Cyber Crimes, Law, Investigation and Forensics


Japan’s Former PM Shinzo Abe Was Reportedly Assassinated Using A 3D Printed Gun
FOSSBYTES

Banks, payment operators report fraud worth ₹1,750 cr in 7 months: RBI

GEORGE MATHEW
MUMBAI, MAY 1

BANKS AND payment operators have reported online payment frauds of Rs 1,750 crore in the seven months ended March 2023 even as online transactions picked up substantially in the last several months.

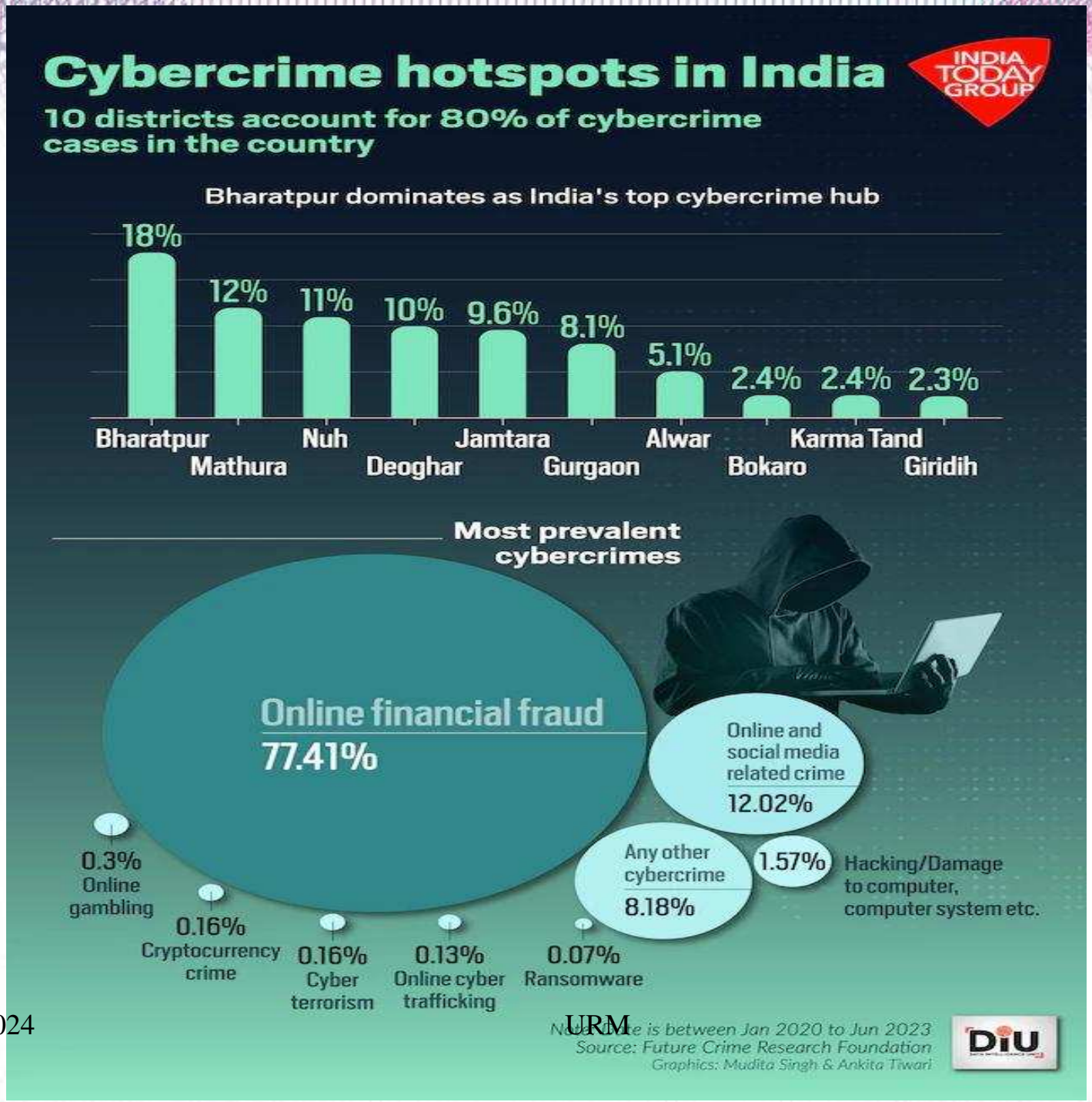
According to data available from the Reserve Bank of India, the fourth quarter ended March 2023 itself witnessed payment frauds of over Rs 800 crore under the new format of fraud reporting. While the month of March saw 2.25 lakh transactions involving Rs 333 crore payment frauds, comparable data for the same period in the previous year is not available.However, when compared to the volume of transactions the exposure to systemic risk, said Krishnan Chari, Chief Risk Officer, Worldline India.

"While policy makers lay out guidelines for paytech institutions for compliance on fraud and cyber risk management, it is also essential that a systemic risk man-

PAYMENT FRAUDS

MONTH	Volume (lakh)	Value (₹ cr)
Sep '22	1.71	249
Oct '22	1.79	220
Nov '22	2.06	257
Dec '22	1.54	204
Jan '23	1.57	195
Feb '23	2.29	317
Mar '23	2.25	333

Source: RBI


Cybercrime hotspots in India
INDIA TODAY GROUP
10 districts account for 80% of cybercrime cases in the country
Bharatpur dominates as India's top cybercrime hub
18%
12%
11%
10%
9.6%
8.1%
5.1%
2.4%
2.4%
2.3%
Bharatpur
Mathura
Nuh
Deoghar
Jamtara
Gurgaon
Alwar
Bokaro
Karma Tand
Giridih
Most prevalent cybercrimes
Online financial fraud
77.41%
Online and social media related crime
12.02%
Any other cybercrime
8.18%
1.57%
Hacking/Damage to computer, computer system etc.
0.3%
Online gambling
0.16%
Cryptocurrency crime
0.16%
Cyber terrorism
0.13%
Online cyber trafficking
0.07%
Ransomware
Source: Future Crime Research Foundation
Graphics: Mudita Singh & Ankita Tiwari
DiU

REPORTING

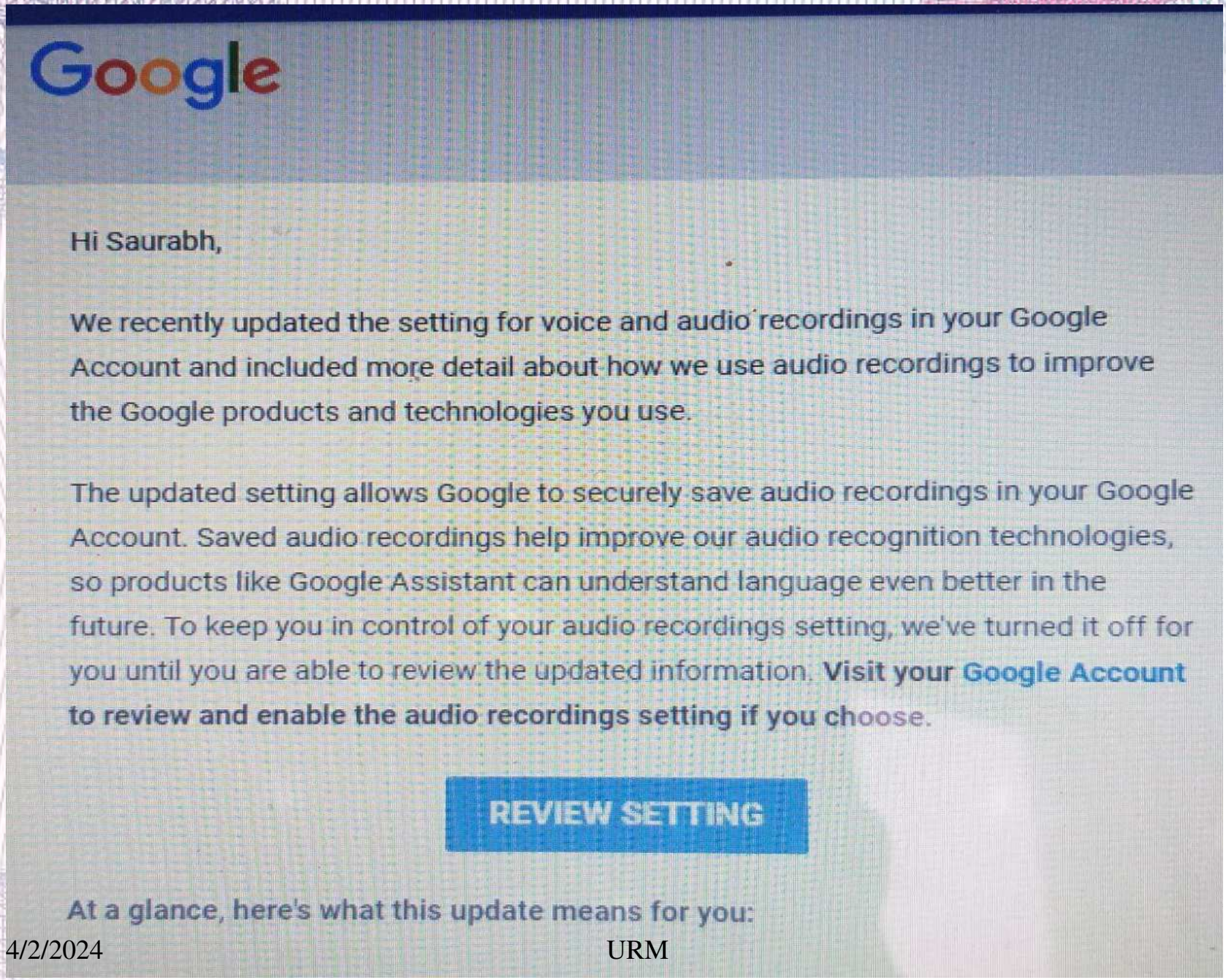
cybercrime.gov.in

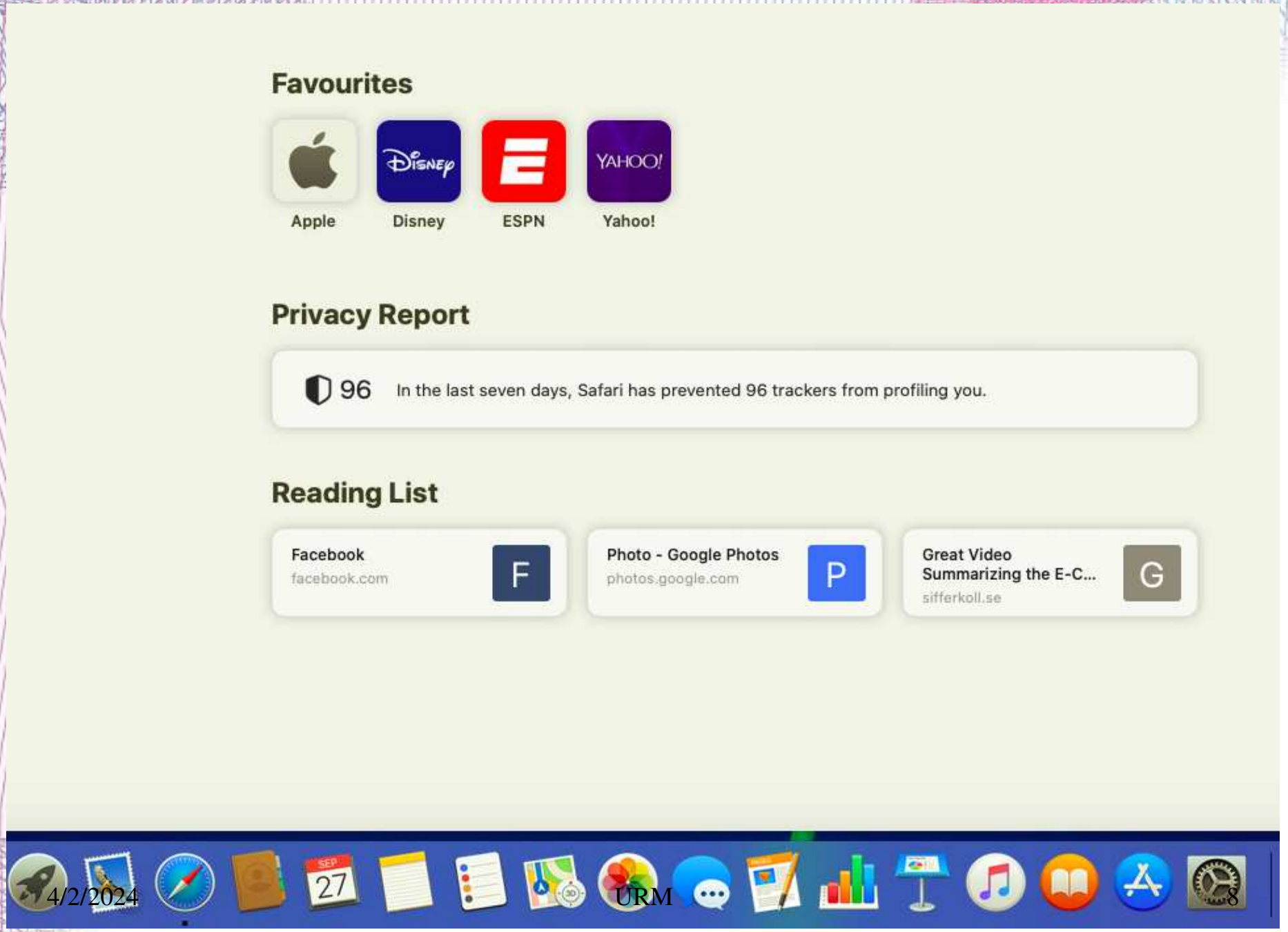
1930

Conventional Crimes, Jurisdiction, Crime Scene Investigation, Material Evidence, confession Leading to Recovery

Vs

Digital Crimes, No Crime Scene, Online Investigation, Technical Evidence.


Google
Hi Saurabh,
We recently updated the setting for voice and audio recordings in your Google Account and included more detail about how we use audio recordings to improve the Google products and technologies you use.
The updated setting allows Google to securely save audio recordings in your Google Account. Saved audio recordings help improve our audio recognition technologies, so products like Google Assistant can understand language even better in the future. To keep you in control of your audio recordings setting, we've turned it off for you until you are able to review the updated information. Visit your Google Account to review and enable the audio recordings setting if you choose.
REVIEW SETTING
At a glance, here's what this update means for you:

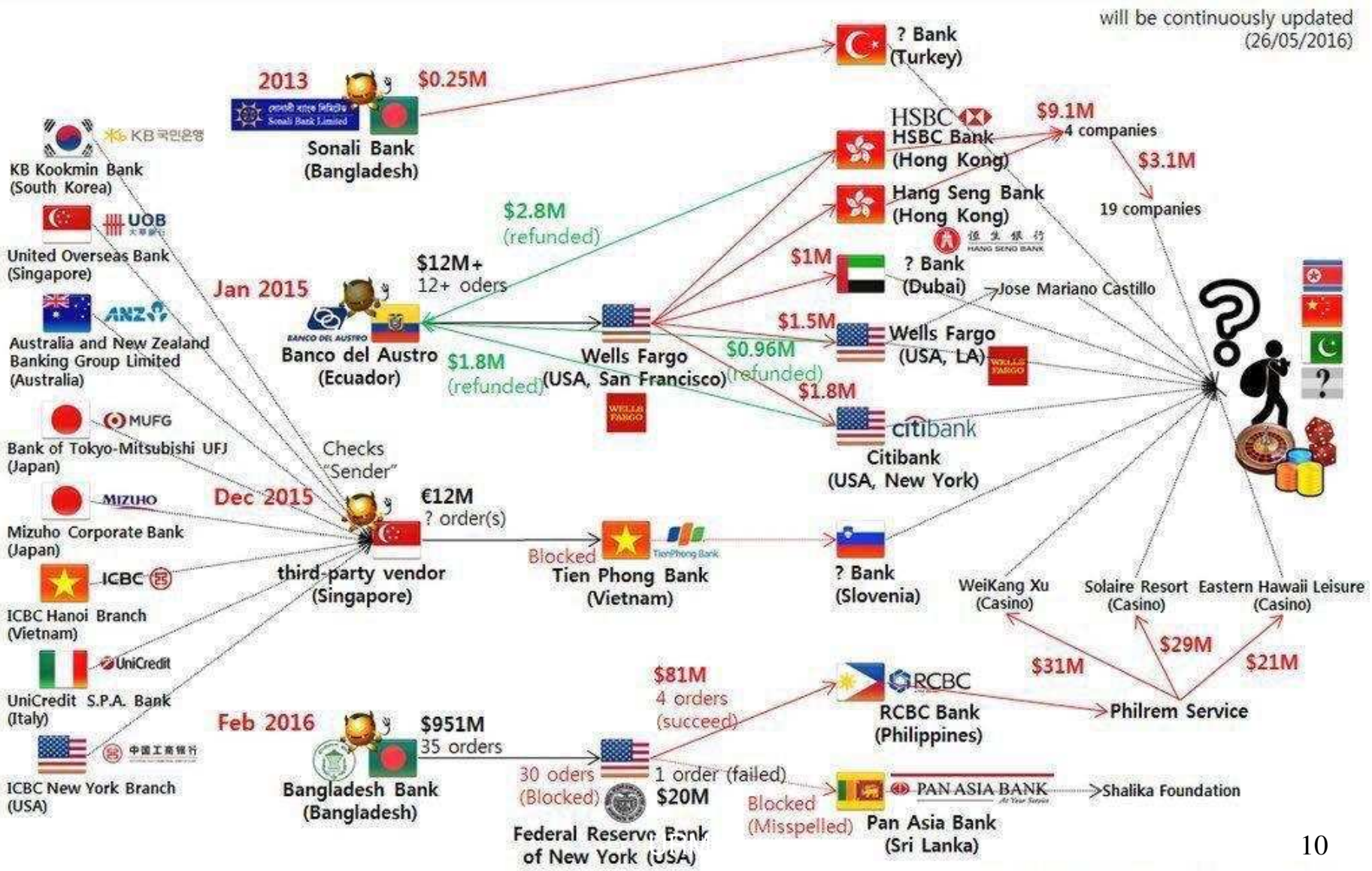

Favourites
Apple
Disney
ESPN
Yahoo!
Privacy Report
96
In the last seven days, Safari has prevented 96 trackers from profiling you.
Reading List
Facebook
facebook.com
F
Photo - Google Photos
photos.google.com
P
Great Video Summarizing the E-C...
sifferkoll.se
G

In Feb 2018, the City Union Bank's computer systems were hacked, transferring nearly $2 million through three unauthorized remittances. This was done using the SWIFT financial platform.

The international cyber criminals started putting India's less known banks on the top of their hacking targets. Pune based Cosmos Bank, was hacked between 11th & 13th Aug 2018, through a malware attack on it's servers. More than 12,000 transactions, criminals in 28 countries involved, debit cards cloned, firewall compromised and proxy server created to manage the authentication. It had all what a high end physical & cyber crime can have.

All these still seems to be a reconnaissance operations. State Bank of Mauritius, located in Mumbai faced a hack on 2nd Oct, accessing it's servers and transfer monies to multiple accounts outside the country. It claims to have recovered 90% of the Rs 190 Crores, does not dilute the gravity, intentions and technical capablities in hands of the hackers.

Hacking the Worldwide Banking System (Using fraudulent SWIFT messages)



From https://twitter.com/issuemakerslab

'EMPTYING' ATMs

Adding to the long list of cyber crimes is ATM hacking, which has seen a considerable increase in few months. This crosses the barriers of skimming based ATM hacks to a full fledged emptying of the ATMs, sounds like a physical type of a operation.

"Lazarus possesses an in-depth knowledge of banking systems and transaction processing protocols and has the expertise to leverage that knowledge in order to steal large sums from vulnerable banks.

Lazarus seems to have been perfecting the modus operandi with every successive hack. Banks network is breached and switch application servers handling ATM transactions compromised. The unsupported versions of AIX operating system is the main culprit.


HCL
12-11-2019 12:29:06
CAM 1
REC
From R/W HDD
Nov
2019
Su Mo Tu We Th Fr


24-06-2017 22:52:27


TP-LINK


SanDisk
Ultra
32GB


POLICE COMMISSIONERATE

Man dupes 20 women with offer of marriage

He creates a matrimonial profile, then lures the victim

JAYENDRA CHAITHANYA | DC
HYDERABAD, NOV. 14

A Class-VIII graduate from Nellore of Andhra Pradesh duped about 20 women including three techies under the pretext of marrying them and stole their money.

The accused N. Jeevan Kumar, 23, used pictures of others to create a matrimonial profile and input false details to lure women.

A woman techie living in Secunderabad who was searching for a prospective groom created her profile on *Jeevansathi.com* in February this year. While searching she found a profile on the name 'Rishi Kumar Nallapti' and expressed her interest.

After exchanging few formal conversations, they exchanged pictures and started talking over the phone. The man informed that he works as a professor at Indian Institute of Science in Bengaluru. One day, he informed her that his mother was suffering from cancer and he needs money for her treatment.

Believing it, the techie provided her credit card details and shared the OTPs with the stranger, who in turn withdrew about ₹2.4 lakh in various instalments. When she pressurised to meet him in person, he blocked her and stopped responding to her messages. Realising that she had been cheated, the techie lodged a complaint with the Hyderabad Cyber Crime Police.

A Cyber Crime official who is part of the probe said, "The accused identified as N. Jeevan Kumar was traced to Nellore based on technical evidence. He is a Class VIII dropout and unemployed. He spends most of his time online and indulges in fraud. His father was a realtor at Goa. After Class VIII, his family suffered financial losses and moved to Nellore and despite not pursuing education, he has a good command over English, which he used to trap innocent women."

By creating fake profiles on matrimony websites, he confessed to having cheated about 20 women so far with a similar modus operandi.

There are four complaints against him at Delhi, Odisha, Karnataka and Telangana, and all victims are software employees.

In March, he duped another techie from Bengaluru and collected ₹10 lakh from her and in April, another woman techie from Bengaluru fell prey to him and gave ₹1.8 lakh, said an official from the cyber crime.

N. Jeevan Kumar

- The accused N. Jeevan Kumar, used pictures of others to create a matrimony profile and lured women.
- The accused told a techie that he needed money for his mother's cancer treatment.

Online markets are the new fraud hubs

Cons Pose As Armymen To Lure Buyers

TIMES NEWS NETWORK

Hyderabad: Online marketplaces have become the new playground for fraudsters. According to Cybercrime police, though one-time password (OTP) frauds have declined, cases of cons at marketplaces like Olx have seen a rise.

There is a peculiar modus operandi. Fraudsters pretend to be army personnel on these sites to build a rapport with prospective buyers. They then post an ad on OLX or Quickr for the sale of mobile phones or other electronic items. If any buyer is interested, the fraudster sends a photo of a fake army identity card to lure them. Insisting on urgency of the sale, the fraudsters ask buyers to send money in advance. They then send a fake courier receipt to convince the buyer that they are sending the goods. Once the money is transferred over PayTm, the fraudsters stop picking buyers' calls.

At least 15 such complaints are received every month, say Cybercrime cops.

POLICE VIGIL ON PORTALS

- Cybercrime cops advised Olx to add a pop-up on **their website warning users of such frauds**
- They also asked the online marketplace portal to **delete duplicate ads and get an ID proof of every seller**
- Police advise users **not to transfer money to PayTm or bank accounts** before receiving the product
- **Victims lose ₹10 lakh on an average in such frauds**

"There are at least15 such cases where the victim was cheated by a seller who claimed to be an Army personnel. As people believe armymen to be honest, the fraudsters could con victims easily," said Additional Deputy Commissioner of Police (Cyber Crime) KCS Raghu Vir.

With rise of such fraud cases in the city the Cybercrime team along with detective department head and additional commissioner of police (crime) held a meeting with the Olx team.

