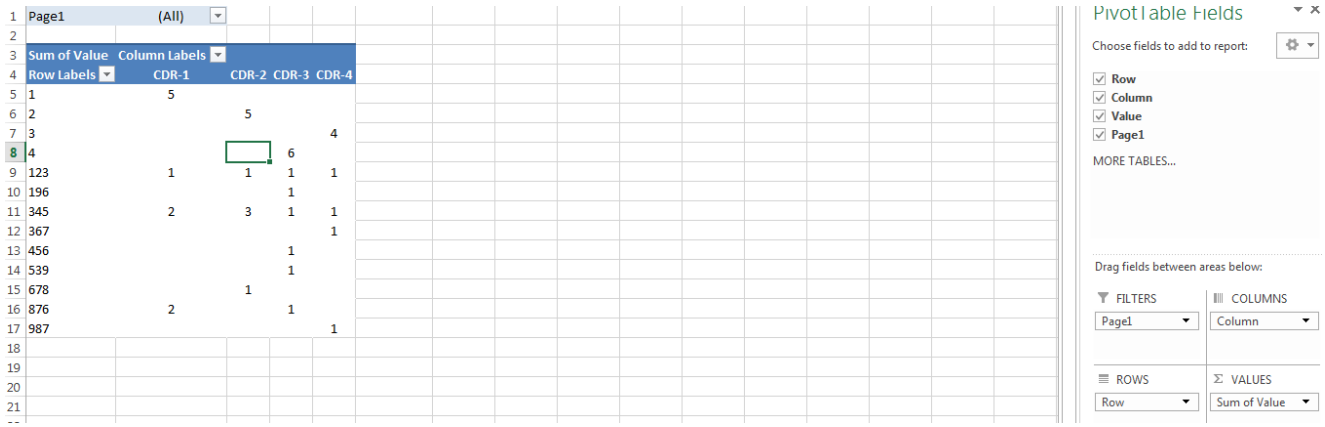


Figure 102: Pivot Wizard

Here following analysis can be made

1. That, number “123” and “345” is interacting with all 4 CDRs
2. That, number “876” is interacting with CDR-1 and CDR-3

This way, Multiple CDRs can be analyzed with M S Excel.

Bibliography

Bowler, L. H. (2004). *Introduction To Mobile Telephone Systems: 1G, 2G, 2.5G, and 3G Wireless Technologies and Services.*

Forouzan, B. A. (2013). *Data Communications & Networking.* McGrawHill.

Kukushkin, A. (2018). *Introduction to Mobile Network Engineering (GSM, 3G-WCDMA, LTE and the Road to 5G).* Wiley.

Mohammad Meraj ud in Mir, D. S. (2015). Evolution of Mobile Wireless Technology from 0G to 5G. *International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2545-2551.*

NDCRTC. (n.d.). *Cyber Crime Investigation Manual.* NDCRTC.

NDCRTC. (n.d.). *Mobile Forensics & Analysis.* NDCRTC.

Sauter, M. (2017). *From GSM to LTE-Advanced Pro and 5G (An Introduction to Mobile Networks and Mobile Broadband).* Wiley.

TutorialsPoint. (n.d.). *Wireless Communication Tutorial*. Retrieved from TutorialsPoint: https://www.tutorialspoint.com/wireless_communication/index.htm

IPDR and VoIP Investigation

1. What is IPDR

The **IP detail record**, abbreviated as **IPDR**, provides information about Internet Protocol (IP)-based service usage. Usually if there is an IP address found or if a suspect is surfing internet, then a request of an IPDR is made.

2. Types of IPDR

- **Mobile number-based** (GPRS/Internet Activity record)

  Example: Internet Activity record of 9700123456

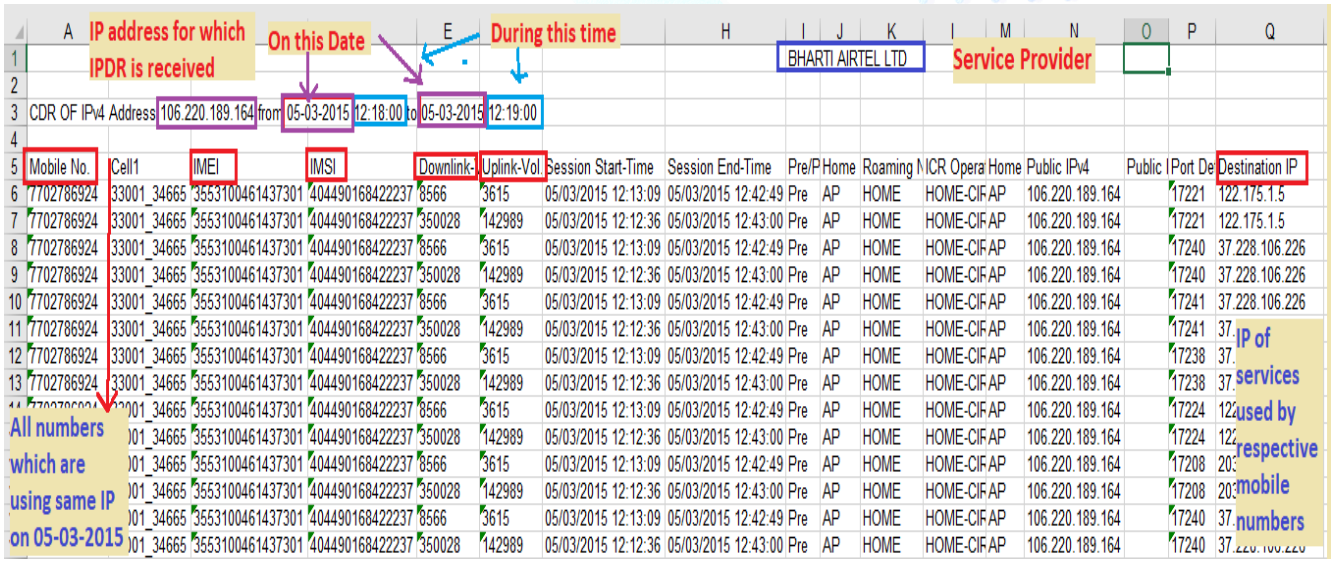
- **IP-based**

  Example: IPDR of 106.11.23.80

- **Tower-based**

  Example: IPDR of Airtel Cell ID 4058740118132

3. IPDR Format



Mobile No.	Cell1	IMEI	IMSI	Downlink-V	Uplink-Vol	Session Start-Time	Session End-Time	Pre/P	Home	Roaming	NCR Opera	Home	Public IPv4	Public I	Port De	Destination IP
7702786924	33001_34665	35531004614373 01	404490168422237	8566	3615	05/03/2015 12:13:09	05/03/2015 12:42:49	Pre	AP	HOME	HOME-CIF	AP	106.220.189.164		17221	122.175.1.5
7702786924	33001_34665	35531004614373 01	404490168422237	350028	142989	05/03/2015 12:12:36	05/03/2015 12:43:00	Pre	AP	HOME	HOME-CIF	AP	106.220.189.164		17221	122.175.1.5
7702786924	33001_34665	35531004614373 01	404490168422237	8566	3615	05/03/2015 12:13:09	05/03/2015 12:42:49	Pre	AP	HOME	HOME-CIF	AP	106.220.189.164		17240	37.228.106.226
7702786924	33001_34665	35531004614373 01	404490168422237	350028	142989	05/03/2015 12:12:36	05/03/2015 12:43:00	Pre	AP	HOME	HOME-CIF	AP	106.220.189.164		17240	37.228.106.226
7702786924	33001_34665	35531004614373 01	404490168422237	8566	3615	05/03/2015 12:13:09	05/03/2015 12:42:49	Pre	AP	HOME	HOME-CIF	AP	106.220.189.164		17241	37.228.106.226
7702786924	33001_34665	35531004614373 01	404490168422237	350028	142989	05/03/2015 12:12:36	05/03/2015 12:43:00	Pre	AP	HOME	HOME-CIF	AP	106.220.189.164		17241	37.
7702786924	33001_34665	35531004614373 01	404490168422237	8566	3615	05/03/2015 12:13:09	05/03/2015 12:42:49	Pre	AP	HOME	HOME-CIF	AP	106.220.189.164		17238	37.
7702786924	33001_34665	35531004614373 01	404490168422237	350028	142989	05/03/2015 12:12:36	05/03/2015 12:43:00	Pre	AP	HOME	HOME-CIF	AP	106.220.189.164		17238	37.
	001_34665	35531004614373 01	404490168422237	8566	3615	05/03/2015 12:13:09	05/03/2015 12:42:49	Pre	AP	HOME	HOME-CIF	AP	106.220.189.164		17224	122
	001_34665	35531004614373 01	404490168422237	350028	142989	05/03/2015 12:12:36	05/03/2015 12:43:00	Pre	AP	HOME	HOME-CIF	AP	106.220.189.164		17224	122
	001_34665	35531004614373 01	404490168422237	8566	3615	05/03/2015 12:13:09	05/03/2015 12:42:49	Pre	AP	HOME	HOME-CIF	AP	106.220.189.164		17208	203
	001_34665	35531004614373 01	404490168422237	350028	142989	05/03/2015 12:12:36	05/03/2015 12:43:00	Pre	AP	HOME	HOME-CIF	AP	106.220.189.164		17208	203
	001_34665	35531004614373 01	404490168422237	8566	3615	05/03/2015 12:13:09	05/03/2015 12:42:49	Pre	AP	HOME	HOME-CIF	AP	106.220.189.164		17240	37.
	001_34665	35531004614373 01	404490168422237	350028	142989	05/03/2015 12:12:36	05/03/2015 12:43:00	Pre	AP	HOME	HOME-CIF	AP	106.220.189.164		17240	37.

Figure 1:IPDR Format

4. Fields provided in IPDR:

- **Landline/MSISDN for Internet Access** – Mobile numbers which are accessing Internet using given IP address (Mobile Station International Subscriber Directory Number)
- **Source IP Address** – Private IP is allocated internally for mobiles or PCs, but actual communication happens over Public IP
- **Source Port** -User can access multiple services simultaneously from single device, port number will differentiate between all the services running on the same device.

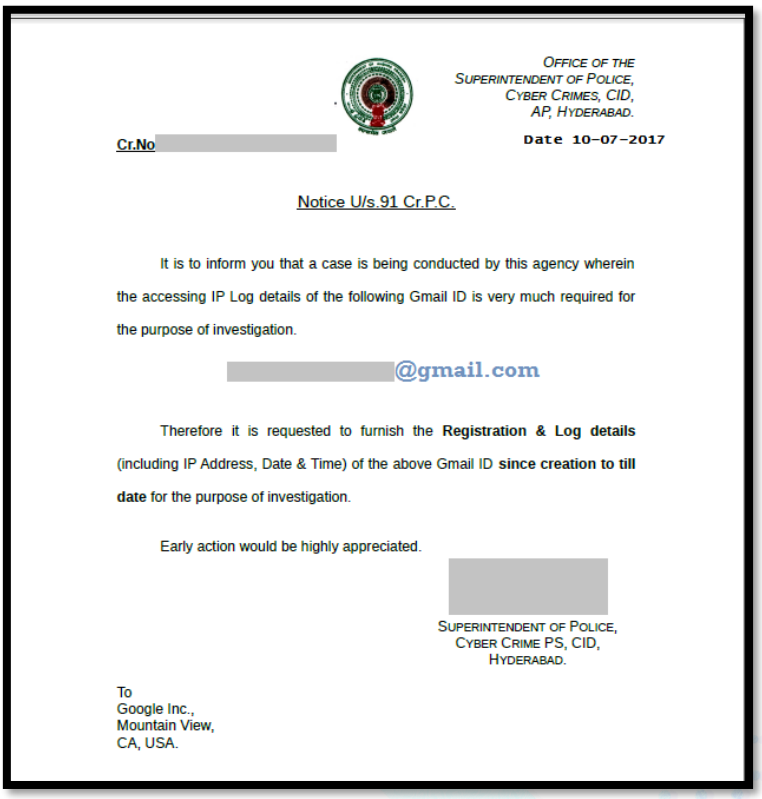
- **Public IP Address** – Public IP address is Identity of user over the Internet. It will be unique organisations and users who have issued or purchased it for exclusive use. But in case of mobile phones, service provider may allocate single public IP to multiple users
- **Public IP Port -** User can access multiple services simultaneously from single IP, port number will differentiate between all the services running on the same IP.
- **Destination IP Address** – Destination IP is identity of the service accessed by user. E.g., if user has accessed 'facebook.com' then IP address of server where 'Facebook' is hosted will be recorded into this column.
- **Destination Port**- Destination port differentiates between multiple services hosted on the same server.
- **Start Date of Public IP Allocation** – Date when given Public IP was allocated to user
- **IST Start Time of Public IP Allocation -** Time when given Public IP was allocated to user
- **End Date of Public IP Allocation -** Date when Public IP allocation to user was stopped
- **IST End Time of Public IP Allocation** – Time when Public IP allocation to user was stopped
- **Static/Dynamic IP Address Allocation** – Types of Public IP allocation, in case of 'Static' allocation IP will not change for given user. In case of 'Dynamic' allocation IP will keep on changing for user.
- **Device Identification number** – MAC address in case of laptop or other IoT devices. IMEI in case of mobile device.
- **IMSI -**
- **PGW IP address –** It allocates Ips to Mobile phones dynamically.
- **CGI ID -** Cell Global Identity (CGI) is a globally unique identifier for a Base Transceiver Station in mobile phone networks.
- **Session Duration** – Duration for which user was active for given session

5. Finding IP address of the suspect

To start with IPDR first we need to know either IP address or mobile number of the suspect. So that we can request IPDR using IP or mobile number. Following are some ways to find IP address of the suspect.

1. Getting IP address from Gmail or Facebook like services

   If we know the Gmail id or Facebook id of the suspect. Then IO can write notice to Gmail or Facebook u/s 91 of CRPC to provide details of the suspect.



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

Cr.No

Date 10-07-2017

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

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

@gmail.com

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

Early action would be highly appreciated.

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

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

Figure 2: 91 Crpc notice

In response we will get logs in following format:

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

GOOGLE SUBSCRIBER INFORMATION

Name:

e-Mail: @gmail.com

Status: Enabled

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

Secondary e-Mail: @gmail.com

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

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

Language Code: en

SMS: 8801886488 [IN]

Nickname:

+----------+----------+----+

| Time | IP Address | Type |

+----------+----------+----+

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

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

Figure 3: 91 crcpc reply

2. Sending tracking link to suspect
   We can create tracking link using available tools (some are enlisted below). It can be sent to suspect via any media like mail, chat or WhatsApp. Once suspect clicks on the link his/her IP address will be logged with us.

   Tools for creating tracking link:
   - grabify.link/
   - iplogger.org/
   - www.ps3cfw.com/
   - linkify.me/
   - clickmeter
   - ip-tracker

3. Getting IP from Facebook account, if we have credentials with us.

   Log in >> 'Settings and Privacy' >> 'Activity Logs' >> 'Logged actions and other activity' >> 'Active Sessions' and 'Logins and Logout'

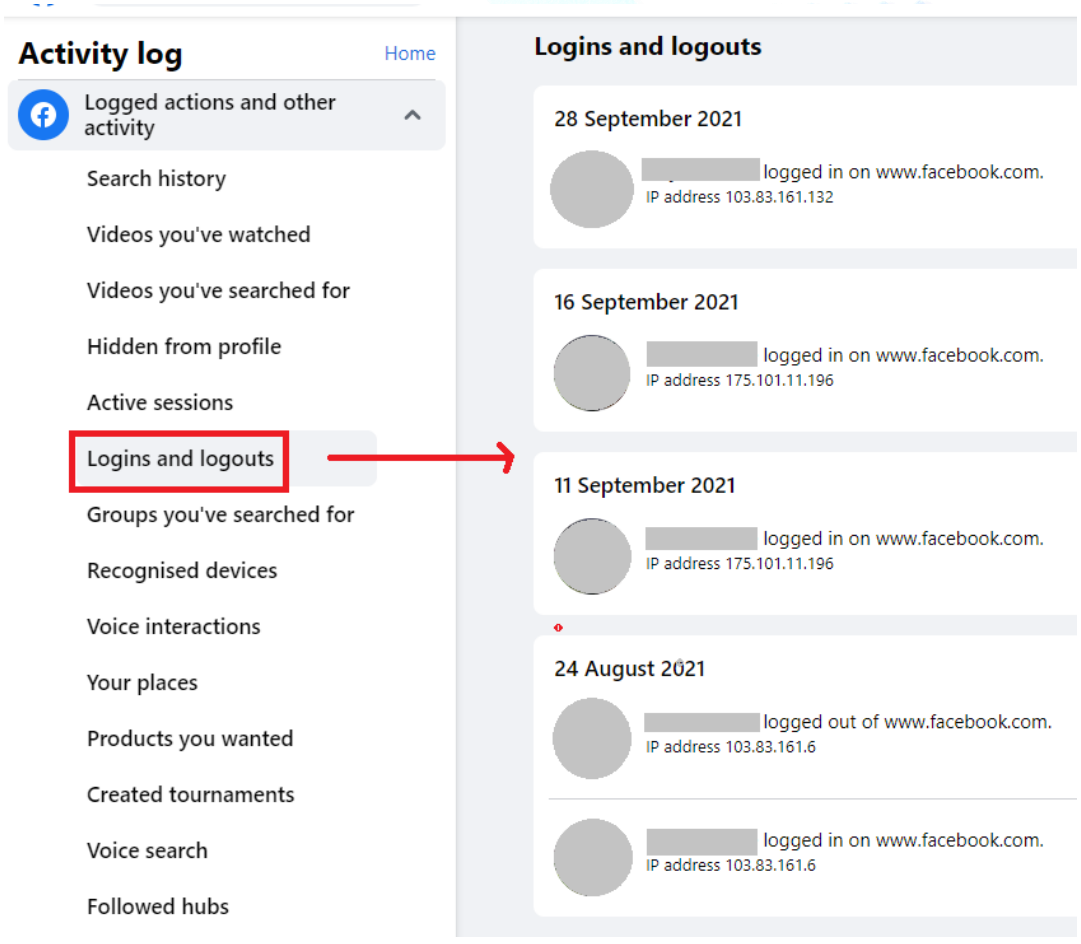


Figure 4: Facebook Logs

4. Getting IP address from Gmail account

Log in Gmail account >> Bottom of the page click ‘Last account activity details’

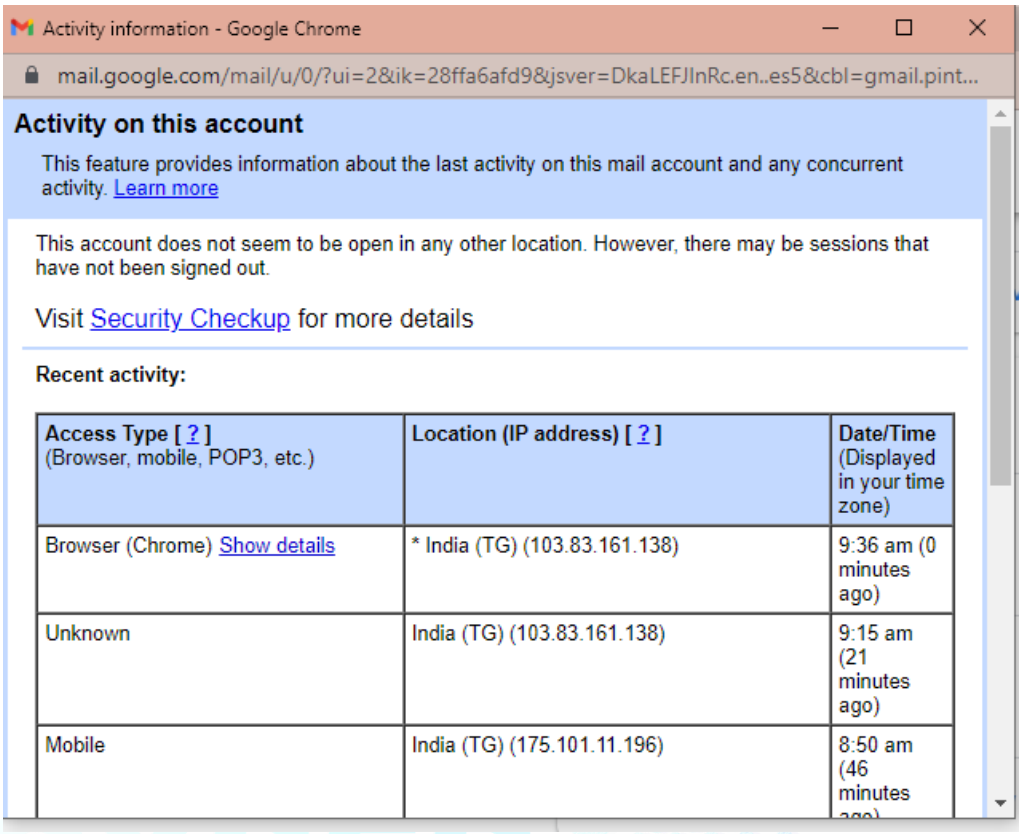


Figure 5: Facebook Logs

6. Gathering information about IP address: Whois lookup

Once we have obtained IP address of the suspect, we need to find out service provider of the IP address so that we can request for IPDR to service provider. To find out ISP we use process called **IP lookup**. There are multiple tools available on the Internet for Whois lookup, we have to simply search our IP address in the tool. Few tools for IP lookup are enlisted below:

- https://whois.domaintools.com/
- https://mxtoolbox.com/
- https://whois.whoisxmlapi.com/
- https://iplocation.io/ip-whois-lookup/
- https://nordvpn.com/ip-lookup/
- https://www.ip2location.com/demo/
- https://www.whatismyip.com/ip-address-lookup/
- https://www.whois.com/
- https://iplocation.io/

7. IPDR request to ISP

Once we know the service provider, further we need to write notice to ISP under 92 CRPC, to obtain IPDR of the same IP address. (Sample notice given below)

Details to Provide to ISP:

1. Public IP address
2. Exact time duration (to get more precise data)
3. Provide timestamp in 24 Hrs format (Most of the reports are machine generated which takes time into 24 Hrs format)

To: Airtel -Nodal

Subject: Re: Cybercrime PS- Request for IPDR details of IP Addresses – Reg (FRI no. [redacted])

Sir,

It is requested to furnish the IPDR of following IP addresses for the purpose of investigation.

Date	Time (IST)	IP address
05-03-2015	12:18 pm	106.220.189.164
09-03-2015	10:58 am	106.220.34.17
13-03-2015	08:21 pm	106.220.53.202

Early action will be highly appreciated.

Use 24 hrs format for timestamp

SHO
Cyber Crime PS,
Hyderabad

Figure 6: IPDR request wrong format

To: Airtel -Nodal

Subject: Re: Cybercrime PS- Request for IPDR details of IP Addresses – Reg (FRI no. [redacted])

Sir,

It is requested to furnish the IPDR of following IP addresses for the purpose of investigation.

Date	Time (IST)	IP address
05-03-2015	12:18:00	106.220.189.164
09-03-2015	10:58:00	106.220.34.17
13-03-2015	20:21:00	106.220.53.202

Early action will be highly appreciated.

SHO
Cyber Crime PS,
Hyderabad

Figure 7: IPDR request correct format

8. Analyzing IPDR:

IPDR are provided in various formats by Mobile Service Providers, but the analysis is same for all formats. During an IPDR analysis, few important fields need to be considered such as MSIDN, Device Identification number (IMEI, MAC), Server IP (Destination IP).

The above fields are important because, based on this information we can identify our suspect activity. Now let us understand the fields which we have been talking about.

- **MSISDN** – We can ascertain name and address of the suspect by investigating his mobile number. If mobile number of the suspect is obtained then investigation can proceed further with help of CDR, CAF and Current location.
- **IMEI** –This would help us understand the type of device being used by our suspect. An IMEI lookup can be made for tracking the make and model of the IMEI.

Mobile No.	IP Address	Cell1	IMEI	IMSI
'9330997971'	'2401:4900:519c:	'404-90-62	'3553430905162802'	'404909177262903'
'9330997971'	'2401:4900:519c:	'404-90-62	'3553430905162802'	'404909177262903'
'9330997971'	'2401:4900:519c:	'404-90-62	'3553430905162802'	'404909177262903'
'9330997971'	'2401:4900:519c:	'404-90-62	'3553430905162802'	'404909177262903'
'9330997971'	'2401:4900:519c:	'404-90-62	'3553430905162802'	'404909177262903'
'9330997971'	'2401:4900:519c:	'404-90-62	'3553430905162802'	'404909177262903'
'9330997971'	'2401:4900:519c:	'404-90-62	'3553430905162802'	'404909177262903'
'9330997971'	'2401:4900:519c:	'404-90-62	'3553430905162802'	'404909177262903'

Figure 8: IMEI column

IMEI column of the IPDR will help to recognise what model of phone the suspect is using with the help of IMEI lookup.

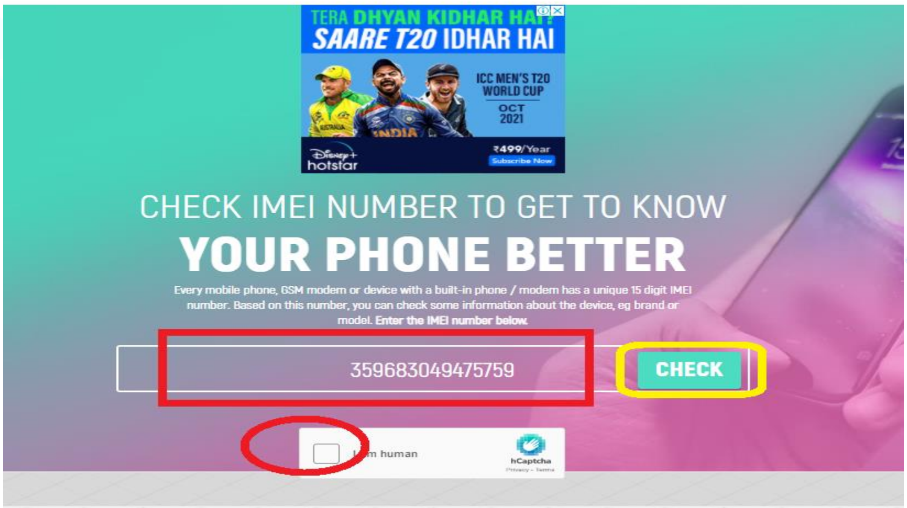


Figure 9: IMEI lookup

Figure 10: IMEI lookup result

- **Destination IP (Server IP)** – In this field an IP address is provided. By performing Bulk IP lookup, we can ascertain the website name being browsed by the suspect.

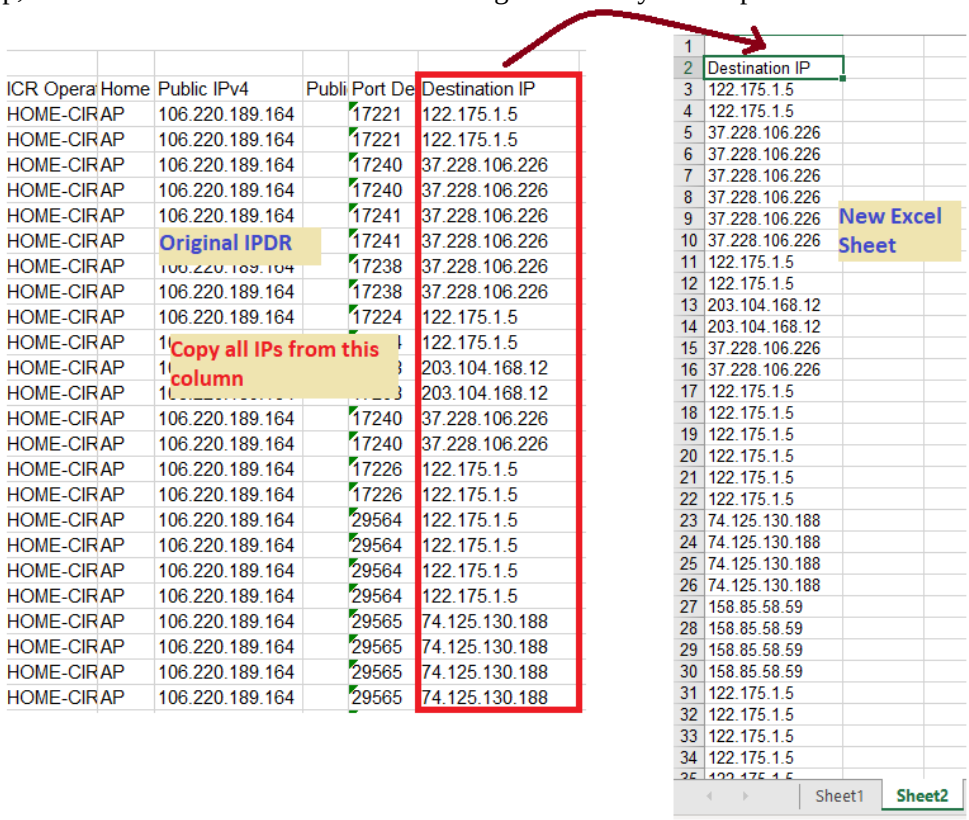


Figure 11: Bulk IP lookup

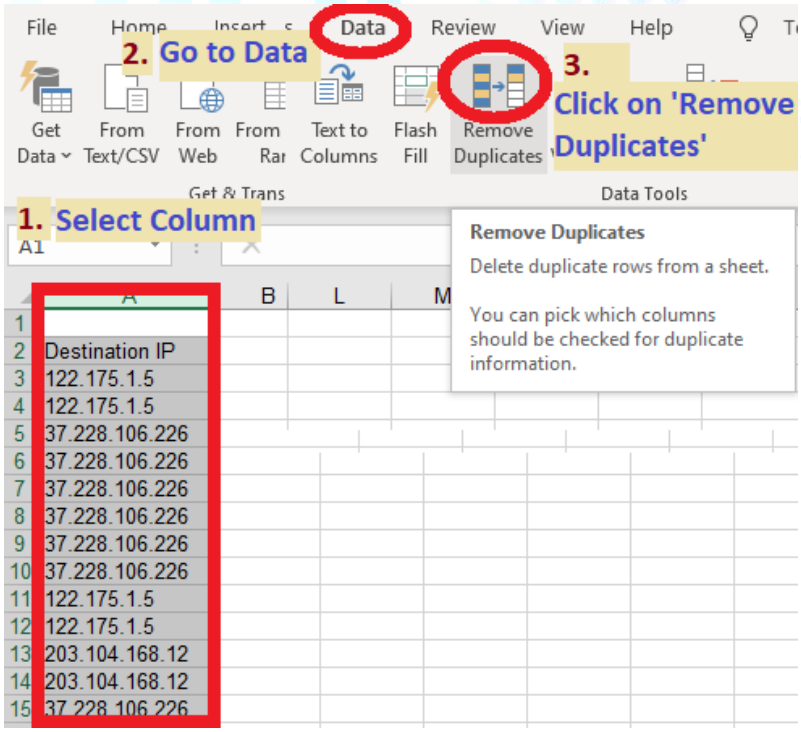


Figure 12: Bulk IP lookup

Bulk IP Lookup

If we want to find out service providers of multiple IP addresses simultaneously to avoid repetitive work, in that case we can use 'bulk IP lookup'. Few tools are enlisted below:

- https://www.infobyip.com/ipbulklookup.php
- https://app.ipapi.co/bulk/
- https://ip-geolocation.whoisxmlapi.com/bulk-gui (supports up to 100000 IPs)
- https://www.ipligence.com/iplocation

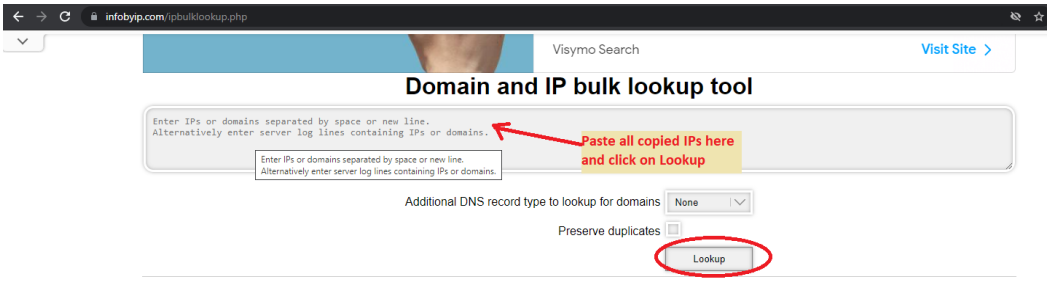


Figure 13 Bulk IP lookup

Also, to know websites hosted on given server IP we can perform 'Reverse IP lookup' for given destination IP. Tools for Reverse IP Lookup are enlisted below:

- MX Tools: https://mxtoolbox.com/ReverseLookup.aspx
- Domain Tools: https://reverseip.domaintools.com/
- Myip Tool: https://myip.ms/

Figure 14 Who is lookup

Result for: 66.254.103.176

Known Websites on IP - 66.254.103.176

No	Web Site	Website IP Address	Web Hosting Company / IP Owner	Web Hosting / Server IP Location	Record Update Time	World Site Popular Rating
1	18exgfs.com	66.254.103.176	Reflected Networks, Inc	USA	29 Sep 2021, 10:04	# 459,957
2	publicbfvideos.com	66.254.103.176	Reflected Networks, Inc	USA	27 Sep 2021, 00:50	# 817,723
3	indiangfvideos.com	66.254.103.176	Reflected Networks, Inc	USA	27 Sep 2021, 00:50	# 908,504
4	madporn.com	66.254.103.176	Reflected Networks, Inc	USA	27 Sep 2021, 00:50	# 1,748,292
5	pawnyoursextape.com	66.254.103.176	Reflected Networks, Inc	USA	27 Sep 2021, 00:50	# 2,211,046
6	latinobfvideos.com	66.254.103.176	Reflected Networks, Inc	USA	28 Sep 2021, 13:43	# 2,261,171
7	gf-members.com	66.254.103.176	Reflected Networks, Inc	USA	27 Sep 2021, 00:50	# 2,296,043
8	mygflikesitbig.com	66.254.103.176	Reflected Networks, Inc	USA	27 Sep 2021, 00:50	# 2,342,249
9	asianbfvideos.com	66.254.103.176	Reflected Networks, Inc	USA	28 Sep 2021, 20:05	# 2,449,489
10	squirtinggfs.com	66.254.103.176	Reflected Networks, Inc	USA	27 Sep 2021, 00:50	# 2,584,186

Total: 28 records *(show first 10 records only)* View All Records »

Figure 15 Result

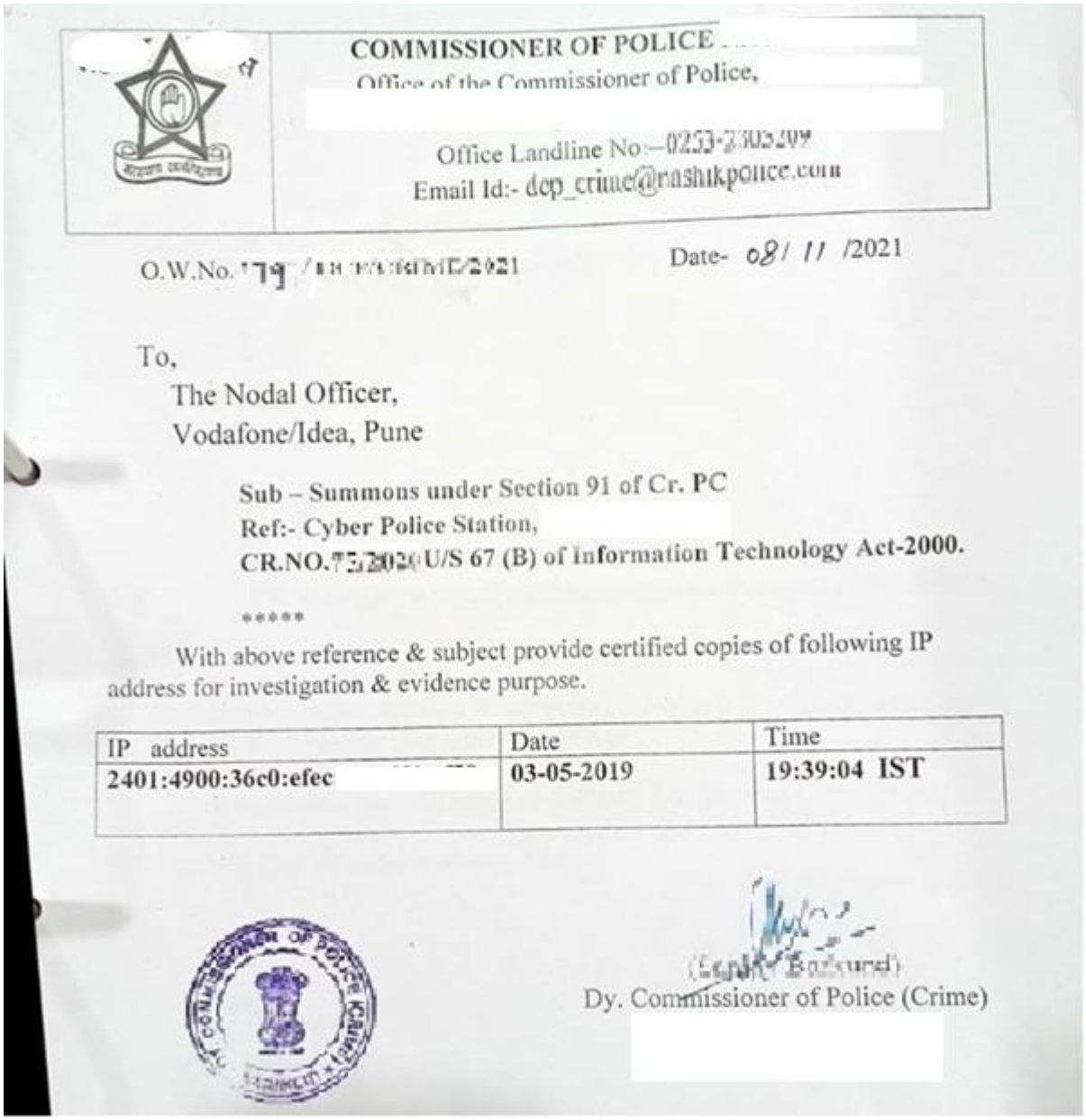
- **CGI** – It uniquely identifies a Location Area of a given operator's network. This is used to identify the location of the suspect.

9. Proprietary Tools used for IPDR analysis:

- Ms-Excel
- C5
- I9
- Purple
- CDR analysis and investigation by Ketan computers

10. Presenting IPDR as an Evidence in the Court of Law:

1. Notice to Nodal Officer u/s 91 CRPC



COMMISSIONER OF POLICE
Office of the Commissioner of Police,
Office Landline No:-0253-2303209
Email Id:- dcp_crime@nashikpolice.com

O.W.No. 179 /[illegible]/2021 Date- 08/ 11 /2021

To,
The Nodal Officer,
Vodafone/Idea, Pune

Sub – Summons under Section 91 of Cr. PC
Ref:- Cyber Police Station,
CR.NO. [illegible] U/S 67 (B) of Information Technology Act-2000.

*****

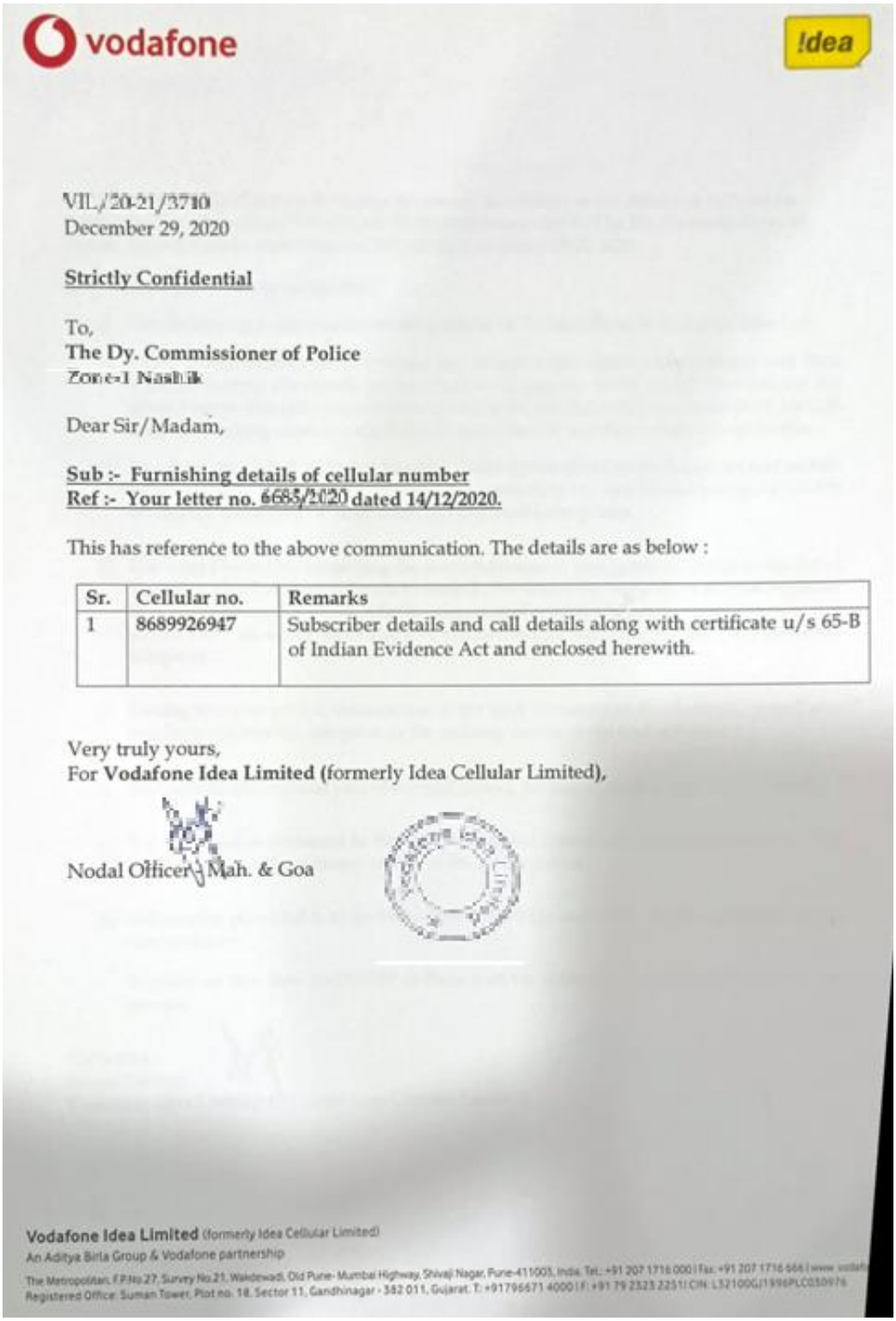
With above reference & subject provide certified copies of following IP address for investigation & evidence purpose.

IP address	Date	Time
2401:4900:36c0:efec	**03-05-2019**	**19:39:04 IST**

(Sanjay Barkung)
Dy. Commissioner of Police (Crime)

Figure 16: 91 crpc notice

2. Getting IPDR from Nodal officer
3. Analysing IPDR and getting findings
4. Getting certified copy of data which is actually case related and need to be submitted in court A certificate by Nodal officer as a reply to the official request to IO's notice u/s 91 CRPC, declaring all the documents he is providing as reply.



vodafone

Idea

VIL/20-21/3710
December 29, 2020

Strictly Confidential

To,
The Dy. Commissioner of Police
Zone-1 Nashik

Dear Sir/Madam,

Sub :- Furnishing details of cellular number
Ref :- Your letter no. 6685/2020 dated 14/12/2020.

This has reference to the above communication. The details are as below :

Sr.	Cellular no.	Remarks
1	8689926947	Subscriber details and call details along with certificate u/s 65-B of Indian Evidence Act and enclosed herewith.

Very truly yours,
For **Vodafone Idea Limited** (formerly Idea Cellular Limited),

Nodal Officer - Mah. & Goa

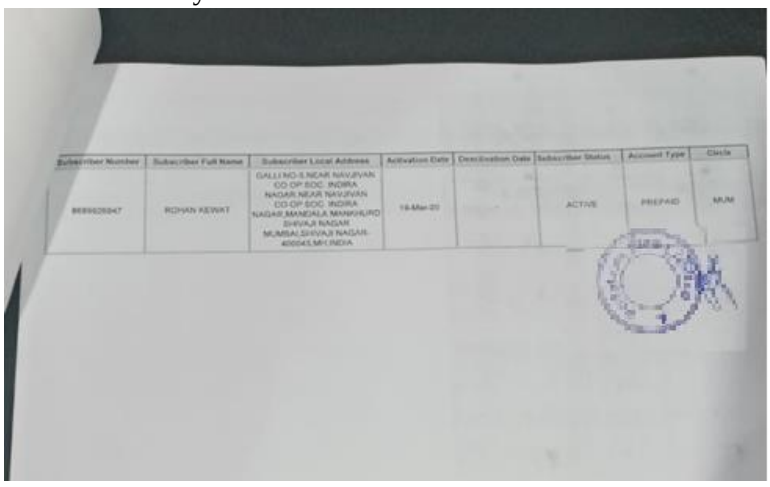
Vodafone Idea Limited (formerly Idea Cellular Limited)
An Aditya Birla Group & Vodafone partnership
The Metropolitan, F.P.No.27, Survey No.21, Wakdewadi, Old Pune- Mumbai Highway, Shivaji Nagar, Pune-411005, India. Tel.: +91 207 1716 000 | Fax. +91 207 1716 566 | www.vodafoneidea.com
Registered Office: Suman Tower, Plot no. 18, Sector 11, Gandhinagar - 382 011, Gujarat. T: +917969671 4000 | F: +91 79 2323 2251 | CIN: L32100GJ1996PLC030976

Figure 17 reply from service provider

Following are IPDR entries of suspect activities which needs to be presented in court hence asked for certified copy of the same from nodal officer.

Figure 18: certified copy from service provder

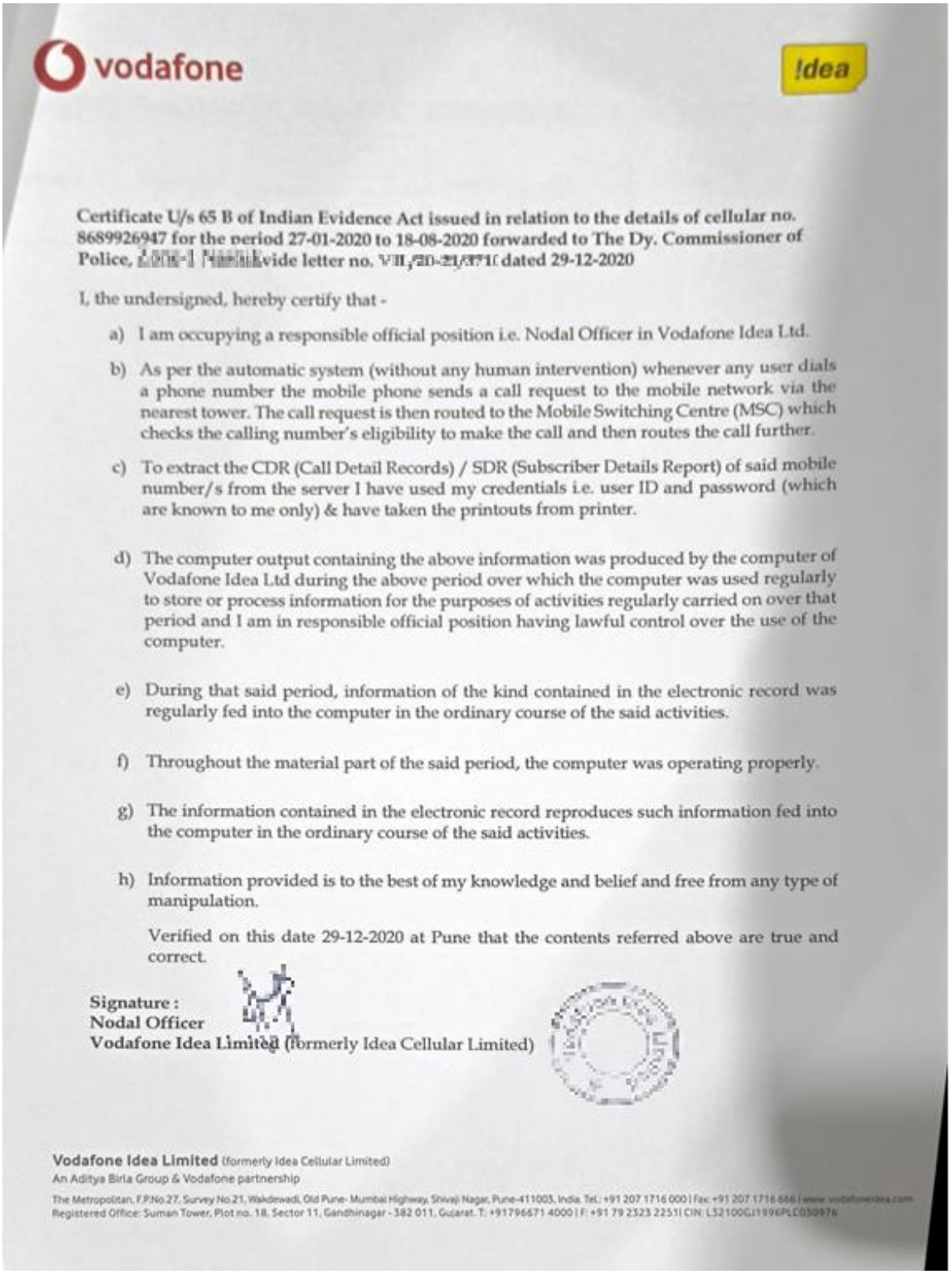
Suspect details in certified document by Nodal officer



Subscriber Number	Subscriber Full Name	Subscriber Local Address	Activation Date	Deactivation Date	Subscriber Status	Account Type	Circle
8698920847	ROHAN KEWAT	GALLI NO-5 NEAR NAVJIVAN CO OP SOC INDIRA NAGAR NEAR NAVJIVAN CO OP SOC INDIRA NAGAR MANDALA MANKHURD SHIVAJI NAGAR MUMBAI,SHIVAJI NAGAR, 400043,MH,INDIA	16-Mar-20	-	ACTIVE	PREPAID	MUM

Figure 19 certified details from service provider

5. 65B certificate for the same by Nodal officer



vodafone

idea

Certificate U/s 65 B of Indian Evidence Act issued in relation to the details of cellular no. 8689926947 for the period 27-01-2020 to 18-08-2020 forwarded to The Dy. Commissioner of Police, [illegible] vide letter no. [illegible] dated 29-12-2020

I, the undersigned, hereby certify that -

a) I am occupying a responsible official position i.e. Nodal Officer in Vodafone Idea Ltd.

b) As per the automatic system (without any human intervention) whenever any user dials a phone number the mobile phone sends a call request to the mobile network via the nearest tower. The call request is then routed to the Mobile Switching Centre (MSC) which checks the calling number's eligibility to make the call and then routes the call further.

c) To extract the CDR (Call Detail Records) / SDR (Subscriber Details Report) of said mobile number/s from the server I have used my credentials i.e. user ID and password (which are known to me only) & have taken the printouts from printer.

d) The computer output containing the above information was produced by the computer of Vodafone Idea Ltd during the above period over which the computer was used regularly to store or process information for the purposes of activities regularly carried on over that period and I am in responsible official position having lawful control over the use of the computer.

e) During that said period, information of the kind contained in the electronic record was regularly fed into the computer in the ordinary course of the said activities.

f) Throughout the material part of the said period, the computer was operating properly.

g) The information contained in the electronic record reproduces such information fed into the computer in the ordinary course of the said activities.

h) Information provided is to the best of my knowledge and belief and free from any type of manipulation.

Verified on this date 29-12-2020 at Pune that the contents referred above are true and correct.

Signature :
Nodal Officer
Vodafone Idea Limited (formerly Idea Cellular Limited)

Vodafone Idea Limited (formerly Idea Cellular Limited)
An Aditya Birla Group & Vodafone partnership
The Metropolitan, F.P.No.27, Survey No.21, Wakdewadi, Old Pune- Mumbai Highway, Shivaji Nagar, Pune-411003, India. Tel.: +91 207 1716 000 | Fax: +91 207 1716 666 | www.vodafoneidea.com
Registered Office: Suman Tower, Plot no. 18, Sector 11, Gandhinagar - 382 011, Gujarat. T: +917966671 4000 | F: +91 79 2323 2251| CIN: L32100GJ1996PLC030976

Figure 20 65B from service provider

Cyber Security

1.1. Introduction to Cyber Security

In 21st century almost all the information is getting shared using digital media and it is very necessary to safeguard this information by applying various measures of security to it. But as the technology is changing rapidly with the time, new measures to security are very high in demand. Information security is a very big aspect of computer science. There are various terms which are being used in information security. Let's have a look to the basic terms.[7]

- **Cyberspace:** It is the environment where the communication between various digital devices occurs.
- **Cyber Security:** Protecting the cyberspace against various threats and information leakage possibilities.
- **Access:** It is defined as the ability to make use of any computing system or resource.
- **Access Authority:** A person or body who monitors and grant the privileges to authorized bodies or persons to take access.
- **Active Attack:** Any kind of activity performed by unauthorized users which alters a system or data.
- **Active Data:** Data present on a computer system which is accessible to user in normal conditions. (Data Present on the system or undeleted data)
- **Acquisition:** The process of collecting data in computer forensic investigation generally this term is used in bit by bit copying or forensic working image of hard drive or any other media.
- **Ad Hoc Network:** A wireless network used to connect various wireless clients with each other's dynamically.
- **Administrative Account:** A user account on system which has all the privileges to access, modify or delete the data or change the system scenario.
- **Agent:** A program acting on behalf of a person or organization.
- **Alert:** Notification that a specific attack has been directed at an organization's information systems.
- **Ambient Data:** Data Which is not visible to normal user like data in file slack or unallocated clusters
- **Application:** A software program running on a system.
- **Archival Data:** The data which is generally compressed and kept on other media like CD or tape. Such data is not usually immediately available to the user and may need to be restored from the archival media to be accessed.
- **Attack:** Any kind of activity performed by an unauthorized user to get access to system, services or information. It may attempt to disrupt, degrade or destroy the information system.
- **Backdoor:** An undefined way to gain access to a computer system. It is a security risk.
- **Backup:** Copy of files and programs created to prevent loss.

[7] (NIST, 2013)

- **Bit-by-Bit Copy:** Copy of every consecutive sector of media device like hard drive.
- **Certificate:** A digital representation of information to uniquely identify and increase the trust over the information.
- **Chain of Custody:** A document which contains the chronological history of (electronic) evidence.
- **Checksum:** Value computed on data to detect errors or manipulation.
- **Computer Forensics:** A process of finding and collecting the evidences from computers which can be used in court of law against any criminal act.
- **Data:** A subset of information in electronic format that allows it to be retrieved or transmitted.
- **Event:** Any occurrence in network or system which can be observed.
- **Exploit:** Use of vulnerability to gain access to a system by using some malicious block of codes.
- **Hash Value:** It is a number generated from a string of text using any algorithm. Used to verify the integrity of any digital evidence.
- **Nonrepudiation:** It refers to a concept that piece of information is genuine.
- **Risk:** The probability that something unwanted may happen.
- **Threat:** An object, person or body or program which can harm a system.
- **Vulnerability:** Any weakness of the system containing the risk of attack.

1.2. Need of cyber security

Basically, information security performs four important functions for an organization. These functions are[8] –

- Protecting the organization's ability to function.
- Enabling the safe operation of applications running on the organization's IT systems
- Protecting the data the organization collects and uses
- Safeguarding the organization's technology assets

1.3. Models to fight cyber security issues

i) CIA Triad

Three of the primary concepts in information security are confidentiality, integrity, and availability, commonly known as the confidentiality, integrity, and availability (CIA) triad, as shown in Figure 1. The CIA triad gives us a model by which we can think about and discuss security concepts, and tends to be very focused on security, as it pertains to data.

[8] (Michael E. Whitman)

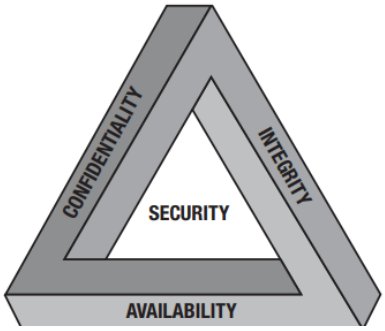


Figure 21 : CIA Triad (ISACA)

Confidentiality is the protection of information from unauthorized access or disclosure. Every different information has different level of confidentiality and it can change over the time. For example, ATM pin should be confidential up to personal level whereas the business plan can be discussed with some other trustworthy persons. Data must be protected from improper disclosure according to its sensitivity and applicable legal requirements. The confidentiality of digital information can be maintained using several different means, including access controls, file permissions and encryption.

Integrity can be defined as the protection of data from unauthorised alteration. For example, a message 'knife' should not be altered to 'wife'. Any infringement of integrity is huge on the grounds that it might be the initial phase in a fruitful attack against availability or confidentiality of the system. The integrity of digital assets can be controlled by logging, digital signatures, hashes, encryption and access controls.

Availability ensures the timely and reliable access to and use of information and systems without any interruption. Availability can be protected by the use of redundancy, backups and access control.

Requirement	Impact and Potential Consequences	Methods of Control
Confidentiality: the protection of information from unauthorized disclosure	Loss of confidentiality can result in the following consequences: • Disclosure of information protected by privacy laws • Loss of public confidence • Loss of competitive advantage • Legal action against the enterprise • Interference with national security	Confidentiality can be preserved using the following methods: • Access Controls • File Permissions • Encryption
Integrity: the accuracy and completeness of information in accordance with business values and expectations	Loss of integrity can result in the following consequences: • Inaccuracy • Erroneous decisions • Fraud	Integrity can be preserved using the following methods: • Access controls • Logging • Digital Signatures • Hashes • Encryptions
Availability: the ability to access information and resources required by the business process following consequences:	Loss of availability can result in the following consequences: • Loss of functionality and operational effectiveness • Loss of productive time • Interference with enterprise's Objectives	Availability can be preserved using the following methods: • Redundancy • Backups • Access Controls

Figure 22 : Impacts Related to CIA Triad (ISACA)

ii) AAA Model

The AAA simply refers to Authentication, Authorization, and Accounting. It is an another approach to cyber security.

Authentication simply means that whether a user is legitimate or not i.e. is the person is the same whom he is claiming to be? For example, 'X' has the power to use a computer system then authentication process will determine that the user who is trying to access is really 'X' or not. It may be done by the help of password, biometric or by any other means to identify a person or object.

Authorization simply means that whether the person who is trying to access the system is authorized to do so or not i.e. authorization defines the access rights of a person towards a system.

Accounting can be understood by means of keeping all the records of various events and activities taking place in the cyberspace of a particular organization in form of audit logs so that in case of any mis happening these logs can be used to identify the source and reason of incident. Events like log-in, log-out, insert/update/delete transactions, source IP, and other information are captured in audit logs.