"We had a meeting with the Olx director and his team on before Diwali. We raised concern about several such cases being recorded. In the past few months we have already registered almost 10 FIRs of such Olx frauds," said the Additional DCP.

A source in cybercrime police claimed that very few people file FIR and most of the cases are verbal petitions as the amount is less. There is a dedicated team to sniff out such suspicious ads on the online marketplace portals. Ifany suspicious activity is observed, the team informs the portal to block the user

"But once the offender is blocked on a particular platform, they move to another forum to lure innocent buyers," said the source.

My sister received a call today I see that as a potential Cyber attack. Details are as below:

3:29 PM

She is seeking for new job opportunities, she received a call saying that the call is from Naukri and we have an opening for Project Manager in Redmi with 6lakhs package. When she said she is ready for interview next week, the guy who called asked her to fill an online form. At the end of the online form it will ask for a payment of RS. 10/-. Payment can be made using debit or credit card details. once all the details including CVV, she received an OTP for 10,000/- . She called the same person to confirm why it is saying 10,000/-. He replied asking her to share the screenshot of the that message which shows 10,000/-

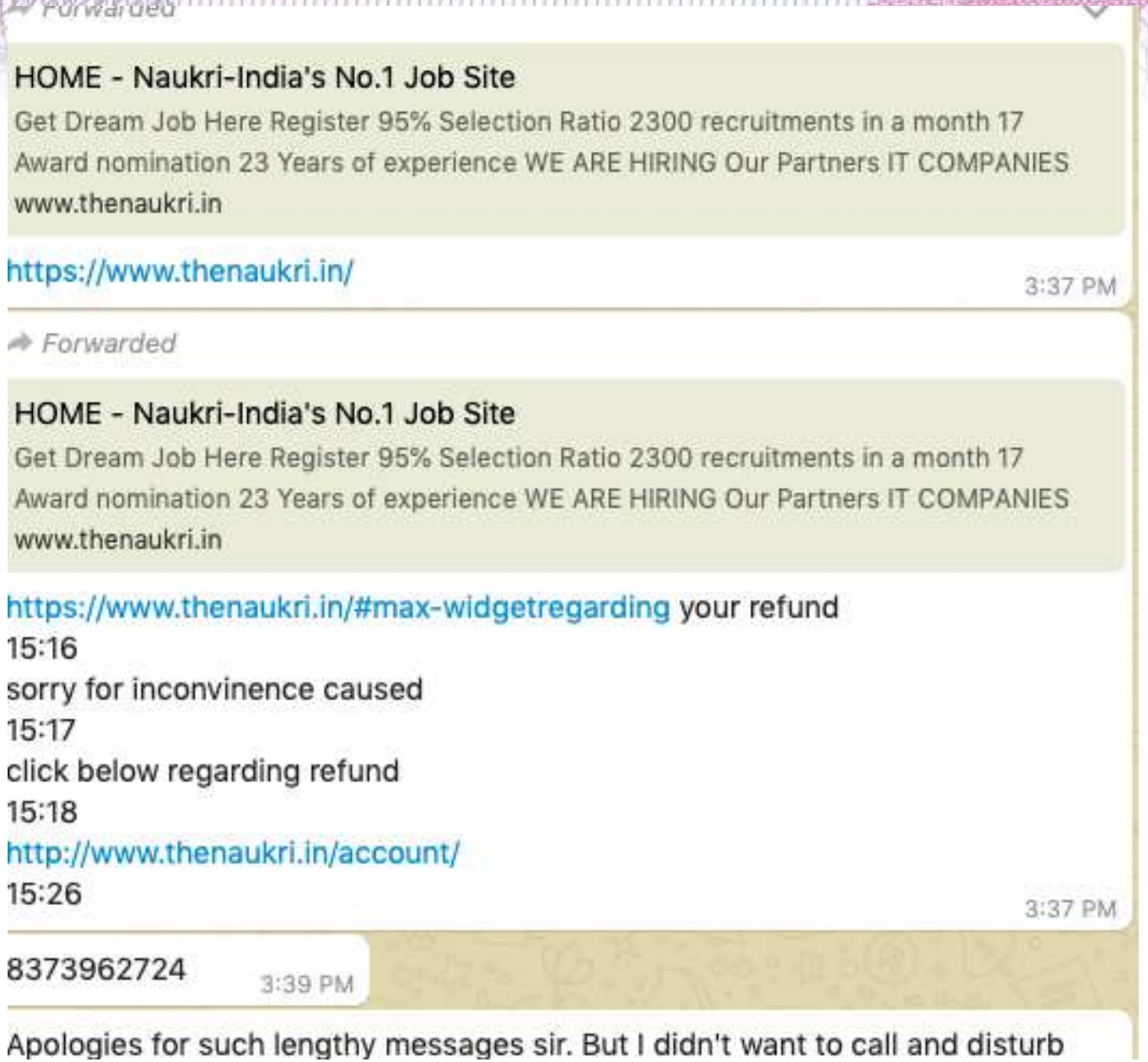
3:35 PM

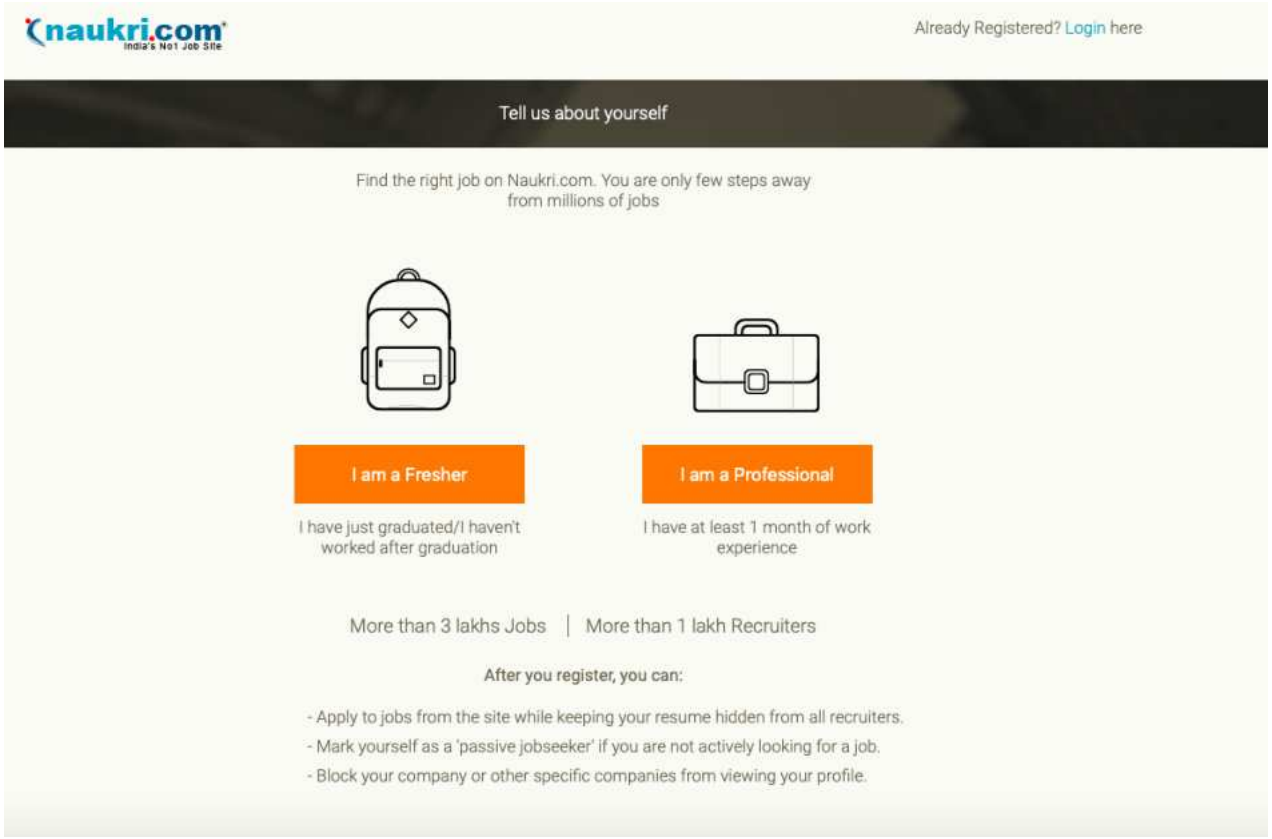
She is unaware of all these attacks shared the screenshot and luckily called me immediately. I made her call customer care and asked to block the card. And fortunately she says she doesn't have money in that particular card anyways.

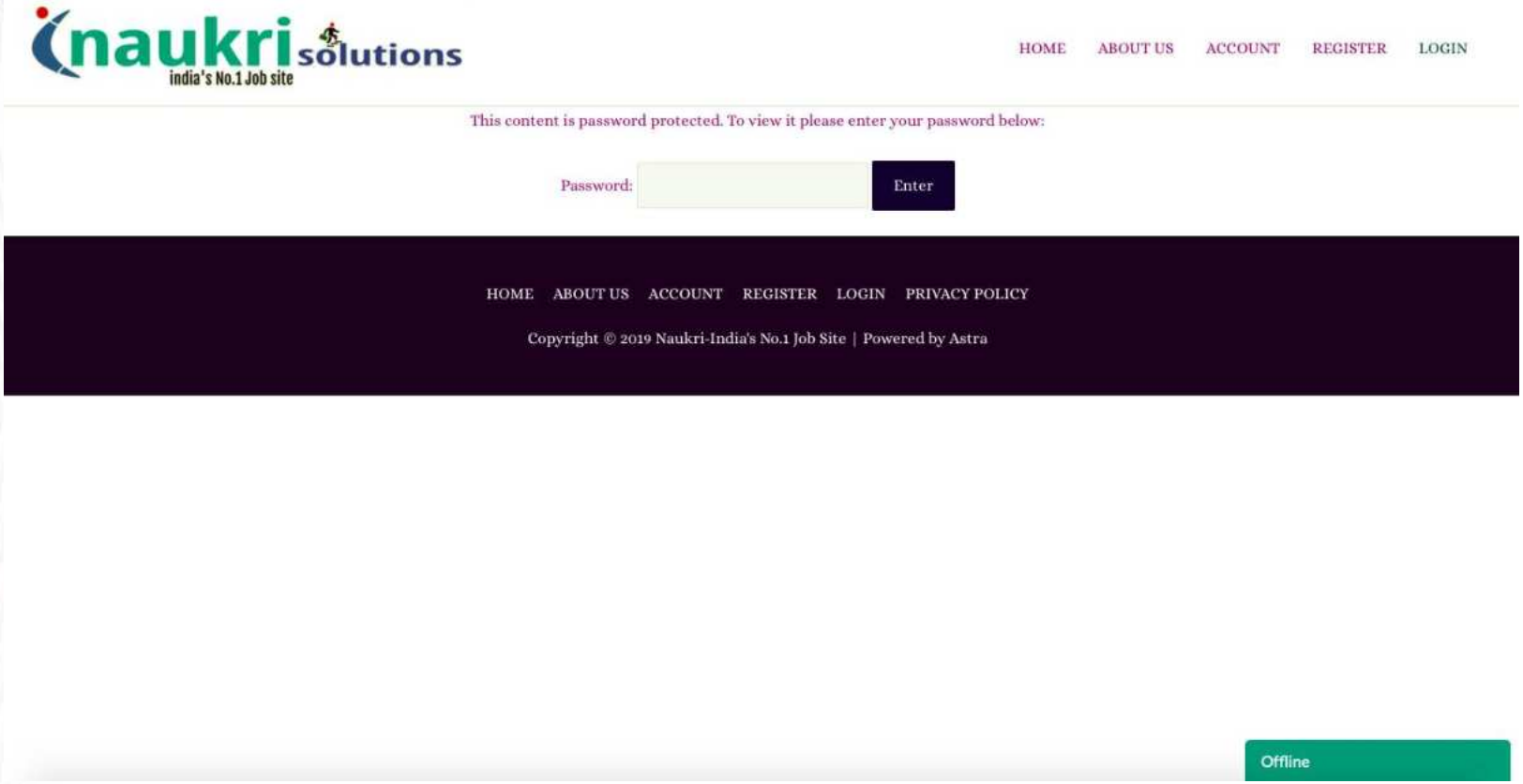
3:36 PM

But I don't want any one else to fall in this trap. Hope you will look into this. Iam sharing contact details and the link for your perusal.

3:37 PM


Forwarded
HOME - Naukri-India's No.1 Job Site
Get Dream Job Here Register 95% Selection Ratio 2300 recruitments in a month 17 Award nomination 23 Years of experience WE ARE HIRING Our Partners IT COMPANIES
www.thenaukri.in
https://www.thenaukri.in/
3:37 PM
Forwarded
HOME - Naukri-India's No.1 Job Site
Get Dream Job Here Register 95% Selection Ratio 2300 recruitments in a month 17 Award nomination 23 Years of experience WE ARE HIRING Our Partners IT COMPANIES
www.thenaukri.in
https://www.thenaukri.in/#max-widgetregarding your refund
15:16
sorry for inconvinence caused
15:17
click below regarding refund
15:18
http://www.thenaukri.in/account/
15:26
3:37 PM
8373962724
3:39 PM
Apologies for such lengthy messages sir. But I didn't want to call and disturb


naukri.com
India's No1 Job Site
Already Registered? Login here
Tell us about yourself
Find the right job on Naukri.com. You are only few steps away from millions of jobs
I am a Fresher
I have just graduated/I haven't worked after graduation
I am a Professional
I have at least 1 month of work experience
More than 3 lakhs Jobs | More than 1 lakh Recruiters
After you register, you can:
- Apply to jobs from the site while keeping your resume hidden from all recruiters.
- Mark yourself as a 'passive jobseeker' if you are not actively looking for a job.
- Block your company or other specific companies from viewing your profile.


naukri solutions
india's No.1 Job site
HOME ABOUT US ACCOUNT REGISTER LOGIN
This content is password protected. To view it please enter your password below:
Password:
Enter
HOME ABOUT US ACCOUNT REGISTER LOGIN PRIVACY POLICY
Copyright © 2019 Naukri-India's No.1 Job Site | Powered by Astra
Offline


TheNaukri.in WHOIS, DNS, & Domain
HOME
RESEARCH
DOMAINTOOLS
Whois Record for TheNaukri.in
— Domain Profile
Registrant Country
in
Registrar
GoDaddy.com, LLC
IANA ID: 146
URL: www.godaddy.com
Whois Server: —
Registrar Status
clientTransferProhibited, clientDele
Dates
310 days old
Created on 2018-10-30
Expires on 2019-10-30
Updated on 2019-07-05
Name Servers
COBY.NS.CLOUDFLARE.COM (has
VENUS.NS.CLOUDFLARE.COM (ha
Tech Contact
—
IP Address
104.31.80.104 - 534 other sites ho
IP Location
- California - San Francisco - Cl
ASN
AS13335 CLOUDFLARENET - (
Hosting History
17 changes on 7 unique name serv


DOMAINTOOLS
Domain Name: thenaukri.in
Registry Domain ID: D4144000000006878914-IN
Registrar WHOIS Server:
Registrar URL: www.godaddy.com
Updated Date: 2019-07-05T09:47:20Z
Creation Date: 2018-10-30T07:27:35Z
Registry Expiry Date: 2019-10-30T07:27:35Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Registry Registrant ID:
Registrant Name:
Registrant Organization:
Registrant Street:
Registrant Street:
Registrant Street:
Registrant City:
Registrant State/Province: Rajasthan
Registrant Postal Code:
Registrant Country: IN


12:26:16
95%
Tweet
A K Verma
@akver85
PAYTM
Dear paytm customer your KYC has been suspended. To Verified Paytm KYC call 6296284755 immediately. Your account will be blocked within 24 hours.
@Paytm @Paytmcare What is this ???
10:01 am · 02 Feb 20 from New Delhi, India · Twitter for Android
1 Like
Paytm Care @Paytmcare · 02 Feb
Replying to @akver85
Hi, this is not official communication from Paytm. Please be aware of such fake callers/ messages. Moreover, thanks for highlighting this to us, we'll take appropriate action against it.
Tweet your reply

INDIA Internet Infrastructure:2022

Internet

260+ IDCs

STPI

Bharti

NIC

Reliance

700+ Major ISPs

ERNET

TATA Communications

BSNL

MTNL

Mail Servers

DNS

300 Mil. High speed Internet

500 Mil. Internet Users

1+ biliion Mobile Phones

Govt.

IT / ITES BPO

Academia

Home

Enterprise

Web Page

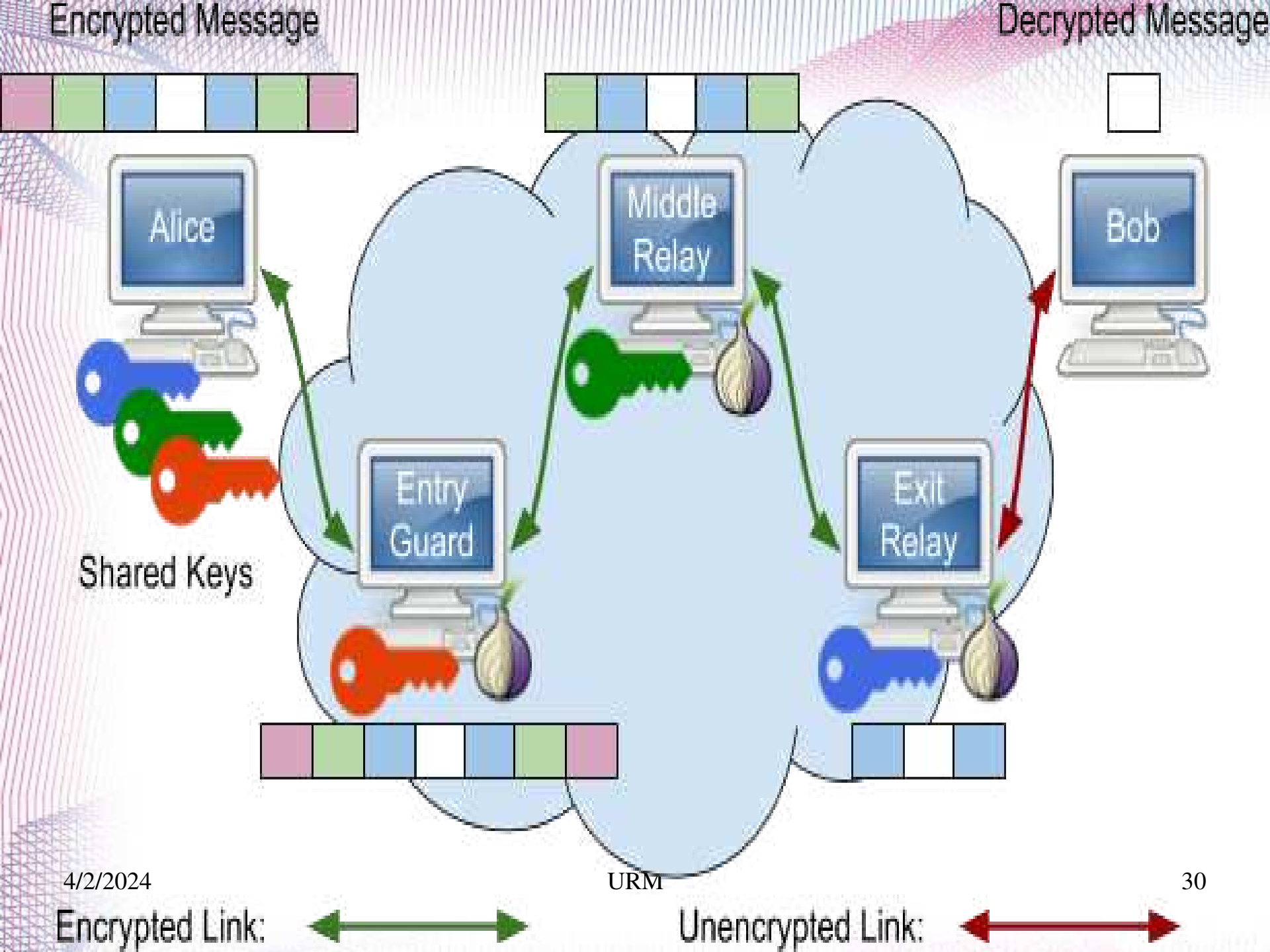
MILK

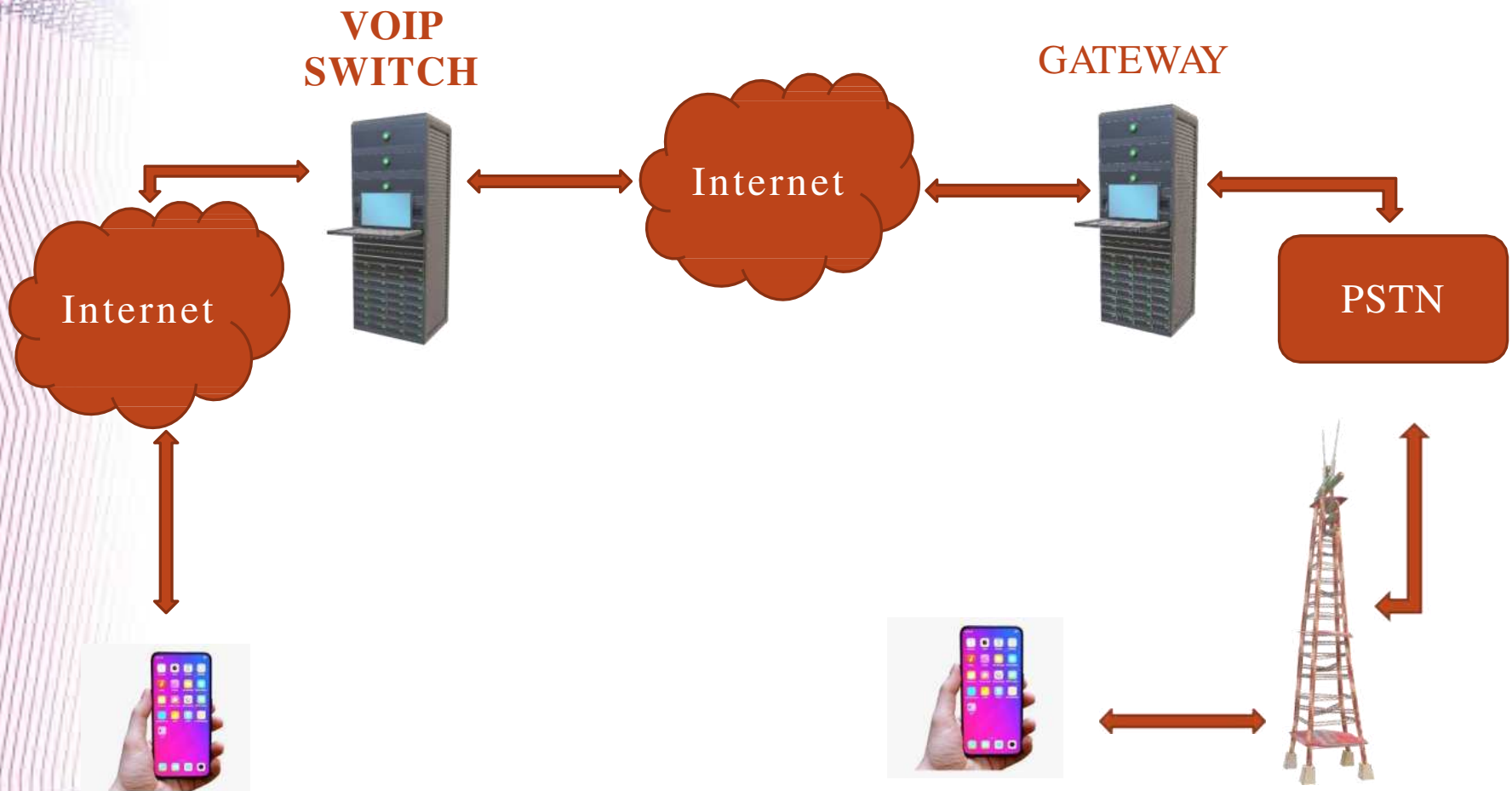
VOIP, IPTV

Targeted Broadband connections=100 Mil.