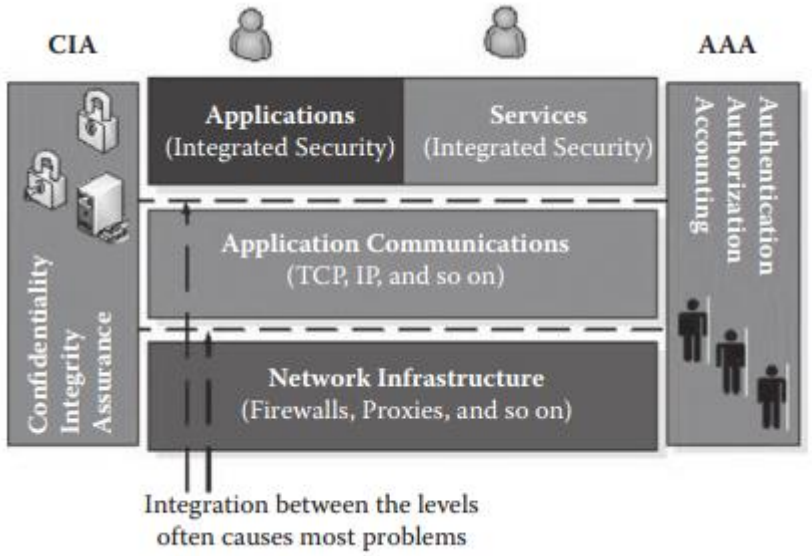


Figure 23 : Security Measures CIA & AAA (Michael E. Whitman)

AAA is a model which is generally used for network security, where many network access devices such as wireless access points can implement some form of AAA.

iii) THE PARKERIAN HEXAD MODEL

The Parkerian hexad, model introduced by Donn Parker in his book 'Fighting Computer Crime', is a somewhat more complex variation of the classic CIA triad. Where the CIA triad consists of confidentiality, integrity, and availability, the Parkerian hexad consists of these three principles, as well as possession or control, authenticity, and utility [3], for a total of six principles, as shown in Figure 4.

Confidentiality, Integrity and Availability have the same meaning as CIA model.

Possession or Control means the physical disposition of media on which data is stored.

Authenticity tells about the identification of authorized person.

Utility indicates the importance of data in terms of its uses.

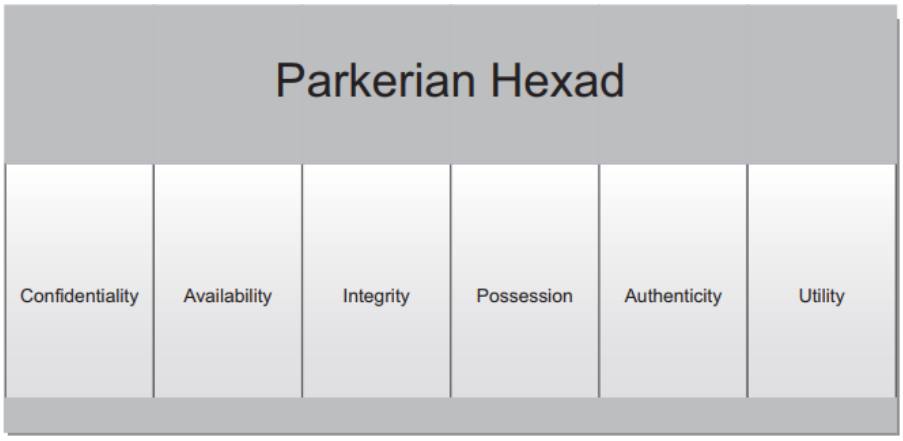


Figure 24 : The Parkerian Hexad (Andress, 2011)

iv) The lollipop Model

It is a defence model in cyber security. The most common form of defence, known as perimeter security, involves building a virtual (or physical) wall around objects of value. Perimeter security is like a lollipop with a hard, crunchy shell on the outside and a soft, chewy center on the inside, as illustrated in Figure 5.

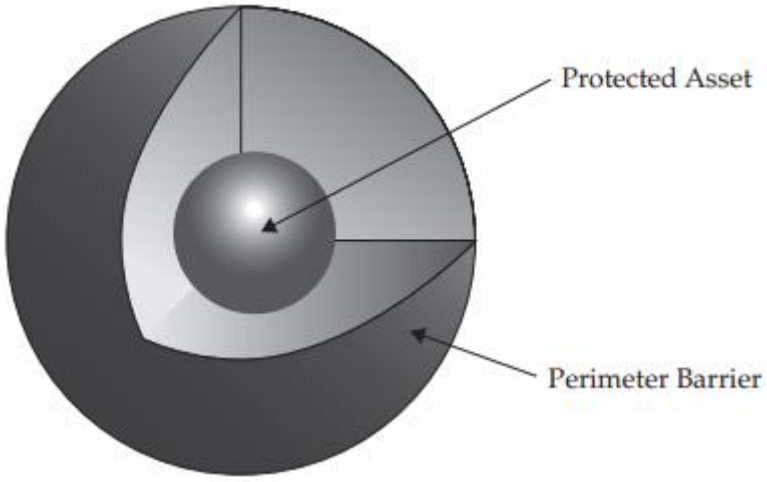


Figure 25 : The Lollipop Model

This model does not provide a lot security as once the perimeter is breached the attacker can access the protected asset easily.

v) The Onion Model

It is a better approach than Lollipop model. It is a layered architecture like an onion consisting various security features. It is also known as defence in depth.

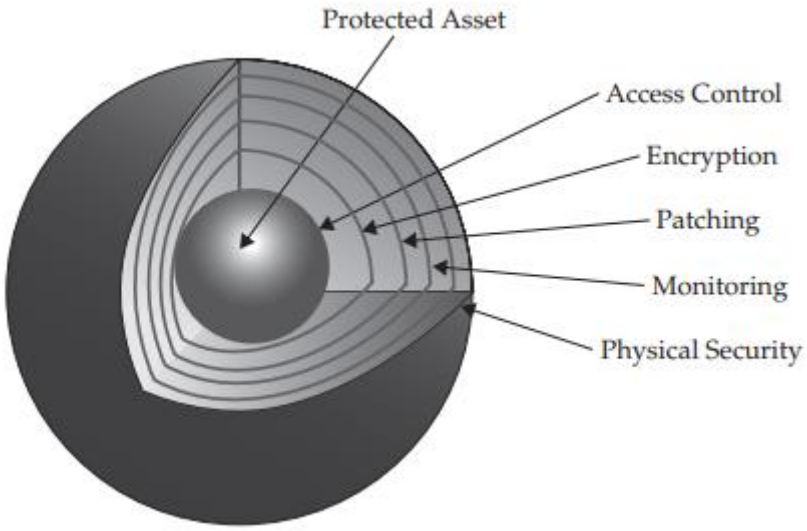
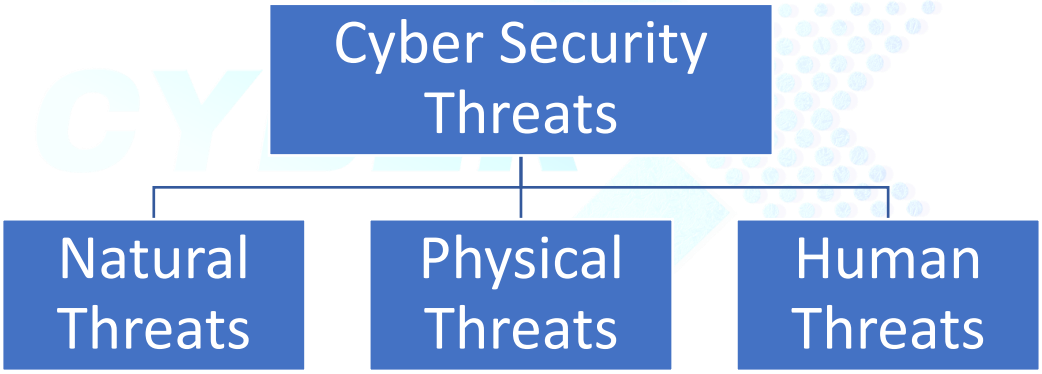


Figure 26 : The Onion Model of Defence

1.4. Cyber Security Threats

There are various threats to cyber infrastructure. These threats can be categorised as follows



Natural threats consist mainly of natural disasters like floods, storms, hurricanes, earthquakes, and so on. Physical threats include damage caused by to theft, fire, water spillage, or collision. Human threats include threats caused by human intervention, either intentionally or unintentionally.

1.5. Policy, Procedure, Guidelines & standards in cyber security framework

Policy	Standard	Procedure	Guideline
A very high-level statement and often generic in nature.	Usually defines the acceptable level of quality.	A detailed sequence of steps to accomplish a certain task.	Simply a piece of advice, suggestion, or a best practice for how to act in a particular situation.
Usually, all the users who are governed by a policy are mandated to follow it.	May or may not be mandatory to follow.	May or may not be mandatory to follow.	Merely recommended and left to the user's discretion whether to follow.
Examples: Internet security policy, email policy, clear desk policy	Examples: ISO 27001, PCI DSS	Example: Disaster recovery standard operating procedure (SOP)	Example: Guidelines on how to set a strong password.

Figure 27 : Policy, Procedure, Standard & Guidelines

1.6. Encryption

Encryption is a security measure which is essential for information security. It is the process of altering the data by using some predefined algorithm so that no any unauthorised person can access that data without the knowledge of decryption key.

Roughly speaking, there are two different broad types of encryption that are used on computers today

- Symmetric encryption relies on keeping keys totally secret
- Asymmetric encryption actually publicizes one key, but keeps some information private also

Neither is really "better" they just use different principles. In reality, both are vulnerable to attacks.

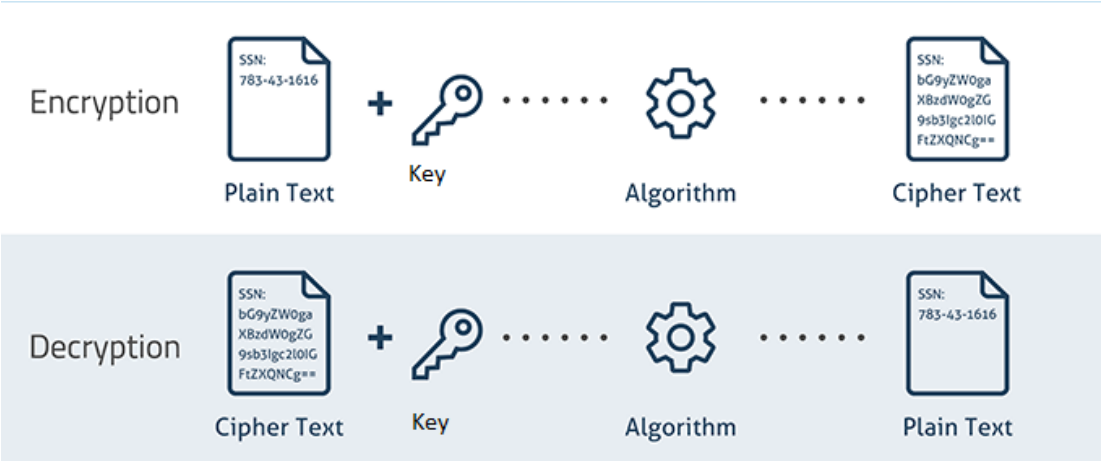


Figure 28 : Encryption & Decryption

The use of encryption technology to protect computer data is growing—and that fact presents a challenge for forensic investigators. Without a decryption key, forensic tools cannot be used

to find digital evidence. Even with the key, searching encrypted data can be tricky and time consuming. Below are some answers to common questions about trends in the use of encryption and what investigators can do to get as much evidence as possible from an encrypted file or drive. The use of encryption provides a different kind of challenge for the forensic investigator. Here, data recovery is only half the story, with the task of decryption providing a potentially greater obstacle to be overcome. Encryption, whether built in to an application or provided by a separate software package, comes in different types and strengths. Some of the most commonly used applications provide encryption protected by passwords that can be readily defeated by investigators with the right tools and the time to use them. Other types of encryption, readily available to the general public, can be configured and used to create encrypted data that goes beyond the ability of the professional investigator to decrypt it using software.

Nevertheless, in these cases it may still be possible to decrypt data by widening the scope of the investigation to include intelligence sources beyond the computer under investigation. For example, public key encryption can be used to create highly secure, encrypted data. To decrypt data encrypted in this fashion a private key and passphrase is needed. The private key may be found on the suspect's machine or backed up to removeable media. Similarly, the passphrase may be recorded somewhere on the computer in case it is forgotten or may be written down somewhere and kept in a nearby location.

Use of Encryption growing in popularity

Corporations and computer users like the idea of encryption as a way to protect their sensitive or personal data from breaches, but the average user still sees this technology as burdensome or too time consuming to implement on a constant basis. So the move to encryption is not necessarily coming from the users. Instead it is coming from hardware and software companies who are embedding encryption technology into their products. The BlackBerry is a good example because all data is encrypted and this protection is automatic. More important, the use of the encryption technology is completely invisible to the user. As investigators, we are limited to the information on the device that we can access. If a hard drive is fully encrypted, we have no easy access to the stored data and our investigative options become limited. The first thing an investigator must do is to determine the level and extent of the encryption. Weak passwords can be cracked, but if the user has implemented a strong password it becomes almost impossible to access via brute force methods. It could be that just a few files are encrypted and there could be unencrypted copies elsewhere on the device. The user could also be a creature of habit and use the same set of passwords. These passwords can be quickly located in easily decipherable formats throughout the system. In all cases, though, I tell investigators that digital evidence is just one piece of the body of evidence in a case. Don’t fall into a trap where you spend too much time trying to decrypt a potentially probative item, when valuable unencrypted data may be found by simply continuing your examination.

Again, most users, including criminals, like the idea—but they just don’t have the knowledge or patience to implement it on a continued-use basis. The majority of the encryption we have seen used is in corporate systems and typically it is not an issue as the company has the passwords. This allows us to leverage the software and hardware tools they already have to easily access the data. Once the data is decrypted an investigator can apply a forensic toolset to gather and analyse the stored data.

There is always a slight chance when working with electronic media that data may be damaged or corrupted. The best advice I can give is to keep your evidence-handling procedure reasonable and defensible. Reasonable means using industry-standard tools. Defensible means you thoroughly documented the process. The bigger concern is that all of the data on the drive must be decrypted—and that can take hours. As you work a drive to decrypt this data, that drive could fail. Thus, it is important to be sure that your forensics tool supports encrypted data, which makes the process more seamless while contributing to the defensibility of the procedure. For many investigator s this is a new area. First, they should try to determine the extent of the encryption. There are many tools that allow you to encrypt the whole hard drive, a portion of the disk space, or even individual files. An investigator should first determine whether the whole drive is encrypted; if not, then they can scan for encrypted files. If encryption software like Encrypt It or TrueCrypt is on the drive, then there is a reasonable expectation that the user may have encrypted some of the content. Examiners can analyze the use of these applications and learn just how often and when an encryption program has been run. This can lead to a search for other digital files that were being accessed around the same time periods.If there is encrypted information on the disk, the next step is to use any known passwords. Defendants to divulge their personal passwords, but people are creatures of habit and they tend to use a single small set of passwords for everything.

These can be found in many places on the hard drive where they are easily deciphered. For example, many web browsers allow a user to store their passwords for various websites. The repository where those passwords are stored is generally easy to crack. The investigator has more options if certain files are encrypted. Computers are redundant by nature. The data that is inside the encrypted volume had to come from somewhere (another device for example) or it might be spread across the drive outside of the encrypted file. For example, Microsoft Word automatically writes copies of a document to a hard drive as it is being modified.

This way, the user has a backup if the computer fails. When that document is closed, the program deletes all the temporary versions. If you encrypt the document and you delete the original document, your machine still has the deleted files that can be accessed by using forensics. Another example: When a suspect is working with digital photos, thumbnail images

are always being created. Finding non-encrypted copies of files will not always be possible, but investigators can and should look for copies of the data across all relevant devices.

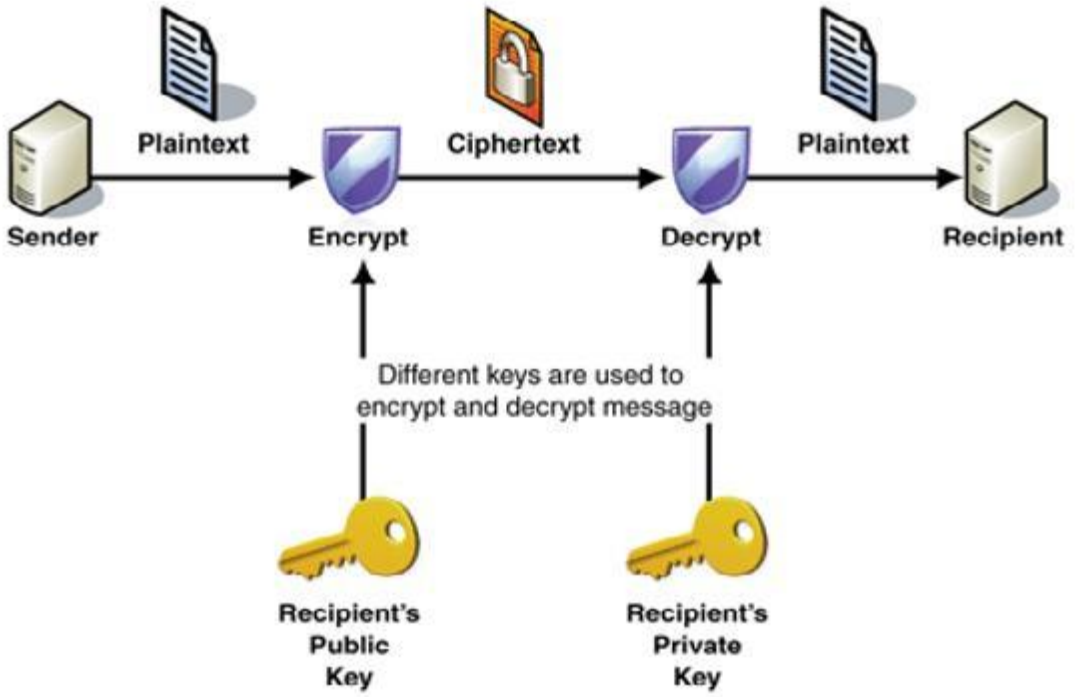


Figure 30 : Process of Encryption & Decryption

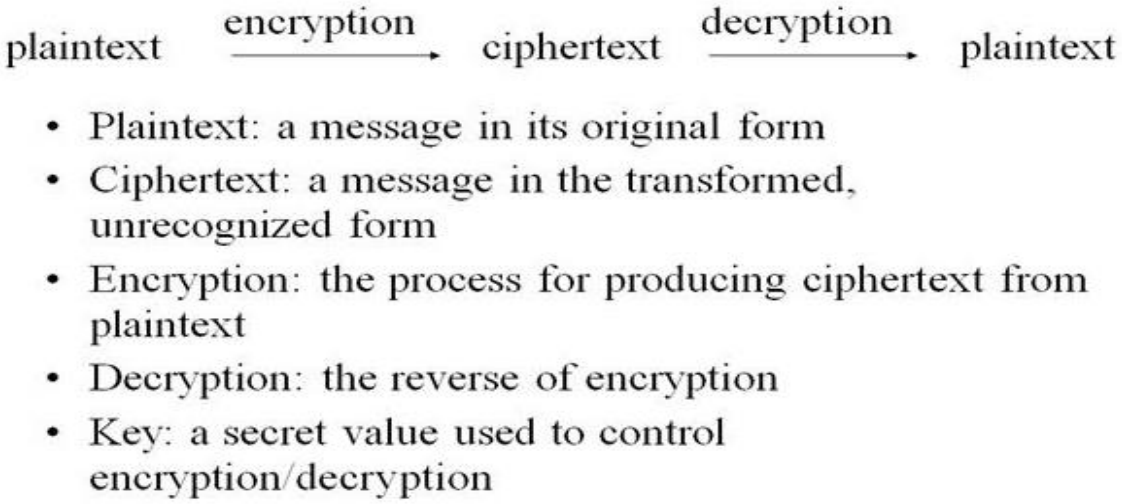


Figure 29 : Line Diagram of Encryption & Decryption

Encryption often presents challenges for analysts. Users might encrypt individual files, folders, volumes, or partitions so that others cannot access their contents without a decryption key or passphrase. The encryption might be performed by the OS or a third-party program. Although it is relatively easy to identify an encrypted file, it is usually not so easy to decrypt it. The analyst might be able to identify the encryption method by examining the file header, identifying encryption programs installed on the system, or finding encryption keys (which are often stored on other media). Once the encryption method is known, the analyst can better

determine the feasibility of decrypting the file. In many cases, it is not possible to decrypt files because the encryption method is strong and the authentication (e.g., passphrase) used to perform decryption is unavailable. Although an analyst can detect the presence of encrypted data rather easily, the use of steganography is more difficult to detect. Steganography, also known as steg, is the embedding of data within other data. Digital watermarks and the hiding of words and information within images are examples of steganography. Some techniques an analyst can use to locate stegged data include looking for multiple versions of the same image, identifying the presence of grayscale images, searching metadata and registries, using histograms, and using hash sets to search for known steganography software. Once certain that stegged data exists, analysts might be able to extract the embedded data by determining what software created the data and then finding the stego key, or by using brute force and cryptographic attacks to determine a password. However, such efforts are often unsuccessful and can be extremely time consuming, particularly if the analyst does not find the presence of known steganography software on the media being reviewed. In addition, some software programs can analyse files and estimate the probability that the files were altered with steganography.

The process involves

- Finding Unencrypted Copies of Data
- Obtaining Encryption Passphrases
- Passphrase Guessing
- Recovering Encrypted Network Traffic

Type of encryption to use and when

- If you are encrypting a laptop to protect data against possible theft: use whole disk encryption.
- If you are sending a sensitive document by email: use an encrypted folder or small disk image.
- If you are sending a sensitive document by email: one of you uses a PC, the other a Macintosh, use Truecrypt.
- If you are carrying some work data home on a USB key: use an encrypted folder or small disk image.
- If as above, but your USB key is an encrypted type: use the USB key accord to it's user instructions
- You use cloud storage like dropbox, or Google drive to store sensitive information: use an encrypted folder or small disk image

Encryption can be performed on:

- Folders
- Volumes
- Internet traffic
- Drop box (or other cloud storage)
- Servers
- File Sharing

- USB
- CD/DVD
- Web based VPNs
- Emails
- Gmail messages
- Word, Excel, and PowerPoint documents
- PDF
- Images (PhotoCrypt)
- Graphic files

Full Disk Encryption Security Model

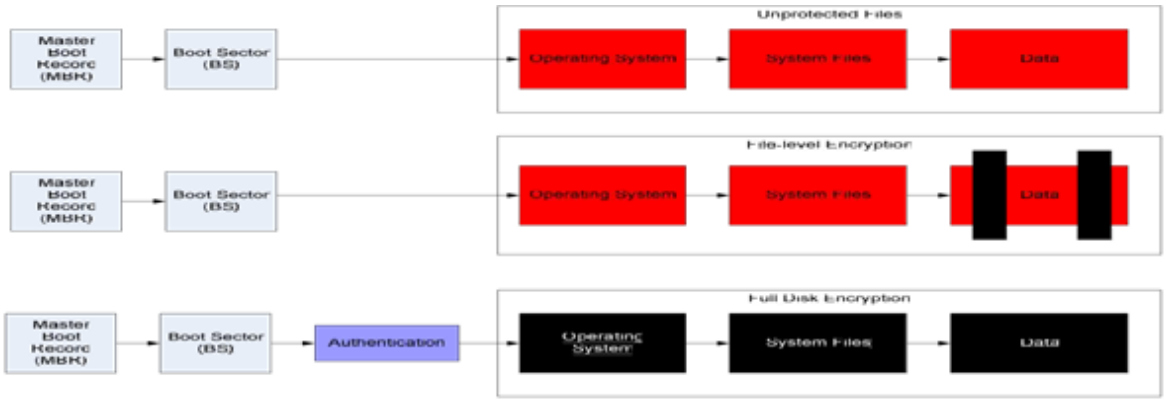


Figure 31 : Full Disk Encryption Security Model

Step Action of Full Disk Encryption using True Crypt

Download and Installation

Download the TrueCrypt installer from **http://www.TrueCrypt.org/.**

Ensure the integrity of the download by checking it against the download signature. Install on your system.

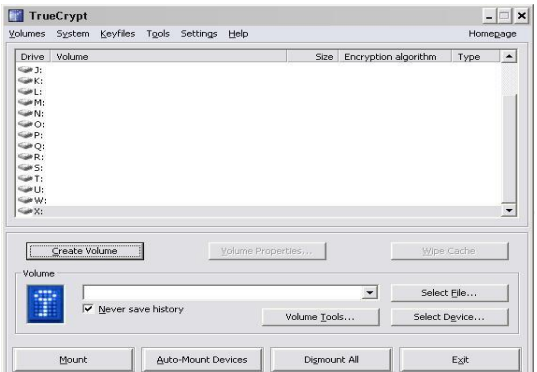
Full Disk Encryption

This guide is for Windows Single boot systems. If you have multiple partitions or alternative operating systems contact IT Services Security Team for advice.

We advise that all important data is backed up before starting this process.

Step 1

Run the application. Select “Create Volume” from the dialogue screen. This launches the TrueCrypt Volume Creation Wizard.



Step 2

Select the "Encrypt the system partition or entire system drive".

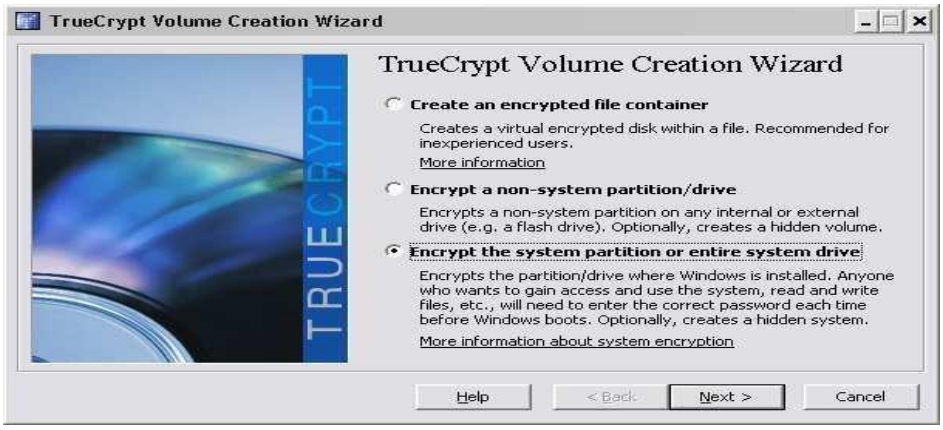


Figure 13 : Step 2

Step 3

Select the "Normal" option on the Type of System Encryption dialogue.

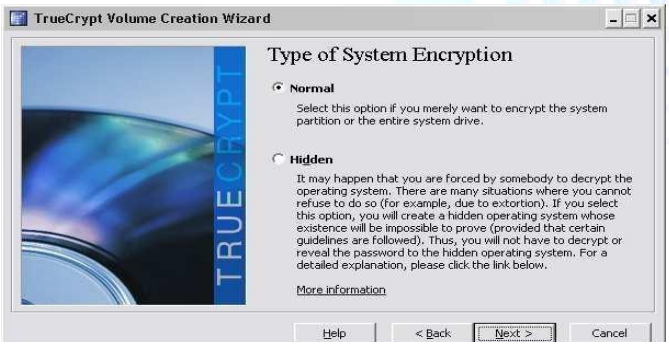


Figure 33 : Step 3

Step 4

Select "Encrypt the whole drive" on the Area to Encrypt dialogue.

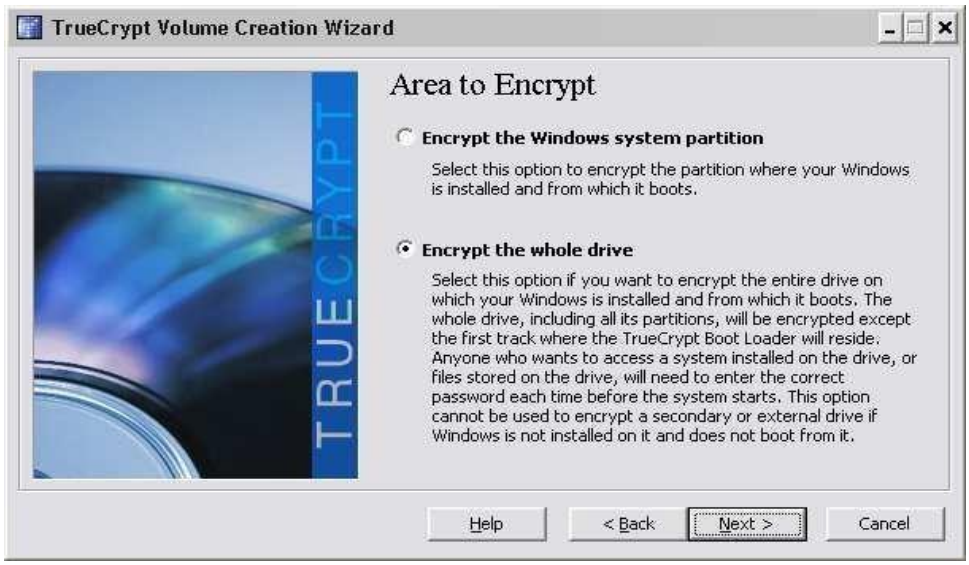


Figure 34 : Step 4

Step 5

Select what best suits your system. Some laptops will have an HPA (Host Protected Area) on the disk that will contain recovery tools for the system. If you select "Yes" from the above dialogue you will see the below.

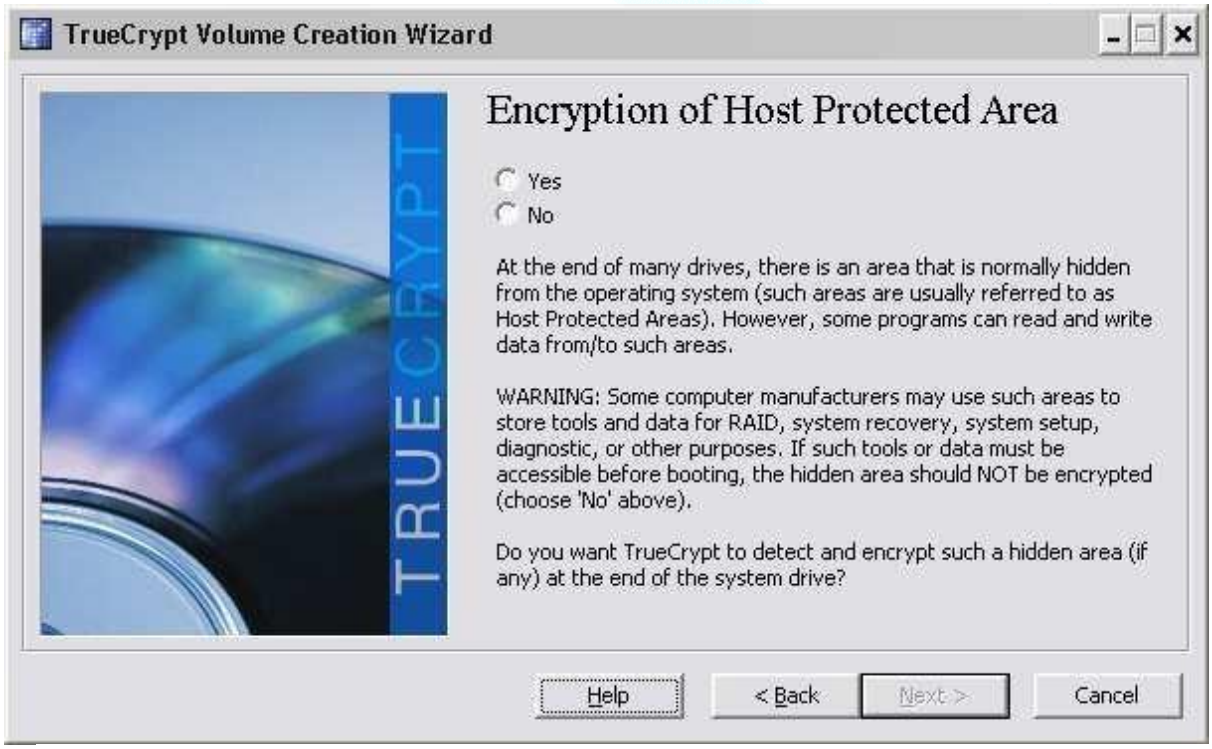


Figure 35 : Step 5

Step 6

If you selected "Yes" you will see the following dialogue before progressing to the one below.

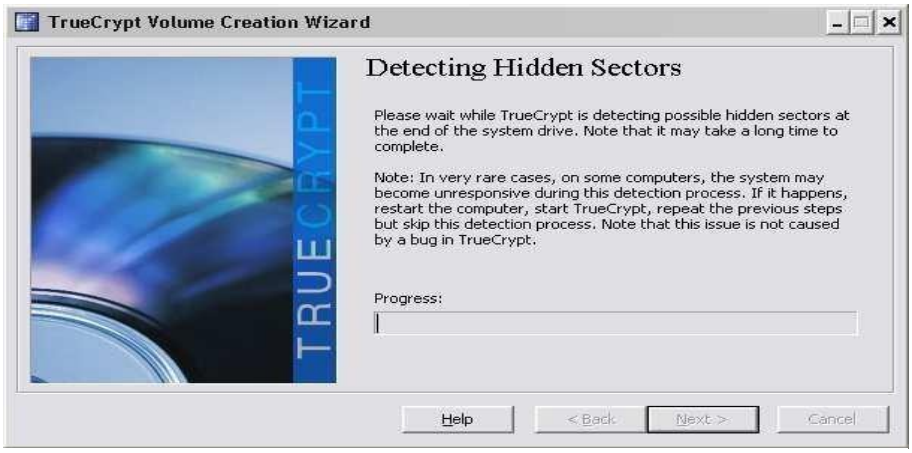


Figure 36 : Step 6

Step 7

Select "Single-boot" from Number of Operating Systems dialogues.

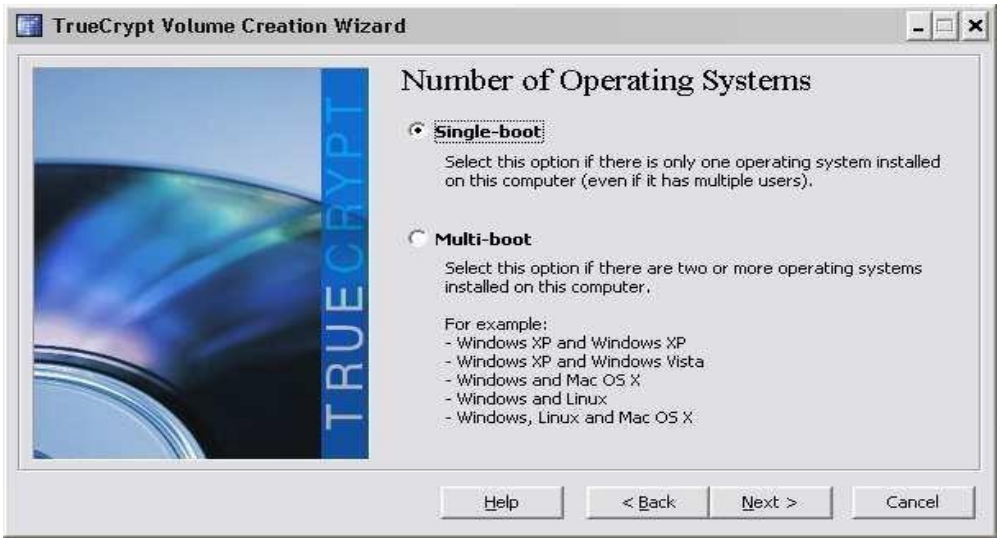


Figure 37 : Step 7

Step 8

On the Encryption Options dialogue Select "AES" for the Encryption Algorithm and "RIPEMD-160" for the Hash Algorithm. This will give you the best performance from your system whilst still providing an excellent encryption level.

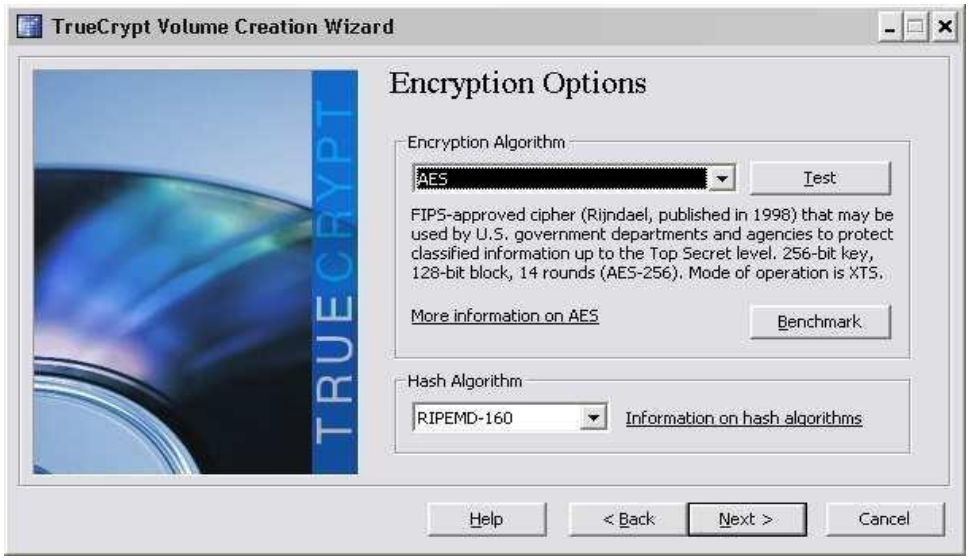


Figure 38 : Step 8

Step 9

Set a password; ensure that it has a reasonable level of complexity.

IMPORTANT NOTE: If this password is lost the information on the hard drive will NOT BE RECOVERABLE, and lost forever. You have been warned!

Figure 39 : Step 9

Step 10

Follow the on screen instructions for the Collecting Random Data dialogue, then press "Next".

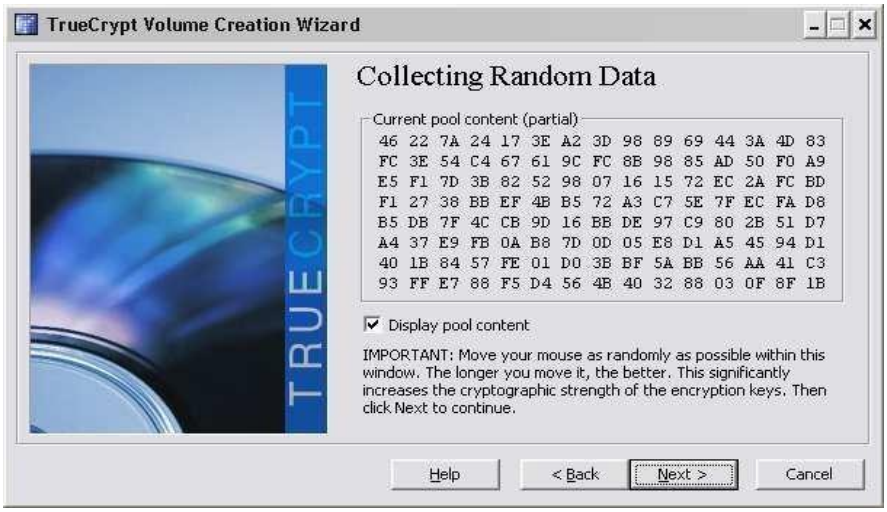


Figure 40 : Step 10

Step 11

Select “Next” on the Keys Generated dialogue.

Figure 41 : Step 11

step 12

You must now create a rescue disk for the encrypted disk. This will contain the necessary boot loader and tool to recover from a system fault and will allow you to mount and decrypt the disk. You will still require the password to perform these actions.

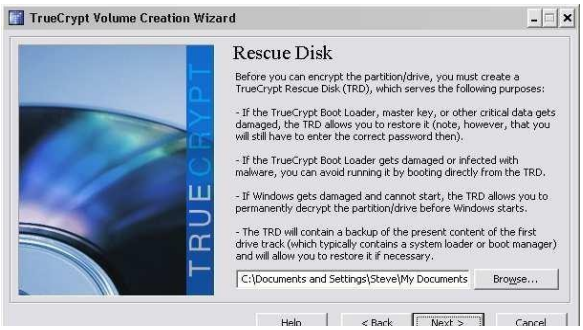


Figure 42 : Step 12

Step 13

TrueCrypt will not let you proceed with the process until you have verified the rescue disk.

Figure 43 : Step 13

Step 14

Once the test has been performed TrueCrypt will you will move onto the next dialogue.

Figure 25 : Step 14

Step 15

TrueCrypt will then ask if you want to securely erase any files during the encryption process, if this is a new machine then select none, otherwise use your discretion.

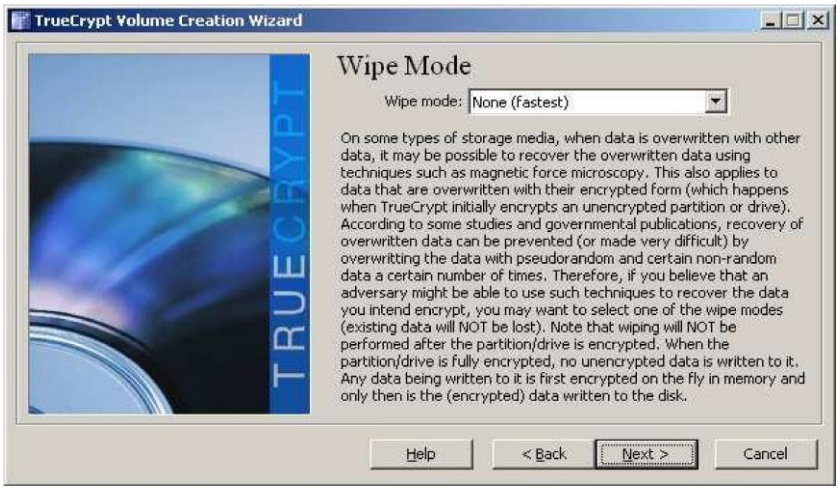


Figure 44 : Step 15

Step 16

TrueCrypt will first perform a test to ensure that everything is working correctly, and that you remember your password, before it encrypts the drive.

Figure 45 : Step 16

Step 17

Read and agree to the following. We suggest that you print or save this to another location for future reference.

Figure 46 : Step 17

Step 18

Restart the system.

Figure 47 : Step 18

Step 19

Once you have entered the boot password and the system is back up you will be presented with the following dialogues.

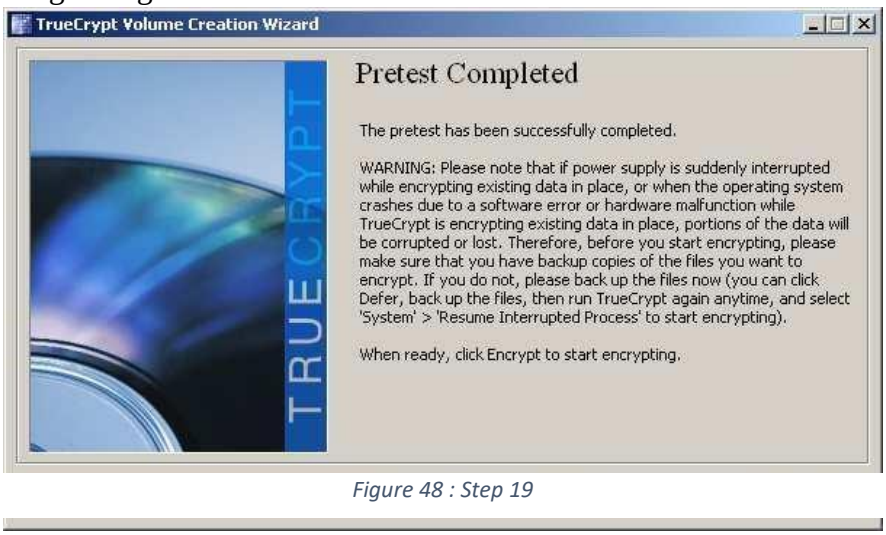


Figure 48 : Step 19

Step 20

It is now time to encrypt the drive. Read the text in the dialogue box and action as appropriate.

Figure 49: Step 20

Step 21

The encryption process starts.

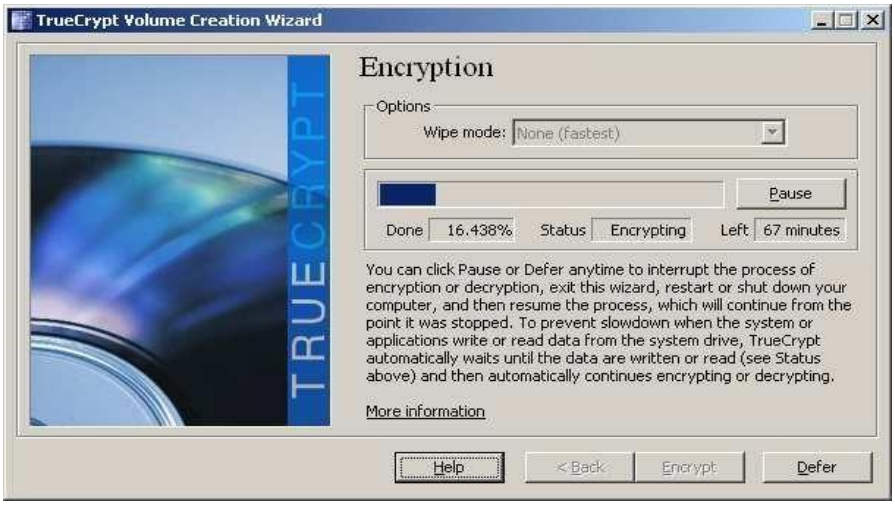


Figure 50 : Step 21

Step 22

You will receive the following dialogue if the process has succeeded.

Figure 33 : Step 22

Once installed, after the BIOS, you will be presented with a new boot loader directly on boot up. It will look similar to this. Enter your password to boot into the system.

Figure 51 : TrueCrypt Encryption Completed

ENCRYPTED DISK DETECTOR

A command-line tool that can quickly and non-intrusively check for encrypted volumes on a computer system during incident response.

Encrypted Disk Detector: What does it do?

Encrypted Disk Detector checks the local physical drives on a system for TrueCrypt, PGP, or Bitlocker encrypted volumes. If no disk encryption signatures are found in the MBR, EDD also

displays the OEM ID and, where applicable, the Volume Label for partitions on that drive, checking for Bitlocker volumes.

Supported Encrypted Volumes

Currently, Encrypted Disk Detector detects TrueCrypt, PGP, Safeboot, and Bitlocker encrypted volumes.

Ref: - https://www.magnetforensics.com/free-tool-encrypted-diskdetector/

Steps Action:

Step 1

Click on exe file. A dialogue box will open

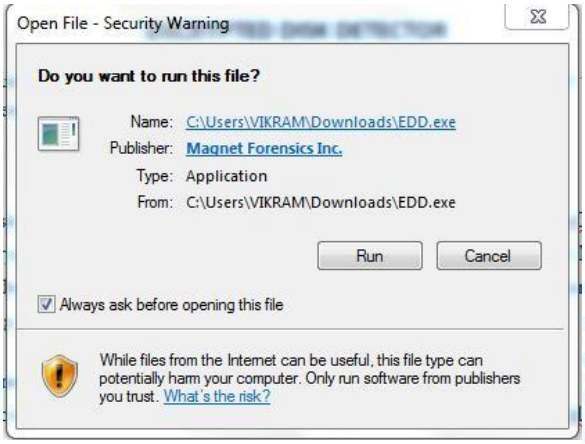


Figure 52 : File Run Permission Box

Step 2

Click on Run and it will start detecting the encrypted drives.

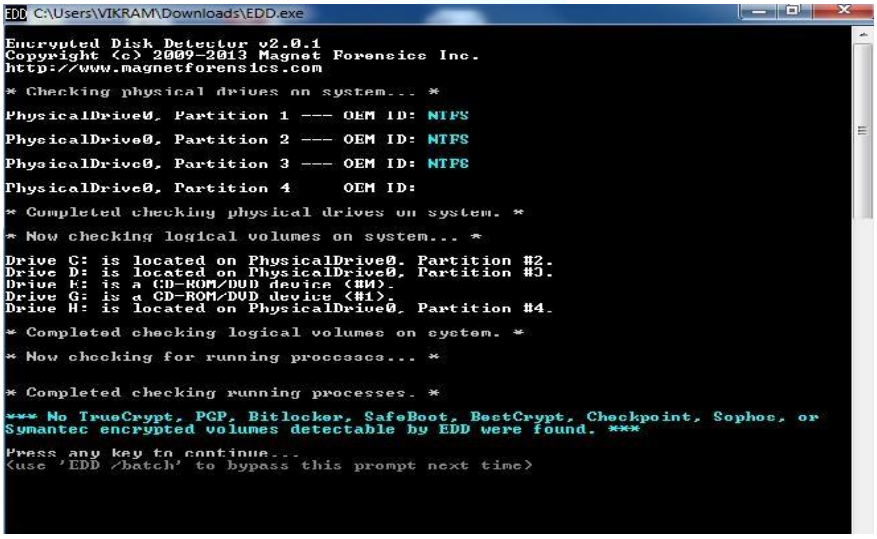


Figure 53 : EDD CMD Window

Summary: No Encrypted Volume is Found

1.7. Hashing

Hashing is the process of converting a data into fixed length value with the help of an irreversible algorithm which is known as hash function. In cyber security or digital forensics hashing techniques are used to define integrity of a data source (i.e. whether the data source is tempered or not).

The hash function is a kind of mathematical algorithm which is used to map the data of arbitrary size to a fixed size value. A good hash function must have following two attributes –

- The values generated by hash function should be unique (i.e. no two values for same data should be there for same algorithm and no two data sets should have same hash value).
- It should be irreversible and of fixed length.

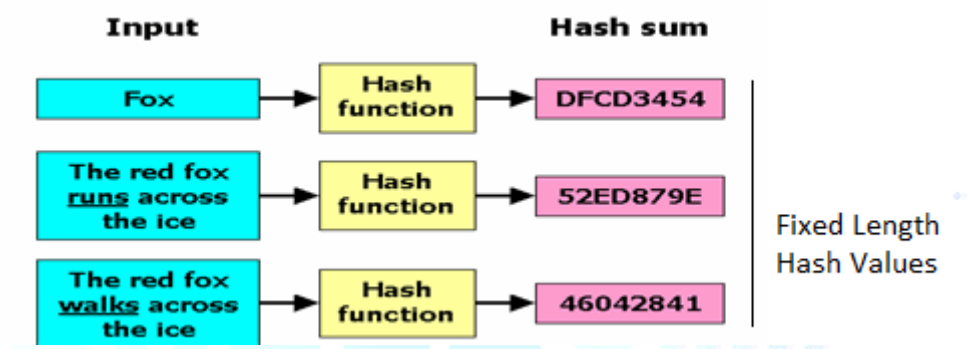
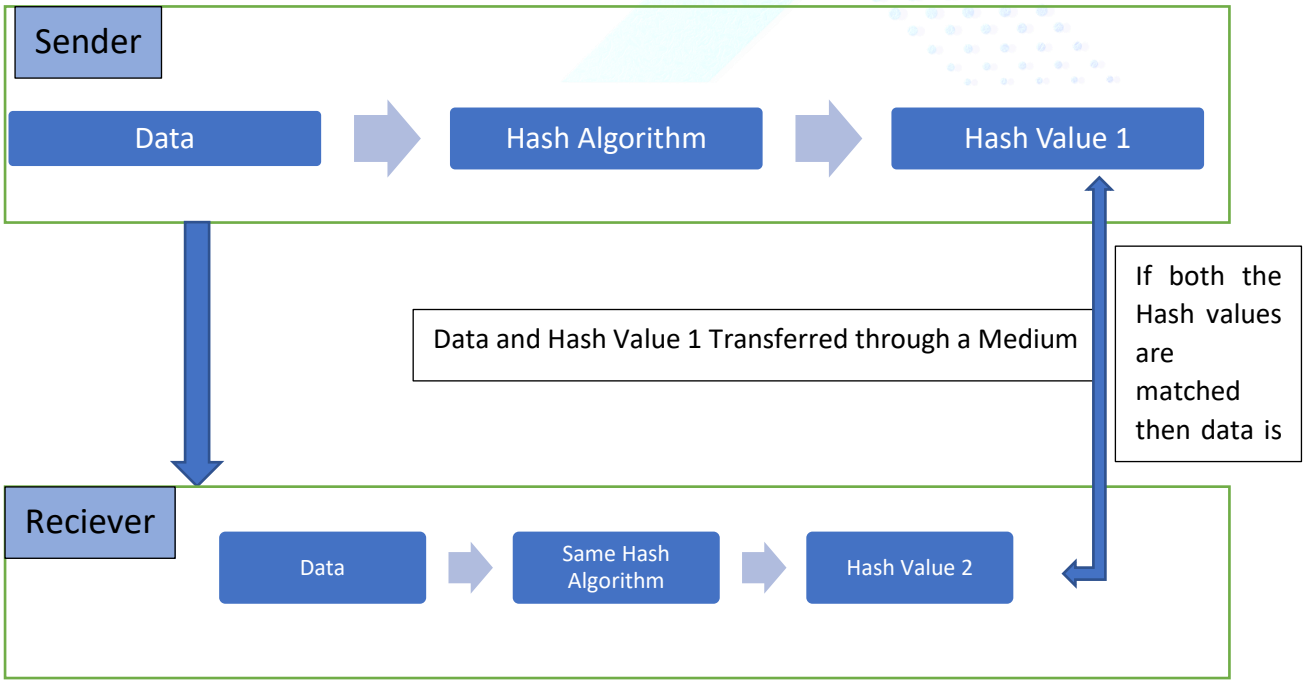


Figure 54 : Example of Hashing

How hashing works to check integrity



Popular Hash Algorithms

There are multiple hashing algorithms available with different result size. Some popular hash functions with their output size are as follows –

Name of Hash Function	Output Size (in Bit)
BLAKE2b	512
BLAKE2s	256
MD2 / MD4/ MD5	128
SHA-0 / SHA-1	160
SHA 512	512
SHA3 (Different Functions)	224 / 256 / 384 / 512

Hash Calculating tool (hashcalc)

Hashcalc is an open source hash calculator used to calcu;ate various hash values of a datasource (file) or text string.

- Open Hashcalc and select data source. (It may be any file or disk or any text or hex string). Here we are selecting file as data source.
- Browse the path for the file and click on calculate button to get various hash values.

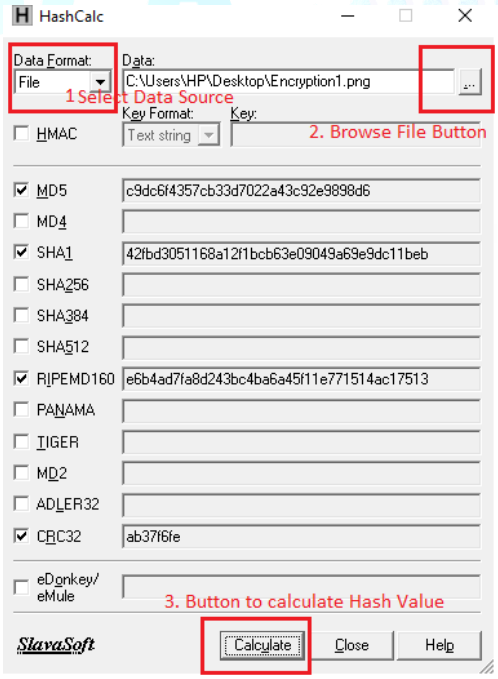


Figure 38 : HashCalc

1.8. digital signature

A Digital Signature is a method to ensure data authenticity. A digital signature is created by generating a hash (message digest) against the data and then encrypting this digest using the cryptography (public or private) key. This signature is then appended to the data.

Once the recipient has received the data + signature they generate a hash against the data, as well as decrypting the signature using their cryptography (public or private) key. These digests are then compared to ensure data authenticity. Data that is appended to a message, made from the message itself and the sender's private key, to ensure the authenticity of the message

1.9. Public Key Infrastructure (PKI) or Digital Certificates

A Digital certificate is a form of electronic credentials. Digital certificates are issued by a Certification Authority (CA) and are used to encrypt and sign digital information. Digital Certificates typically contain the Owner's public key/name, expiration date of the public key, Name of the issuer (CA), Serial number and the Digital signature of the issuer (CA). A representation of a sender's authenticated public key used to minimize malicious forgeries

Digital certificate is a digital identity of a person much like a driver license. It can also be issued to a computer or a network device identifying it while communicating. A digital certificate is issued by a Certification Authority (CA) complying with the X.509 standard and it normally contains mainly the following information:

- Public key of the certificate owner
- Name of the owner
- Validity “from” and “to” dates
- Name of the issuing authority
- Serial number of the certificate
- Digital signature of the issuing authority
- Digital Signature Algorithm
- Custom information

Digital certificate or digital signature relies on digital cryptography; a sophisticated, mathematically proven method of encrypting and decrypting information. A digital certificate contains information about the owner’s identity e.g., their name, email address, the date the digital certificate was issued and the name of the Certifying Authority that issued it. The certificate also contains the public key. The private key (correspond to the public key) is stored on the user's computer hard disk or on an external device such as a smart card. The user retains the control of the private key and it can only be used with the issued password or PIN.

As the above-mentioned processes require a public key hence a need of a Public Key Infrastructure (PKI) arises which is responsible for managing all aspects of digital certificate issuance, publication, revocation, renewal etc, in short managing the full lifecycle of digital certificates. Every Digital certificate usually can be chained to a Root CA (which is the final trust point and issues a certificate to itself). The Root CA then issues a certificate to one or more subordinate CA s) which is used to issue certificates for end-entities, which can be human users, network devices, machines, databases or other software components. There are also different types of certificates like CA certificate, Root CA certificates, SSL server or SSL client

certificates, object signing certificates (to sign code e.g. jar files) and user/end-entity certificates for document or email signing. There are also certificates for encryption purposes.