The seized drugs include over 258 kg of amphetamines, 43 kg of cocaine, 43 kg of MDMA, and over 10 kg of LSD and ecstasy pills. In addition, over EUR 50.8 million (USD 53.4 million) in cash and virtual currencies, and 117 firearms were also seized. The suspects were arrested in the United States, the United Kingdom, Germany, the Netherlands, Austria, France, Switzerland, Poland, and Brazil. Investigations to identify additional individuals behind dark web accounts are still ongoing.

Supervision of Various Wings in Dark Web


Encrypted Message
Decrypted Message
Alice
Middle Relay
Bob
Entry Guard
Exit Relay
Shared Keys
Encrypted Link:
Unencrypted Link:


VOIP
SWITCH
GATEWAY
Internet
Internet
PSTN

Six from T, AP caught from Kolkata in call centre bust

Tele-callers Spoke Telugu, Lured Victims

TIMES NEWS NETWORK

Hyderabad: Nine persons, including six from Telangana and Andhra Pradesh, working in call centres operated by cyber fraudsters in Kolkata have been arrested by Rachakonda cyber crime sleuths. The fraudsters were reportedly recruiting men with knowledge of regional languages to dupe customers from different states.

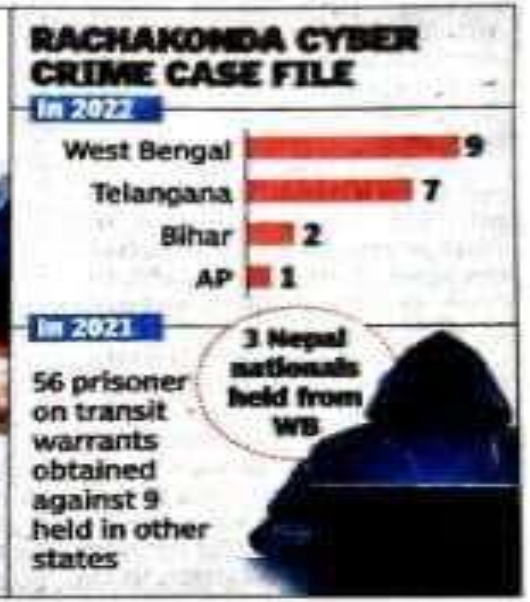
Among the arrested accused were Uttam Kumar Yadav, a native of Bihar, and Mudhavath Ramesh from Mahabubnagar, who have been operating three call centres in Kolkata and recruiting people from various states to talk to the cyber crime victims.

Uttam has been working at the mini-call centres operated by the cyber fraudsters in Kolkata in coordination with organised offenders operating from Jharkhand and Bihar. Ramesh, a close associate of Uttam, has been recruiting Telugu-speaking tele-callers and acting as in charge of Telugu tele-callers. The other accused were identified as J Shankar, L Raju, K Ramchander, telecallers from Mahabubnagar district, Mukesh Kumar, an associate of Uttam from Bihar, and tele-callers K Jagan Mohan Reddy of Guntur, O Chandu of Warangal and G Srisailam from Medak.

On June 8, 2022, a victim, K Kishan from Ibrahimpatnam, had lodged a complaint with police stating that he had purchased a sewing machine through an e-commerce website and, a few days after the machine was delivered, he received a scratch card through post with an e-commerce company's name on it. Kishan scratched the card and it showed that he had won an XUV worth ₹8.2 lakh.

An Elated Kishan called the cell phone number mentioned on the card and, by posing as representatives of the e-commerce company, the fraudsters made Kishan transfer ₹48,200 to various bank accounts towards various charges, taxes and delivery fee of the vehicle. As they kept on asking for more money, Kishan lodged a police complaint.

Police identified three call centres in Kolkata to be responsible for making the phone calls to the victim. Simultaneous searches were conducted at the three centres recently and the nine accused were arrested. Police seized property worth over ₹16 lakh from the possession of the accused.



the Company by the name “IGS Digital Center Limited” was established and is operated in Jaipur, Rajasthan and has a branch in White House, Begumpet, Hyderabad.

The company’s call center posts attractive and deceptive ads to target and lure gullible citizens who are searching online for some opportunity to earn extra income. The company claims in its ads and telecalls that it provides total 300 services viz.,

1) Domestic money transfer, 2) Recharge bills payment-related services, 3) CA services, 4) Travel bookings, 5) Aadhaar-enabled payment system (AEPS), 6) PAN Card services, 7) Express payout, Bharat Bill Payment system (BBTS), 9) Website design and portal services, 10) Micro ATM services, 11) Legal and IT services, 12) Biometric verification and various other services. But in fact, they do not provide all these services

1. Mr Prateek Chauvey s/o Radheshyam Chaturvedi, CEO and Director of IGS Digital Centre Ltd, r/o Manasarovar, Jaipur, Rajasthan
2. Smt Dasari Swarnalatha w/o B Prem Kumar, HR head at IGS Digital Centre Ltd
3. Shravan Lal Sharma s/o Suja Lal, r/o Phagi, Jaipur, Rajasthan (mediator engaged by the company's MD for allegedly influencing and forcing the victim citizen/complainant to desist from pursuing the case against the company offering to pay money).

VISHING

PHISHING

SMISHING

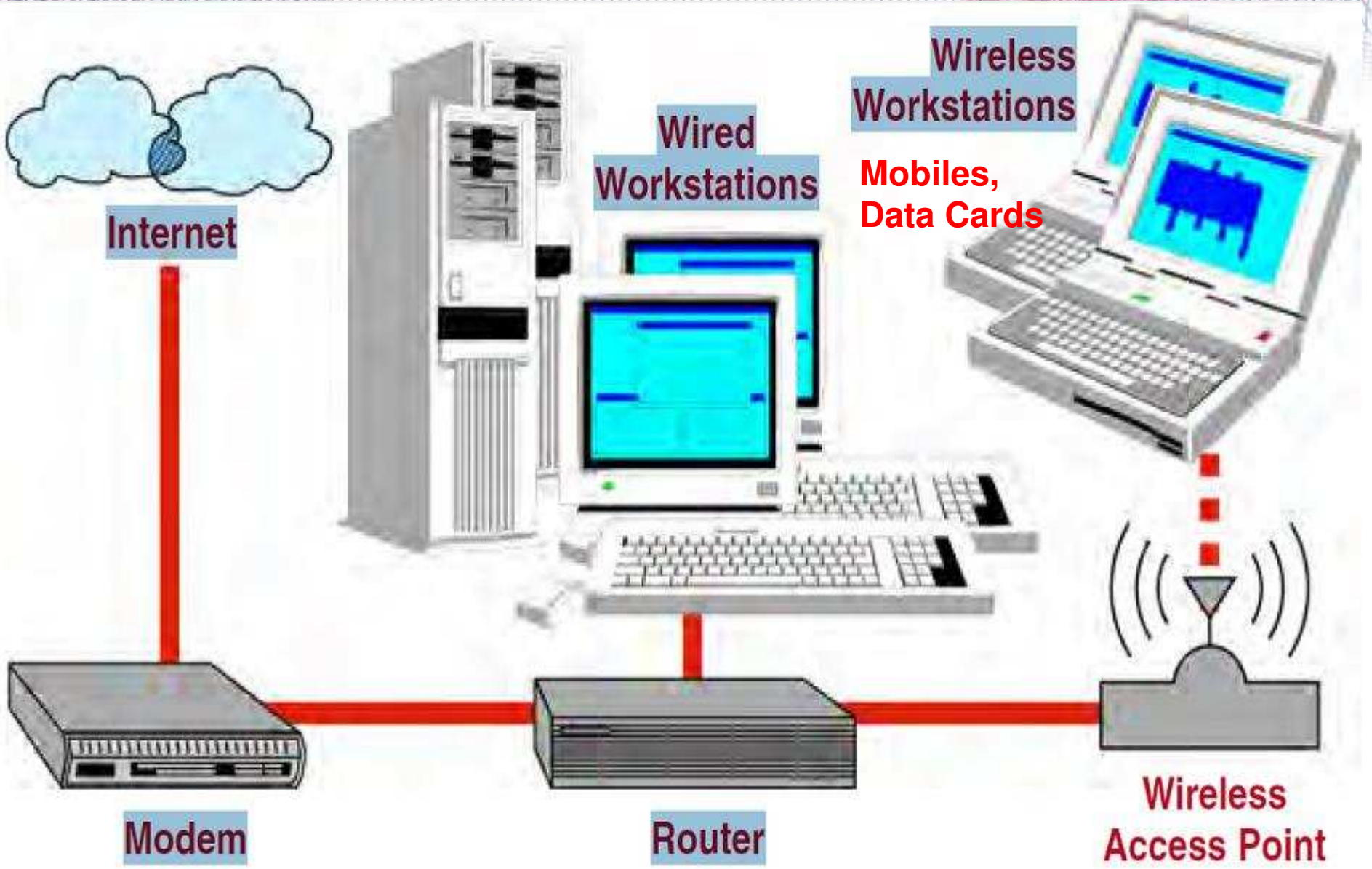
SKIMMING

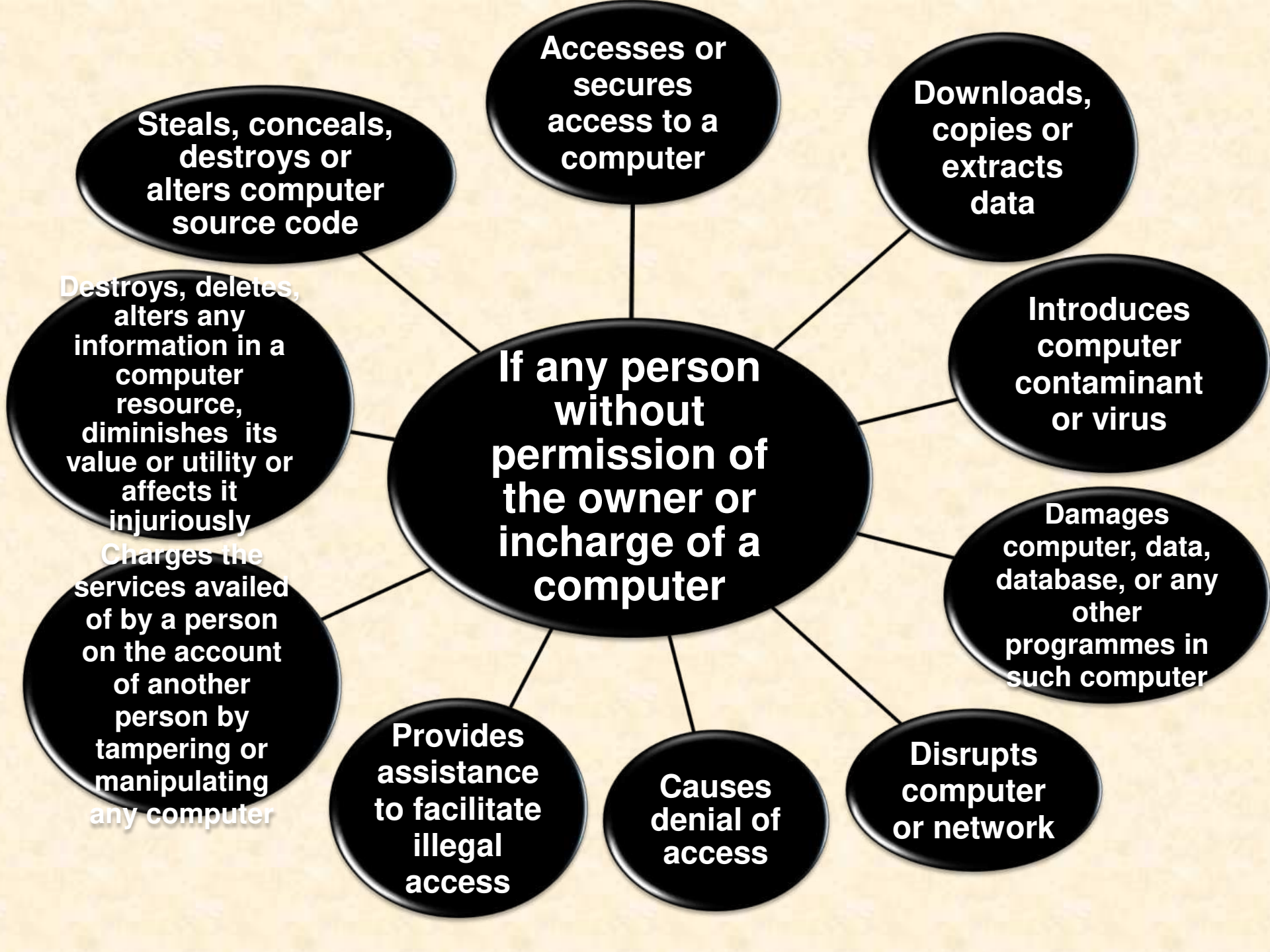
BUGGING

STEALING ONLINE CREDENTIALS FROM INMATES

COLLECTING CREDENTIALS FROM ONLINE SITES

E MAIL SPOOFING/ HACKING


Internet
Wired
Workstations
Wireless
Workstations
Mobiles,
Data Cards
Modem
Router
Wireless
Access Point


If any person without permission of the owner or incharge of a computer
Accesses or secures access to a computer
Downloads, copies or extracts data
Introduces computer contaminant or virus
Damages computer, data, database, or any other programmes in such computer
Disrupts computer or network
Causes denial of access
Provides assistance to facilitate illegal access
Charges the services availed of by a person on the account of another person by tampering or manipulating any computer
Destroys, deletes, alters any information in a computer resource, diminishes its value or utility or affects it injuriously
Steals, conceals, destroys or alters computer source code

CYBER CRIMES - I.T. ACT.

SECTION - 65 SOURCE CODE ALTERATION

PUNISHABLE WITH IMPRISONMENT UPTO 3 YEARS

Offences of Source Code Theft & Alteration in Corporate Offices, MNC Etc.,

SECTION - 66 UNAUTHORIZED ACCESS OF COMPUTER OT COMPUTER RESORCE

PUNISHABLE WITH IMPRISONMENT UPTO 3 YEARS

Hacking of Computer, Websites, Email, Cards, Online Banking Sites, Social Media Profiles

SECTION - 66 C PUNISHMENT OF IDENTITY THEFT

PUNISHABLE WITH IMPRISONMENT UPTO 3 YEARS

Stealing of Security Credentials of People, Computer Resource, Stealing of Pin Numbers, OTP'S, Passwords, CVV Numbers, Phishing, vishing, Clonning, Fake Websites.

SECTION - 66 D PUNISHMENT FOR CHEATING BY ONLINE PERSONATION

PUNISHABLE WITH IMPRISONMENT UPTO 3 YEARS

Fake Lottery, Jobs, Loan Scams, Fake Charity Scams, fake Social Media Profiles, Matrimonial Etc.,

SECTION - 66 E PUNISHMENT FOR VIOLATION OF PRIVACY

PUNISHABLE WITH IMPRISONMENT UPTO 3 YEARS

Taking photos Of Private Parts of individuals or Groups. Spy Camers In Hotels, Toilets, Dressing Rooms.

SECTION - 67 PUBLISHING OR TRANSMITTING OBSCENE MATERIAL

PUNISHABLE WITH IMPRISONMENT UPTO 5 YEARS

Publication of Obscene Content, Text Messages, Emails Etc.,

SECTION - 67 A PUNISHMENT FOR PUBLISHING OR TRANSMITTING OF MATERIAL CONTAINING SEXUALLY EXPLICIT ACT

PUNISHABLE WITH IMPRISONMENT UPTO 5 YEARS, SECOND OFFENCE 7 YEARS

Publication in Electronic Form of Obscene Act, Circulating Obscene Video, Images in Social Media, Emails, Websites Etc.,

SECTION - 67 B PUBLISHING OR TRANSMITTING OF MATERIAL DEPICTING CHILDREN IN SEXUALLY EXPLICIT ACT

PUNISHABLE WITH IMPRISONMENT UPTO 5 YEARS, SECOND OFFENCE 7 YEARS

Publication / Pocession in Electronic Form of Child Porn. Child Porn Making.

SECTION - 72 DISCLOSURE OF INFORMATION

PUNISHABLE WITH IMPRISONMENT UPTO 2 YEARS,

Revealing Data of customers without Proper Authority by the Content Possesors in Soft Copy.

SECTION - 66 F CYBER TERRORISM

PUNISHABLE WITH IMPRISONMENT WHICH MAY EXTEND TO LIFE

Mobile

ATM images and CCTV clippings

Bank AC details/KYC

E-Mails

Websites

Payment Gateways

Bank server details

Online Investigation

LR based investigation

Memory Forensics

Mobile Phone Forensics

Live Forensics

Audio Video Forensics

Network Forensics

Drone Forensics

Live Forensics

Onsite Forensics

Online Cloud Forensics

GPS Forensics

Registry Forensics Etc.,

Intranet Portal | 3rd Eye: An Investigation

tes.appolice.gov.in/3rdEye/HomePage.aspx

Technology Partner Satyam Computer Services Ltd.

Andhra Pradesh Police Computer Services

cyberforensicstandar....ppt

cyberforensicstandar....ppt

Show all downloads...

CDR Analysis & 3rd E... | Skype™ - gajavelli.ve... | 3rd Eye: An Investiga... | Screen shot - WordP... | Microsoft PowerPoin...

2:20 PM

RELIANCE

Airtel

BSNL
Connecting India

uninor

!dea

vodafone

MTC

MTNL

TATA indicom
Do More. Live More

AIRCEL

Important terminology

CDR: Call Data Record

SDR: Subscriber Data Record

CAF: Customer Application Form

SIM: Subscriber Identity Module Card

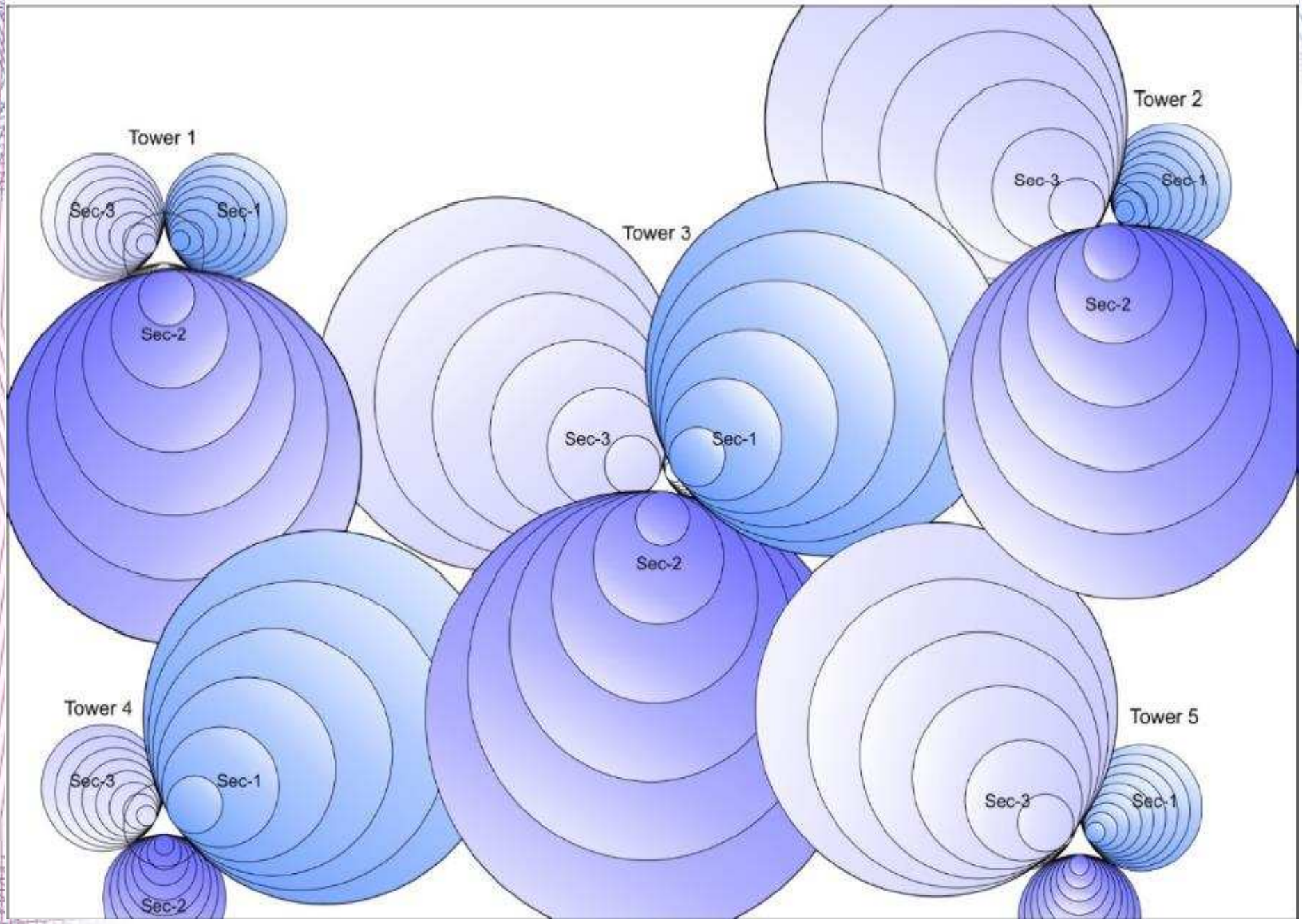
IMEI: International Mobile Equipment Identity (It is a 15 digit number)
ex: 355386042568511

IMSI: International Mobile Subscriber Identity (It is also a 15 -20 digit number)
ex: 404490371646188

SMSC: Short Message Service Center

Timeline to MSP

1. Subscriber Data Record (SDR)	1 hour, in all cases of subscribers acquired before 15 days and in other cases where subscribers data has been updated. 24 hours, in case of subscribers acquired within 15 days.
2. (i) CDRs up to 6 months old	12 hours.
(ii) CDRs more than 6 months old	24 hours.
3. Copy of CAF	In 72 hours, during 3 months from now. In 48 hours, in other cases.
4. BTS Location Information	1 hour to 6 hours.


Tower 1
Sec-3
Sec-1
Sec-2
Tower 2
Sec-3
Sec-1
Sec-2
Tower 3
Sec-3
Sec-1
Sec-2
Tower 4
Sec-3
Sec-1
Sec-2
Tower 5
Sec-3
Sec-1

Lawful intercept and monitoring

According to ***TRAI*** (Telecom regulation authority of India) act of 1997, each and every service provider has to save the record of customer information for a stipulated time and will be given on demand.

This regulation is mandatory for every telecom provider and only those who agree on terms can be given licenses from ***DOT***.

C-DoT (Center for development of telematics) is responsible for lawful interception of voice's, SMS's, CAF's, CDR's and also Internet traffic. Which again complies with section 5(2) of the ***Indian telegraph act*** r/w rule 419(A) of IT Rules.