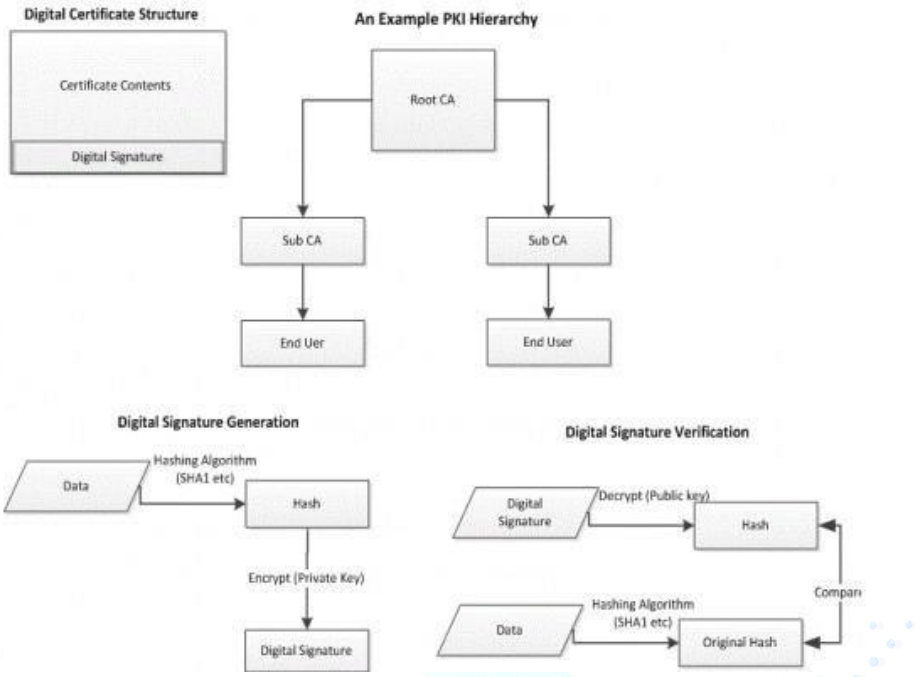


Figure 55 : Digital Signature Process

Technically speaking the difference between a digital signature and digital certificate is that a certificate is an electronic document that binds a public key using digital signature to an individual or a person, a computer or a network device where as a digital signature is to ensure that a data/information remain secure from the point it was issued. Imagine the havoc would have created if all the data travelling between governments, military installations or banks is hacked and updated without no one to detect.

For extra security and performance reasons, a digital signature is created by first hashing (using a secure hashing algorithm like SHA-1 or SHA-2) the data to be digitally signed and then signing this hash value using the private key of the signing digital certificate. Note the hashing process creates a small unique fingerprint of the data, such that it's very hard to find two different input data values which produce the same hash value. To verify the signature on uses the public key of the signer to reverse the process and verify that the data received produces the same hash value as the one that was signed. Following diagram illustrates this:

Digital certificate themselves are digitally signed by the by the issuing Certification authority to ensure they cannot be modified by an attacker. So first the digital certificate is verified using the issuing CA's public key, to obtain trust in the sender's public key. Then the sender's public key is used to verify the digital signature on the actual data message.

Digital certificate Certifying Authorities in India

In India Certifying Authorities (CA) has been granted a license to issue a digital signature certificate under Section 24 of the Indian IT-Act 2000. One can procure Class 2 or 3 certificates from any of the certifying authorities.

- National Informatics Centre (NIC)

- IDRBT Certifying Authority
- SafeScrypt CA Services, Sify Communications Ltd
- (n) Code Solutions CA
- E-MUDHRA
- CDAC
- NSDL
- Capricorn

1.10. ssl certificate

These are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser. SSL certificates provides SSL/TLS encryption to the site, and they contain the website's public key and the website's identity, along with related information. During this communication the private key is kept secret and secure whereas devices attempting to communicate with the origin server will reference this file to obtain the public key and verify the server's identity.

To establish a secure session with browsers an organization needs to install the SSL Certificate onto its web server and when the certificate is successfully installed the HTTP (Hyper Text Transfer Protocol) protocol changes to HTTPs (Secure Hyper Text Transfer Protocol).

TLS (Transport Layer Security) or SSL (Secure Socket Layer) is a security protocol encrypting Internet traffic and verifying server identity. An SSL / TLS Certificate includes the following details –

- The domain name that the certificate was issued for
- Which person, organization, or device it was issued to
- Which certificate authority issued it
- The certificate authority's digital signature
- Associated subdomains
- Issue date of the certificate
- Expiration date of the certificate
- The public key (the private key is kept secret)

Working of ssl / tls

There are three main components to TLS these are –

- Encryption: hides the data being transferred from third parties.
- Authentication: ensures that the parties involved in communication are really who they are claiming to be.
- Integrity: verifies whether the data has been changed or tampered or not.

A TLS connection is initialised using a sequence of steps known as the TLS handshake. The TLS handshake creates a cypher suite (a set of algorithms that contains details like shared

encryption keys, or session keys for that session) for each communication session. TLS is able to set the matching session keys over an unencrypted channel using public key cryptography.

The handshake maintains authentication, by consisting the server proving its identity to the client. This is done using public keys. Public keys are encryption keys that use one-way encryption, meaning that anyone can unscramble data encrypted with the private key to ensure its authenticity, but only the original sender can encrypt data with the private key.

Once data is encrypted and authenticated, it is then signed with a message authentication code (MAC). The recipient can then verify the MAC to ensure the integrity of the data. This is kind of like the tamper-proof foil found on a bottle of aspirin; the consumer knows no one has tampered with their medicine because the foil is intact when they purchase it.

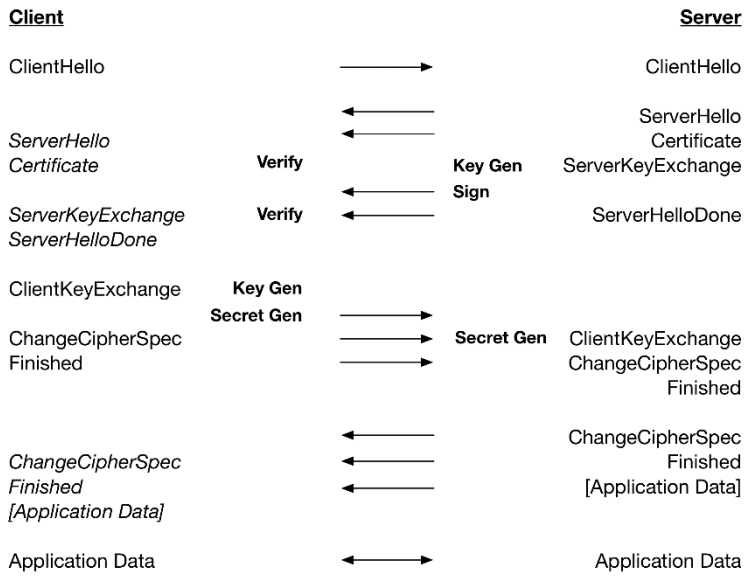


Figure 56 : SSL/TLS Handshake

Chain of Trust

The Chain of Trust refers to that how an SSL certificate is linked back to a trusted Certificate Authority. In order for an SSL certificate to be trusted it has to be traceable back to the trust root it was signed off of, meaning all certificates in the chain – server, intermediate, and root, need to be properly trusted. There are 3 parts to the chain of trust:

- **Root Certificate :** It is a digital certificate that belongs to the issuing Certificate Authority. It comes pre-downloaded in most browsers and is stored in what is called a "trust store." The root certificates are closely guarded by the Certificate Authorities.
- **Intermediate Certificate :** These certificates act as middle-men between the protected root certificates and the server certificates issued out to the public. There will always be at least one intermediate certificate in a chain, but there can be more than one.
- **End - Entity Certificate :** This certificate is the one issued to the specific domain which will be accessed by the user.

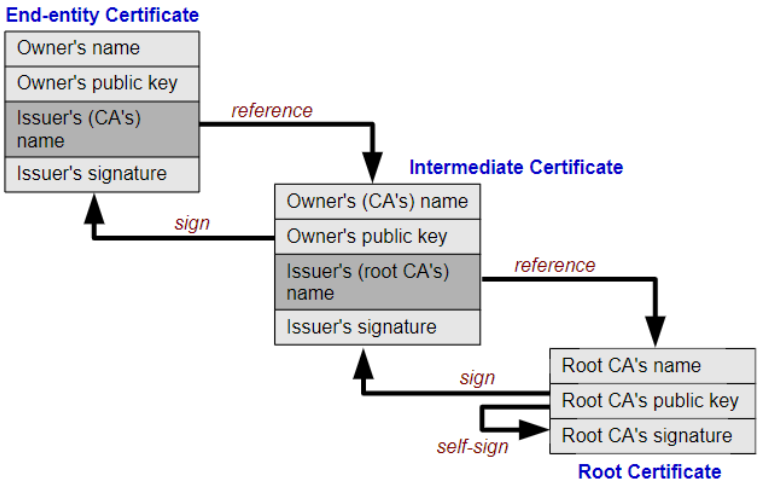


Figure 57 : Certificate Chain of Trust

1.11. personal security

Security of personal data of an individual in cyber world is a critical aspect. One can avoid the attacks by following some security measures. There is no any standard defined for personal security but some things can be considered for cyber awareness.

- Use of genuine software and keep them up to date.
- Use of good antivirus software and firewalls to protect against malwares.
- Use strong passwords for various accounts and keep it confidential. A strong password has various features –
    - If the length of password is more it will be difficult to brute force it.
    - It must contain upper- and lower-case letters, numerals and special symbols.
- Use multi factor Authentication while logging in to your public accounts.
- Be aware about phishing mails, phone calls etc. Don't share your personal information to anyone
- Protect personal identification information (PII) while dealing with untrusted sites
- Backup your data on a regular interval
- Don't use public wifi.
- Review your social media accounts regularly and change the password in a timely manner.

Windows firewall

Microsoft provides an inbuilt security mechanism to windows from the launch of Windows Xp named as windows firewall (Windows Defender Firewall in Windows 10). Which can be configured to get protection from unknown threats while surfing on internet. Which can be configured by the user easily to get the desired setting.

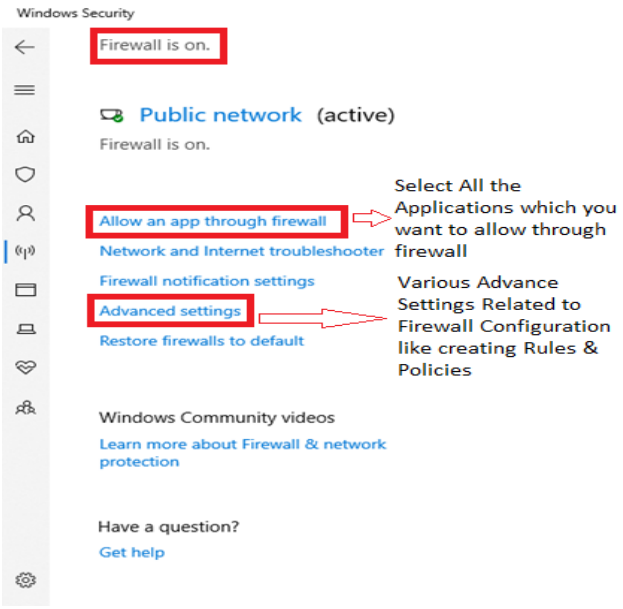


Figure 58 : Windows Firewall

1.12. Organizational security

As organizations increasingly rely on global networks for supply chain and communications, and amass distributed data in terabyte amounts, it has become apparent that the old models for computer security are no longer effective. An organization may define various positions to look over security factors. An example of positions for security field in an organization is illustrated in below figure –

There are various resources which are primarily being used by organizations for security

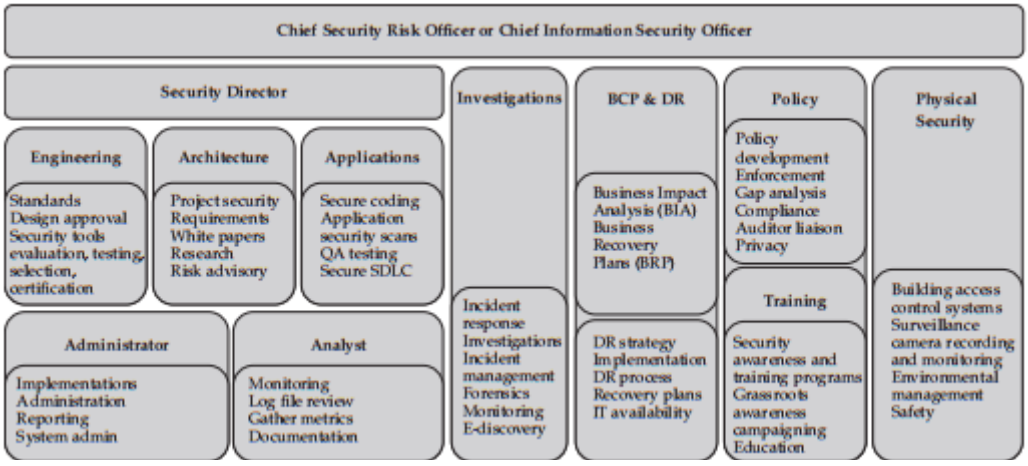


Figure 59 : Positions in Organizational Security

purpose. These are –

- UTM (Unified Threat Management)
- Firewalls
- Intrusion Detection System (IDS) & Intrusion Prevention System (IPS)

- Honeypots

Generally organizational security structures follow layered models of security.

UTM (Unified Threat Management)

Unified threat management (UTM) provides multiple security features and services in a single device or service on the network, protecting users from security threats in a simplified way. UTM includes functions such as anti-virus, anti-spam, content filtering, and web filtering.

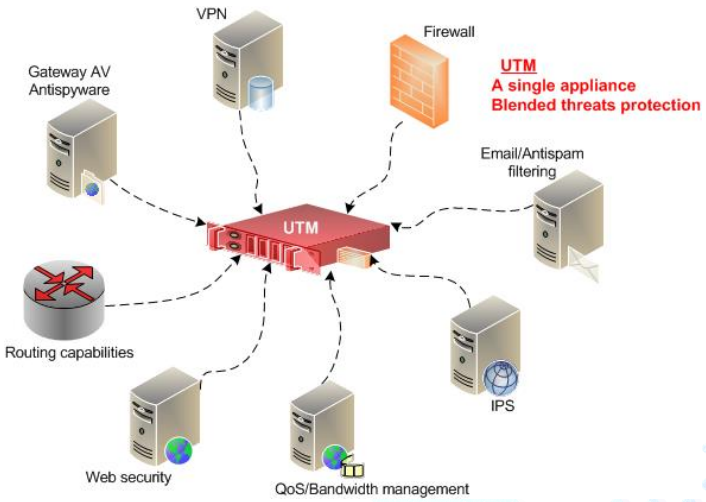


Figure 60 : Unified Threat Management

Intrusion Detection System (ids) / intrusion prevention system (IPs)

Intrusion Detection Systems (IDS) analyse network traffic for signatures that match known cyberattacks. Intrusion Prevention Systems (IPS) also analyses packets, but can also stop the packet from being delivered based on what kind of attacks it detects.

IDS/IPS compare the traffic or data packets to a cyberthreat database know as signatures. It will raise an alert if any matching packets found.

The main difference between them is that IDS is a monitoring system, while IPS is a control system. IDS don't alter the network packets in any way, whereas IPS prevents the packet from delivery based on the contents of the packet, much like how a firewall prevents traffic by IP address.

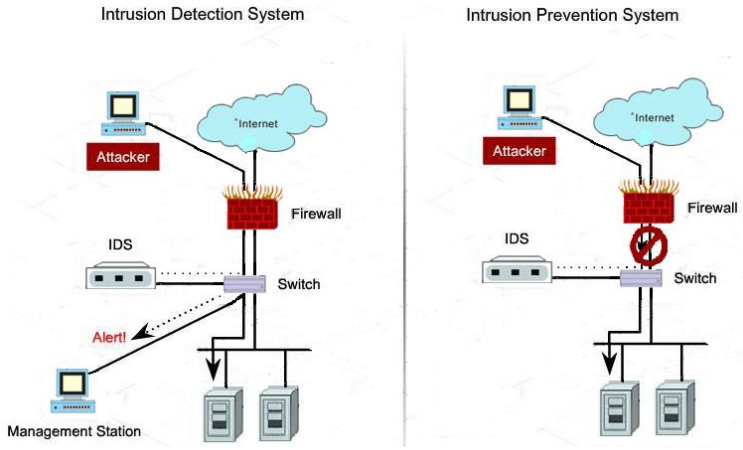


Figure 61 : IDS / IPS

Honeypot

In cyberspace honeypot is a security mechanism used to detect and counter the cyber-attacks by creating a fake system similar to original one to lure the attacker and make him belief that he is attacking an original system.

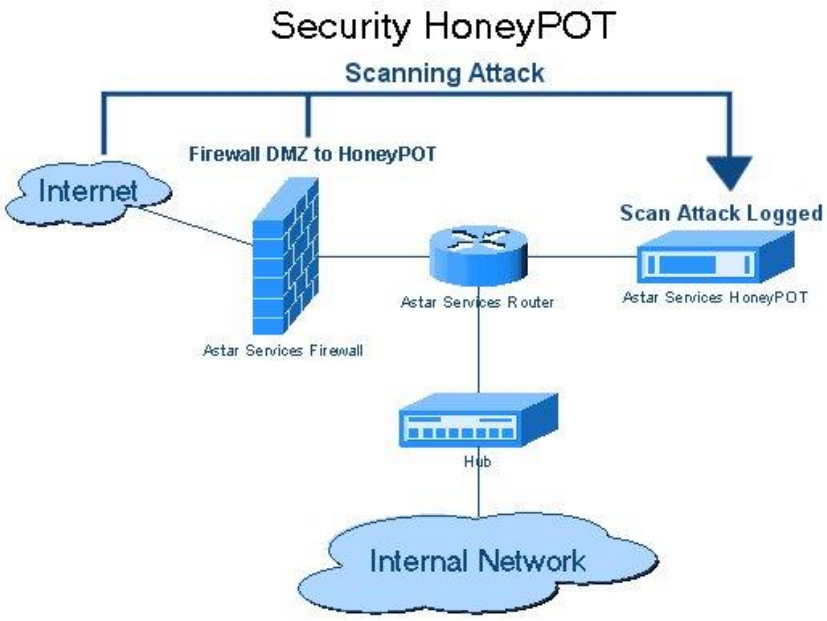


Figure 62 : Honeypot

ORGANISATIONAL SECURITY STRUCTURE

In present scenario although various tools are available for prevention from cyber-attacks but still there is a huge need of a security structure in the organisation to fight with the regular attacks and manage all the security activities being performed in the organisation. The basic structure of an organisational security can be as follows –

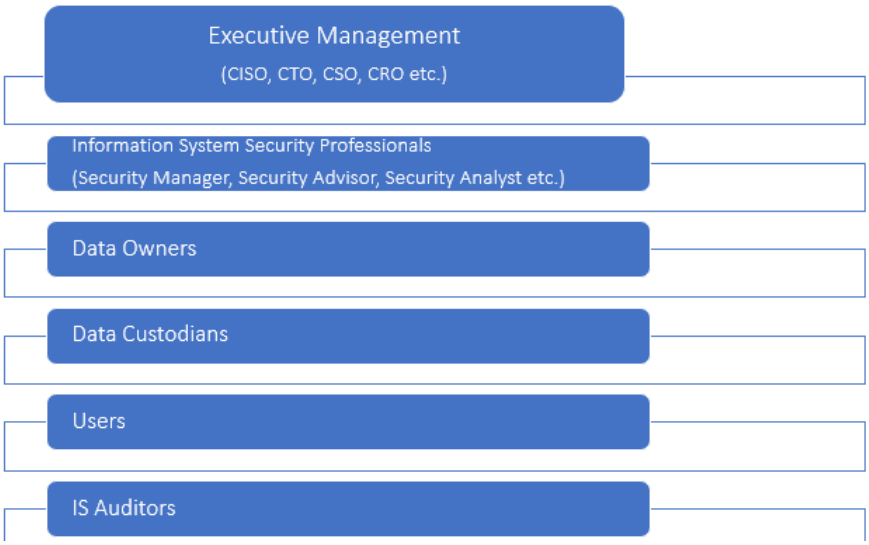


Figure 63 : Organisational Security Structure

Roles in Organisational security structure

Security Structure	Members	Roles & Responsibilities
Executive Management	Chief information Security Officer (CISO), Chief Technology Officer (CTO), Chief Risk Officer (CRO), Chief Security Officer (CSO) etc.	overseeing the enterprise information security strategy that ensures information assets are protected.
Information System Security Professionals	IT security manager, Risk management manager, Compliance manager, IT security analyst, etc.	design, implement, manage, and review the organization's security policies, standards, baselines, procedures, and guidelines.
Data Owners	Owner of any information or data	Ensuring that appropriate security Determining appropriate sensitivity or classification levels and access privileges
Users	Someone who uses the data	using resources and preserving availability, integrity, and confidentiality of assets; responsible for adhering to security policy.

IS Auditors	Someone who Audits the organisational security policies	Providing independent assurance to management on the appropriateness of the security objectives Determining whether the security policy, standards, baselines, procedures, and guidelines are appropriate and effective to comply with the organization's security objectives Identifying whether the objectives and controls are being achieved

CISO (Chief information security officer)

The chief information security officer (CISO) is the executive whose responsibility is to manage an organization's information and data security. Now a day CISO and VP of security titles are used interchangeably indicating its more expansive role in the organization.

The CISO coordinates staff in identifying, developing, implementing and maintaining processes across the enterprise to reduce information and information technology (IT) risks. They respond to incidents, establish appropriate standards and controls, manage security technologies, and direct the establishment and implementation of policies and procedures. The CISO is also usually responsible for information-related compliance (e.g. supervises the implementation to achieve ISO/IEC 27001 certification for an entity or a part of it).

A CISO is the executive-level manager who directs strategy, operations and the budget for the protection of the enterprise information assets and manages that program. The scope of responsibility will encompass communications, applications and infrastructure, including the policies and procedures which apply.

This position can have different titles for the same or similar duties:

- Chief Information Technology Officer (CIO)
- Information Systems (IS) Security Manager
- Corporate Security Executive
- Information Security Director

Roles & Responsibilities of ciso

Following are CISO's roles and responsibilities as per the recommendation of 'NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE' (NCIIPC) which may include but not limited to the following:

- **Strategic Planning**
  - **I)** Proposed responsibilities under this role are:
  - II) Look for top administration support and direction for implementing information security measures in the organization.

III) Recognize information security objectives and goals aligned with organization business need/objectives.
IV) Define the scope and boundaries of the information security program.
V) Comprehend legal and regulatory prerequisites.
VI) Define information security implementation strategies.
VII) Estimate budget and resources required.
VIII) Plan and establish organization-wide Information security Management System (ISMS) in accordance with ISO/IEC 27001 Standard and other significant security guidelines.
IX) Define risk management framework.
X) Define information security measurement metrics and other key performance indicators.
XI) Get approval for information security plan, budget and resources from higher management.

- **Policy Planning**

Proposed responsibilities under this role are:

I) Design information security polices, standards, procedures, guidelines and processes
II) Define formal process for creating, documenting, reviewing, updating, and implementing security policies.
III) Define information security policy.
IV) Define policy for classification of information and information assets.
V) Lead and coordinate development of organization specific information security policies, procedures, guideline and processes in consultation with various stake holders.
VI) Get approval of information security policies, procedures, guidelines and processes.

- **Information Security Management**

Responsibilities under this role are:

I) Assist in developing, maintaining, reviewing and improving strategic organization wide information security and risk management plan.
II) Creating awareness about information security policies, procedures and guideline to all concerned.
III) Monitoring implementation of approved information security policies, procedures, guideline and ISMS etc.
IV) Combining information security procedures with organization's business processes.
V) Ensure that information security considerations are integrated with IT system planning, development / acquisition life cycle.
VI) Regularly reviewing performance of information security policies, procedures, standards, guideline and processes, ISMS etc.
VII) Sending alerts and guidelines with respect to new vulnerabilities / threats to all concerned.
VIII) Conducting risk assessment:

a) Identify and make inventory of assets within the scope of information security plan;
b) Identify and record threats to those assets;
c) Perform vulnerability analysis;
d) Impact analysis;
e) Calculate level of risk;
f) Decide acceptability or treatment of risk based on risk acceptance criteria.

IX) Perform risk treatment:
a) Identify appropriate controls for treatment of risk;
b) Seek approval from senior management for implementation of identified security con trols;
c) Monitor implementation of information security controls;
d) Determine residual risk;
e) Approval from senior management for residual risk.

X) Implementing automated and continuous monitoring of security incidents.
XI) Maintaining a record of information security incidents and breaches.
XII) Taking action to reduce / diminish the impact of information security incidents and breaches.
XIII) Sharing management approval report on information security and breaches to concerned parties.
XIV) Compliance with legal and regulatory requirements for information security.
XV) Organizing information security awareness program for management, employees, contractors and other stake holders.
XVI) Facilitating role-based training on information security to the employees.
XVII) Compute effectiveness of training & awareness program and continuously upgrade it.
XVIII) Define and coordinate 'Business Continuity Plan (BCP)'.
XIX) Conduct mock drill regularly to evaluate effectiveness of business continuity plan.
XX) Define and implement change management plan for both the change in information systems and the change in ISMS itself.
XXI) Ensuring compliance of information security on part of contractors/suppliers etc.

- **Information Security Auditing**

I) Proposed responsibilities under this role are:
II) Periodically evaluate and review effectiveness of Information Security Management System.
III) Evaluate compliance of information security with respect to legal and regulatory requirement.
IV) Monitor compliance of organization specific information security policies, procedures with respect to standards, guidelines and directives.
V) Plan information security audit at least annually or whenever significant changes have been made in IT systems/ Infrastructure.

VI) Release information security audit report along with recommendations for improving information security.

VII) Seek higher management approval of information security audit report.

- **Other responsibilities may include:**

I) Ensure that before issuing NOC (No Objection Certificate) to the employee, who has resigned or has been terminated or is leaving organization, all equipments have been taken back and all his accounts either have been deleted or their passwords have been changed.

II) Maintain asset inventory containing details of asset, its owner and its security classification.

III) Ensure safe disposal of all storage media, when no longer required as per laid down procedures.

IV) Make sure safety and security of portable computing devices/storage media when they are taken outside of the organization.

V) Ensure all information systems with organization are adequately patched and updated.

Risk assessment or contingency planning

Risk assessment and contingency planning is the process of determining the risks a business faces and what it must do if those risks are realized. While it may not be possible to plan for every possible emergency, most businesses can identify those they are most likely to face and those that will cost them the most if they are realized.

Contingency plan is an essential part of risk management. It helps to ensure that organization has always got a backup option when things go wrong, or when the unexpected happens. It is often used for risk management for an exceptional risk that, though unlikely, would have catastrophic consequences.

Contingency planning isn't just about major crises and natural disasters. It also prepares organization for more commonplace problems, such as the loss of data, staff, customers, or business relationships. Therefore, it is important to make contingency planning a routine part of the regular work in organization.

To develop a contingency plan, first a risk assessment should be conducted: identify business-critical operations, identify the threats to those operations, and analyse the potential impact of each threat.

Conducting a Risk Assessment

Each organization has to face some unique risks in its routine work, and for those risks it needs to be prepared. Hence the key is to identify most of the possible risks beforehand and prepare a backup plan for the same.

The first step is to conduct risk assessment to identify all the possible risks.

So, we start with **identifying business-critical operations of the organization**. These are the key processes and functions without which organization could not operate, such as supply chain, internet connection, or ability to comply with legal standards.

Next is to **identify the threats** that could harm each critical operation. Threat could be human, operational, financial, environmental/weather-related, political, procedural, technical or project-based. Then measure each of these threats based on how likely they are to occur and how much damage they could do to the business. There are several techniques for identifying risks including group brainstorming, interviews, surveys, root cause analysis, review of past accident reports, SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis and diagramming.

Often there is a chance to come up with a long list of potential threats. It becomes unrealistic to attempt contingency planning for all of them, so here prioritization of risks comes into picture. The standard formula for risk assessment is that risk equals the probability of an event multiplied by the cost of the event. Each identified risk can be rated on a scale of one to five, with one being the least likely to occur and causing the least damage and five being the most likely to occur and causing the most damage. All risks can then be sorted into low, medium or high depending on the rating.

Risk Assessment helps to **analyse the impact of each risk**, and to estimate likelihood of it. This defines which risks require the expense and effort of risk mitigation. Business processes that are essential to organization, such as maintaining cash flow and market share, are typically at the top of the list.

The four basic approaches to risk are risk avoidance, risk reduction, risk sharing or transfer, and risk retention.

- **Risk avoidance** involves not doing the project or task that will bring the business into contact with the risk.
- **Risk reduction** means putting procedures into place that will make the risk less likely to occur or mitigate the effects if it does occur.
- **Risk sharing** or transfer typically involves buying insurance to cover losses or outsourcing the task so that someone else bears the burden of risk.
- **Risk retention** is the process of accepting the possibility of loss and budgeting to cover the risk.

If a business decides to mitigate or accept the risk, it will benefit from having a contingency plan in place to deal with the critical situation should if occurs.

What is a Contingency Plan?

A good contingency plan can prevent a business from disruption when unexpected events occur, so it's necessary to ensure that it totally serves the purpose.
Some of the key elements to include are:

Scenarios

It refers to the risk assessment to choose the most impacting or most likely scenarios for which organization wants to plan for. Then, map out what should be response in each case.

Here organization should aim to include a broad range of scenarios – for instance, cyber-attacks, prolonged staff absences, IT malfunctions, loss of suppliers, serious power outages, or structural problems with business premises.

Triggers

Here we have to specify exactly what incidence, will cause to put contingency plan into action. For example, if organization have a plan for heavy rainfall, it should specify whether it will be triggered by a severe weather warning, or only by actual rainfall?

Response

It includes a brief overview of the strategy that will be followed in response to the event. This provides a context for the actions that organization ask employees to take.

Whom to Inform

Designate the people who need to know about what has happened. This could include employees, suppliers, customers, and the wider public, as appropriate. It designs a clear path to deliver effective communication in difficult situations.

Organization should also be aware of its legal obligations, and should make sure that incidents are reported to the relevant authorities where necessary.

Key Responsibilities

Roles and Responsibilities should be clearly defined for each element of the plan, such as who will be in charge at each stage and what they are supposed to accomplish.

Timeline

Determine what needs to be done within the first hour, day and week of the plan being implemented.

There might be simple situations where you just need to inform employees about situation, but at times situation could be very critical as well which will need far more detailed timeline guidance, such as data breaches, serious workplace injuries, or leaks of hazardous materials.

This should also include details of when organization would expect normal business to resume, and what will signal that organization is ready for this.

Developing Contingency Plan

The primary aim of developing contingency plan for an organization is to maintain or restore critical business operations, so it should be closely analysed that how critical operations might be affected by each scenario.

Organization must consider knock-on effects. Whether organization will be able to function at full capacity when "Plan B" is implemented or it will reduce organization’s productivity. If yes, then for how long?

Involve Employees

It always proves beneficial to consult people from across organization during designing phase of contingency plan. Managers from different departments can advise on the impact of disruptive events on services, staff, resources, and business functions. And "frontline" employees are often best placed to tell about the minimum tools and support they require in order to maintain essential operations.

Contingency plan should be kept open for feedbacks from employees to make it even more robust. And, if possible, mock drills should be conducted to assess the efficacy of the plan. This will highlight areas for improvement, and reveal skills gaps or training needed.

Simple Design

While writing contingency plan, make sure to use simple, plain language since it is not known when the plan will be used, or who will read and implement it when it is needed. For the same reason, job titles or roles should be used instead of names while defining people's responsibilities. This will help to keep the plan relevant, regardless of any changes in personnel.

Maintaining Contingency Plan

The contingency plan must be reviewed and updated regularly, in order to remain useful and credible.

While reviewing it, all relevant technological, operational and personnel changes should be taken into account and reassess the risks accordingly. Then, discard old versions of the plan.

When new employees join organization, provide them with the contingency plan as part of their induction so that they are familiar with it, and so that they know what to do if critical situation occurs.

And finally, it is also necessary to back up the backup plan. This could be achieved by means of keeping a digital version in the cloud, storing physical copies in an easily accessible offsite location, or both.

Sample Contingency Plan

Scenario	Trigger	Response	Who To Inform?	Key Responsibilities		Timeline	
				Who	What	What	When
Severe Flooding of Office and Warehouse	**Trigger 1:** Flood warning issued by weather department	Alert employees, suppliers and customers of risk	Employees	CEO	Oversee Implementation of plan	Contact who will be affected / need to be notified	Immediately
				Marketing / PR	Handle media inquiries		

Organisational security standards in India

In India basically there are two major information security standards are being followed by various organisation. These are –

- ISO 27001 Family part of Information Security Management System (ISMS)
- COBIT (Control Objectives for Information and Related Technology) by ISACA

Information Security certifications

There are a lot of certifications available for an information security professional. Some of them are –

- CEH (Certified Ethical Hacker)
- CISSP (Certified Information Systems Security Professional)
- CISM (Certified Information Security Manager)
- CCSP (Certified Cloud Security Professional)
- CISA (Certified Information Systems Auditor)
- COBIT 5
- CompTIA Security+
- ISO 27001 Standards etc.

1.13. Perimeter device security

A perimeter can be defined as a cave in IT infrastructure which is covered by various security layers to be protected from the risks of cyber world. A perimeter device can be protected using layered methodology from a cyber-attack. The layers can include

- Firewall
- IPS/IDS System
- ADS (Anomaly Detection System) etc.

How an ADS Works?

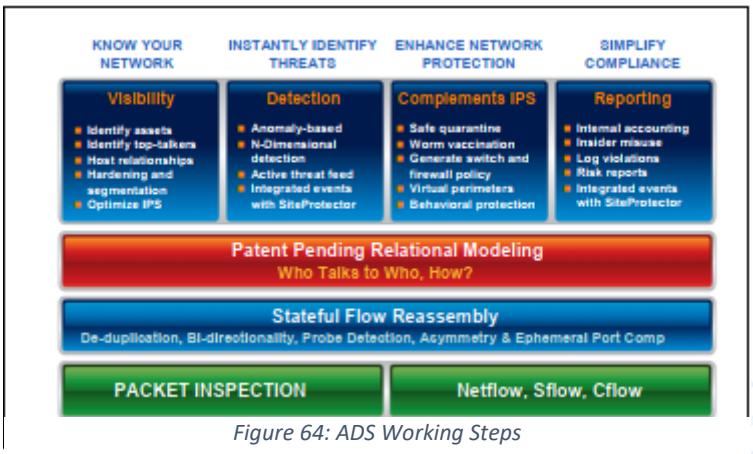


Figure 64: ADS Working Steps

1.14. Data Leak Prevention

Organisations handle a plethora of sensitive data, such as trade secrets, customer data, pricing lists, trading algorithms and acquisition plans. This data can be leaked to unscrupulous competitors, organised criminal groups and other entities via a multitude of channels, including email, the internet, portable storage devices and cloud services.

Data leaks can be expensive, harm an organisation's brand and reputation, and diminish trust. Customers and shareholders alike expect organisations to take appropriate measures to properly safeguard their data and investment. A successful data leakage prevention (DLP) programme can significantly reduce these risks.

Data leakage prevention or Data Loss Prevention Policy can be defined as the set of rules to prevent the unauthorised disclosure of data. A DLP generally performs three types of core activities to prevent the data. These are –

- Identify data according to their category like highly confidential, low confidential etc.
- Monitoring of channels to check whether the data is leaking or not
- If data is being leaked then it performs some actions for leakage prevention.

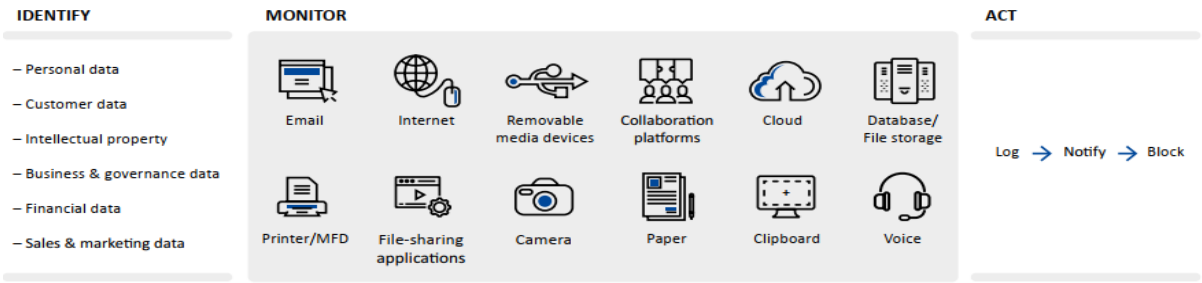


Figure 65 : DLP Process

A DLP policy can apply to one or more channels of data leakage. It need not apply enterprise-wide; it may be more appropriate to limit its application to certain users, a user group or geographic region. Examples of DLP policies are shown in the figure below.

DLP POLICY	CONDITION	EXCEPTION	ACTION
Source code	Detect content containing proprietary source code	Allow transfer of data to company X, selected to conduct a source code review	Block transfers containing source code (including web postings, email messages and copy of files)
Credit cards	Detect content that matches the credit card number, using a Luhn algorithm	None	Quarantine data in cloud applications, files and messages: – send an email notification to the user – allow the user to provide business justification for release
Project penguin	Detect content containing key phrase 'project penguin' and intended for an external recipient	Allow transfer of data to John Doe (external legal counsel)	Block transfer of content to external recipients Encrypt email transmissions to John Doe
Medical records	Detect content that matches words or expressions from a list of common medical conditions	Exclude emails marked as 'personal'	Block transfers including copy of health data to a portable storage device Display on-screen notification stating file transfer violates a specific DLP policy

Figure 66 : Example of DLP Policy

In windows 10 Microsoft has initialised WIP (Windows Information Protection) which was previously known as EDP (Enterprise Data Protection) to manage the data leakage prevention effectively without interfering with an employee existence.

Features of WIP

- It encrypts the data which is being copied or downloaded from enterprise endpoint.
- Manage the data used by protected and nonprotected apps.
- Manage the data access level of employees.
- Protects the data stored in local files or host.
- Prevents accidental data disclosure.

WIP Protection Modes

WIP Policies have following four protection and management modes from which any one can be configured.

Mode	Description
Block	WIP looks for inappropriate data sharing practices and stops the employee from completing the action. This can include sharing enterprise data to non-enterprise-protected apps in addition to sharing enterprise data between apps or attempting to share outside of your organization's network.
Allow overrides	WIP looks for inappropriate data sharing, warning employees if they do something deemed potentially unsafe. However, this management mode lets the employee override the policy and share the data, logging the action to your audit log.
Silent	WIP runs silently, logging inappropriate data sharing, without stopping anything that would've been prompted for employee interaction while in Allow overrides mode. Unallowed actions, like apps inappropriately trying to access a network resource or WIP-protected data, are still stopped.
Off	WIP is turned off and doesn't help to protect or audit your data. After you turn off WIP, an attempt is made to decrypt any WIP-tagged files on the locally attached drives. Be aware that your previous decryption and policy info isn't automatically reapplied if you turn WIP protection back on.

Figure 67 : WIP Protection Modes

1.15. Data Execution Prevention (dep)

It is a security feature within operating system used to prevents applications from executing code from a non-executable memory location and thus it can help prevent damage to computer system from viruses and other security threats. DEP can help in protecting the computer by monitoring programs to make sure that they use system memory safely. If DEP notices a program using memory incorrectly, it closes the program and notifies the user.

Configuration of dep in computer

In computer system DEP can be configured by following simple steps.

- Right Click on My Computer (This PC in Windows 8 & Above) & click on properties in the menu open.

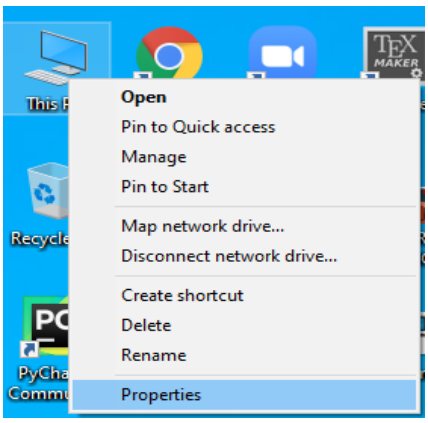


Figure 68 : DEP Configuration Step -1

- Click Advanced system settings.

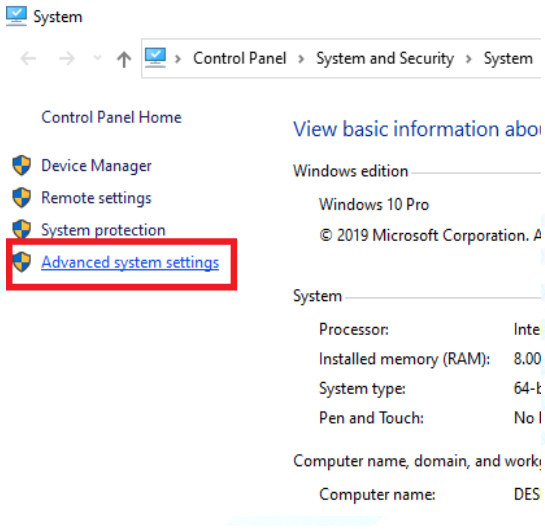


Figure 69 : DEP Configuration Step - 2

- Under Performance, click Settings.

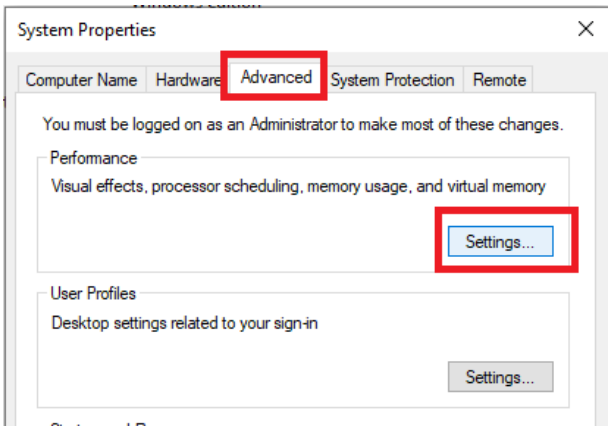


Figure 70 : DEP Configuration Step - 3

- Click the Data Execution Prevention tab, and then click Turn on DEP for all programs and services except those I select.

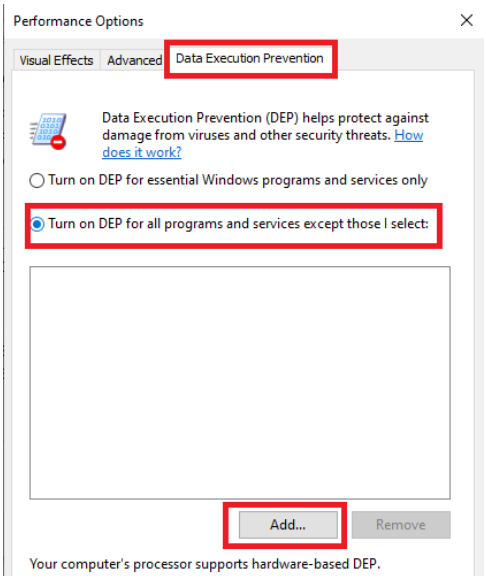


Figure 71 : DEP Configuration Step - 4

1.16. Techniques for safe internet browsing

Internet is always on cyber risk by using some measures while browsing the internet one can be safe in the cyber world.

- Be realistic about your presence in cyber space
- Always browse using safe network, with strong password, and safe websites and also keep an eye on your transactions regularly.
- Be careful while making online friends.
- Always trace your digital steps by making list of all your online accounts with strong password. Delete your old accounts which are not in use.
- Never disclose your personal confidential details (like accounts passwords, ATM card number, pin etc.) to anyone.
- To protect against ransomwares, create backup regularly, make copies of your data, don't click on unknown links and use a god antivirus tool.
- While visiting any website check for SSL encryption.
- Develop good security habits.

Cyber Security Framework in India

India has defined various cyber security frameworks to protect the people against cyber-attacks. Some of them are –

- CERT – In
- NCIIPC
- NTRO
- National Cyber Security Policy (NCSP)
- National Cyber Co-ordination Centre (NCCC)
- Personal Data Protection Bill
- National Security Council of India (NSC)

2.1 Computer Emergency response team of India (cert - in)[9]

CERT-In is an acronym for 'Indian Computer Emergency Response Team'. CERT-In is the National Incident Response Centre for major computer security incidents in its constituency i.e. Indian cyber community. It has been established by, and runs under the aegis of Ministry of Electronics and Information Technology, Government of India.

CERT-In's primary role is to raise security awareness among Indian cyber community and to provide technical assistance and advise them to help them recover form computer security incidents. It provides technical advice to System Administrators and users to respond to computer security incidents. It also identifies trends in intruder activity, works with other similar institutions & organisations to resolve major security issues, and disseminates information to the Indian cyber community. CERT-In also enlightens its constituents about the security awareness and best practices for various systems & networks by publishing advisories, guidelines and other technical documents.

Roles & Responsibilities of Cert – in

Reactive Roles

- Provide a single point of contact for reporting local problems.
- Assist the organisational constituency and general computing community in preventing and handling computer security incidents.
- Share information and lessons learned with CERT/CC, other CERTs, response teams, organisations and sites.
- Incident Response.
- Provide a 24 x 7 security service.
- Offer recovery procedures.
- Artifact analysis
- Incident tracing

Proactive Roles

- Issue security guidelines, advisories and timely advise.
- Vulnerability analysis and response
- Risk Analysis
- Collaboration with vendors
- National Repository of, and a referral agency for, cyber-intrusions.
- Profiling attackers.
- Conduct Training
- Interact with vendors and others at large to investigate and provide solutions for incidents.

functions of cert – in

Reporting

- Central point for reporting incidents

[9] (In, n.d.)

- Database of incidents

Analysis

- Analysis of trends and patterns of intruder activity
- Develop preventive strategies for the whole constituency
- In-depth look at an incident report or an incident activity to determine the scope, priority and threat of the incident.

Response

- Incident response is a process devoted to restoring affected systems to operation
- Send out recommendations for recovery from, and containment of damage caused by the incidents.
- Help the System Administrators take follow up action to prevent recurrence of similar incidents

Types of incidents which can be reported to cert – in

Users and System Administrators can report computer security incidents and vulnerabilities to CERT-In.

- If anyone encounter any of the violations given below, you may contact CERT-In for technical assistance
    - Attempts (either failed or successful) to gain unauthorised access to a system or data therein
    - Disruption or denial of service
    - Unauthorised use of a system for the processing or storage of data
    - Changes to system hardware, firmware, or software characteristics without owner's knowledge, instruction, or consent
    - Email-related security issues, spamming, mail bombing etc.
- Users of different systems working on various platforms and using different applications may report any vulnerability found in these systems, platforms, applications, services and devices to CERT-In.

Way of reporting an INCIDENT

One can report an incident to CERT-In by filling up the form on our website, electronic mail, telephone hotline or by Fax.

Website

The incident can be reported by filling up incident reporting form on our website. Fill in as many of the fields as possible to enable us to assess the severity and nature of the incident and assist in recovery, as needed.

Electronic Mail

The CERT-In email address for reporting incidents is: incident@cert-in.org.in

For all other inquiries and correspondence, write to:: info@cert-in.org.in

Occasionally, a compromised system's electronic mail may be under surveillance by the intruder. If that is suspected, one is advised to use other means (telephone or fax) to file his report.

Telephone Hotline

One can contact the CERT-In on +91-11-24368572.

Fax
Incident report can be faxed to CERT-In at 91-11-24368546

Reporting a Vulnerability to cert – in

A vulnerability can be reported to CERT-In by filling up the Vulnerability Reporting Form provided on our website. The information about a particular vulnerability can also be sent to CERT-In by Fax or by e-mail : vulnerability@ cert-in.org.in

2.2 National Technical Research Organisation (NTRO)10

The National Technical Research Organisation (NTRO) is a technical intelligence Agency under the National Security Advisor in the Prime Minister's Office, India. It was set up in 2004. It also includes National Institute of Cryptology Research and Development (NICRD), which is first of its kind in Asia. NTRO has the same "norms of conduct" as the Intelligence Bureau (IB) and the Research and Analysis Wing (R&AW).

2.3 National Critical information infrastructure protection centre (nciipc)

National Critical Information Infrastructure Protection Centre (NCIIPC) is an organisation of the Government of India created under Sec 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on 16th Jan 2014 based in New Delhi, India. It is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection. It is a unit of National Technical research organisation.

Functions & Duties of NCIIPC

It is a National nodal agency for all measures to protect nation's critical information infrastructure and its functions are –

- Protect and deliver advice that aims to reduce the vulnerabilities of critical information infrastructure, against cyber terrorism, cyber warfare and other threats.
- Identification of all critical information infrastructure elements for approval by the appropriate Government for notifying the same.
- Provide strategic leadership and coherence across Government to respond to cyber security threats against the identified critical information infrastructure.
- Coordinate, share, monitor, collect, analyse and forecast, national level threat to CII for policy guidance, expertise sharing and situational awareness for early warning or alerts. The basic responsibility for protecting CII system shall lie with the agency running that CII.

[10] (Wikipedia, National Technical Research Organisation, n.d.)

- Assisting in the development of appropriate plans, adoption of standards, sharing of best practices and refinement of procurement processes in respect of protection of Critical Information Infrastructure.
- Evolving protection strategies, policies, vulnerability assessment and auditing methodologies and plans for their dissemination and implementation for protection of Critical Information Infrastructure.
- Undertaking research and development and allied activities, providing funding (including grants-in-aid) for creating, collaborating and development of innovative future technology for developing and enabling the growth of skills, working closely with wider public sector industries, academia et al and with international partners for protection of Critical Information Infrastructure.
- Developing or organising training and awareness programs as also nurturing and development of audit and certification agencies for protection of Critical Information Infrastructure.
- Developing and executing national and international cooperation strategies for protection of Critical Information Infrastructure.
- Issuing guidelines, advisories and vulnerability or audit notes etc. relating to protection of critical information infrastructure and practices, procedures, prevention and response in consultation with the stake holders, in close coordination with Indian Computer Emergency Response Team and other organisations working in the field or related fields.
- Exchanging cyber incidents and other information relating to attacks and vulnerabilities with Indian Computer Emergency Response Team and other concerned organisations in the field.
- In the event of any threat to critical information infrastructure the National Critical Information Infrastructure Protection Centre may call for information and give directions to the critical sectors or persons serving or having a critical impact on Critical Information Infrastructure.

Reporting vulnerability & security incidents to nciipc

General Help:

helpdesk1 @nciipc .gov .in
helpdesk2 @nciipc .gov .in

Site Administrator: kms @nciipc .gov .in

Incident Reporting: ir @nciipc .gov .in

Vulnerability Disclosure: rvdp @nciipc .gov .in

Malware Upload: mal.repository @nciipc .gov .in

2.4 National cyber security policy (NCSP)

It is a policy framework by Department of Electronics and Information Technology (DeitY) to protect the public and private infrastructure from cyber attacks andcy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data".[11]

Preamble

1. Cyberspace is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.

2. Owing to the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses, critical information infrastructure, military and governments in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace is expected to be more complex in the foreseeable future, with many folds increase in networks and devices connected to it.

3. Information Technology (IT) is one of the critical sectors that rides on and resides in cyberspace. It has emerged as one of the most significant growth catalysts for the Indian economy. In addition to fuelling India's economy, this sector is also positively influencing the lives of its people through direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others. The sector has played a significant role in transforming India's image to that of a global player in providing world-class technology solutions and IT business services. The government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics), Education (e-Learning, virtual classrooms, etc) and Financial services (mobile banking / payment gateways), etc. Such initiatives have enabled increased IT adoption in the country through sectoral reforms and National programmes which have led to creation of large-scale IT infrastructure with corporate / private participation.

4. In the light of the growth of IT sector in the country, ambitious plans for rapid social transformation & inclusive growth and India's prominent role in the IT global market, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities for the country. Such a focus enables creation of a

[11] (Wikipedia, National Cyber Security Policy 2013, n.d.)

suitable cyber security eco-system in the country, in tune with globally networked environment.

5. Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation- states and non-state actors. Cyber-attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures. A cyber related incident of national significance may take any form; an organized cyber-attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, hacktivism, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

6. There are various ongoing activities and programs of the Government to address the cyber security challenges which have significantly contributed to the creation of a platform that is now capable of supporting and sustaining the efforts in securing the cyber space. Due to the dynamic nature of cyberspace, there is now a need for these actions to be unified under a **National Cyber Security Policy**, with an integrated vision and a set of sustained & coordinated strategies for implementation.

7. The cyber security policy is an evolving task and it caters to the whole spectrum of ICT users and providers including home users and small, medium and large enterprises and Government & non- Government entities. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace. It also enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs. The

policy provides an overview of what it takes to effectively protect information, information systems & networks and also gives an insight into the Government's approach and strategy for protection of cyber space in the country. It also outlines some pointers to enable collaborative working of all key players in public & private to safeguard country's information and information systems. This policy, therefore, aims to create a cyber security framework, which leads to specific actions and programmes to enhance the security posture of country's cyber space.

I. Vision

To build a secure and resilient cyberspace for citizens, businesses and Government

II. Mission

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

III. Objectives

1. To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
2. To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).
3. To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.
4. To enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.
5. To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition,

development, use and operation of information resources.

6. To develop suitable indigenous security technologies through frontier technology research, solution-oriented research, proof of concept, pilot development, transition, diffusion and commercialisation leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.
7. To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.
8. To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.
9. To provide fiscal benefits to businesses for adoption of standard security practices and processes.
10. To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cybercrime or data theft.
11. To enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.
12. To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.
13. To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.
14. To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

IV. Strategies

- *Creating a secure cyber ecosystem*

1. To designate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.
2. To encourage all organizations, private and public to designate a member of senior management, as Chief Information Security Officer (CISO), responsible for cyber security efforts and initiatives.
3. To encourage all organizations to develop information security policies duly

integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

4. To ensure that all organizations earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.
5. To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security.
6. To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions.
7. To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.
8. To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications.

➢ Creating a*n assurance framework*

1. To promote adoption of global best practices in information security and compliance and thereby enhance cyber security posture.
2. To create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines (Eg. ISO 27001 ISMS certification, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing).
3. To enable implementation of global security best practices in formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all entities within Government and in critical sectors, to reduce the risk of disruption and improve the security posture.
4. To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.
5. To encourage secure application / software development processes based on global best practices.
6. To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security.

7. To encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and in networks.

➢ Encouraging Open Standards

1. To encourage use of open standards to facilitate interoperability and data exchange among different products or services.
2. To promote a consortium of Government and private sector to enhance the availability of tested and certified IT products based on open standards.

➢ Strengthening the Regulatory framework

1. To develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance.
2. To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.
3. To enable, educate and facilitate awareness of the regulatory framework.

➢ *Creating mechanisms for security threat early warning, vulnerability management and response to security threats*

1. To create National level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.
2. To operate a 24x7 National Level Computer Emergency Response Team (CERT-In) to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management. CERT-In will function as an umbrella organization in enabling creation and operationalization of sectoral CERTs as well as facilitating communication and coordination actions in dealing with cyber crisis situations.
3. To operationalise 24x7 sectoral CERTs for all coordination and communication actions within the respective sectors for effective incidence response & resolution and cyber crisis management.

4. To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the Nation, by way of well-coordinated, multi-disciplinary approach at the National, Sectoral as well as entity levels.
5. To conduct and facilitate regular cyber security drills & exercises at National, sectoral and entity levels to enable assessment of the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.

➢ Securing E-Governance services

1. To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the country, to reduce the risk of disruption and improve the security posture.
2. To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.
3. To engage information security professionals / organisations to assist e-Governance initiatives and ensure conformance to security best practices.

➢ Protection and resilience of Critical Information Infrastructure

1. To develop a plan for protection of Critical Information Infrastructure and its integration with business plan at the entity level and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.
2. To Operate a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country.
3. To facilitate identification, prioritisation, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure.
4. To mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all critical sector entities, to reduce the risk of disruption and improve the security posture.
5. To encourage and mandate as appropriate, the use of validated and certified IT products.
6. To mandate security audit of critical information infrastructure on a periodic basis.

7. To mandate certification for all security roles right from CISO / CSO to those involved in operation of critical information infrastructure.
8. To mandate secure application / software development process (from design through retirement) based on global best practices.

➢ Promotion of Research & Development in cyber security

1. To undertake Research & Development programs for addressing all aspects of development aimed at short term, medium term and long-term goals. The Research & Development programs shall address all aspects including development of trustworthy systems, their testing, deployment and maintenance throughout the life cycle and include R&D on cutting edge security technologies.
2. To encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets.
3. To facilitate transition, diffusion and commercialisation of the outputs of Research & Development into commercial products and services for use in public and private sectors.
4. To set up Centres of Excellence in areas of strategic importance for the point of security of cyber space.
5. To collaborate in joint Research & Development projects with industry and academia in frontline technologies and solution oriented research.

➢ Reducing supply chain risks

1. To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.
2. To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility.
3. To create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT (products, systems or services) procurement.

➢ Human Resource Development

1. To foster education and training programs both in formal and informal sectors to support the Nation's cyber security needs and build capacity.
2. To establish cyber security training infrastructure across the country by way of public private partnership arrangements.
3. To establish cyber security concept labs for awareness and skill development in key

areas.

4. To establish institutional mechanisms for capacity building for Law Enforcement Agencies.

➢ Creating Cyber Security Awareness

1. To promote and launch a comprehensive national awareness program on security of cyberspace.
2. To sustain security literacy awareness and publicity campaign through electronic media to help citizens to be aware of the challenges of cyber security.
3. To conduct, support and enable cyber security workshops / seminars and certifications.

➢ Developing effective Public Private Partnerships

1. To facilitate collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices.
2. To create models for collaborations and engagement with all relevant stakeholders.
3. To create a think tank for cyber security policy inputs, discussion and deliberations.

➢ Information sharing and cooperation

1. To develop bilateral and multi-lateral relationships in the area of cyber security with other countries.
2. To enhance National and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement Agencies and the judicial systems.
3. To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resilience of systems including critical information infrastructure.

➢ Prioritized approach for implementation

1. To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.

V. Operationalisation of the Policy

This policy shall be operationalised by way of detailed guidelines and plans of action at various levels such as national, sectoral, state, ministry, department and enterprise, as may be appropriate, to address the challenging requirements of security of the cyberspace.

2.5 National Cyber Co-ordination Center (NCCC)12

[12] (Wikipedia, National Cyber Coordination Centre, n.d.)

The National Cyber Coordination Centre (NCCC) is an operational cybersecurity and e-surveillance agency in India. It is intended to screen communication metadata and co-ordinate the intelligence gathering activities of other agencies. Some have expressed concern that the body could encroach on Indian citizens' privacy and civil-liberties, given the lack of explicit privacy laws in the country.

Components of the NCCC include a cybercrime prevention strategy, cybercrime investigation training and review of outdated laws. Indian and U.S. intelligence agencies are also working together to curb misuse of social media platforms in the virtual world by terror groups.

2.6 Personal Data Protection Bill13

The Personal Data Protection Bill 2019 (PDP Bill 2019) was tabled in the Indian Parliament by the Minister of Electronics and Information Technology on 11 December 2019. As of 17 December 2019, the Bill is being analysed by a Joint Parliamentary Committee (JPC) in consultation with various groups.

The Bill covers mechanisms for protection of personal data and proposes the setting up of a Data Protection Authority of India for the same. Some key provisions the 2019 Bill provides for which the 2018 draft Bill did not such as that the central government can exempt any government agency from the Bill and the Right to Be Forgotten has been included.