I AIRTEL LIMITED

cle

tails of Mobile No 7702222337 FROM 01-Oct-2012 TO 03-Oct-2012

N	Called No	Date	Time	Dur(s)	Cell1	Cell2	Call Type	IMEI	I
9	9.18E+09	01-Oct-12	07:40:40	30	5038--190(	19001	OUT	3.59E+14	
	7.7E+09	01-Oct-12	08:14:12	0	5038--190(	-	SMT	3.59E+14	
9	7.7E+09	01-Oct-12	09:19:01	13	5038--198	19823	IN	3.59E+14	
9	7.7E+09	01-Oct-12	10:56:03	125	5038--198	19823	IN	3.59E+14	
9	7.7E+09	01-Oct-12	12:16:46	110	5038--190(	19001	OUT	3.59E+14	
9	7.7E+09	01-Oct-12	12:40:26	13	5038--190(	19002	OUT	3.59E+14	
9	7.7E+09	01-Oct-12	12:42:04	108	5038--190(	19001	IN	3.59E+14	
9	7.7E+09	01-Oct-12	12:54:22	21	5038--102	10251	OUT	3.59E+14	
9	7.7E+09	01-Oct-12	13:01:00	30	5038--869	8693	OUT	3.59E+14	
9	7.7E+09	01-Oct-12	13:38:47	25	118--2222	22222	OUT	3.59E+14	
9	7.7E+09	01-Oct-12	13:59:20	29	51--50972	50971	OUT	3.59E+14	
9	7.7E+09	01-Oct-12	14:02:56	30	51--9161	9161	IN	3.59E+14	
9	7.7E+09	01-Oct-12	14:21:49	10	18--23321	23321	IN	3.59E+14	
9	9.44E+09	01-Oct-12	16:25:12	50	18--23321	23321	OUT	3.59E+14	
9	8.89E+09	01-Oct-12	16:51:09	81	18--23321	23321	OUT	3.59E+14	
9	7.7E+09	01-Oct-12	16:51:54	0	18--23321	-	SMT	3.59E+14	
9	7.7E+09	01-Oct-12	16:52:09	0	18--23321	-	SMT	3.59E+14	
9	7.7E+09	01-Oct-12	16:53:55	0	18--23321	-	SMT	3.59E+14	
9	7.7E+09	01-Oct-12	16:53:59	0	18--23321	-	SMT	3.59E+14	

Segregated CDR

A	B	C	D	E	F	G	H	I	J	K
S.No	Calling No	Called No	Date	Time	Dur(s)	Cell1	Cell2	Call Type	IMEI	IMSI No
1	7702222337	9177941435	01-Oct-12	07:40:40	30	5038--190	19001	OUT	359292046545180	40449015552921
2	7702222337	1395C0	01-Oct-12	08:14:12	0	5038--190	-	SMT	359292046545180	40449015552921
3	7702222337	7702222056	01-Oct-12	09:19:01	13	5038--198	19823	IN	359292046545180	40449015552921
4	7702222337	8143248413	01-Oct-12	10:56:03	125	5038--198	19823	IN	359292046545180	40449015552921
5	7702222337	7702222056	01-Oct-12	12:16:46	110	5038--190	19001	OUT	359292046545180	40449015552921
6	7702222337	7702222056	01-Oct-12	12:40:26	13	5038--190	19002	OUT	359292046545180	40449015552921
7	7702222337	7702222056	01-Oct-12	12:42:04	108	5038--190	19001	IN	359292046545180	40449015552921
8	7702222337	7702222056	01-Oct-12	12:54:22	21	5038--102	10251	OUT	359292046545180	40449015552921
9	7702222337	7702222056	01-Oct-12	13:01:00	30	5038--869	8693	OUT	359292046545180	40449015552921
10	7702222337	7702222056	01-Oct-12	13:38:47	25	118--2222	22222	OUT	359292046545180	40449015552921
11	7702222337	7702222056	01-Oct-12	13:59:20	29	51--50972	50971	OUT	359292046545180	40449015552921
12	7702222337	8143248413	01-Oct-12	14:02:56	30	51--9161	9161	IN	359292046545180	40449015552921
13	7702222337	8702440740	01-Oct-12	14:21:49	10	18--23321	23321	IN	359292046545180	40449015552921
14	7702222337	9440807077	01-Oct-12	16:25:12	50	18--23321	23321	OUT	359292046545180	40449015552921
15	7702222337	8888888888	01-Oct-12	16:51:09	81	18--23321	23321	OUT	359292046545180	40449015552921
16	7702222337	4526B491126A3CC	01-Oct-12	16:51:54	0	18--23321	-	SMT	359292046545180	40449015552921
17	7702222337	4526B491126A3CC	01-Oct-12	16:52:09	0	18--23321	-	SMT	359292046545180	40449015552921
18	7702222337	4526B491126A3CC	01-Oct-12	16:53:55	0	18--23321	-	SMT	359292046545180	40449015552921
19	7702222337	4526B491126A3CC	01-Oct-12	16:53:59	0	18--23321	-	SMT	359292046545180	40449015552921

Sample Cell ID List

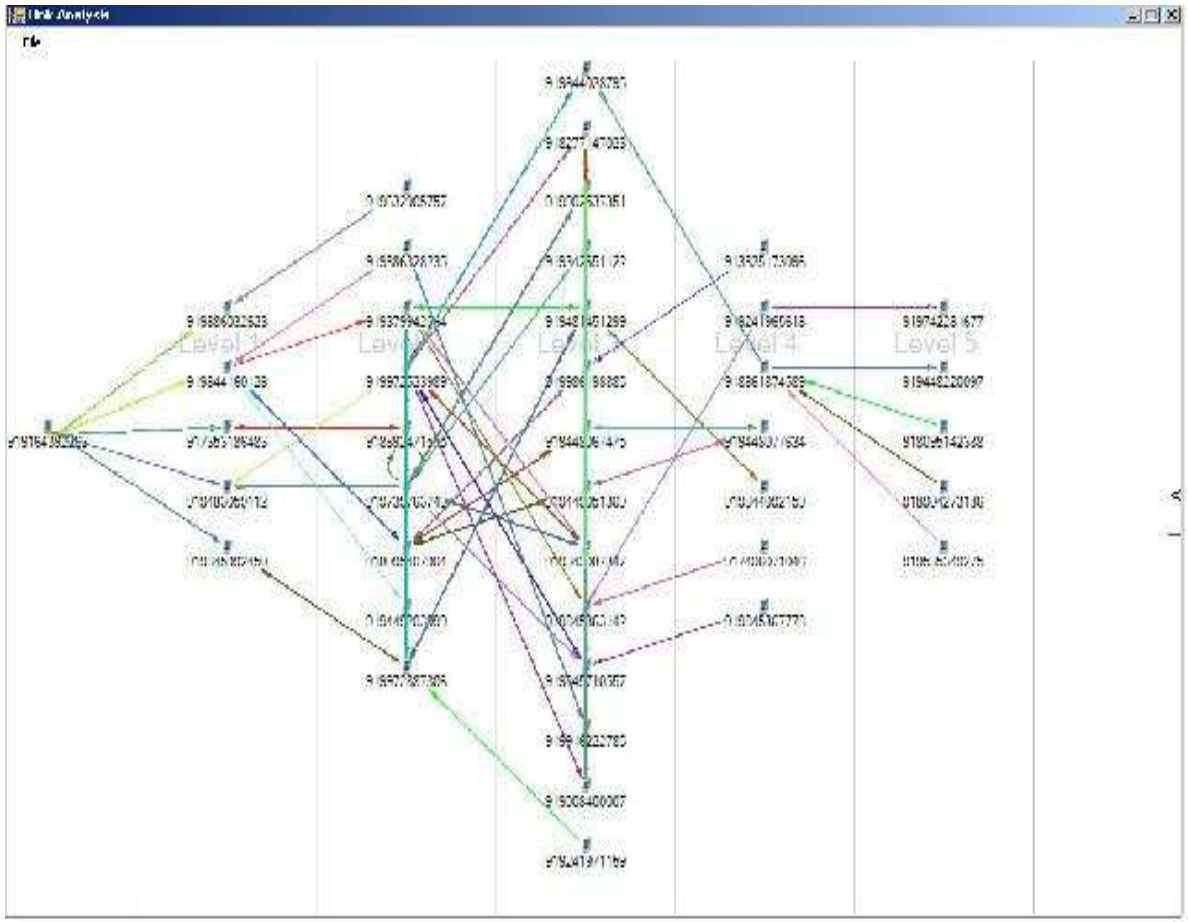
A	B	C	D	E	F	G
Cell_ID	SITE_NAME	TOWN	DIST	LAT	LONG	AZIMUT
5040--31971	PILER	PILERU	TIRUPATI	13.65507	78.95013	0
5040--31972	PILER	PILERU	TIRUPATI	13.65507	78.95013	180
5040--31973	PILER	PILERU	TIRUPATI	13.65507	78.95013	270
5591--40261	NTPCPAGWADA	VIZAG	VIZAG	17.5788	83.0881	40
5591--40262	NTPCPAGWADA	VIZAG	VIZAG	17.5788	83.0881	160
5591--40263	NTPCPAGWADA	VIZAG	VIZAG	17.5788	83.0881	220
5571--36131	GAJAPATINAGARAM	GAJAPATINAGARAM	VIJZIANAGARAM	18.2823	83.3321	0
5571--36132	GAJAPATINAGARAM	GAJAPATINAGARAM	VIJZIANAGARAM	18.2823	83.3321	120
5571--36133	GAJAPATINAGARAM	GAJAPATINAGARAM	VIJZIANAGARAM	18.2823	83.3321	180
5567--36391	SALUR	SALUR	VIJZIANAGARAM	18.518	83.2016	100
5567--36392	SALUR	SALUR	VIJZIANAGARAM	18.518	83.2016	220
5567--36393	SALUR	SALUR	VIJZIANAGARAM	18.518	83.2016	340
5021--50051	TIRUPATI	TIRUPATI	TIRUPATI	13.64949	79.42294	80
5021--50052	TIRUPATI	TIRUPATI	TIRUPATI	13.64949	79.42294	150
5021--50053	TIRUPATI	TIRUPATI	TIRUPATI	13.64949	79.42294	260
5005--13011	ADILABAD	ADILABAD	ADILABAD	19.671	78.5354	10
5005--13012	ADILABAD	ADILABAD	ADILABAD	19.671	78.5354	120

Import Cell ID's to CDR

B	C	D	E	F	G	H	I	J	K	L	M	N
Calling No	Called No	Date	Time	Dur(s)	Cell1	Cell2	Call Type	IMEI	IMSI No	Sitename	Dist	Azimut
7702222337	9177941435	01-Oct-12	07:40:40	30	5038--190	19001	OUT	359292046545180	404490155529219	MADINAGUDA	HYDERABAD	20
7702222337	1395C0	01-Oct-12	08:14:12	0	5038--190	-	SMT	359292046545180	404490155529219	MADINAGUDA	HYDERABAD	20
7702222337	7702222056	01-Oct-12	09:19:01	13	5038--198	19823	IN	359292046545180	404490155529219	SRI RAM COLONY	HYDERABAD	290
7702222337	8143248413	01-Oct-12	10:56:03	125	5038--198	19823	IN	359292046545180	404490155529219	SRI RAM COLONY	HYDERABAD	290
7702222337	7702222056	01-Oct-12	12:16:46	110	5038--190	19001	OUT	359292046545180	404490155529219	MADINAGUDA	HYDERABAD	20
7702222337	7702222056	01-Oct-12	12:40:26	13	5038--190	19002	OUT	359292046545180	404490155529219	MADINAGUDA	HYDERABAD	20
7702222337	7702222056	01-Oct-12	12:42:04	108	5038--190	19001	IN	359292046545180	404490155529219	MADINAGUDA	HYDERABAD	20
7702222337	7702222056	01-Oct-12	12:54:22	21	5038--102	10251	OUT	359292046545180	404490155529219	MIYAPUR X ROADS	HYDERABAD	20
7702222337	7702222056	01-Oct-12	13:01:00	30	5038--869	8693	OUT	359292046545180	404490155529219	KONDAPUR	HYDERABAD	320
7702222337	7702222056	01-Oct-12	13:38:47	25	118--2222	22222	OUT	359292046545180	404490155529219	N.A.	N.A.	N.A.
7702222337	7702222056	01-Oct-12	13:59:20	29	51--50972	50971	OUT	359292046545180	404490155529219	CHAMPAPET	HYDERABAD	80
7702222337	8143248413	01-Oct-12	14:02:56	30	51--9161	9161	IN	359292046545180	404490155529219	NEW MARUTHI NAGAR	HYDERABAD	120
7702222337	8702440740	01-Oct-12	14:21:49	10	18--23321	23321	IN	359292046545180	404490155529219	JILLELGUDA	HYDERABAD	0
7702222337	9440807077	01-Oct-12	16:25:12	50	18--23321	23321	OUT	359292046545180	404490155529219	JILLELGUDA	HYDERABAD	0
7702222337	8888888888	01-Oct-12	16:51:09	81	18--23321	23321	OUT	359292046545180	404490155529219	JILLELGUDA	HYDERABAD	0
7702222337	4526B491126A3CC6	01-Oct-12	16:51:54	0	18--23321	-	SMT	359292046545180	404490155529219	JILLELGUDA	HYDERABAD	0
7702222337	4526B491126A3CC6	01-Oct-12	16:52:09	0	18--23321	-	SMT	359292046545180	404490155529219	JILLELGUDA	HYDERABAD	0
7702222337	4526B491126A3CC6	01-Oct-12	16:53:55	0	18--23321	-	SMT	359292046545180	404490155529219	JILLELGUDA	HYDERABAD	0
7702222337	4526B491126A3CC6	01-Oct-12	16:53:59	0	18--23321	-	SMT	359292046545180	404490155529219	JILLELGUDA	HYDERABAD	0
7702222337	4526B491126A3CC6	01-Oct-12	16:54:05	0	18--23321	-	SMT	359292046545180	404490155529219	JILLELGUDA	HYDERABAD	0
7702222337	4526B491126A3CC6	01-Oct-12	16:54:10	0	18--23321	-	SMT	359292046545180	404490155529219	JILLELGUDA	HYDERABAD	0
7702222337	4526B491126A3CC6	01-Oct-12	16:54:16	0	18--23321	-	SMT	359292046545180	404490155529219	JILLELGUDA	HYDERABAD	0
7702222337	4526B491126A3CC6	01-Oct-12	16:54:21	0	18--23321	-	SMT	359292046545180	404490155529219	JILLELGUDA	HYDERABAD	0
7702222337	4526B491126A3CC6	01-Oct-12	16:54:26	0	18--23321	-	SMT	359292046545180	404490155529219	JILLELGUDA	HYDERABAD	0

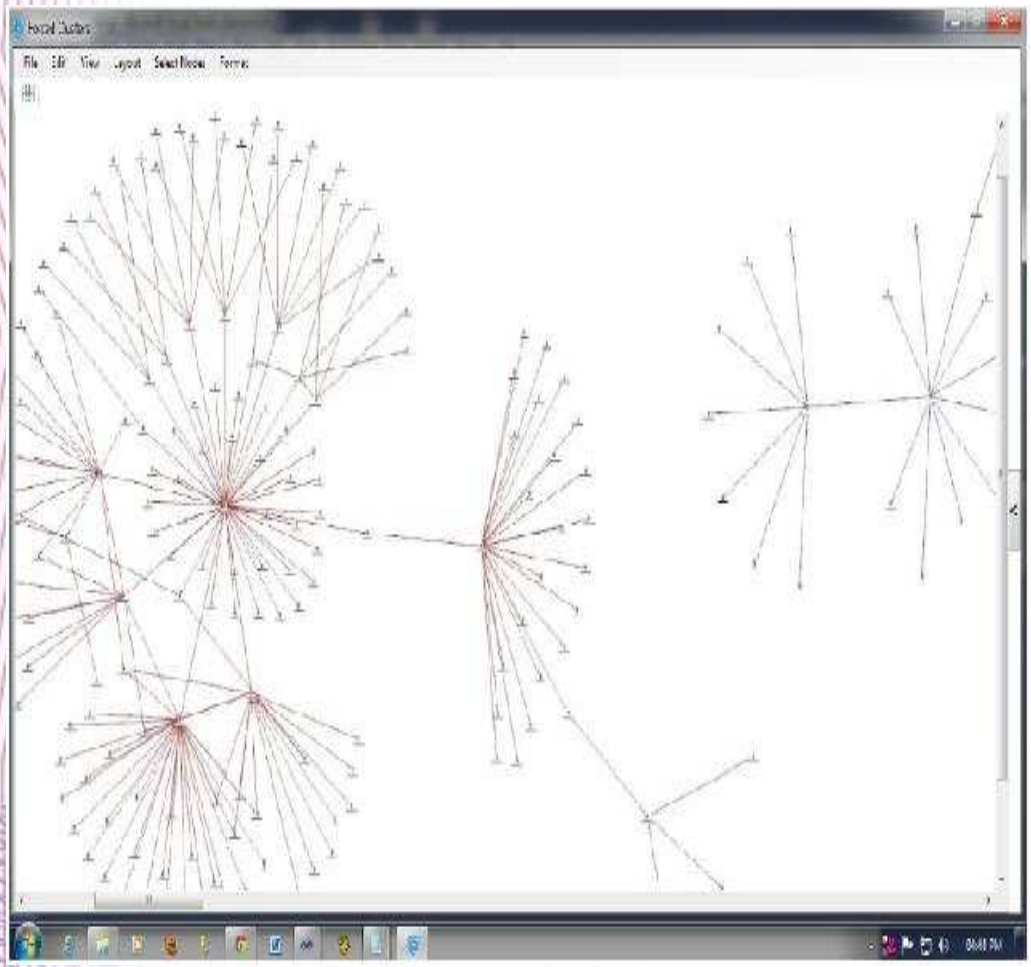
Number Link analysis

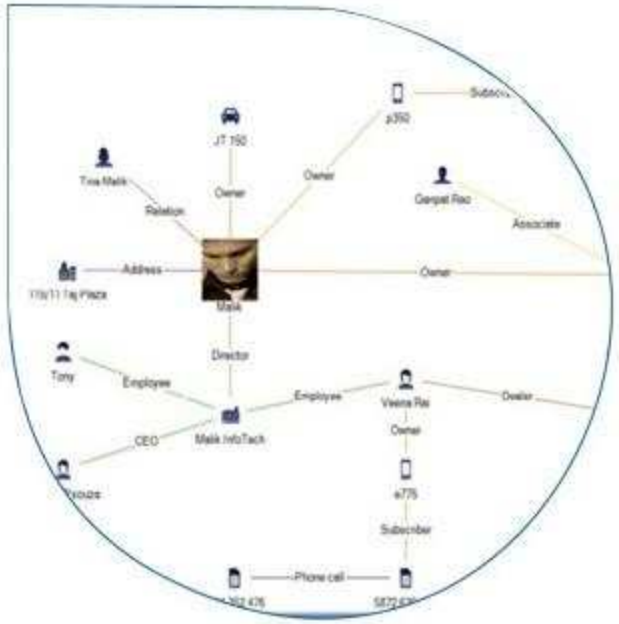
CDR Analyzers are designed for interactive data visualization which enables Investigating Officers to visually interrogate the data using various types of graphics such as Geo maping, timeline etc.



Geo-spatial analysis

Group analysis |Call Map





Protocol

Collection from Complainant

Collection from internet

Collection from Banks/ Payment gateways

Collection from Internet Service Providers

Collection from Mobile Service Provider

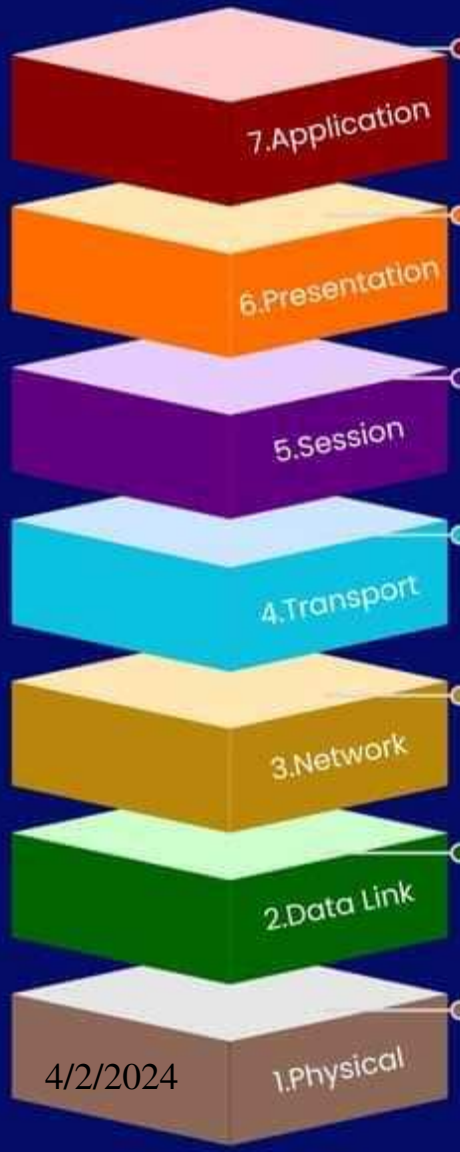
Collection from Social Media

Collection from Mail Service Providers.

Collection from Business Sites

Collection From Storage Media/cloud.

Attacks And Exploits With OSI Layers



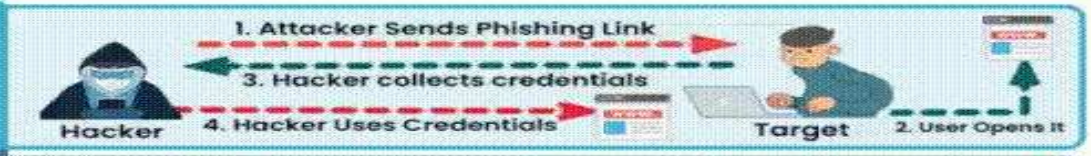
Attacks & Exploits	Function	Examples
Interface to end user, interaction directly with software application	Phishing & email compromise Password cracking Buffer overflow/SQL injection	**Software App Layer** Directory services, email, network management, file transfer, web pages, database access → FTP, HTTP, WWW. SMTP, TELNET, DNS, TFTP, NFS
Formats data to be "presented" between application-layer entities	Injection attacks File inclusion vulnerabilities Cross-site scripting Cross-site request forgery	**Syntax/Semantics Layer** Data representation, compression, encryption/decryption, formatting → ASCII, PDF, HTML, DOCX, AVI, SOCKETS ASCII
Manages connections between local and remore application	Session hijacking Access control bypass Adversary-in-the-middle.	**Application Session Management** Session establishment/teardown, file transfer checkpoints, interactive login → SQL, SIP, RTP, RPC-named pipes
Ensires integrity of data transmission	Port scanning DNS Poisoning Lateral movement	**End-to-end Reliable Connection** Data segmentation, reliability, multiplexing, connection-oriented, flow control, sequencing, error checking → TCP, UDP, SSL, TLS
Determines how data. gets from one host to another	IP spoofing Manipulating routing tables DDoS flooding	**Routing** Packets, subnetting, logical IP addressing, path determination, connectionless → IP, ARP, IPSec, ICMP, OSPF, BGP
Defines format of data on the network	MAC & ARP spoofing Gateway i.d. check Rogue APS	**Switching** Frame traffic contro, CRC checking, encapsulates packets, MAC addresses → Ethernet, Wi-Fi, MAC/LLC, 4G/5G/6G, LoRaWAN
Transmits raw bit stream over physical. medium	Device tampering Physical disruption Traffic eavesdropping	**Cabling/Network Interface** Manages physical connections, interpretation of bit stream into electrical signals → RS-232, RJ45, Ethernet, Wi-Fi

Ethical Hackers Academy

Top 8 Types of Cyber Attacks

1 Phishing Attack

Deceptive emails, messages, or websites to obtain sensitive information.



2 Ransomware

Software designed to encrypt files and demand payment for their release.

3 Denial-of-Service (DoS)

Overloading a system or network to disrupt normal functioning.

4 Man-in-the-Middle (MitM)

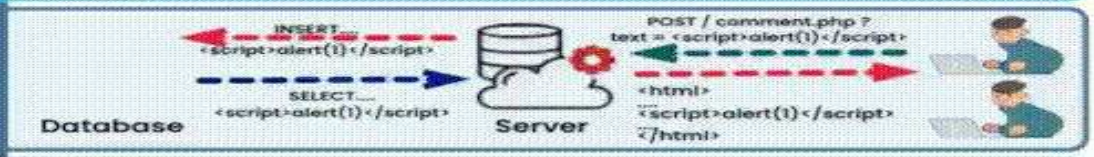
Intercepting and manipulating communication between two parties without their knowledge.

5 SQL Injection

Exploiting vulnerabilities in database queries to gain unauthorized access.

6 Cross-Site Scripting (XSS)

Injecting malicious scripts into websites viewed by other users.



7 Zero-Day Exploits

Attacks exploiting unknown vulnerabilities before developers can address them.

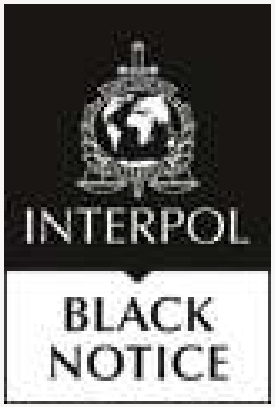
8 DNS Spoofing

Redirecting DNS queries to malicious sites for unauthorized access.

INCIDENT RESPONSE FOR COMMON ATTACK TYPES

Attack Name	What It Is?	Threat Indicators	Where to Investigate	Possible Actions
Brute Forcing	Attacker trying to guess a password by attempting several different password	Multiple login failures in a short period of time	Active Directory Logs Application Logs Operational System logs Contact User	**If not legit action**, disable the account and investigate/block attacker
Botnets	Attackers are using the victim server to perform DDOS attacks or other malicious activities	Connection to suspicious IPs. Abnormal high volume of network traffic	Network Traffic OS Logs (New processes) Contact Server Owner Contact Support Team	**If confirmed:** Isolate the server Remove malicious processes Patch the vulnerability utilized for infection
Ransomware	A type of malware that encrypts files and reuests a ransom(money payment) from the user to decrypt the files	User contacting; Burst of "file update"logs Anti Virus alerts Connection to suspicious IPs.	AV Logs OS Logs Account Logs Network Traffic	Request AV Checks Isolate the machine
Data Exfiltration	Attacker (or rogue employee) exfiltrate data to external sources	Abnormal high network traffic Connection to cloud-storage solutions(Dropbox, Google Cloud) Unusual USB Sticks	Network Traffic Proxy Logs OS Logs	**If rougue employee:** Contact manager, perform full forensics **If external Threat:** Isolate the machine, disconnect from network
Compromised Account	Attackers get access to one account (via social engineering or any other method)	Off-hours account logins, Account group changes, Abnormal high network rtaffic	Active Directory Logs, OS Logs, Network Traffic, Contact User for Clarifications	**If confirmed:** Disable Account, Password Changes, Forensic investigations
Denial Of Service (DoS/DDos)	When attacker is able to cause interference in a system by exploiting DoS Vulnerabilities or by generating a high volume of traffic	Abnormal high network traffic in public facing servers	Network traffic, Firewall Logs, OS Logs	**If DoS due to vulnerabilities:** Contact patching team for remediation. **If DDoS due to network traffic:** Contact network Support or ISP.
Advanced Persistent Threats (APTs)	Attackers get access to the system and create backdoors for further exploitation. Usually hard to detect.	Connection to suspicious IPs, Abnormal high volume of network tarffic, Off-hours access logs, New Admin account creations.	Netwotk traffic, Access Logs, OS Logs (new processes, new connections, abnormal users), Contact server owner/support teams.	**If confirmed;** Isolate the machine, start formal forensics process, Start escalation/commuication plan.

INTERPOL Notices

	**Red Notice** To seek the location and arrest of wanted persons with a view to extradition or similar lawful action. FORM		**Yellow Notice** To help locate missing persons, often minors, or to help identify persons who are unable to identify themselves.
	**Blue Notice** To collect additional information about a person's identity, location or activities in relation to a crime.		**Black Notice** To seek information on unidentified bodies.

	**Green Notice** To provide warnings and intelligence about persons who have committed criminal offences and are likely to repeat these crimes in other countries.		**Orange Notice** To warn of an event, a person, an object or a process representing a serious and imminent threat to public safety.
	**INTERPOL–United Nations Security Council Special Notice** Issued for groups and individuals who are the targets of UN Security Council Sanctions Committees.		**Purple Notice** To seek or provide information on modi operandi, objects, devices and concealment methods used by criminals.

Social Media Analysis

Social Media is being the most potential source for the cyber criminals to conduct any sort of crime (online harassment/ hacking/ phishing or cheating)

There is a challenge to trace these sophisticated cyber criminals as they grow with the evolving technology.

Further law enforcement cell(s) are being formed to help the local police to conduct their investigation with regards to the online crimes and investigations.

a. Automated AI Driven Collection Mechanism

i. Near Real Time Collection: from across networks for individual, group or topics

ii. Anonymous & Untraceable: ensuring security, latest updates & proactive intelligence

iii. Multiple Social Networks: enhancing ability to collect data across networks at once

iv. Volume of Data Collected: simultaneously for topics, individuals, and groups

v. Speed of Data Collection: across networks, social id's, groups, topics, and individuals.

vi. Private Accounts: collected with privacy compliance &referred as Inferred Data.

vii. Closed Groups: Semi Automated collection mechanism (3 Clicks)

viii. Ease of Use Interface: for investigators & analysts (basic computer operations)

ix. Security of Collection: maintained using End to End Encryption

x. Data Privacy Compliance: is maintained for the overall platform.

b. *Automated AI Based Analysis & In-depth Insights*

i. Relationships– Automatic 1st Level, 2nd Level, TNT& Hidden Connections

ii. Relationship Strengths – Automated showcase of closeness of individuals in a relationship

iii. Automated Discovery - Mediators, Top Connections, Identified & Ghosts

iv. Automated Analysis – Individual/s, Group, Across Groups and Topic/s

v. Fake Profiles, Propaganda Accounts& Bots – Single Click Identification

vi. Profile Insights – all details including automatic Collection of Likes & Comments

vii. Automated Impact Analysis of topics with auto identification of major Influencers & Contributors

viii. Automated Real Time Risk Assessment for millions of individuals at an instance

ix. Enhanced Profile Finder using only image, email id's, social idand/or phone numbers.

x. Analysis & Viewing of profile/s without Internet as well

xi. Visual Data Relationship Correlationwith Single Click Database &Watchlist creation

xii. Visual Data Acceptance from offline sources like Laptops, Phone, USB, CCTV, etc.

xiii. Offline to Online Visual Data Integration with Social Networks

xiv. Cross Topology Visual Images Correlation &Automated finding of Hidden Connections

Benefit:*Automated Precise AI Based In-depth Insights without need for manual intervention.*

c. Automated Detailed Reporting, Content Availability & Judicial Acceptability

i. Hash Value Generation& integrated for content
ii. Enhanced Reporting Functionality
iii. Automated Spotlight Reports
iv. Automated Alert Mechanism
v. Automated Download& Storage of Media &Content

Benefit: *Legal Admissibility for Judicial Purposes*

Open Source Intelligence

Digital investigations

- Identifying and securing the crime scene
- ‘As is where is’ documentation of the scene of offence
- Collection of evidence
  — *Procedure for gathering evidences from Switched-off Systems*
  — *Procedure for gathering evidence from live systems*
- Forensic duplication
- Conducting interviews
- Labeling and, documenting of the evidence
- Packaging, and transportation of the evidences

Questions to be asked

- Which are the user accounts that are present in the computer?
- What financial applications/software applications are installed in the system?
- Are there any logs available for these applications?
- Please provide the list of files/filenames that were recently accessed
- What external devices (like thumb drives/external hard drives) were connected to the computer?
- Are there any databases and excel spread sheets available in active or deleted state?
- Are there any accounting packages/software installed?
- Are there any encrypted or password-protected files available? If so, please extract the content from them?
- Are there any pornographic images/videos present in the computer system?
- Was the system date and time changed at any point of time?

Model Questions to be asked

- – What type of operating system has been installed in the computer?
- – When was the operating system installed?
- – Please provide the user names/users present in the system
- – What programs or software is installed in the computer?
- – What is the IP address assigned to the system, if any?
- – What is the MAC address of the system?
- – Are there any information relating e-mail addresses present in the computer system?
- – Are there any chat messenger software installed. If so, are there any chat IDs/profiles?
- – Any suspicious or malicious software installed?
- – Please provide the Internet history of the computer (Web sites accessed, files uploaded, downloaded, etc.)?
- – Are there any firewall logs available in the system?

Opinion from the Forensic Examiner

- The forwarding letter to the FSL for scientific analysis and opinion should mention the following information.
- Brief history of the case
- The details of the exhibits seized and their place of seizure
- The model, make and description of the hard disk or any storage media
- The date and time of the visit to the scene of crime
- The condition of the computer system (on or off) at the scene of crime
- Is the photograph of the scene of crime is taken?
- Is it a stand-alone computer or a network?
- Is the computer has any Internet connection or any means to communicate with external computers?

Preliminary Review of the Scene

Residence of the individual

Cyber Café/Public places

Companies/Organizations

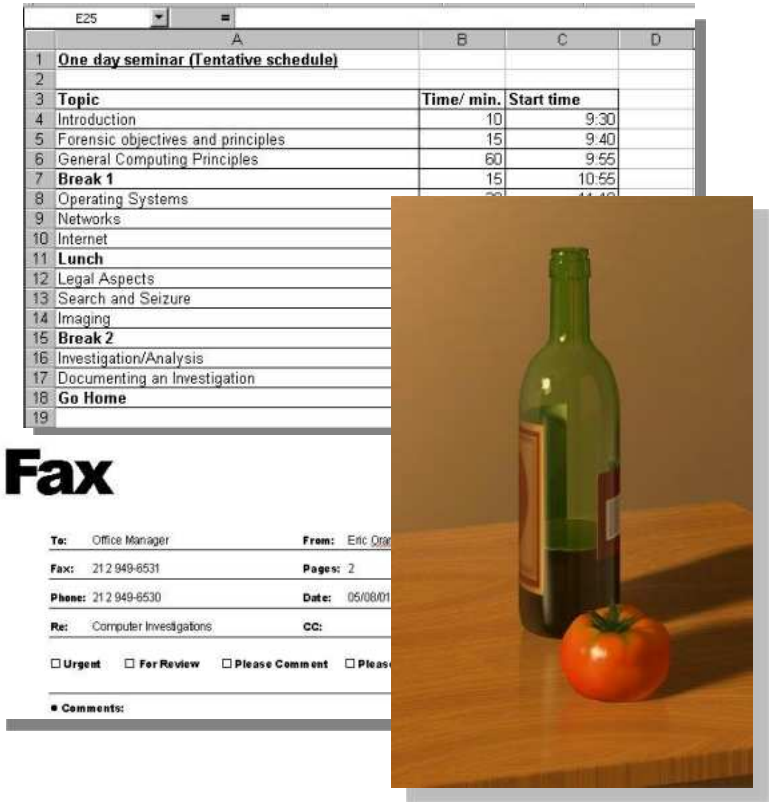
With or without networks

Information exists on the computer in the form of data.

Data is processed by the computer to produce items such as letters, images or spreadsheets

001010110101
0100111101011
0111010001001
1101 10

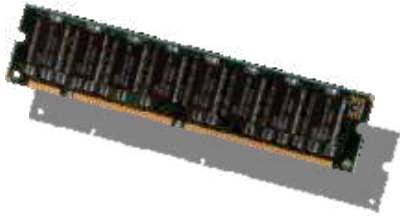
Processor



Three Common Types of Storage

Magnetic

Silicon



Optical

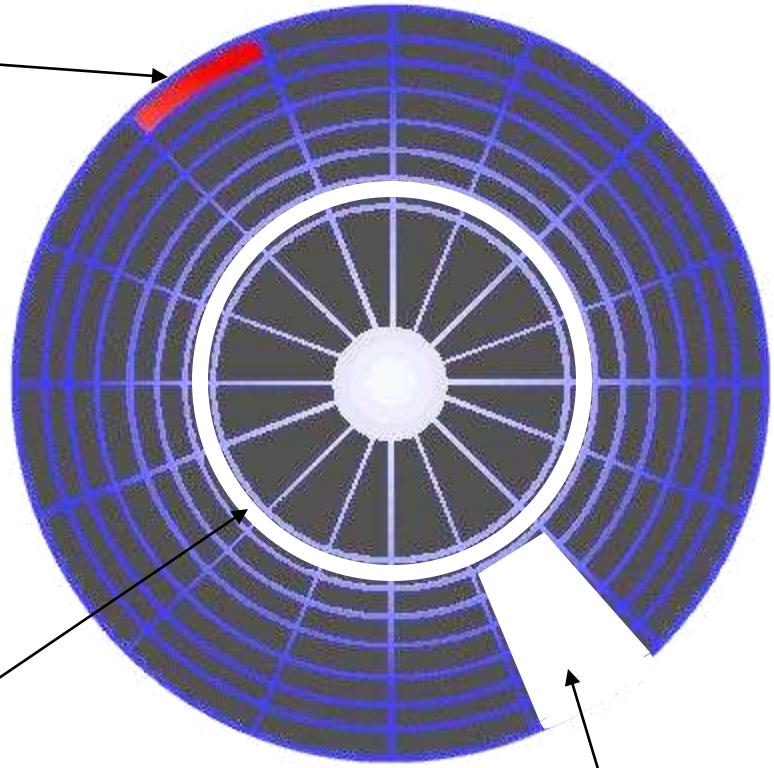
Typical Hard Drive Construction

Accessing Information on a Hard Drive

The computer must have a reference point from which to access all other points on the disk – the file allocation table or FAT

The hard disk must be divided into a grid like pattern to allow for "packets" of information to be stored

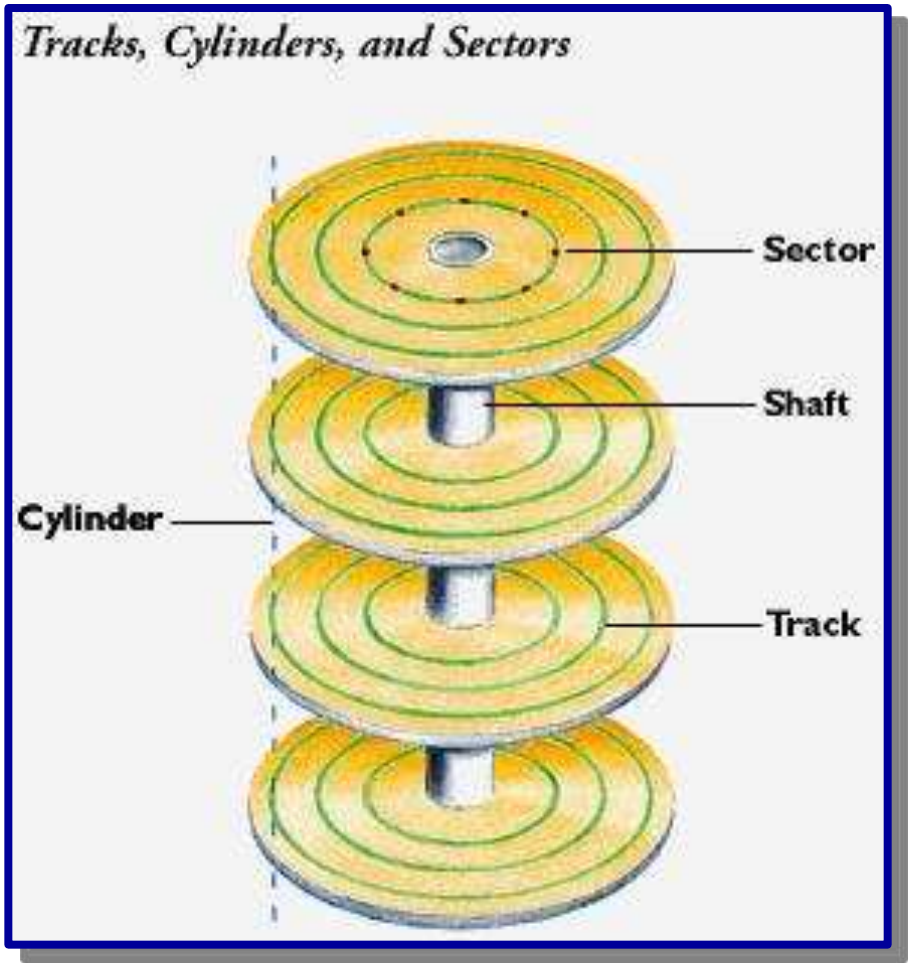
The disk is therefore divided into:

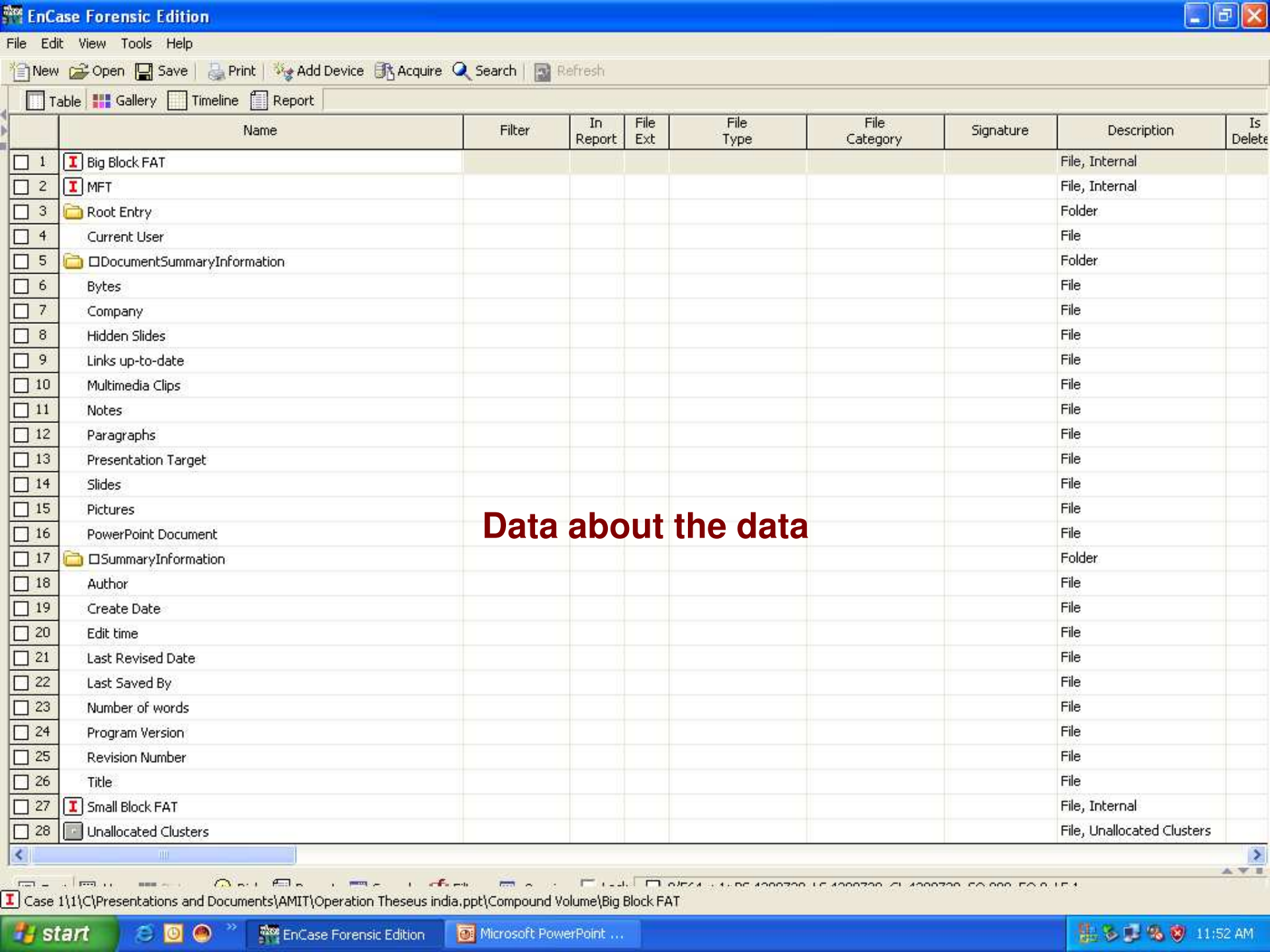


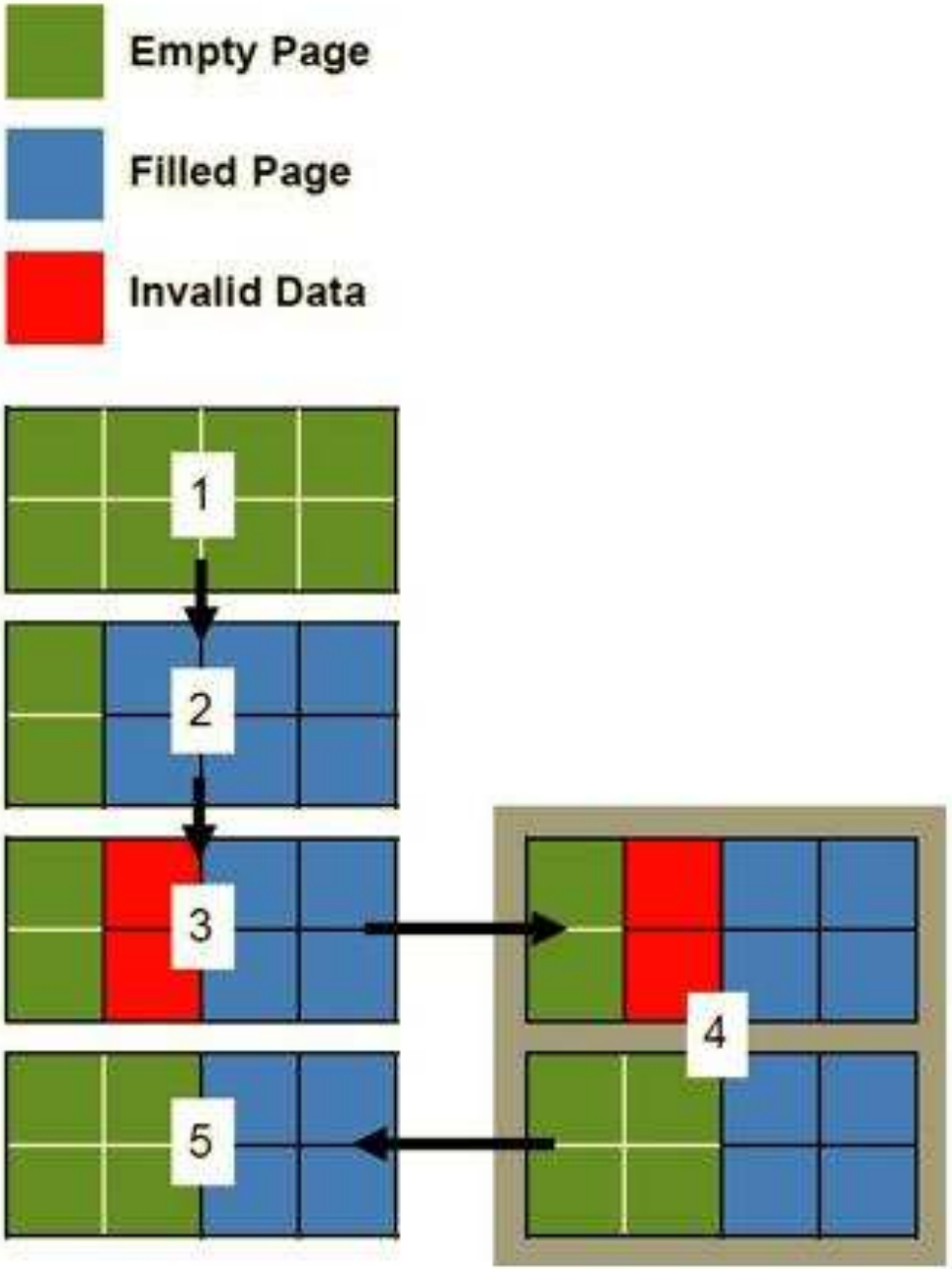
Tracks

Sectors

Accessing Information on a Hard Drive




EnCase Forensic Edition
File Edit View Tools Help
New Open Save Print Add Device Acquire Search Refresh
Table Gallery Timeline Report
Name Filter In Report File Ext File Type File Category Signature Description Is Delete
1 Big Block FAT File, Internal
2 MFT File, Internal
3 Root Entry Folder
4 Current User File
5 DocumentSummaryInformation Folder
6 Bytes File
7 Company File
8 Hidden Slides File
9 Links up-to-date File
10 Multimedia Clips File
11 Notes File
12 Paragraphs File
13 Presentation Target File
14 Slides File
15 Pictures File
16 PowerPoint Document File
17 SummaryInformation Folder
18 Author File
19 Create Date File
20 Edit time File
21 Last Revised Date File
22 Last Saved By File
23 Number of words File
24 Program Version File
25 Revision Number File
26 Title File
27 Small Block FAT File, Internal
28 Unallocated Clusters File, Unallocated Clusters
Data about the data
Case 1\1\C\Presentations and Documents\AMIT\Operation Theseus india.ppt\Compound Volume\Big Block FAT
start
EnCase Forensic Edition
Microsoft PowerPoint ...
11:52 AM