According to this bill -

- WHEREAS the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy;
- WHEREAS the growth of the digital economy has meant the use of data as a critical means of communication between persons;
- WHEREAS it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation;
- AND WHEREAS it is expedient to make provision: toprotect the autonomy of individuals in relation with their personal data, to specify where the flow and usage of personal data is appropriate, to create a relationship of trust between persons and entities processing their personal data, to specify the rights of individuals whose personal data are processed, to create a framework for implementing organisational and technical measures in processing personal data, to lay down norms for cross-border transfer of personal data, to ensure the accountability of entities processing personal data, to provide remedies for unauthorised and harmful processing, and to establish a Data Protection Authority for overseeing processing activities.

[13] (Wikipedia, Personal Data Protection Bill 2019, n.d.)

2.7 National Security Council (NSC)14

It is an executive government agency tasked with advising the Prime Minister's Office on matters of national security and strategic interest. It was established by the former prime minister of India Atal Bihari Vajpayee on 19 November 1998, with Brajesh Mishra as the first National Security Advisor. Prior to the formation of the NSC, these activities were overseen by the Principal Secretary to the preceding Prime Minister.

Besides the National Security Advisor (NSA), the Deputy National Security Advisors (Dy.NSA), the Ministers of Defence, External Affairs, Home, Finance of the Government of India, and the Vice Chairman of the NITI Aayog are members of the National Security Council.

2.8 National Security Council Secretariat (NSCS)

The Indian Government under the aegis of National Security Council Secretariat through a well-represented Task Force is in the process of formulating the National Cyber Security Strategy 2020 (NCSS 2020) to cater for a time horizon of five years (2020-25).

Proposed vision of NSCS is to ensure a safe, secure, trusted, resilient and vibrant cyber space for our Nation's prosperity.

Pillars of Strategy We are examining various facets of cyber security under the following pillars:

- Secure (The National Cyberspace)
- Strengthen (Structures, People, Processes, Capabilities)
- Synergise (Resources including Cooperation and Collaboration)

Cyber Security-Practical Aspects

3.1. CMD Essentials

In windows operating system command prompt (CMD) is an essential utility to perform various tasks using command line like Linux. It is command line interpreter utility in Windows

[14] (Wikipedia, National Security Council (India), n.d.)

Operating System. With the help of command prompt administrative functions can be performed to troubleshoot various problems of the system.

I) how to open cmd

There are multiple ways to open CMD in windows operating system. These are –

i) Using Windows Search Bar

- Go to windows search bar and type cmd there.

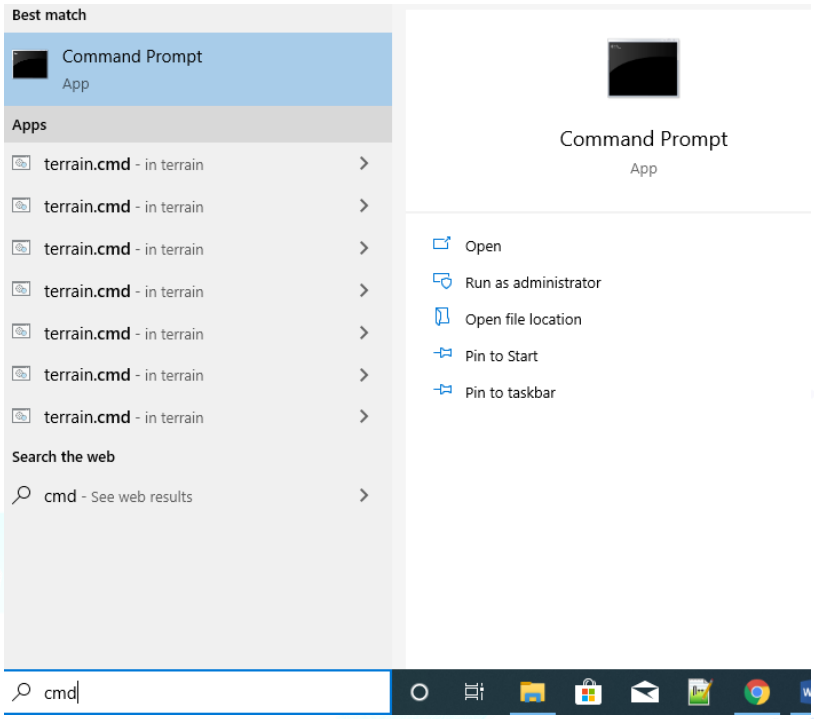


Figure 72 : Opening Command Prompt

- On the right panel appeared, click on 'Run as Administrator'
- A dialog box will appear. Click on yes.

ii) Using run utility

- Press ;Window key + R' on the keyboard. It will open Run utility dialog box.

- Type ‘cmd’ and press enter.

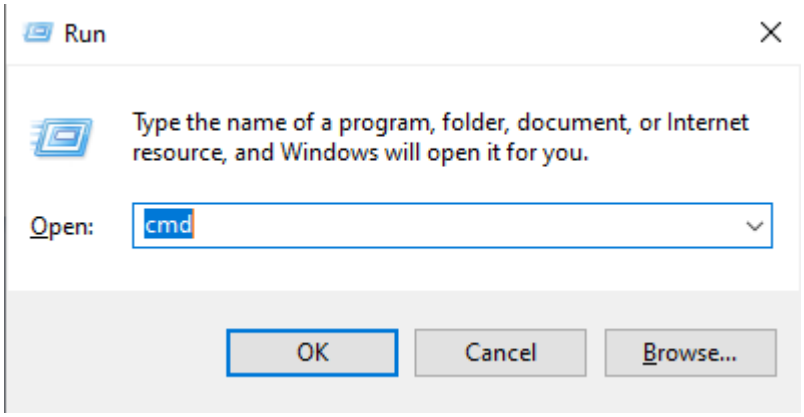


Figure 73 : Opening CMD using RUN

- Command prompt will open.

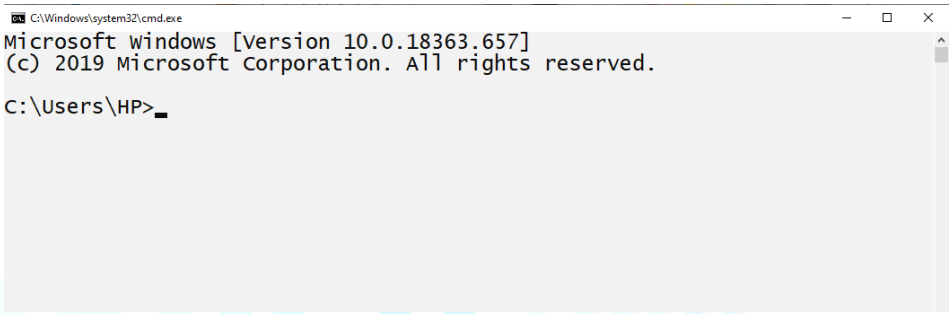


Figure 74 : Command Prompt Window

II) Some essential commands of cmd

ASSOC	Displays or modifies file extension associations.
ATTRIB	Displays or changes file attributes.
BREAK	Sets or clears extended CTRL+C checking.
BCDEDIT	Sets properties in boot database to control boot loading.
CACLS	Displays or modifies access control lists (ACLs) of files.
CALL	Calls one batch program from another.
CD	Displays the name of or changes the current directory.
CHCP	Displays or sets the active code page number.
CHDIR	Displays the name of or changes the current directory.
CHKDSK	Checks a disk and displays a status report.
CHKNTFS	Displays or modifies the checking of disk at boot time.

CLS	Clears the screen.
CMD	Starts a new instance of the Windows command interpreter.
COLOR	Sets the default console foreground and background colors.
COMP	Compares the contents of two files or sets of files.
COMPACT partitions.	Displays or alters the compression of files on NTFS
CONVERT the current drive.	Converts FAT volumes to NTFS. You cannot convert
COPY	Copies one or more files to another location.
DATE	Displays or sets the date.
DEL	Deletes one or more files.
DIR	Displays a list of files and subdirectories in a directory.
DISKPART	Displays or configures Disk Partition properties.
DOSKEY creates macros.	Edits command lines, recalls Windows commands, and
DRIVERQUERY	Displays current device driver status and properties.
ECHO	Displays messages, or turns command echoing on or off.
ENDLOCAL file.	Ends localization of environment changes in a batch
ERASE	Deletes one or more files.
EXIT	Quits the CMD.EXE program (command interpreter).
FC differences.	Compares two files or sets of files, and displays the
FIND	Searches for a text string in a file or files.
FINDSTR	Searches for strings in files.
FOR	Runs a specified command for each file in a set of files.
FORMAT	Formats a disk for use with Windows.
FSUTIL	Displays or configures the file system properties.
FTYPE associations.	Displays or modifies file types used in file extension

GOTO	Directs the Windows command interpreter to a labelled line in a batch program.
GPRESULT	Displays Group Policy information for machine or user.
GRAFTABL	Enables Windows to display an extended character set in graphics mode.
HELP	Provides Help information for Windows commands.
ICACLS	Display, modify, backup, or restore ACLs for files and directories.
IF	Performs conditional processing in batch programs.
LABEL	Creates, changes, or deletes the volume label of a disk.
MD	Creates a directory.
MKDIR	Creates a directory.
MKLINK	Creates Symbolic Links and Hard Links
MODE	Configures a system device.
MORE	Displays output one screen at a time.
MOVE	Moves one or more files from one directory to another directory.
OPENFILES	Displays files opened by remote users for a file share.
PATH	Displays or sets a search path for executable files.
PAUSE	Suspends processing of a batch file and displays a message.
POPD	Restores the previous value of the current directory saved by PUSHD.
PRINT	Prints a text file.
PROMPT	Changes the Windows command prompt.
PUSHD	Saves the current directory then changes it.
RD	Removes a directory.
RECOVER	Recovers readable information from a bad or defective disk.
REM	Records comments (remarks) in batch files or CONFIG.SYS.
REN	Renames a file or files.

RENAME	Renames a file or files.
REPLACE	Replaces files.
RMDIR	Removes a directory.
ROBOCOPY	Advanced utility to copy files and directory trees
SET	Displays, sets, or removes Windows environment variables.
SETLOCAL	Begins localization of environment changes in a batch file.
SC	Displays or configures services (background processes).
SCHTASKS	Schedules commands and programs to run on a computer.
SHIFT	Shifts the position of replaceable parameters in batch files.
SHUTDOWN	Allows proper local or remote shutdown of machine.
SORT	Sorts input.
START	Starts a separate window to run a specified program or command.
SUBST	Associates a path with a drive letter.
SYSTEMINFO	Displays machine specific properties and configuration.
TASKLIST	Displays all currently running tasks including services.
TASKKILL	Kill or stop a running process or application.
TIME	Displays or sets the system time.
TITLE	Sets the window title for a CMD.EXE session.
TREE	Graphically displays the directory structure of a drive or path.
TYPE	Displays the contents of a text file.
VER	Displays the Windows version.
VERIFY	Tells Windows whether to verify that your files are written correctly to a disk.
VOL	Displays a disk volume label and serial number.
XCOPY	Copies files and directory trees.
WMIC	Displays WMI information inside interactive command shell.

III)Other cmd Commands essential for incident response or cyber security

i) systeminfo command

This tool displays operating system configuration information for a local or remote machine, including service pack levels.

Parameter List:

/S system	Specifies the remote system to connect to.
/U [domain\]user	Specifies the user context under which the command should execute.
/P [password]	Specifies the password for the given user context. Prompts for input if omitted.
/FO format	Specifies the format in which the output is to be displayed. Valid values: "TABLE", "LIST", "CSV".
/NH	Specifies that the "Column Header" should not be displayed in the output. Valid only for "TABLE" and "CSV" formats.

Examples:

SYSTEMINFO

SYSTEMINFO /S system

SYSTEMINFO /S system /U user

SYSTEMINFO /S system /U domain\user /P password /FO TABLE

```
C:\Users\HP>systeminfo

Host Name:                 DESKTOP-UEOODAC
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.18363 N/A Build 18363
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          HP
Registered Organization:
Product ID:                00331-10000-00001-AA028
Original Install Date:     27-02-2020, 18:54:40
System Boot Time:          11-05-2020, 10:45:38
System Manufacturer:       Hewlett-Packard
System Model:              HP Pavilion 15 Notebook PC
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 69 Stepping 1 GenuineIntel ~1900 Mhz
BIOS Version:              Insyde F.53, 10-04-2017
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     8,122 MB
Available Physical Memory: 4,071 MB
Virtual Memory: Max Size:  9,402 MB
```

Figure 75 : Systeminfo Command

ii) Whoami

This command shows the currently logged on user on the system.

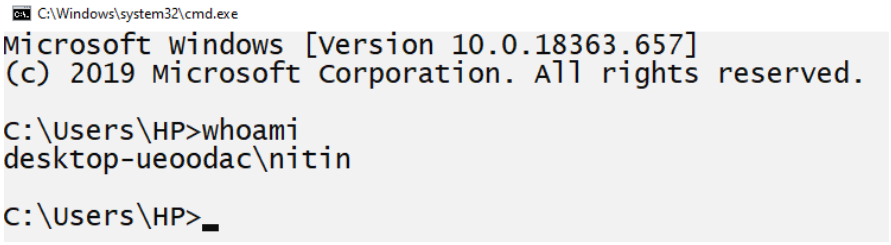


Figure 76 : whoami Command

WhoAmI has three ways of working:

Syntax 1:

WHOAMI [/UPN | /FQDN | /LOGONID]

Syntax 2:

WHOAMI { [/USER] [/GROUPS] [/CLAIMS] [/PRIV] } [/FO format] [/NH]

Syntax 3:

WHOAMI /ALL [/FO format] [/NH]

Description:

This utility can be used to get user name and group information along with the respective security identifiers (SID), claims, privileges, logon identifier (logon ID) for the current user on the local system. I.e. who is the current logged on user? If no switch is specified, tool displays the user name in NTLM format (domain\username).

Parameter List:

/UPN	Displays the user name in User Principal Name (UPN) format.
/FQDN	Displays the user name in Fully Qualified Distinguished Name (FQDN) format.
/USER	Displays information on the current user along with the security identifier (SID).
/GROUPS	Displays group membership for current user, type of account, security identifiers (SID) and attributes.
/CLAIMS	Displays claims for current user, including claim name, flags, type and values.
/PRIV	Displays security privileges of the current user.
/LOGONID	Displays the logon ID of the current user.

/ALL	Displays the current user name, groups belonged to along with the security identifiers (SID), claims and privileges for the current user access token.
/FO	format Specifies the output format to be displayed. Valid values are TABLE, LIST, CSV. Column headings are not displayed with CSV format. Default format is TABLE.
/NH	Specifies that the column header should not be displayed in the output. This is valid only for TABLE and CSV formats.
/?	Displays this help message.

Examples:

WHOAMI

WHOAMI /LOGONID

WHOAMI /USER

WHOAMI /USER /FO LIST

WHOAMI /USER /FO CSV

WHOAMI /GROUPS

WHOAMI /USER /GROUPS

WHOAMI /USER /GROUPS /CLAIMS /PRIV

WHOAMI /ALL

WHOAMI /ALL /FO LIST

WHOAMI /ALL /FO CSV /NH

iii) where comand

It displays the location of files that match the search pattern. By default, the search is done along the current directory and in the paths specified by the PATH environment variable.

Parameter List:

/R	Recursively searches and displays the files that match the given pattern starting from the specified directory.
/Q	Returns only the exit code, without displaying the list of matched files. (Quiet mode)
/F	Displays the matched filename in double quotes.
/T	Displays the file size, last modified date and time for all matched files.

Pattern Specifies the search pattern for the files to match. Wildcards * and ? can be used in the pattern. The "$env:pattern" and "path:pattern" formats can also be specified, where "env" is an environment variable and the search is done in the specified paths of the "env" environment variable. These formats should not be used with /R. The search is also done by appending the extensions of the PATHEXT variable to the pattern.

NOTE: The tool returns an error level of 0 if the search is successful, of 1 if the search is unsuccessful and of 2 for failures or errors.

Examples:

WHERE myfilename1 myfile????.*

WHERE $windir:*.*

WHERE /R c:\windows *.exe *.dll *.bat

WHERE /Q ??.???

WHERE "c:\windows;c:\windows\system32:*.dll"

WHERE /F /T *.dll

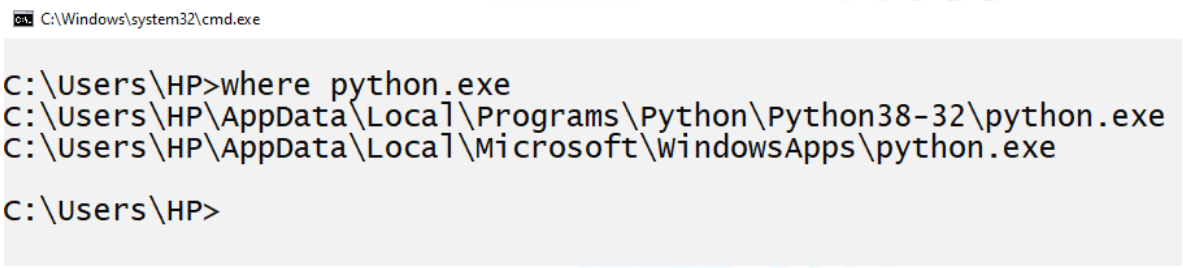


Figure 77 : Where Command

iv) ping command

This command sends ICMP packets to the target specified in the command. The target can be a URL or an IP address.

Syntax:

ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list] | [-k host-list]][-w timeout] [-R] [-S srcaddr] [-c compartment] [-p][-4] [-6] target_name

Options:

-t	Ping the specified host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C.
-a	Resolve addresses to hostnames.
-n count	Number of echo requests to send.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet (IPv4-only).

-i TTL	Time To Live.
-v TOS	Type of Service (IPv4-only. This setting has been deprecated and has no effect on the type of service field in the IP Header).
-r count	Record route for count hops (IPv4-only).
-s count	Timestamp for count hops (IPv4-only).
-j host-list	Loose source route along host-list (IPv4-only).
-k host-list	Strict source route along host-list (IPv4-only).
-w timeout	Timeout in milliseconds to wait for each reply.
-R	Use routing header to test reverse route also (IPv6-only). Per RFC 5095 the use of this routing header has been deprecated. Some systems may drop echo requests if this header is used.
-S srcaddr	Source address to use.
-c	compartment Routing compartment identifier.
-p	Ping a Hyper-V Network Virtualization provider address.
-4	Force using IPv4.
-6	Force using IPv6.

v) nsloolup command

It queries configured DNS server to find IP address of any website URL.

vi) tracert command

It shows the complete route of the path from your computer to website.

Syntax:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout][-R] [-S srcaddr] [-4] [-6] target-name

Options:

-d	Do not resolve addresses to hostnames.
-h maximum_hops	Maximum number of hops to search for target.
-j host-list	Loose source route along host-list (IPv4-only).
-w timeout	Wait timeout milliseconds for each reply.
-R	Trace round-trip path (IPv6-only).
-S srcaddr	Source address to use (IPv6-only).
-4	Force using IPv4.

-6	Force using IPv6.

vii) IPconfig command

This command provides detailed information about each and every network adapter in the system utilizing TCP/IP.

Syntax:

ipconfig [/allcompartments] [/? | /all | /renew [connection-name] | /release [connection-name] | /renew6 [connection-name] | /release6 [connection-name] |/flushdns | /displaydns | /registerdns | /showclassid connection-name | /setclassid connection-name [classid] |/showclassid6 connection-name |/setclassid6 connection-name [classid]]

Options:

/all	Display full configuration information.
/release	Release the IPv4 address for the specified adapter.
/release6	Release the IPv6 address for the specified adapter.
/renew	Renew the IPv4 address for the specified adapter.
/renew6	Renew the IPv6 address for the specified adapter.
/flushdns	Purges the DNS Resolver cache.
/registerdns	Refreshes all DHCP leases and re-registers DNS names
/displaydns	Display the contents of the DNS Resolver Cache.
/showclassid	Displays all the dhcp class IDs allowed for adapter.
/setclassid	Modifies the dhcp class id.
/showclassid6	Displays all the IPv6 DHCP class IDs allowed for adapter.
/setclassid6	Modifies the IPv6 DHCP class id.

Examples:

> ipconfig ... Show information

> ipconfig /all ... Show detailed information

> ipconfig /renew ... renew all adapters

> ipconfig /renew EL* ... renew any connection that has its name starting with EL

> ipconfig /release *Con* ... release all matching connections, eg. "Wired Ethernet Connection 1" or "Wired Ethernet Connection 2"

> ipconfig /allcompartments ... Show information about all compartments

> ipconfig /allcompartments /all ... Show detailed information about all compartments

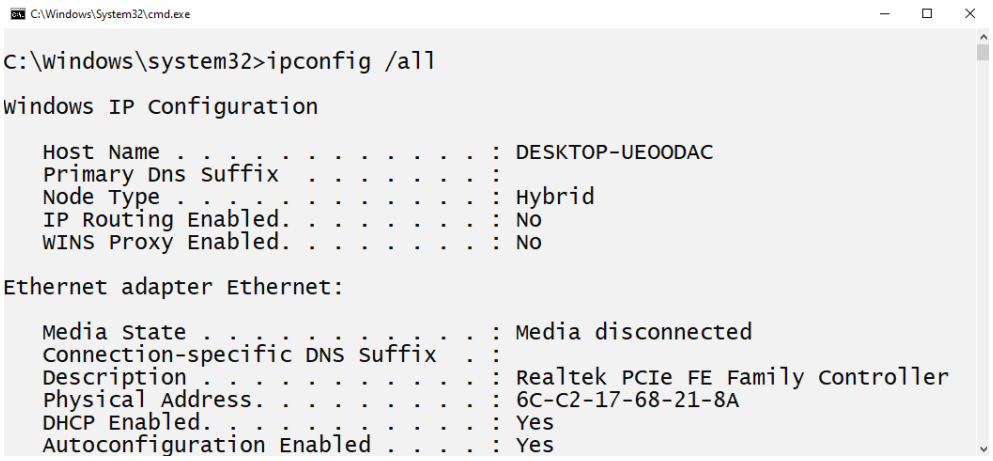


Figure 78 : IPCONFIG

viii) System file checker (sfc) command

Scans the integrity of all protected system files and replaces incorrect versions with correct Microsoft versions.

Syntax:

SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<file>] [/VERIFYFILE=<file>][/OFFWINDIR=<offline windows directory> /OFFBOOTDIR=<offline boot directory> [/OFFLOGFILE=<log file path>]]

Options:

/SCANNOW	Scans integrity of all protected system files and repairs files with problems when possible.
/VERIFYONLY	Scans integrity of all protected system files. No repair operation is performed.
/SCANFILE	Scans integrity of the referenced file, repairs file if problems are identified. Specify full path <file>
/VERIFYFILE	Verifies the integrity of the file with full path <file>. No repair operation is performed.
/OFFBOOTDIR	For offline repair, specify the location of the offline boot directory
/OFFWINDIR directory	For offline repair, specify the location of the offline windows
/OFFLOGFILE file path	For offline repair, optionally enable logging by specifying a log

Example:

sfc /SCANNOW

sfc /VERIFYFILE=c:\windows\system32\kernel32.dll

sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows

sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows /OFFLOGFILE=c:\log.txt

sfc /VERIFYONLY

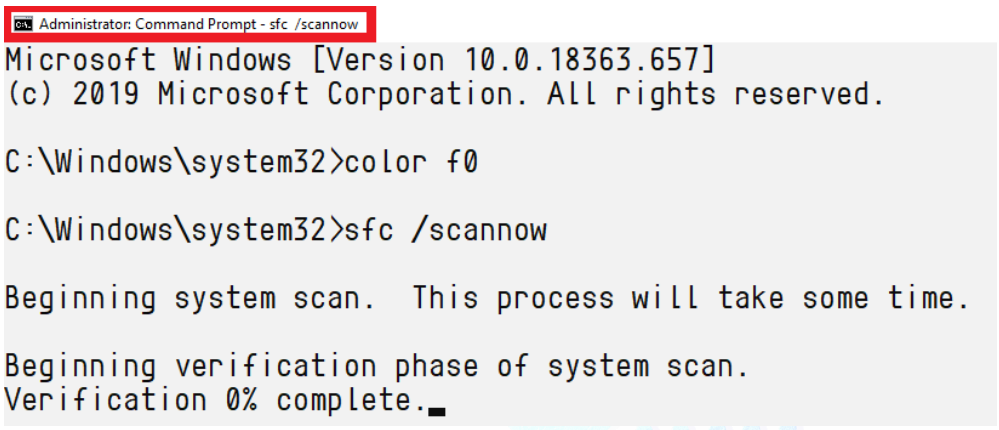


Figure 79 : SFC Command

Note :
SFC Command will work only in administrative mode.

ix) Windows management instrumentation command-line (wmic) command

In windows wmic is a command line utility which allows an administrative user to access all the detailed information about a windows machine. It is a very powerful tool in windows which also includes display of detailed information about attributes of thousands of settings and objects. It contains a lot handles for displaying various things.

Example:

Wmic process list full will show the complete detailed list of windows processes.

Wmic process list brief will show a brief list of processes.

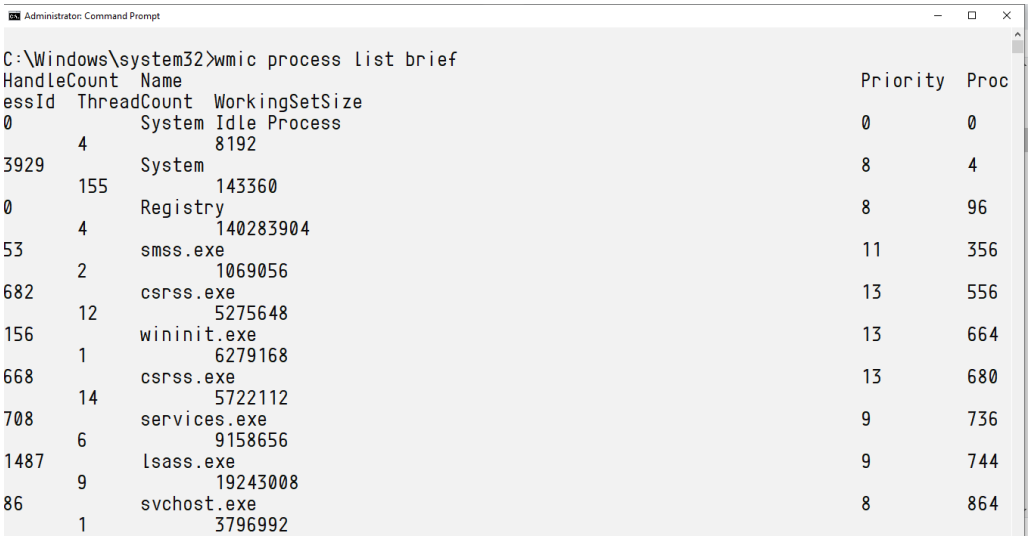


Figure 80 : WMIC Command

x) net command

It is very useful command in windows command prompt which can be used by administrators to see various kind of information related to windows system.

Syntax:

NET [ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |STATISTICS | STOP | TIME | USE | USER | VIEW]

Example:

Net user -- It will display list of all the users of the computer.

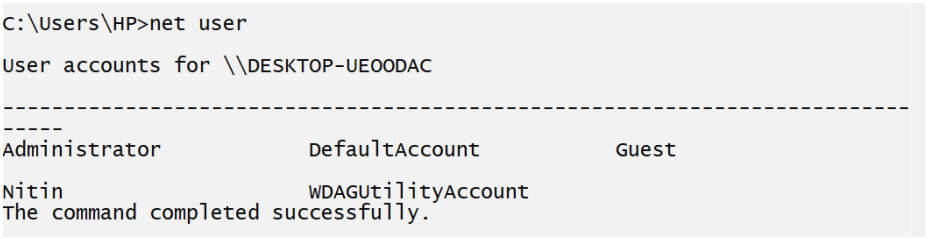


Figure 81 : Net Command

xi) attrib command

This command is used to display or change/modify the attributes of a file or folder present in computer system.

Syntax:

ATTRIB [+R | -R] [+A | -A] [+S | -S] [+H | -H] [+O | -O] [+I | -I] [+X | -X] [+P | -P] [+U | -U[drive:][path][filename] [/S [/D]] [/L]

Options:

+	Sets an attribute.
-	Clears an attribute.
R	Read-only file attribute.
A	Archive file attribute.
S	System file attribute.
H	Hidden file attribute.
O	Offline attribute.
I	Not content indexed file attribute.
X	No scrub file attribute.
V	Integrity attribute.
P	Pinned attribute.
U	Unpinned attribute.
B	SMR Blob attribute.
[drive:][path][filename]	Specifies a file or files for attrib to process.
/S	Processes matching files in the current folder and all subfolders.
/D	Processes folders as well.
/L	Work on the attributes of the Symbolic Link versus the target of the Symbolic Link

Example:

Command ***attrib +r +s abc.txt*** will make the file abc..txt as read only system file.

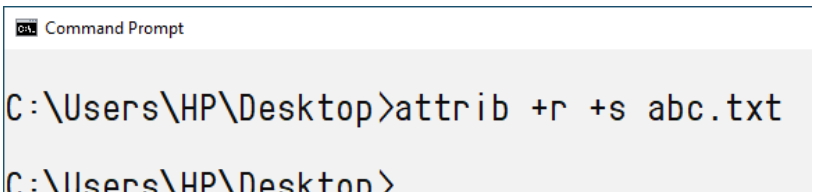


Figure 82 : Attrib Example

Now if anyone tries to delete that file the window will popup a message.