1.) SSD pages contain no data

2.) User writes data to SSD pages

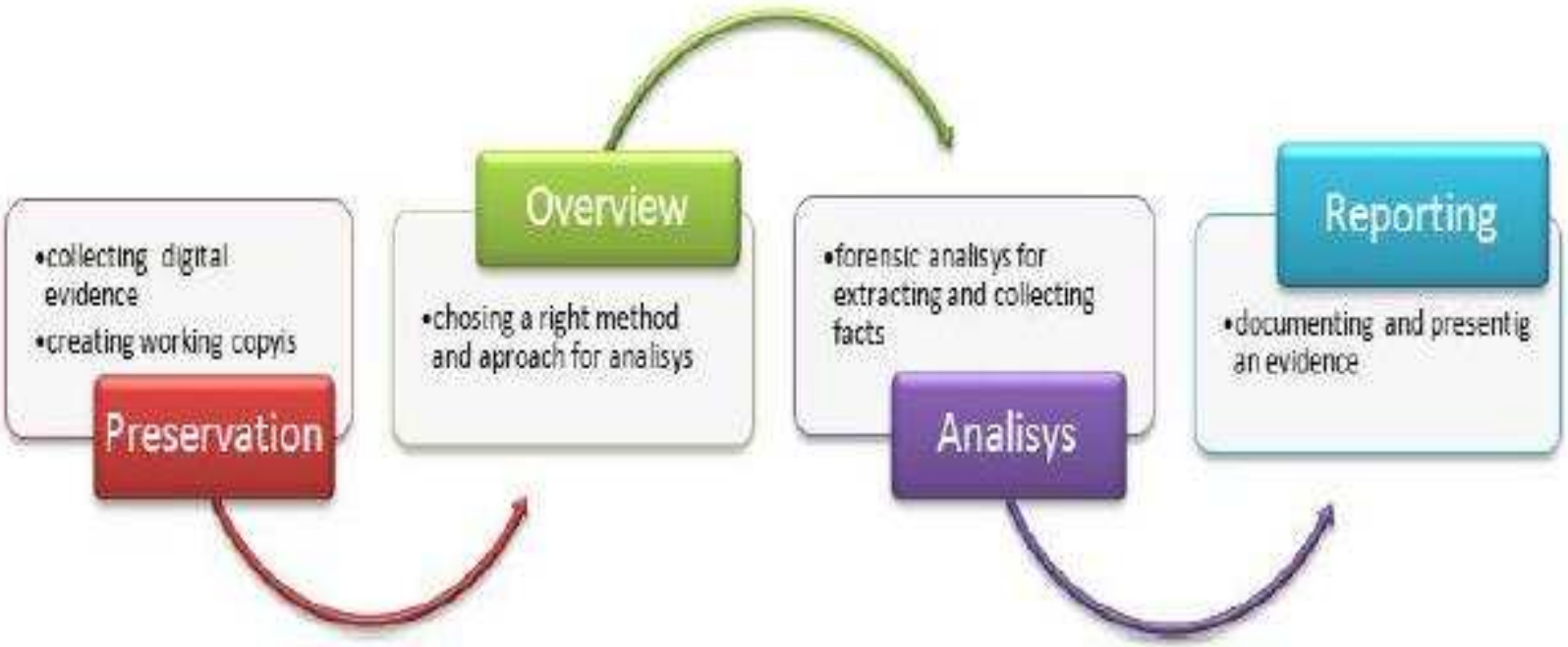
3.) User deletes some data. Pages are marked as 'not in use' by the host OS, but data remains on SSD.

4.) TRIM command tells SSD controller that pages contain invalid data. Pages with invalid data are cleaned.

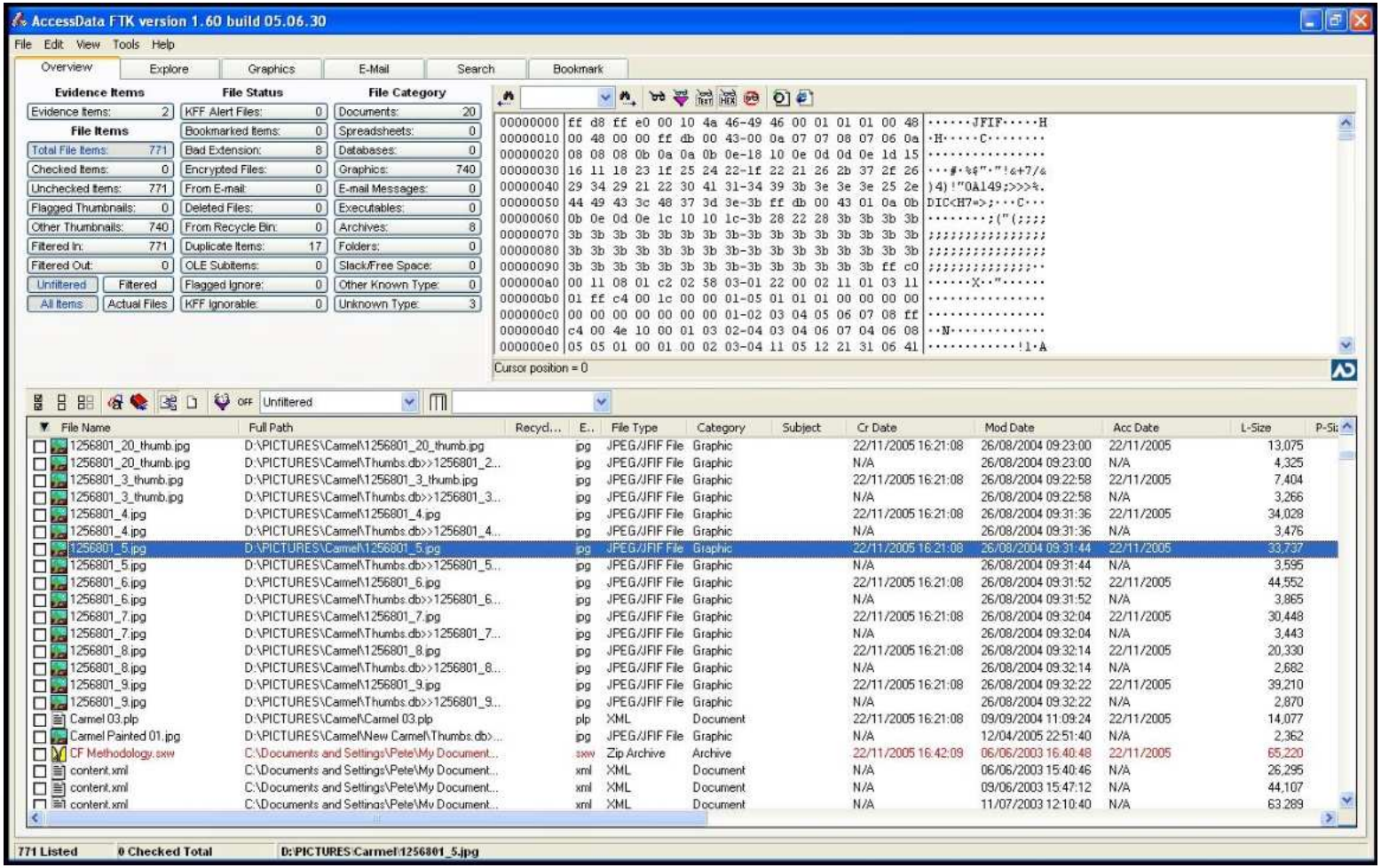
5.) Data is written back to SSD memory cells. The invalid data has been cleaned and data is able to be written to the pages at full speed.

TRIM, image from http://www.corsair.com/us/blog/how-to-check-that-trim-is-active/

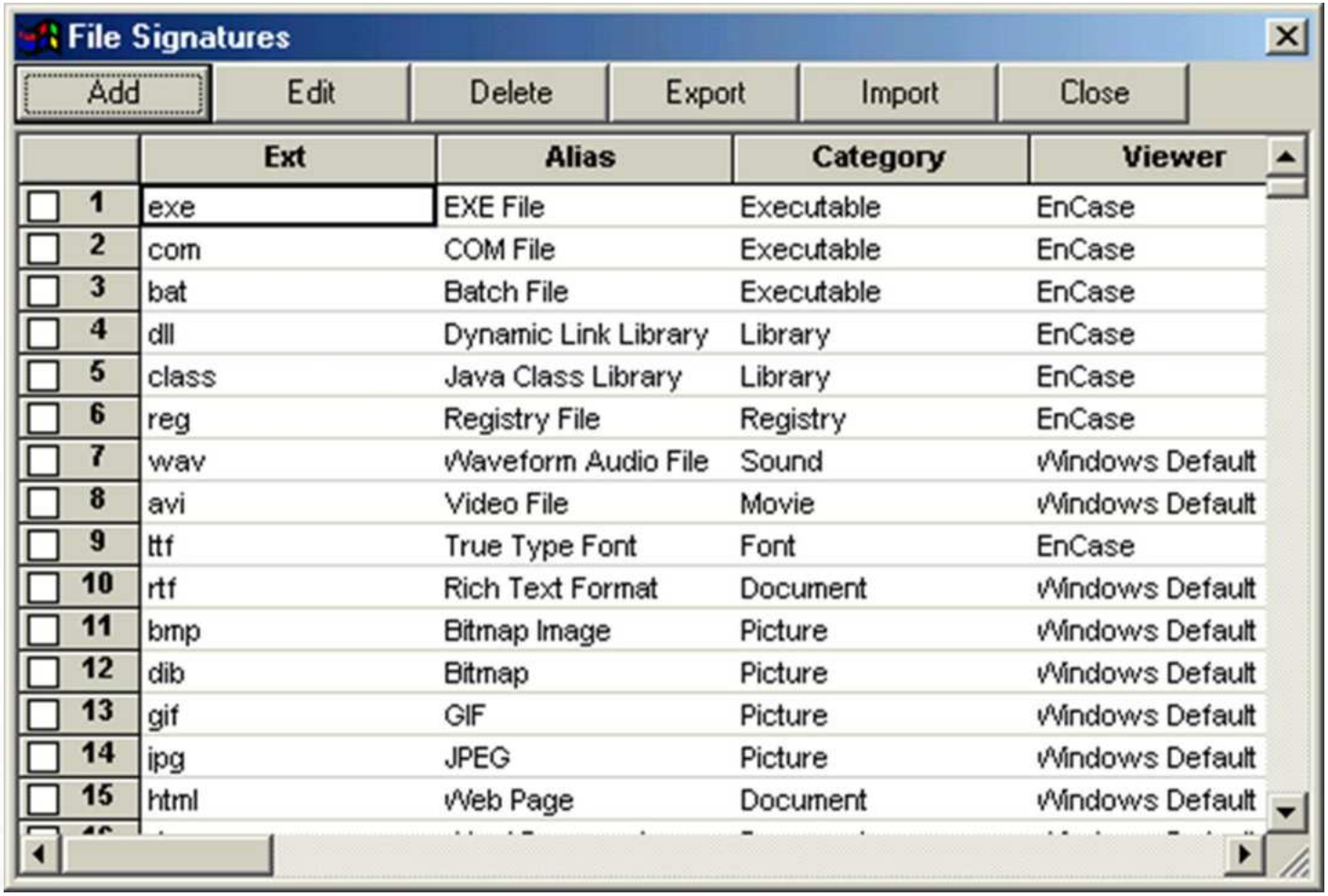
Forensic Process



Forensic Analysis Software

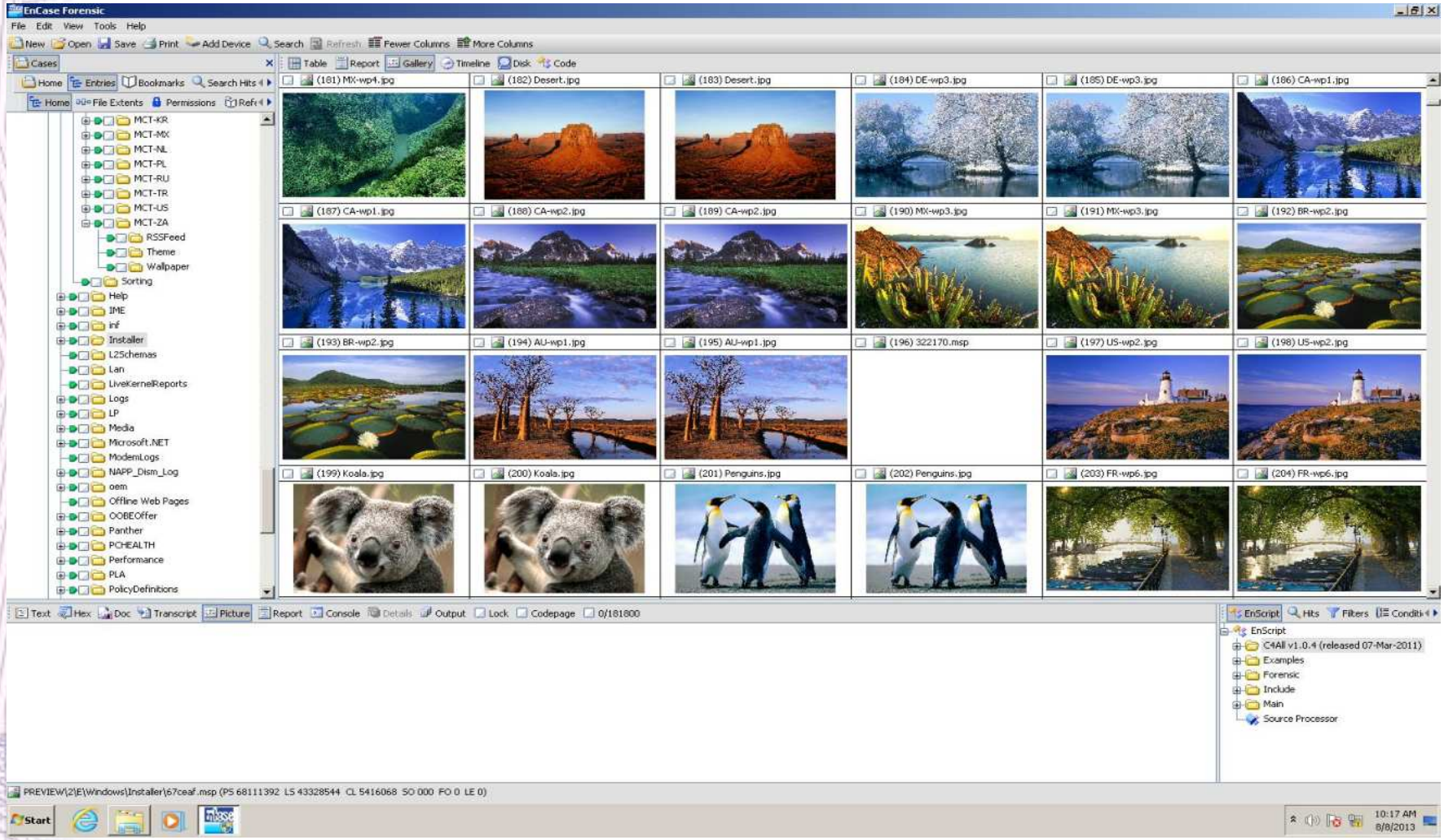


File Signatures



	Ext	Alias	Category	Viewer
1	exe	EXE File	Executable	EnCase
2	com	COM File	Executable	EnCase
3	bat	Batch File	Executable	EnCase
4	dll	Dynamic Link Library	Library	EnCase
5	class	Java Class Library	Library	EnCase
6	reg	Registry File	Registry	EnCase
7	wav	Waveform Audio File	Sound	Windows Default
8	avi	Video File	Movie	Windows Default
9	ttf	True Type Font	Font	EnCase
10	rtf	Rich Text Format	Document	Windows Default
11	bmp	Bitmap Image	Picture	Windows Default
12	dib	Bitmap	Picture	Windows Default
13	gif	GIF	Picture	Windows Default
14	jpg	JPEG	Picture	Windows Default
15	html	Web Page	Document	Windows Default

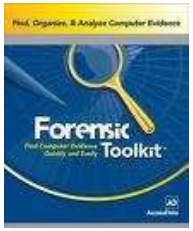
EnCase Gallery



Popular Forensic Software Tools

For Disk Forensics

- Encase
- FTK
- Belkasoft

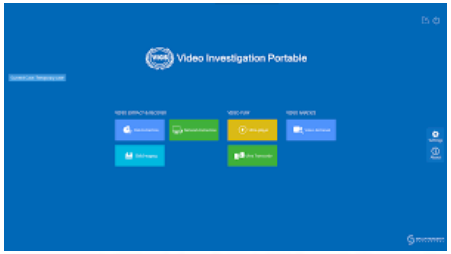


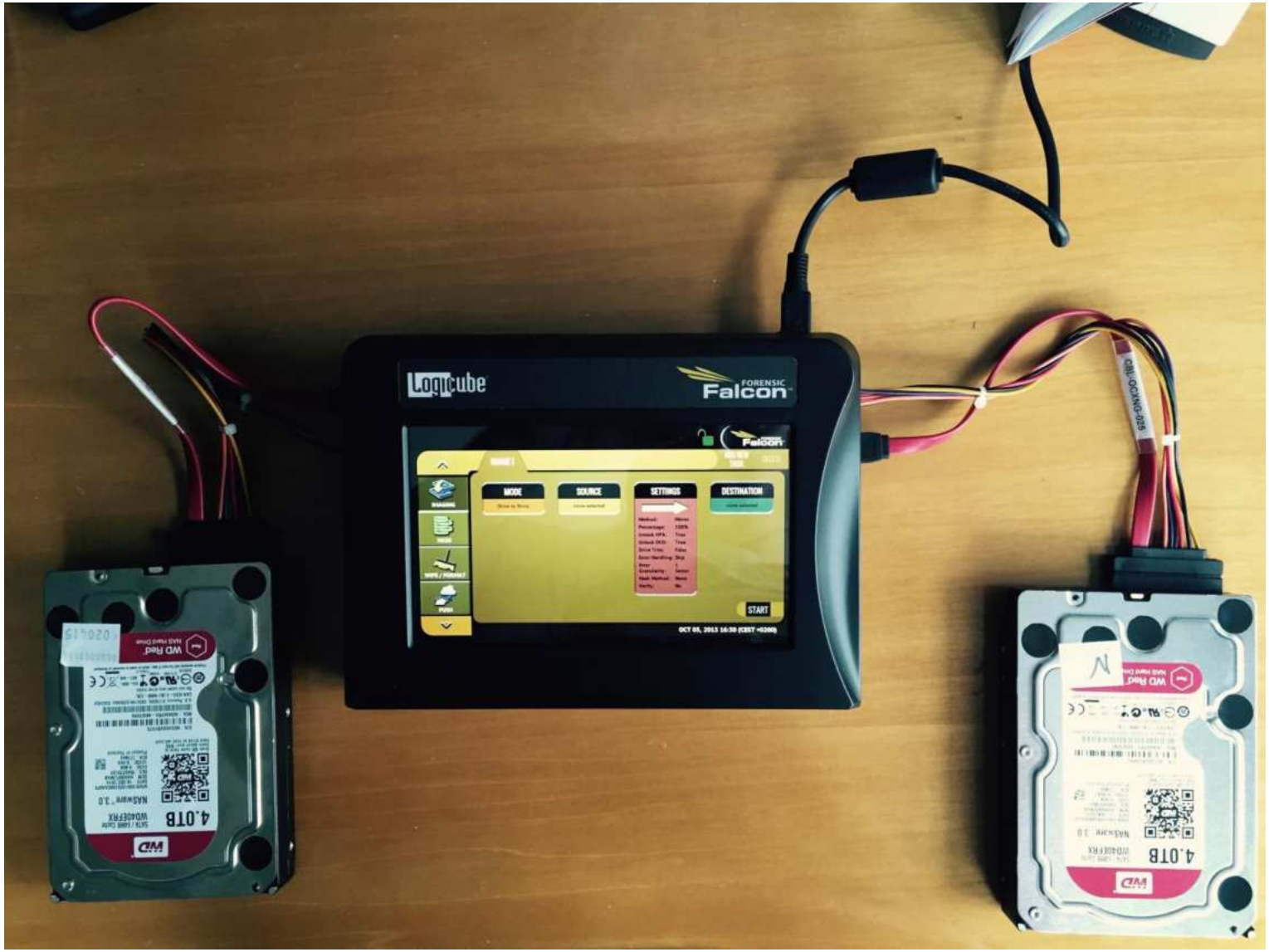
For Mobile Forensics

- UFED 4 PC, UFED Touch
- XRY
- Mobiledit
- Oxygen Detective

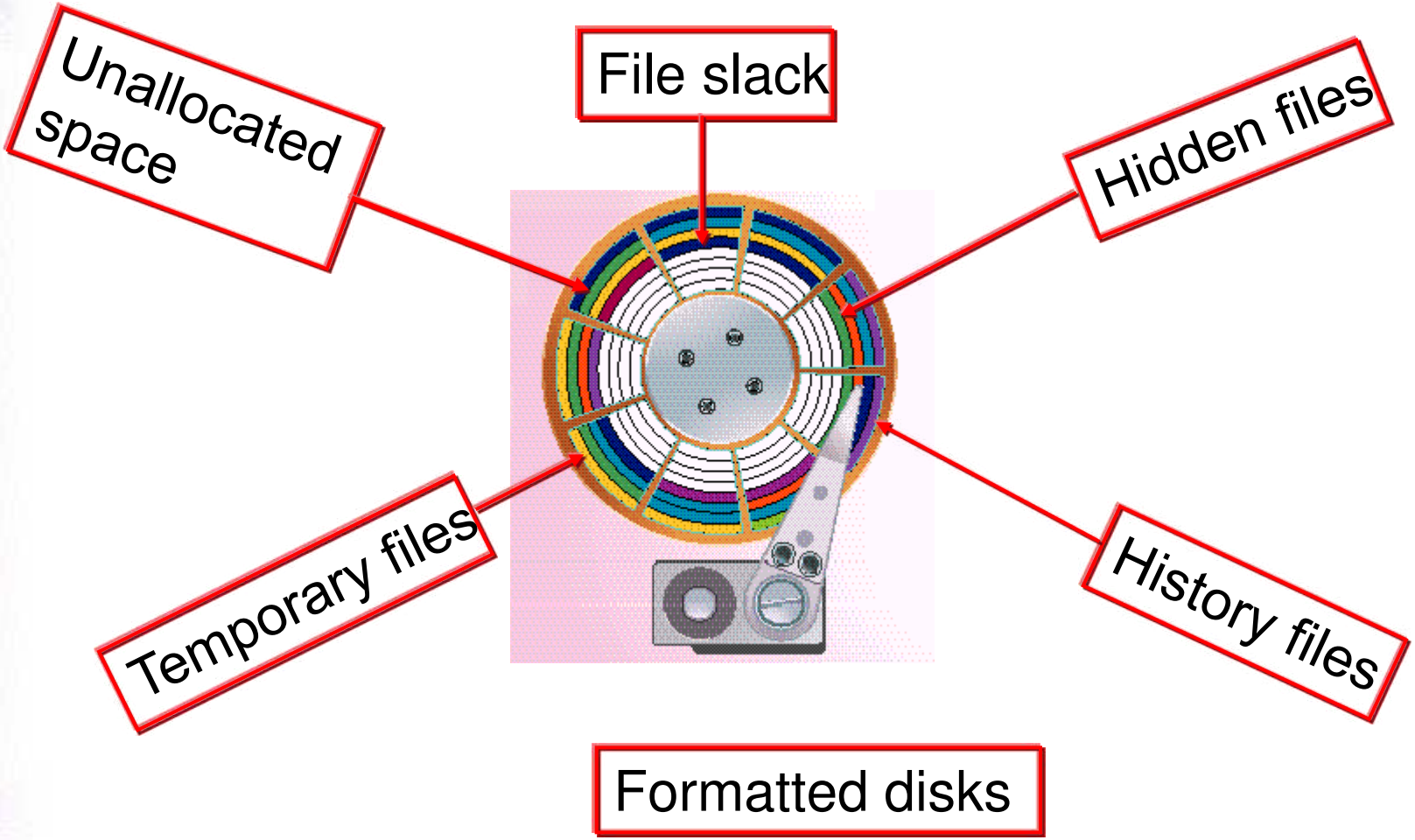
For Social Media Related

- Magnet Axiom
- X1 Social Discovery




Logicube
FORENSIC
Falcon
MODE
SOURCE
SETTINGS
DESTINATION
START
4.0TB

Why To Image

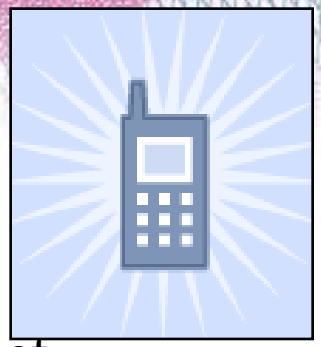

Unallocated space
File slack
Hidden files
Temporary files
History files
Formatted disks

Hardware Write Blocker

Smartphone is a small PC

- Cell phone
- Address book
- Planner & Organizer
- Messenger
- Photo & Video camera
- GPS navigator
- Web client
- Platform for 3rd party apps

Mobile Device Forensics Overview



Data Capture Options

Screen Captures: The simplest way. Use a camera to take pictures of what's on the screen. Reporting tools available. Sometimes this is the only way.

Logical Analysis: – Extracting the data on the device that you see and can access on the device. No deleted information with this method. Call logs, phone books, sms messages, pictures, email, browsing etc. The "active" information on the device can be extracted using a "Logical" extraction tool. This is the standard method today. Plenty of tools and easy to use.

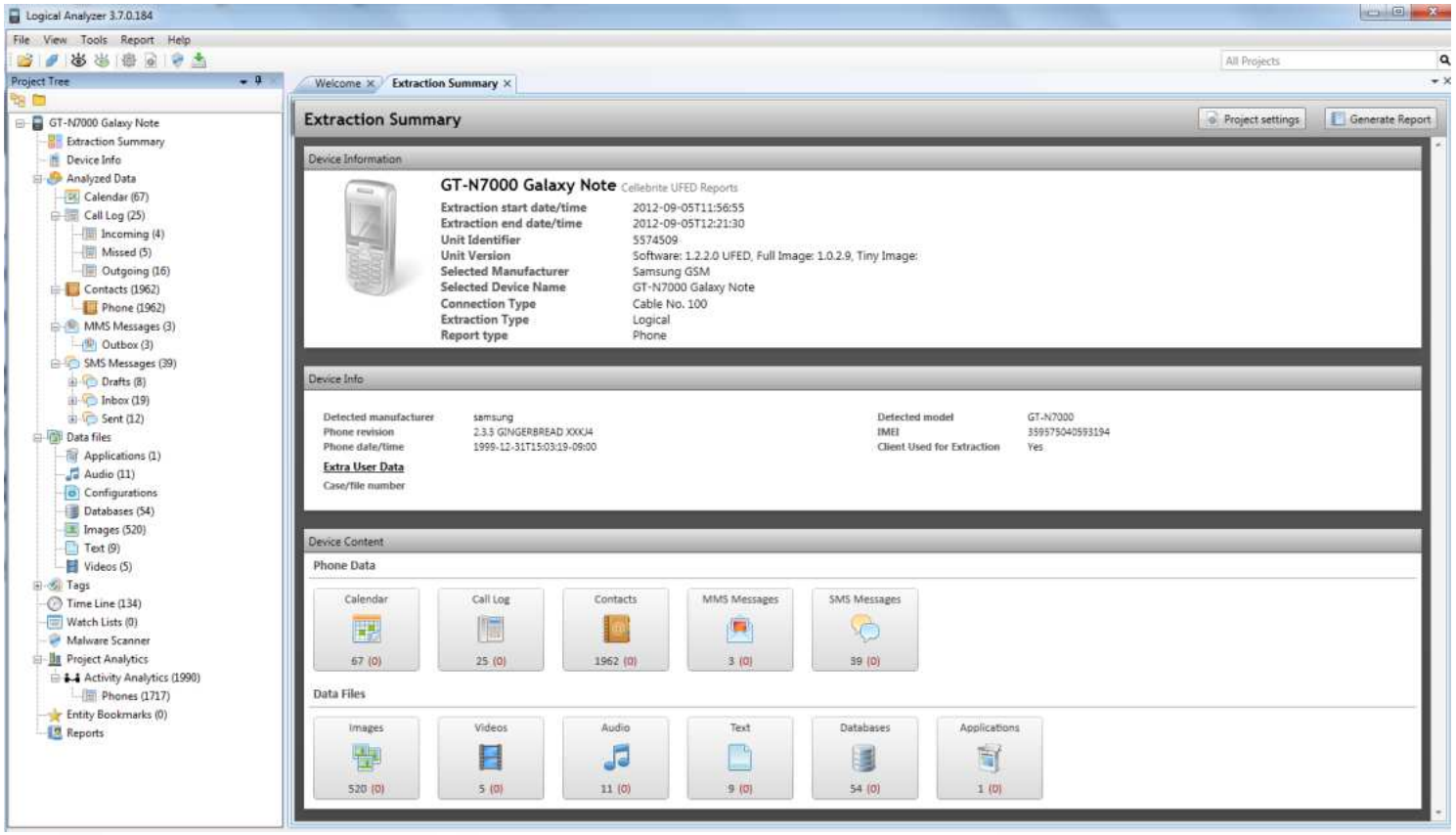
File System & Advanced Logical Analysis:

Physical Analysis: – The practice of extracting data from the physical memory of the device, and removable memory. Like PC forensics, you are getting the raw binary / hex data. Requires decoding and understanding of language and techniques used by device manufacturers. Physical analysis is the way to deleted information, but it is difficult and sparsely supported. Only a few tools. Mostly Nokia supported. Early days of the new standard.

Chip Level Analysis: - Analysis of the chips in the phone by removing them from the device and probing for data, or rebuilding another phone. Extremely technical. Broken SIMs analyzed this way.

Logical Extraction Results

- A well formatted report:
  - Call logs, Contacts, SMS messages, Videos, Photos, Audio, Music



File System Extraction Results

- SMS, Contacts, Call Logs, MMS, Notes, Applications, Voice Mails, Calendar, Bluetooth, GPS, Notes, Bookmarks, Skype, Chat, Cookies, Facebook Content

- .plist files containing great forensic data

  'keychain-2.db' - Networks the user connected to including Wi-Fi, VPN, Bluetooth and the Apple iTunes Store ID.

  Other databases contain information from Apps

Registry: A Wealth of Information

Information that can be recovered include:

- System Configuration
- Devices on the System
- User Names
- Personal Settings and Browser Preferences
- Web Browsing Activity
- Files Opened
- Programs Executed
- Passwords

Sec. 65B-Admissibility of Electronic Records

Section 65B(1) –

Electronic record in form of CD, DVD, Print Out admissible subject to condition in Section 65B(2).

Section 65B(2)-

The computer from which the record is generated was regularly used to store or process information in respect of activity regularly carried on by a person having lawful control over the period, and relates to the period over which the computer was regularly used;

Information was fed in computer in the ordinary course of the activities of the person having lawful control over the computer;

The computer was operating properly, and if not, was not such as to affect the electronic record or its accuracy;

Information reproduced is such as is fed into computer in the ordinary course of activity.

Sec. 65B-Admissibility of Electronic Records

Section 65B(3) –

The combination of computer used for storage or processing shall be constituted as a single computer.

Section 65B(4) – The certificate is to be given:

Identifying relevant electronic record and the manner of production;

Particular of the device producing the electronic record.

and purporting to be signed by a person occupying a responsible official position in relation to -

the operation of the relevant device or

the management of the relevant activities

Computer-stored versus computer-generated.

Computer-stored evidence includes documents and other records that were created by a human being and that just happen to be stored in electronic form.

Examples include word processing files, e-mail messages, and Internet chat room messages.

LOG FILES are computer generated files

Hash value and utility.

When you apply the **hashing** algorithm to an arbitrary amount of data, such as a binary **file**, the result is a **hash** . This **hash** has a fixed size. MD5 is a **hashing** algorithm that creates a 128-bit **hash value**. SHA-1 is a **hashing** algorithm that creates a 160-bit **hash value**.

Hash value is generated for the memory used(both active and passive) not for the Hard disk as people think.

This function is required in case of imaging the original storage media on to another sterile media and if the resultant copy has the same hash value it indicates that, it is as good as original.

A 65 B certificate is required from the system administrator or lawful authority.

Where Hash value is being collected.

The CCTV captured clippings, bank related servers and servers which can't be seized, such situations we do imaging with the help of our Cyber Lab or FSL.

The CDRs which are relevant for proving a fact requires IE Act-65 B certificate from the concerned.

65 B certificate is to be collected at the time taking the data from the concerned not at the time of submitting the charge sheet.

Anwar vs Basheer case of Hon'ble Supreme court.

Copy vs Original

Many a times people feel that the evidence found in portable storage media(USB drive, CD, DVD)is copy which requires 65 B certificate, but many cases we found if a file is generated and saved directly in portable storage media then it is original though it is in portable storage media.

In DATA BASE related issues, there is confusion to establish which is original and which is copy. It requires in depth understanding of the structure of data base.

Blocking of sites.

Section 69 A: Blocking sites for national security only and not for pornography or defamation or copy right violation.

Section 79 (3)B : Blocking/removing of content in cases of cognizable offences.

CYCORD- MHA initiative to help all the state police

Types of IP address

Static IP address

Remains constant even if the user disconnects & reconnects to the Internet

Tracing the IP may identify the owner, or it may also just identify an ISP

Version 4(4 Billion IP Addresses only)

0-255.0-255.0-255.0-255 (FOUR SEGMENTS)

Ex 62.135.45.01

Version 6(Trillion, Trillion, Trillion IP's)

EX:
ABCD:EF01:2345:6789:ABCD:B201:5482:D024

(EIGHT SEGMENTS)

Dynamic IP address

- Changes each time the user logs onto the Internet
- Tracing will only provide the details of the ISP
- Need to conduct a further check with the customer records of that ISP

MUST provide an accurate date and time!!

Private IP address

Private IP addresses can only be used in internal LANs

If investigator come across one of these in an Internet investigation, there must have been a mistake (or a forged IP address)

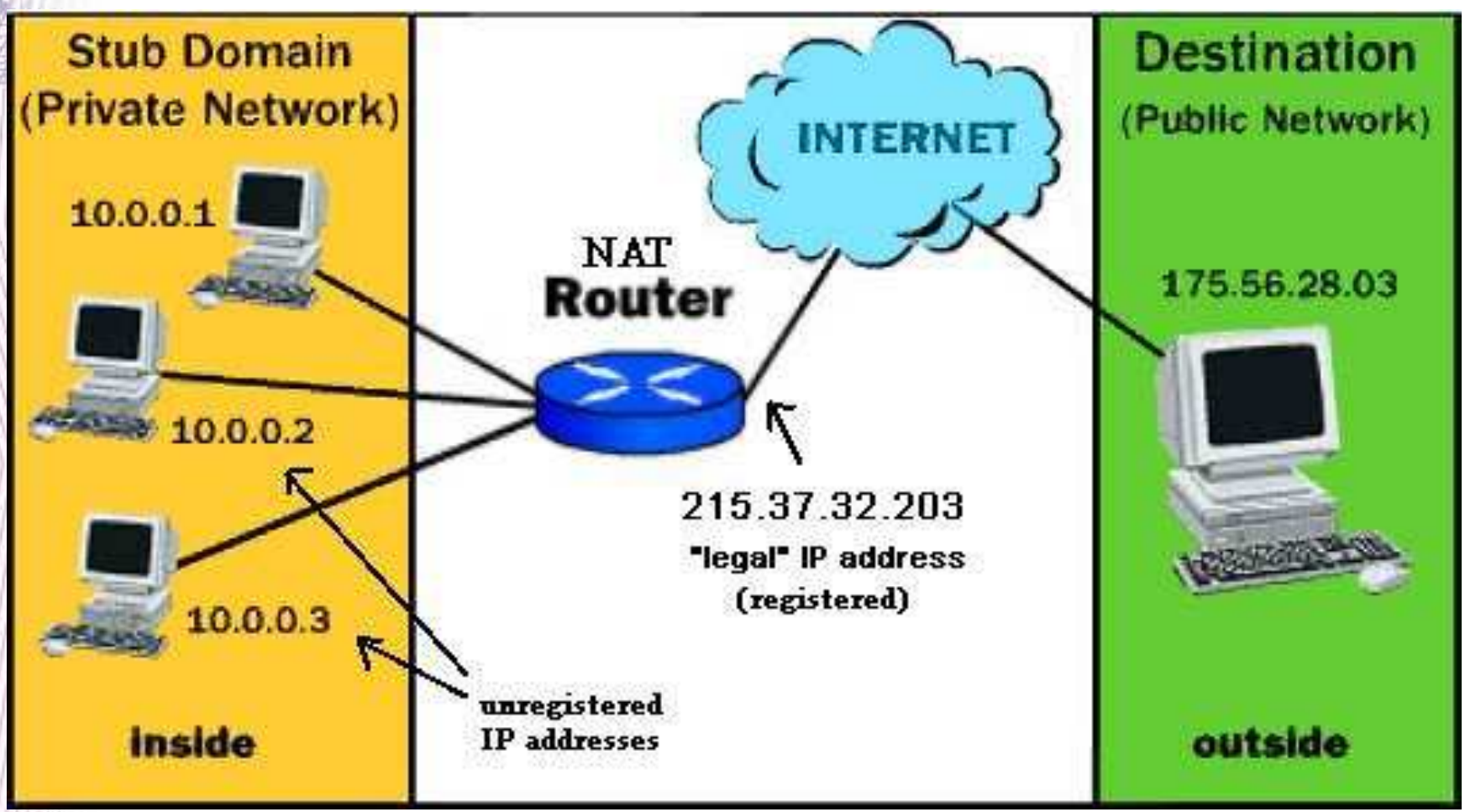
IP addresses: 10.0. 0.0 – 10.255. 255.255.

IP addresses: 172.16. 0.0 – 172.31. 255.255.

IP addresses: 192.168. 0.0 – 192.168. 255.255.

Framed IP/ IP NATing

Same public IP address given to multiple mobiles/ data cards at same time with private IP


Stub Domain
(Private Network)
10.0.0.1
10.0.0.2
10.0.0.3
Inside
NAT
Router
INTERNET
215.37.32.203
"legal" IP address
(registered)
unregistered
IP addresses
Destination
(Public Network)
175.56.28.03
outside

```
Delivered-To: goodguys244@gmail.com
Received: by 10.31.186.130 with SMTP id k124csp119929vkf;
        Mon, 29 Aug 2016 22:15:02 -0700 (PDT)
X-Received: by 10.36.47.6 with SMTP id j6mr22053583itj.82.1472534102270;
        Mon, 29 Aug 2016 22:15:02 -0700 (PDT)
Return-Path: <kishore.kumar690@yahoo.com>
Received: from nm48-vm7.bullet.mail.ne1.yahoo.com (nm48-vm7.bullet.mail.ne1.yahoo.com. [98.138.121.119])
        by mx.google.com with ESMTPS id o84si3133099itd.64.2016.08.29.22.15.01
        for <goodguys244@gmail.com>
        (version=TLS1 cipher=ECDHE-RSA-AES128-SHA bits=128/128);
        Mon, 29 Aug 2016 22:15:02 -0700 (PDT)
Received-SPF: pass (google.com: domain of kishore.kumar690@yahoo.com designates 98.138.121.119 as permitted sender) client-
ip=98.138.121.119;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@yahoo.com;
       spf=pass (google.com: domain of kishore.kumar690@yahoo.com designates 98.138.121.119 as permitted sender)
smtp.mailfrom=kishore.kumar690@yahoo.com;
       dmarc=pass (p=REJECT dis=NONE) header.from=yahoo.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1472534101;
bh=fkyfaCERUYMEpUWAhfUJLQUxF2jpWfW3T5zlAFP3s9Y=; h=Date:From:Reply-To:To:Subject:References:From:Subject;
b=oCSAtx53kQZCyleUyr8cK+mrJdcgIDR+Z73rA7J7eKDVx0vhLe/rdUVTBXrhprzSCITT9bRzautW9jwLXEwIOnuoUuZLmoXw5Cc20gJDxKs75TMtgrsdtKYzCNKnN++e0Z
S2BuGPnzo74q7k0BNpsLcM77ap6DyOldrEabCHqF1MPwaxjpIjmx6Jun3P6sz4+PeU47eaO5pPXTzRx5AkAiSFyMjxT3tuLcMUbp3Iv2u6Sv0Sw8/IEqLUw+o6vOpLkipH3s
ObLsA4Hx+7x+8nfLxzNYHBfl2lJt89o9T5ISuk5hBj7BDkZgWlS6xhYYAwASqn0qF8WNpw2n5DMvStiQ==
Received: from [127.0.0.1] by nm48.bullet.mail.ne1.yahoo.com with NNFMP; 30 Aug 2016 05:15:01 -0000
Received: from [98.138.226.178] by nm48.bullet.mail.ne1.yahoo.com with NNFMP; 30 Aug 2016 05:12:20 -0000
Received: from [98.138.89.198] by tm13.bullet.mail.ne1.yahoo.com with NNFMP; 30 Aug 2016 05:10:20 -0000
Received: from [127.0.0.1] by omp1056.mail.ne1.yahoo.com with NNFMP; 30 Aug 2016 05:10:20 -0000
X-Yahoo-Newman-Property: ymail-4
X-Yahoo-Newman-Id: 818386.2923.bm@omp1056.mail.ne1.yahoo.com
X-YMail-OSG: 2Ga_aXsVM1nEoHFMHvmr80kX80A_x6IMloP.34ViUxoxICEd2dOhsIdQ_mRx.Sj
wfjpBTDXbKrhLP1NgzOWcNF8OhEE9r_Q8CYPAL9M5R1gfvRBZrgsntLLxkPVCTnJYOMtRbs.KnJ7
Owo5uYia6uG190Q.27v9NxRd.twPTDSVt9RCNEfXfe3Gi2B3H1.rj0cBWTa8AjuaTC5tpp_nxg8K
eRNav2pkeFcb.QYC36jNSHPqOt2HMu8CnPmIoy8hpuZjBnIn_dYef6sn6Iaq_qxGt8.1qlveCEu8
b3BnivyZFn4_S0NL9Oq7.Tyk27zZ8yEaK0fSo0HTcahWT0rg2CCOD32gJ_GqX0QSEhXW2feKe4H2
lP_hw0oTxrOq9WFdBnavD9UbVDnsrpTmU8D6myyjmZUg6Nbb7Dw.G6QOmeZG3Zhf8wuoMw2czSyQ
Gp3zy2a5OgsYKUAKlORa3MJbvZLQQvWJBYQRryV7qGT0EzqDscLt6LEplZCJ82o.ZpTrJygCfNC7
```

CYBER CRIME POLICE STATION,
CRIME INVESTIGATION DEPT.,
A. P., HYDERABAD, INDIA.

Cr.No.202/VZA/CCPS/CID/2016. **Date: 12-05-2016.**

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

I am the Superintendent of Police working at Cyber Crime Police Station, CID, Hyderabad, Andhra Pradesh State, India. I am investigating a case wherein a complainant named LAVNAYA who is working for reputed company, has found her personal photos posted with 2 profiles. The postings contains her personal photos and contains vulgar title "Sexy Desi Aunty ready for SEX!". Hence the details are very much essential for the purpose of investigation. The URL of the Facebook profiles is appended below for your reference.

https://www.facebook.com/profile.php?id=100011862167399\

https://www.facebook.com/profile.php?id=100011990291447

In this connection it is requested to furnish the **Registration & accessing IP Log details** of the above said profile including dates & timings for the purpose of investigation. You are further requested to remove the said profile soon after furnishing of information.

DECLARATION

I declare that the case upon charge sheeted will be tried before Hon'ble VI Additional Chief Metropolitan Magistrate Court, Hyderabad.

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

C.No.1120/CCPS/CID/2015.

Date: 13-11-2015.

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

-o0o-

It is to inform you that a case is being investigating by this agency wherein some unknown accused has sent a threatening email which contains her personal photos. The email has some private photos of the victim. Further in this connection the Registration & accessing IP Log details of the following Email ID are very much required for the purpose of investigation.

Kishore.kumar69@yahoo.com

Therefore you are requested to furnish the **Registration & accessing IP Log details (including the IP Addresses, dates & timings)** of the above Email ID **since its creation to till date** for the purpose of investigation.

Early action would be highly appreciated.

Early action would be highly appreciated.

Office of the
Superintendent of Police,
Cyber Crimes, CID,
T.S, Hyderabad.

C.No.166/CCPS/CID/2016. Date: 18-08-2016.

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

-ooo-

It is to inform you that a case vide reference cited above is being investigated by this agency wherein some unknown online fraudsters gained access to the confidential details of the **STATE BANK OF HYDERABAD Debit card** information which belongs to **Mohammed Kaleem Uddin** of **HYD Dist** bearing A/c No.**52097508118** and **Debit Card No.5044352008400040135** and made a fraudulent transaction on **03-09-2016** and tuned an amount **Rs.4,999/-** with your services(domain) causing wrongful loss to the complainant, wrongful gain to the fraudsters. The details of the transaction is appended below.

Date of Tranc	Service Name	POS	Amount
03/09/2016	SBI_BUDDY	GU4726268852	4999

Therefore you are requested to furnish the following information with regard to the above said transactions for the purpose of investigation.

1. **Please stop payment to the merchant and refund the amount to the actual customer's account.**
2. **Complete details of the transaction including beneficiary account / mobile holders.**
3. **Accessing IP Log details of the above transactions.**
4. **Any other information which may be useful to trace the fraudsters.**

Early action will be highly appreciated.

Superintendent of Police,
Cyber Crimes, CID,
Hyderabad.