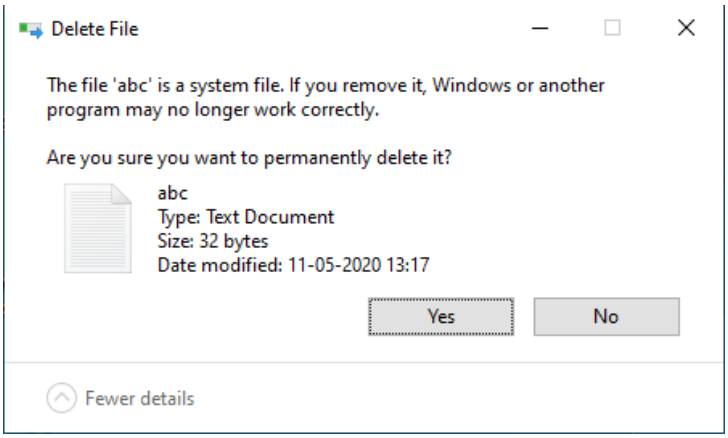


Figure 83 : System Popup

3.2. Windows Event Viewer

It is a tool in windows operating system which shows the detailed information about all the events happening in the operating system. It shows logs of applications and system messages (including errors, information messages, and warnings). It's a useful tool for troubleshooting all kinds of different Windows problems.

I) Steps to open event viewer

- Go to the windows search bar and type event manager.
- In the right-side panel click on 'Run as administrator'

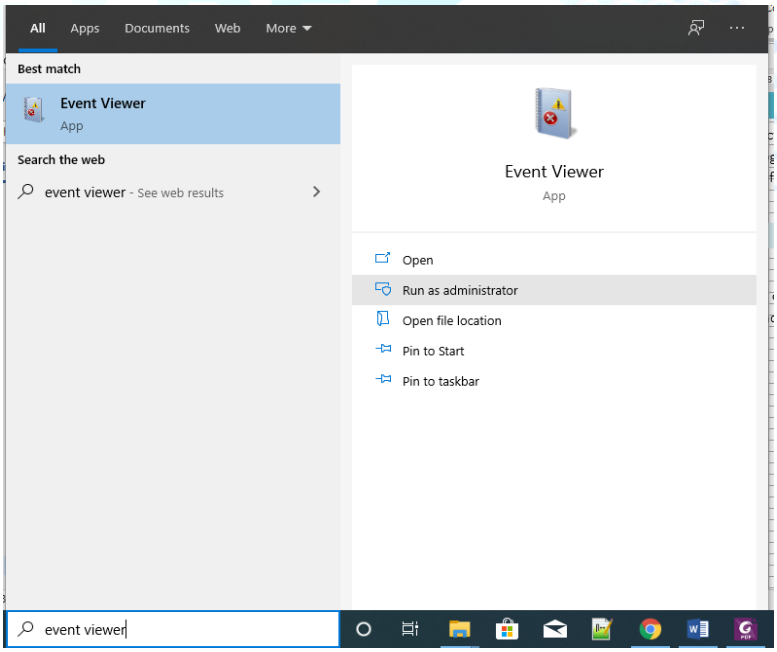


Figure 84: Opening Event Viewer

- A system dialog box will appear in that click on 'yes'.

- Event viewer window will open.

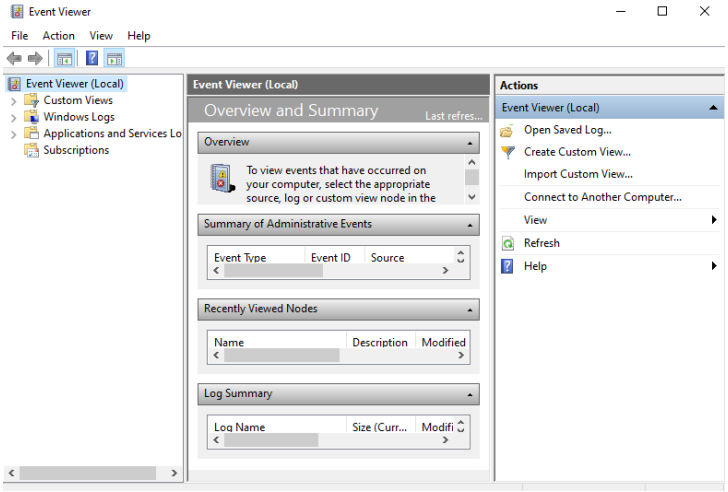


Figure 85 : Event Viewer

II) Types of events (or logs)

Generally, logs can be divided into three categories. These are –

- **System Logs :** Events & logs related to programs installed in the system.
- **Application Logs :** These are events & logs related to system components like drivers installed etc.
- **Security Logs :** Logs & Events related to security of system like logon attempts etc.

On the basis of type of event occur the event viewer can display various messages related to failure audit, success audit, system error, system warning etc.

3.3. Log2Timeline Tool[15]

It is a python-based tool for generating forensic timelines from digital evidence, such as disk images or event logs. It is based on command line.

Log2Timeline tool can be downloaded from https://github.com/log2timeline/plaso

This tool contains various switches and parameters to perform effective actions. It extract events from individual files, recursing a directory (e.g. mount point) or storage media image or device. This tool creates a plaso storage file and this file can be analysed with tools like pinfo and psort.

The plaso storage file contains the extracted events and various metadata about the collection process alongside information collected from the source data. It may also contain information about tags applied to events and reports from analysis plugins.

[15] (Palso, n.d.)

Example of info switch in the tool is presented below :

```
log2timeline.py --info
======================== log2timeline/plaso information ========================

****************************** Parser Presets *******************************
                android : android_app_usage, android_calls, android_sms
                  linux : bencode, filestat, google_drive, java_idx, olecf,
                          openxml, pls_recall, popularity_contest, selinux,
                          skype, syslog, utmp, webhist, xchatlog,
                          xchatscrollback, zeitgeist
                 macosx : appusage, asl_log, bencode, bsm_log, cups_ipp,
                          filestat, google_drive, java_idx, ls_quarantine,
                          mac_appfirewall_log, mac_document_versions,
                          mac_keychain, mac_securityd, mackeeper_cache,
                          macwifi, olecf, openxml, plist, skype, utmpx,
                          webhist
..
```

Figure 86 : Log2Timeline Tool

I) How to run log2timeline

- Download the Log2Timeline tool from the above given link.

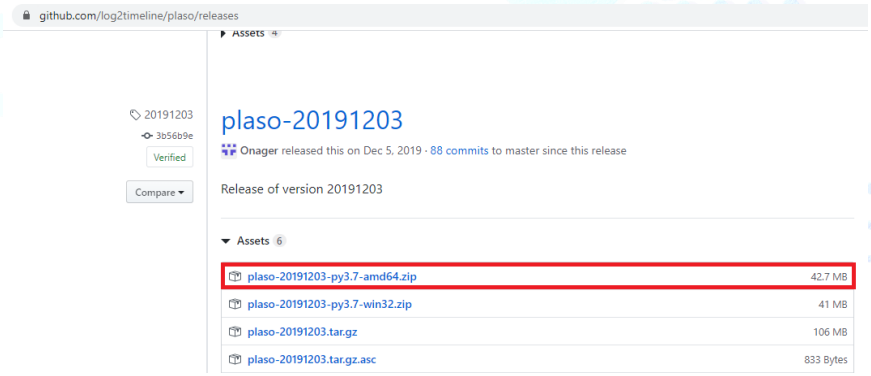


Figure 87 : Download Log2Timeline

- Extract the zip file using any zip extractor.

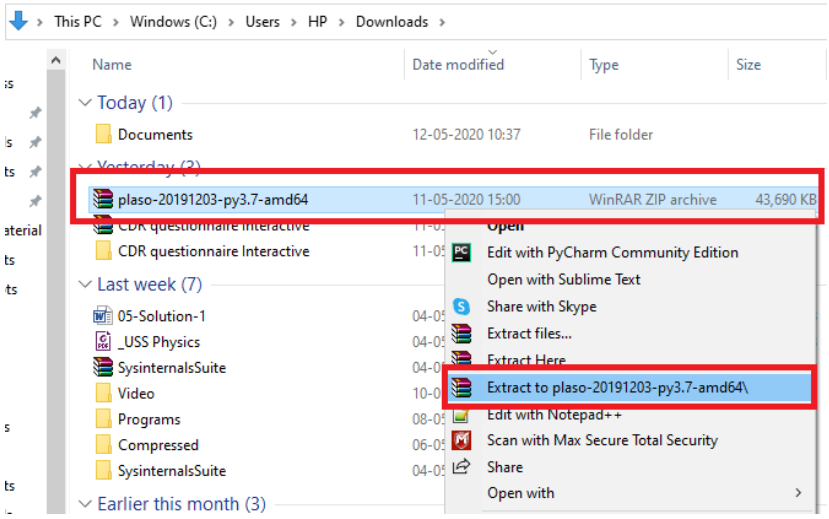


Figure 88 : Extraction of Plaso Zip file

- Now open the extracted folder & Look for Log2timeline.exe and psort.exe in the folder.

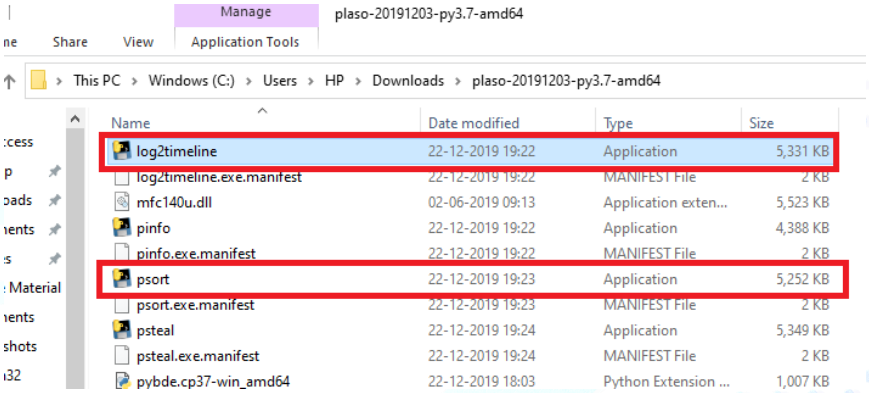


Figure 89 : Application Log2Timeline & psort in Folder

- If both the files are there open the command prompt in the folder. (To open CMD in windows 7 & 8 press shift and right click in the window and click on open command prompt window here and for windows 8.1 & above go to the address bar and type cmd there.)

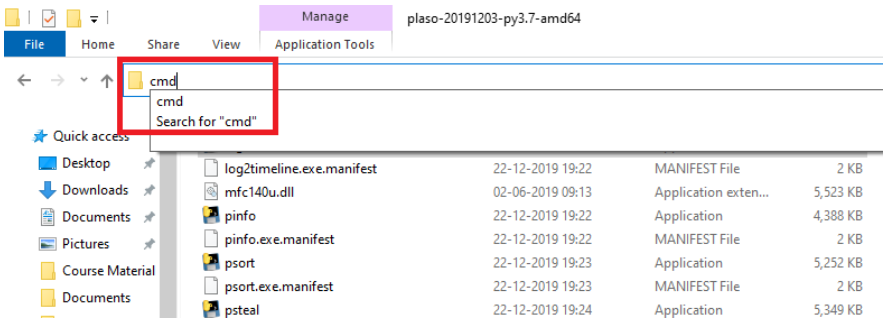


Figure 90 : Opening CMD in the same folder

- CMD window with same folder address will open.

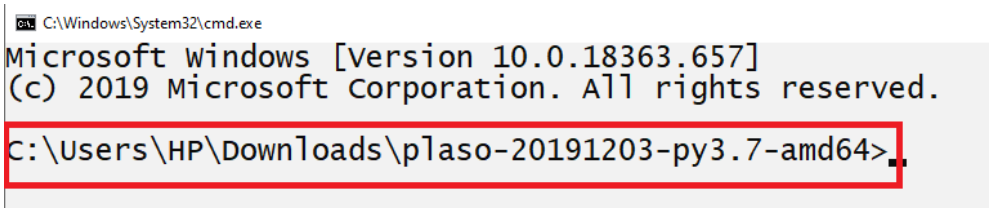


Figure 91 : CMD Prompt in Plaso Folder

II) commands to execute

- Open the CMD in the same folder where Log2Timeline.exe is present.
- Execute the following command to run Log2Timeline.exe

log2timeline.exe "Output_File_Name.plaso" "Input_File_Name"

- It will give a plaso file in output which can be converted into csv by using psort tool with the following command.

psort.exe -z timezone -o l2tcsv -w "Output_File_Name.csv" "Input_Plaso_File.plaso"

"-o" specifies the format of the output file (L2TCSV).
"-z" specifies the timezone that you want (US/Pacific).
Output_File_Name.csv is the time line CSV output.
Input_Plaso_File.plaso is the input plaso file.

Example – 1 :

We have taken a PNG file named as screenshot.png. Let's convert it into plaso file using Log2Timeline

- Run the command with address & name of input & output file.

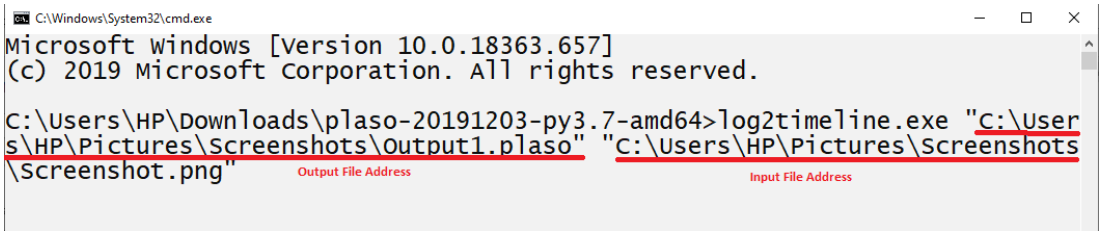


Figure 92 : Running Log2Timeline

- Wait till the process ends.

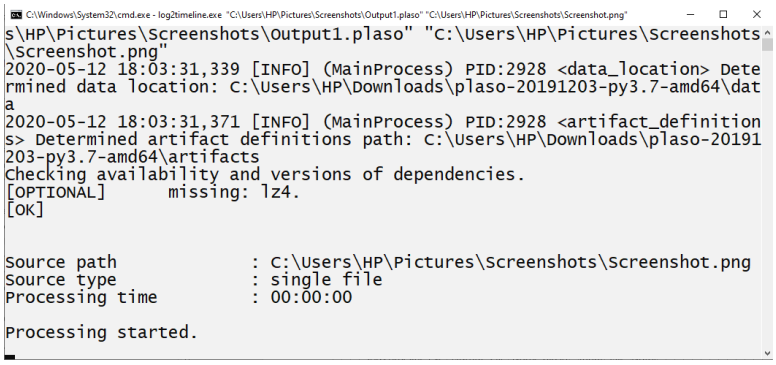


Figure 93 : Log2Timeline Processing

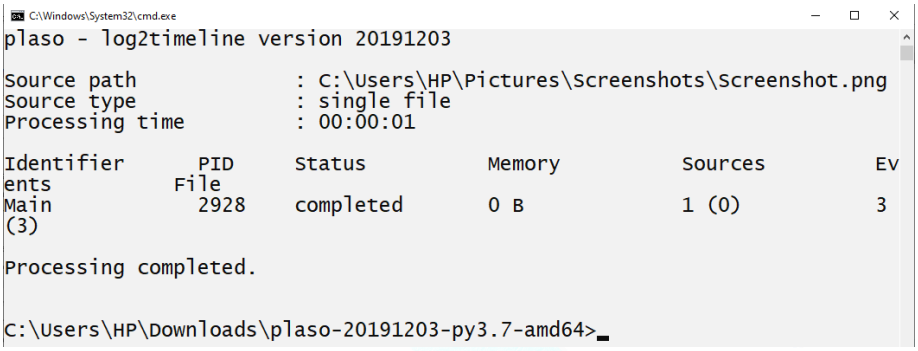


Figure94 : Process Completion

- Now the plaso file is generated in the output folder whose path is defined in the command.
- To convert this output plaso file into other desired readable format use psort.ext with the following commad.
  psort.exe -z UTC -o l2tcsv -w "outpputfile.csv" "inputfile.plaso.

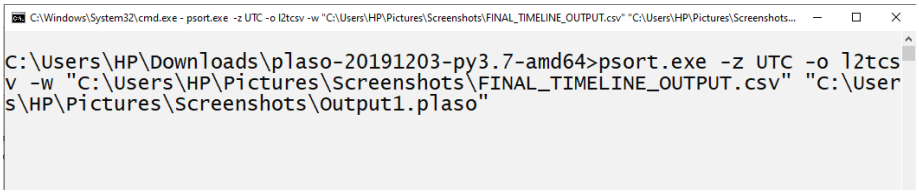


Figure 95 : Psort Input Command

- As the process will complete you will see the following screen.

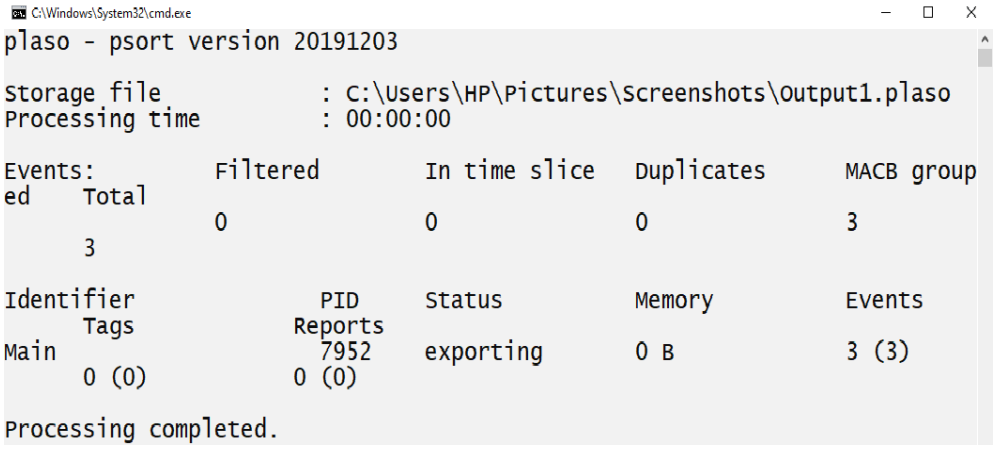


Figure 96 : Psort Process Complete

- The csv file is created and stored at output path. It can be viewed by using excel.

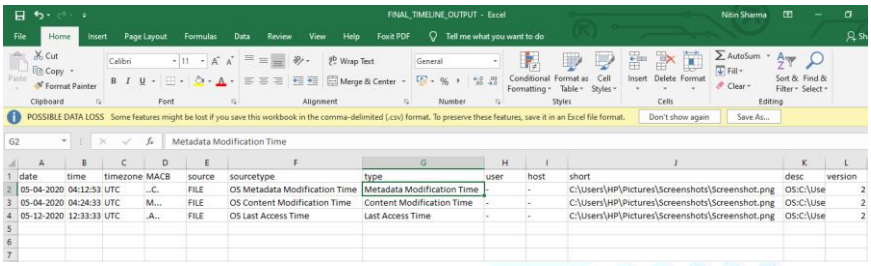


Figure 97 : CSV File

III)Output formats supported by log2timeline

- **l2tcsv :** CSV format used by legacy log2timeline, with 17 fixed fields.
- **xlsx :** Excel Spreadsheet (XLSX) output
- **l2ttln :** Extended TLN 7 field | delimited output.
- **4n6time_sqlite :** Saves the data in a SQLite database, used by the tool 4n6time.
- **kml :** Saves events with geography data into a KML format.
- **dynamic :** Dynamic selection of fields for a separated value output format.
- **rawpy :** "raw" (or native) Python output.
- **json :** Saves the events into a JSON format.
- **null :** Output module that does not output anything.
- **tln :** TLN 5 field | delimited output.
- **json_line :** Saves the events into a JSON line format.

Example – 2:

Let’s have a folder named as Test which contains different types of file in it. Now we will examine it using log2timeline tool.

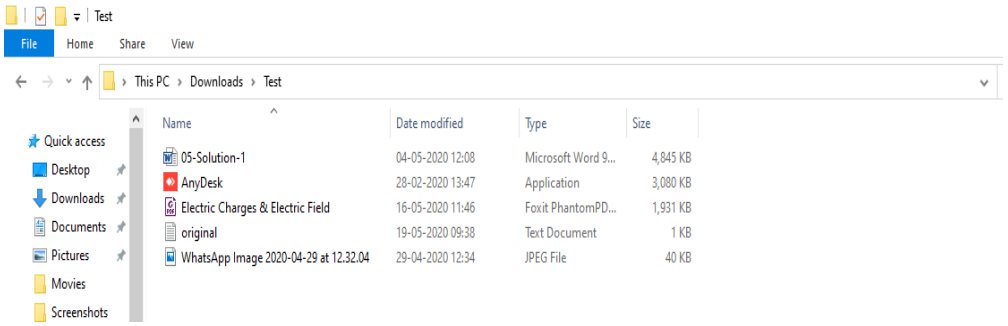


Figure 98 : Test Folder

- Use the similar command used above to create a plaso file for test folder.

```
C:\Users\HP\Downloads\plaso-20191203-py3.7-amd64>log2timeline.exe "C:\User
s\HP\Downloads\Test_output.plaso" "C:\Users\HP\Downloads\Test"
2020-05-24 12:15:49,000 [INFO] (MainProcess) PID:8360 <data_location> Dete
rmined data location: C:\Users\HP\Downloads\plaso-20191203-py3.7-amd64\dat
a
2020-05-24 12:15:49,047 [INFO] (MainProcess) PID:8360 <artifact_definition
s> Determined artifact definitions path: C:\Users\HP\Downloads\plaso-20191
203-py3.7-amd64\artifacts
Checking availability and versions of dependencies.
[OPTIONAL]      missing: lz4.
[OK]
```

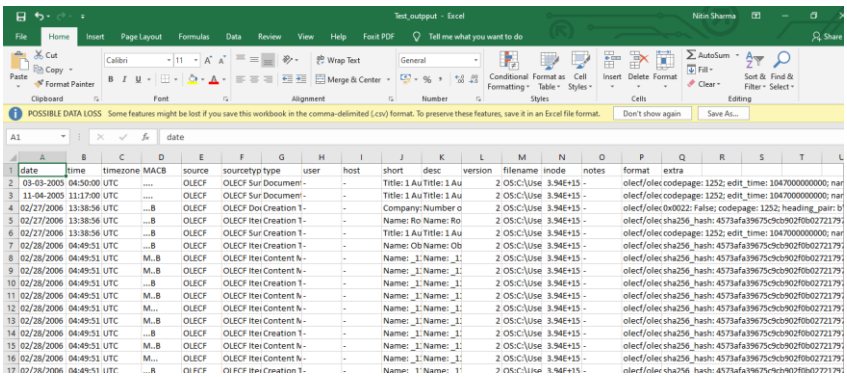
Figure 99 : Plaso Generation

- Now a plaso file is generated named as Test_Output.plaso. Use psort tool to convert this plaso file into readable format.

```
C:\Users\HP\Downloads\plaso-20191203-py3.7-amd64>psort.exe -z UTC -o l2tcs
v -w "C:\Users\HP\Downloads\Test_outpput.csv" "C:\Users\HP\Downloads\Test_
Output.plaso"
2020-05-24 12:25:02,861 [INFO] (MainProcess) PID:1764 <data_location> Dete
rmined data location: C:\Users\HP\Downloads\plaso-20191203-py3.7-amd64\dat
a
plaso - psort version 20191203

Storage file            : C:\Users\HP\Downloads\Test_Output.plaso
Processing time         : 00:00:00

Events:         Filtered        In time slice   Duplicates      MACB group
ed    Total
                0               0               0               0
      1040

Identifier              PID     Status          Memory          Events
      Tags            Reports
Main                    1764    exporting       0 B             1040 (1040
)     0 (0)           0 (0)

Processing completed.

C:\Users\HP\Downloads\plaso-20191203-py3.7-amd64>
```

Figure 100 : Psort Output Generation

- Check the output csv file using excel software.



date	time	timezone	MACB	source	sourcetyp	type	user	host	short	desc	version	filename	inode	notes	format	extra
03-03-2005	04:50:00	UTC	....	OLECF	OLECF Sur	Document	-	-	Title: 1 Au	Title: 1 Au	2	OS:C:\Use	3.94E+15	-	olecf/olec	codepage: 1252; edit_time: 1047000000000; nar
11-04-2005	11:17:00	UTC	....	OLECF	OLECF Sur	Document	-	-	Title: 1 Au	Title: 1 Au	2	OS:C:\Use	3.94E+15	-	olecf/olec	codepage: 1252; edit_time: 1047000000000; nar
02/27/2006	13:38:56	UTC	...B	OLECF	OLECF Do	Creation T	-	-	Company:	Number o	2	OS:C:\Use	3.94E+15	-	olecf/olec	0x0022: False; codepage: 1252; heading_pair: b
02/27/2006	13:38:56	UTC	...B	OLECF	OLECF Ite	Creation T	-	-	Name: Ro	Name: Ro	2	OS:C:\Use	3.94E+15	-	olecf/olec	sha256_hash: 4573afa39675c9cb902f0b0272179
02/27/2006	13:38:56	UTC	...B	OLECF	OLECF Sur	Creation T	-	-	Title: 1 Au	Title: 1 Au	2	OS:C:\Use	3.94E+15	-	olecf/olec	codepage: 1252; edit_time: 1047000000000; nar
02/28/2006	04:49:51	UTC	...B	OLECF	OLECF Ite	Creation T	-	-	Name: Ob	Name: Ob	2	OS:C:\Use	3.94E+15	-	olecf/olec	sha256_hash: 4573afa39675c9cb902f0b0272179
02/28/2006	04:49:51	UTC	M..B	OLECF	OLECF Ite	Content N	-	-	Name: _1	Name: _1	2	OS:C:\Use	3.94E+15	-	olecf/olec	sha256_hash: 4573afa39675c9cb902f0b0272179
02/28/2006	04:49:51	UTC	M..B	OLECF	OLECF Ite	Content N	-	-	Name: _1	Name: _1	2	OS:C:\Use	3.94E+15	-	olecf/olec	sha256_hash: 4573afa39675c9cb902f0b0272179
02/28/2006	04:49:51	UTC	...B	OLECF	OLECF Ite	Creation T	-	-	Name: _1	Name: _1	2	OS:C:\Use	3.94E+15	-	olecf/olec	sha256_hash: 4573afa39675c9cb902f0b0272179
02/28/2006	04:49:51	UTC	M..B	OLECF	OLECF Ite	Content N	-	-	Name: _1	Name: _1	2	OS:C:\Use	3.94E+15	-	olecf/olec	sha256_hash: 4573afa39675c9cb902f0b0272179
02/28/2006	04:49:51	UTC	M...	OLECF	OLECF Ite	Content N	-	-	Name: _1	Name: _1	2	OS:C:\Use	3.94E+15	-	olecf/olec	sha256_hash: 4573afa39675c9cb902f0b0272179
02/28/2006	04:49:51	UTC	M..B	OLECF	OLECF Ite	Content N	-	-	Name: _1	Name: _1	2	OS:C:\Use	3.94E+15	-	olecf/olec	sha256_hash: 4573afa39675c9cb902f0b0272179
02/28/2006	04:49:51	UTC	...B	OLECF	OLECF Ite	Creation T	-	-	Name: _1	Name: _1	2	OS:C:\Use	3.94E+15	-	olecf/olec	sha256_hash: 4573afa39675c9cb902f0b0272179
02/28/2006	04:49:51	UTC	M..B	OLECF	OLECF Ite	Content N	-	-	Name: _1	Name: _1	2	OS:C:\Use	3.94E+15	-	olecf/olec	sha256_hash: 4573afa39675c9cb902f0b0272179
02/28/2006	04:49:51	UTC	M...	OLECF	OLECF Ite	Content N	-	-	Name: _1	Name: _1	2	OS:C:\Use	3.94E+15	-	olecf/olec	sha256_hash: 4573afa39675c9cb902f0b0272179

Figure 101 : Final CSV Output

Bibliography

Andress, J. (2011). *The Basics of Information Security.* Elsevier.

In, C. . (n.d.). *Indian Computer Emergency Response Team*. Retrieved from certin: https://www.cert-in.org.in/

ISACA. (n.d.). *Cyber Security Fundamentals Study Guide.* ISACA.

Michael E. Whitman, H. J. (n.d.). *Principles of Information Security.* Cehgage Learning.

NIST. (2013). *Glossary of Key Information Security Terms.* NIST.

Palso. (n.d.). *Using log2timeline.py*. Retrieved from Palso: https://plaso.readthedocs.io/en/latest/sources/user/Using-log2timeline.html

Rahalkar, S. A. (2016). *Cetrified Ethical Hacker (CEH) Foundation Guide.* Apress.

Wikipedia. (n.d.). *National Cyber Security Policy 2013*. Retrieved from Wikipedia - The Free Encyclopedia: https://en.wikipedia.org/wiki/National_Cyber_Security_Policy_2013

Wikipedia. (n.d.). *National Cyber Coordination Centre*. Retrieved from Wikipedia - The Free Encyclopedia: https://en.wikipedia.org/wiki/National_Cyber_Coordination_Centre

Wikipedia. (n.d.). *National Security Council (India)*. Retrieved from Wikipedia - The Free Encyclopedia: https://en.wikipedia.org/wiki/National_Security_Council_(India)

Wikipedia. (n.d.). *National Technical Research Organisation*. Retrieved from Wikipedia - The Free Encyclopedia: https://en.wikipedia.org/wiki/National_Technical_Research_Organisation

Wikipedia. (n.d.). *Personal Data Protection Bill 2019*. Retrieved from Wikipedia, the free encyclopedia: https://en.wikipedia.org/wiki/Personal_Data_Protection_Bill_2019

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