YAHOO! ACCOUNT MANAGEMENT TOOL

Login Name:	**oo4kunv3a4se7y4atwkjefzddknhqviem3lz4dzx**
GUID:	**F5HJQ6D55Q5UVAMGRUF4E5CKUI**
Properties Used:	**Mail**
Yahoo Mail Name:	**collinspaul534@yahoo.com**
Alternate Communication Channels:	**91 9599365610**
Account Created (reg):	**Sat Apr 23 04:56:53 2016 GMT**
Other Identities:	**oo4kunv3a4se7y4atwkjefzddknhqviem3lz4dzx** **collinspaul534**
Full Name	**Collins Paul**
Address1:	
Address2:	
City:	
State, territory or province:	
Country:	
Zip/Postal Code:	
Phone:	
Time Zone:	
Birthday:	**October 26, 1917**
Gender:	**Male**
Occupation:	
Business Name:	
Business Address:	
Business City:	
Business State:	
Business Country:	
Business Zip:	
Business Phone:	
Business Email:	
Account Status:	**Active**

Facebook Business Record

Service		Facebook
Target		100009887861370
Generated		2015-10-07 12:59:32 UTC
Date Range		2015-06-01 00:00:00 UTC to 2015-09-10 23:59:59 UTC
NCMEC CyberTip Numbers		
Name	**First**	Rakesh
	Middle	
	Last	Reddy
Registered Email Addresses		100009887861370@facebook.com y11eee263@gmail.com
Vanity Name		
Registration Date		2015-07-29 05:46:33 UTC
Registration Ip		117.201.219.221
Account Closure Date	**Account Still Active**	false
	Time	2015-09-28 10:56:04 UTC
Phone Numbers		
Ip Addresses	**IP Address**	117.201.219.221
	Time	2015-07-29 06:22:31 UTC

Data Networks Circle
BB-NOC Bangalore, O/o DGM BB
Ph –080-25809988, Fax-25806666
e-mail- bbnoc@dataone.in

भारत संचार निगम लिमिटेड
(भारत सरकार का उपक्रम)
BHARAT SANCHAR NIGAM LIMITED
(A Govt. of India Enterprise)

CONFIDENTIAL

No-DNW/DGM-BG/BB-NOC/IP-Detail/01 Dated @Bangalore the 08-10-2015

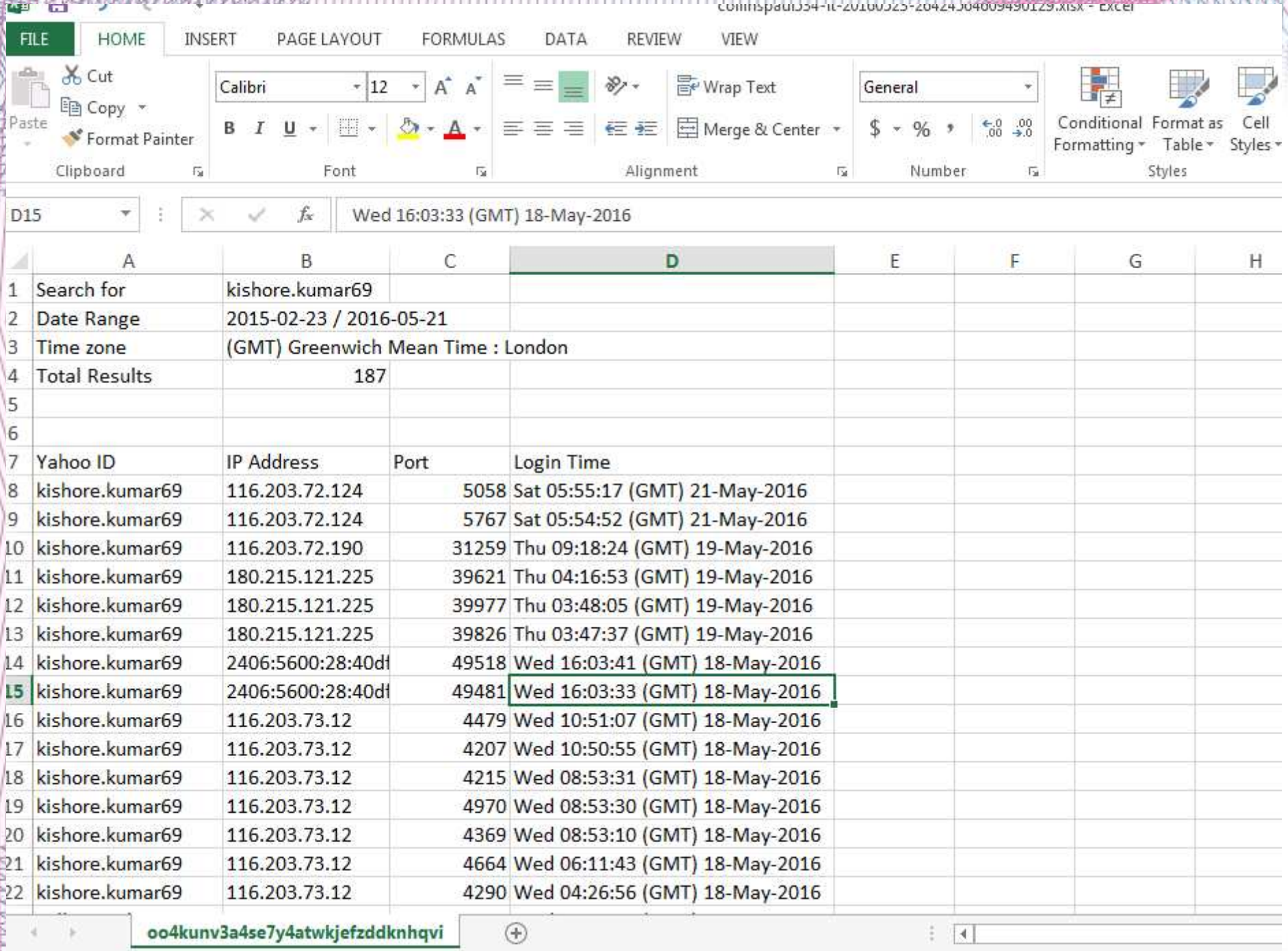
To,

The Circle Co-ordinator, BSNL.

Sub.:- Details of IP address :-

Sl. No.	Details Provided			Time in IST	User Information [For Date/Time given & converted in IST]
	IP Address	Date	Time in GMT		
1.	117.201.219.221	2015-07-29		11:16:33	**User-id:** id8641233015_scdrid@bsnl.in **Name:** G VENKAYAMMA **Phone No:** 08641-233015 **Address :** 8-3-35, SBI ROAD, OPP APNGOS HOME CENTER, SATTENAPALLI , SATTENAPALLI GUNTUR – 522403, AP **Start Time :Wed 29 Jul 2015 10:00:26** **Stop Time :Wed 29 Jul 2015 13:02:34** MAC: c0:a0:bb:8f:96:78 PORT: 9/1 vlan-id 2008;536 pppoe 466 BNG: gtr-ras-bng-gtr-01

BNG: gtr-ras-bng-gtr-01


FILE
HOME
INSERT
PAGE LAYOUT
FORMULAS
DATA
REVIEW
VIEW
Cut
Copy
Format Painter
Paste
Clipboard
Calibri
12
Font
Wrap Text
Merge & Center
Alignment
General
Number
Conditional Formatting
Format as Table
Cell Styles
Styles
D15
Wed 16:03:33 (GMT) 18-May-2016
A
B
C
D
E
F
G
H
1 Search for kishore.kumar69
2 Date Range 2015-02-23 / 2016-05-21
3 Time zone (GMT) Greenwich Mean Time : London
4 Total Results 187
5
6
7 Yahoo ID IP Address Port Login Time
8 kishore.kumar69 116.203.72.124 5058 Sat 05:55:17 (GMT) 21-May-2016
9 kishore.kumar69 116.203.72.124 5767 Sat 05:54:52 (GMT) 21-May-2016
10 kishore.kumar69 116.203.72.190 31259 Thu 09:18:24 (GMT) 19-May-2016
11 kishore.kumar69 180.215.121.225 39621 Thu 04:16:53 (GMT) 19-May-2016
12 kishore.kumar69 180.215.121.225 39977 Thu 03:48:05 (GMT) 19-May-2016
13 kishore.kumar69 180.215.121.225 39826 Thu 03:47:37 (GMT) 19-May-2016
14 kishore.kumar69 2406:5600:28:40d 49518 Wed 16:03:41 (GMT) 18-May-2016
15 kishore.kumar69 2406:5600:28:40d 49481 Wed 16:03:33 (GMT) 18-May-2016
16 kishore.kumar69 116.203.73.12 4479 Wed 10:51:07 (GMT) 18-May-2016
17 kishore.kumar69 116.203.73.12 4207 Wed 10:50:55 (GMT) 18-May-2016
18 kishore.kumar69 116.203.73.12 4215 Wed 08:53:31 (GMT) 18-May-2016
19 kishore.kumar69 116.203.73.12 4970 Wed 08:53:30 (GMT) 18-May-2016
20 kishore.kumar69 116.203.73.12 4369 Wed 08:53:10 (GMT) 18-May-2016
21 kishore.kumar69 116.203.73.12 4664 Wed 06:11:43 (GMT) 18-May-2016
22 kishore.kumar69 116.203.73.12 4290 Wed 04:26:56 (GMT) 18-May-2016
oo4kunv3a4se7y4atwkjefzddknhqvi

REMINDER: CID - Cyber Crime PS Hyderabad - Request for IP end user particulars [C.No.1409/2016/TANUJAS/CCPS/CID]- Regarding.

CYBERPS 09/19/2016 10:5

To: nodal.term;

\\\\\ URGENT \\\\\

Dear Sir,

It is requested to furnish the **end-user particulars** of the following IP Addresses for the purpose of investigation.

IP ADDRESS	DATE	TIME(IST)
183.82.231.200	30-Jul-16	23:07:15
183.82.231.200	30-Jul-16	00:20:34
183.82.231.200	31-Jul-16	08:24:20
183.82.231.200	31-Jul-16	23:38:16
49.206.203.100	7-Aug-16	20:51:48
49.206.203.100	7-Aug-16	21:51:08
183.82.229.132	9-Aug-16	22:22:19
183.82.229.132	9-Aug-16	23:04:22
49.32.24.221	11-Sep-16	23:16:52
183.82.230.176	11-Sep-16	22:56:15
183.82.230.176	11-Sep-16	20:44:37
183.82.229.22	11-Sep-16	20:40:28
183.82.229.22	11-Sep-16	20:28:50
183.82.225.223	10-Sep-16	16:08:31
183.82.225.223	10-Sep-16	15:27:10

URGENT: CID Cyber Crimes - Hyderabad - Request to furnish certain information [C.No.1312/CCPS/CID/2016/AVG/SP]

File | Message

Junk | Delete | Reply | Reply all | Forward | Instant message | Add to calendar | Move to | Copy to | Flag | Watch | Copy | Find text | Encoding | Previous | Next

Delete | Respond | Actions | Navigate

URGENT: CID Cyber Crimes - Hyderabad - Request to furnish certain information [C.No.1312/CCPS/CID/2016/AVG/SP]

CYBERPS

To: Cellone; sdetecvig;

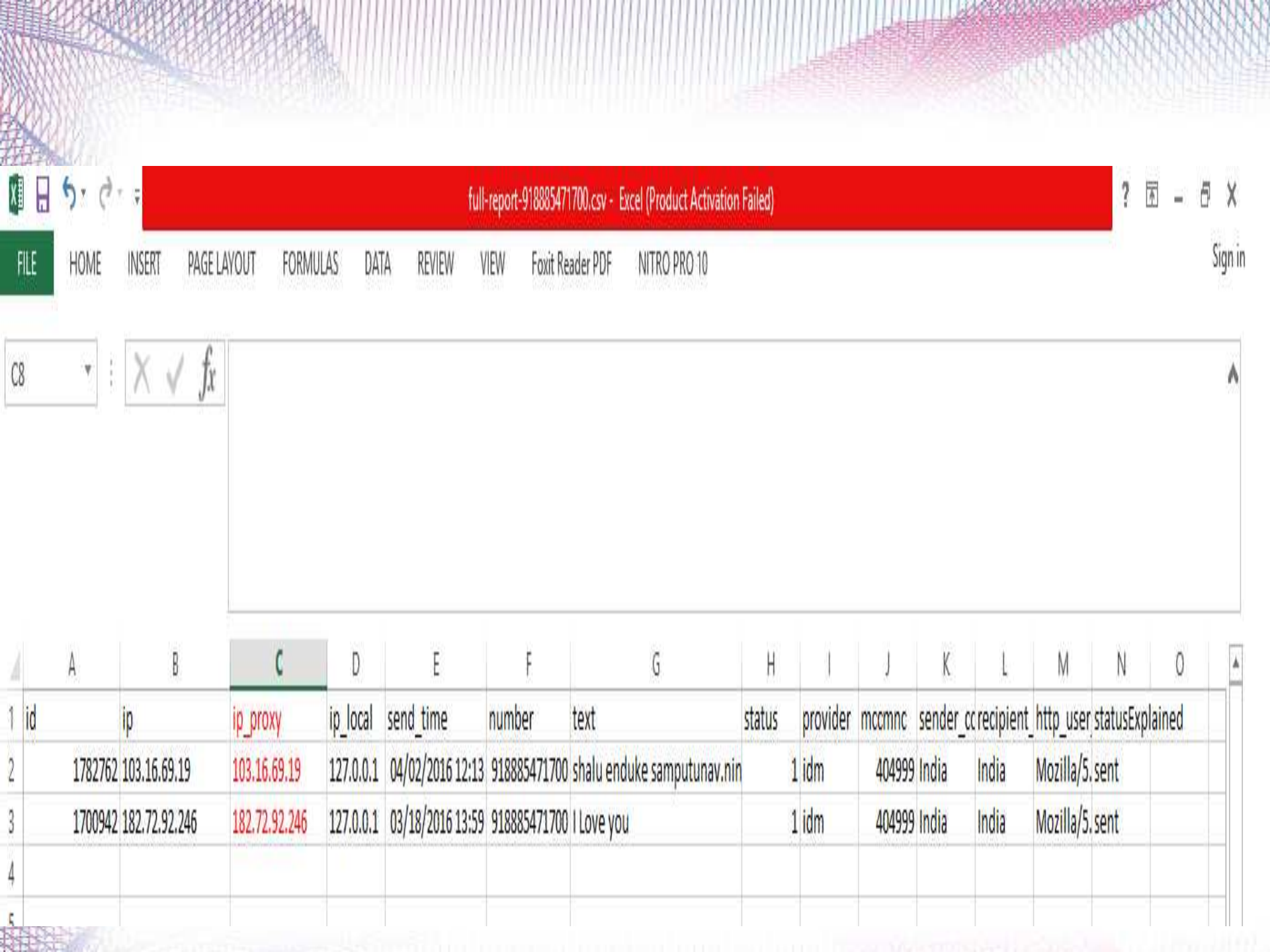
Sir,

It is requested to furnish the end-user particulars of the following IP Addresses belong to your network for the purpose of investigation.

IP ADDRESS	DATE	TIME
61.3.2.96	29-Mar-16	09:21:52
61.3.2.96	29-Mar-16	09:34:23
61.3.2.96	29-Mar-16	09:44:24
61.3.2.96	29-Mar-16	09:45:39
117.216.221.250	28-Mar-16	11:01:24
45.120.213.59	28-Mar-16	09:46:57
117.197.222.91	28-Mar-16	09:26:39
117.197.222.91	28-Mar-16	10:16:31
117.197.230.54	30-Mar-16	10:36:05
117.197.230.54	30-Mar-16	10:59:24
125.16.18.106	30-Mar-16	09:41:49
125.16.18.106	29-Mar-16	09:48:25

Early action will be highly appreciated.

Superintendentof Police,
Cyber Crimes, CID,
Hyderabad.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	id	ip	ip_proxy	ip_local	send_time	number	text	status	provider	mccmnc	sender_cc	recipient_	http_user_	statusExplained	
2	1782762	103.16.69.19	103.16.69.19	127.0.0.1	04/02/2016 12:13	918885471700	shalu enduke samputunav.nin	1	idm	404999	India	India	Mozilla/5.	sent	
3	1700942	182.72.92.246	182.72.92.246	127.0.0.1	03/18/2016 13:59	918885471700	I Love you	1	idm	404999	India	India	Mozilla/5.	sent	
4															
5															

Re: CDR Request from Crime Investigation Department - Cyber Crimes Hyderabad - Unicode (UTF-8)

File | Message

Junk | Delete | Reply | Reply all | Forward | Instant message | Add to calendar | Move to | Copy to | Flag | Watch | Copy | Find text | Encoding | Previous | Next

Delete | Respond | Actions | Navigate

Re: CDR Request from Crime Investigation Department - Cyber Crimes Hyderabad

Globfone Support Team (support@globfone.com) Add contact

05/23/2016 06:09 PM

To: CYBERPS;

Cc: support@globfone.com;

full-report-918885471700.csv

cyberps@cid.appolice.gov.in

Victim tel: +918885471700
Date of event: 2016-04-02

Case reason:
Dear Sir/Madam, we have received a case from a female victim stating that she had been getting threatening and abusive message from a stranger. During the course of investigation we found that those messages where having a name in header that is your domain/website name. Further it is requested that to disclose the details of the sender who had been sending the messages to the victim. The headers show DM_022655 (Globfone.com) which were received on april 02 2016.

--
This e-mail was sent from a CDR Request form on Globfone.com/CDR

--

Best regards
Globfone Support Team

09:19 AM

RE: CID - Cyber Crimes - Hyderabad - Request to furnish certain information [C.No.2209/2016/CCPS/SOM/CID/2016] - Unicode (UTF-8)

File Message

Junk Delete Reply Reply all Forward Instant message Add to calendar Move to Copy to Flag Watch Copy Find text Encoding Previous Next

Delete Respond Actions Navigate

RE: CID - Cyber Crimes - Hyderabad - Request to furnish certain information [C.No.2209/2016/CCPS/SOM/CID/2016]

Report Fraud 09/23/2016 05:06 PM

To: 'CYBERPS';

Cc: 'Anuj Shrivastava'; 'Shubham (Paytm Cybercell)'; 'Security';

PayU ID	Date	Merchant URL	Transaction ID	Transaction Fee	Payment Gateway	Status	Customer Phone	Customer IP Address	Card Number	Customer Emai
5876875793	22/09/2016 12:32:37	www.apna.csc.gov.in	PAYU20160922123236975253 9	15499.00	SBIPG	Transaction Successful	9999999999	223.231.40.202	504435XXXXXX8419	JH040500922@
5876885444	22/09/2016 12:46:14	www.apna.csc.gov.in	PAYU20160922124554536803 6	7499.00	SBIPG	Transaction Successful	9999999999	223.231.40.202	504435XXXXXX8419	JH040500922@

Please be advised that FRAUD e-mail ID have changed to reportfraud@payu.in. Request you to please don't send any fraud related email at disutes@payu.in or Payu-chargeback@payu.in.

Regards

Aakash Yadav

PayU fraud prevention team

reportfraud@payu.in | +91-9891297450 | Desk – 0124-6624-987, 820, 927

From: CYBERPS [mailto:cyberps@cid.appolice.gov.in]
Sent: 23 September 2016 13:11
To: Report Fraud <reportfraud@payu.in>; Gurpal Kumar <gurpal.kumar@payu.in>
Cc: Anuj Shrivastava <anuj.shrivastava@paytm.com>; Shubham (Paytm Cybercell) <cybercell@paytm.com>; Security <security@paytm.com>
Subject: CID - Cyber Crimes - Hyderabad - Request to furnish certain information [C.No.2209/2016/CCPS/SOM/CID/2016]

Dear sir,

It is to inform you that an enquiry vide reference cited above is being conducted by this agency wherein some unknown online fraudsters gained access to the confidential **STATE BANK OF HYDERABAD Debit card**

09:14 AM

Re: URGENT: CID - Cyber Crimes - Hyderabad - Request to furnish certain information (C.No.1028/CCPS/CID-LAVANYA/2016) - Unicode (UTF-8)

File | Message

Junk | Delete | Reply | Reply all | Forward | Instant message | Add to calendar | Move to | Copy to | Flag | Watch | Copy | Find text | Encoding | Previous | Next

Delete | Respond | Actions | Navigate

Re: URGENT: CID - Cyber Crimes - Hyderabad - Request to furnish certain information (C.No.1028/CCPS/CID-LAVANYA/2016)

Xvideos content

03/28/2016 04:40 PM

To: CYBERPS;

Hello,

The images are being deleted.
Please find below the information related to the users.

****

1/ http://www.xvideos.com/profiles/titu_mani/photos/267795/swapna_aunty

Email
titu_mani@yahoo.com

IP logs:
Date Type IP Proxy IP
March 28, 2016 6:33:15 AM UTC Login India 117.223.74.22 - ISP/Mobile ADSL Low traffic
March 28, 2016 6:03:59 AM UTC Login India 117.223.74.22 - ISP/Mobile ADSL Low traffic
March 28, 2016 4:57:26 AM UTC Login India 117.223.74.31 - ISP/Mobile ADSL Low traffic
March 27, 2016 1:36:45 PM UTC Upload India 117.223.72.142 - ISP/Mobile ADSL Low traffic
March 27, 2016 12:39:09 PM UTC Login India 117.223.72.142 - ISP/Mobile ADSL Low traffic
March 26, 2016 1:36:38 PM UTC Login India 117.223.73.89 - ISP/Mobile ADSL Low traffic
March 25, 2016 10:18:42 AM UTC Login India 117.223.73.91 - ISP/Mobile ADSL Low traffic
March 25, 2016 4:41:35 AM UTC Login India 117.223.73.113 - ISP/Mobile ADSL Low traffic
March 23, 2016 10:47:46 AM UTC Login India 117.223.72.181 - ISP/Mobile ADSL Low traffic
March 23, 2016 5:30:13 AM UTC Login India 117.223.73.214 - ISP/Mobile ADSL Low traffic
March 22, 2016 10:46:57 AM UTC Login India 117.223.73.204 - ISP/Mobile ADSL Low traffic
March 22, 2016 6:23:02 AM UTC Login India 117.223.73.204 - ISP/Mobile ADSL Low traffic

A	B	C	D	E	F
IP	DATE	TIME	user-id	mac-id	name
183.82.231.200	30-Jul-16	23:07:15	raghuramk111@gmail.com	ec:08:6b:ea:52:2d	K Gopi Krishna
183.82.231.200	31-Jul-16	8:24:20	raghuramk111@gmail.com	ec:08:6b:ea:52:2d	K Gopi Krishna
			raghuramk111@gmail.com	ec:08:6b:ea:52:2d	K Gopi Krishna
49.206.203.100	7-Aug-16	20:51:48	raghuramk111@gmail.com	ec:08:6b:ea:52:2d	K Gopi Krishna
49.206.203.100	7-Aug-16	21:51:08	raghuramk111@gmail.com	ec:08:6b:ea:52:2d	K Gopi Krishna
183.82.229.132	9-Aug-16	22:22:19	raghuramk111@gmail.com	ec:08:6b:ea:52:2d	K Gopi Krishna
183.82.229.132	9-Aug-16	23:04:22	raghuramk111@gmail.com	ec:08:6b:ea:52:2d	K Gopi Krishna

F	G	H
name	**address**	**mobile no**
K Gopi Krishna	Flat-201,I-block,Cp-srinivasa Heights,Hyderabad, Telangana, India	9963573272
K Gopi Krishna	Flat-201,I-block,Cp-srinivasa Heights,Hyderabad, Telangana, India	9963573272
K Gopi Krishna	Flat-201,I-block,Cp-srinivasa Heights,Hyderabad, Telangana, India	9963573272
K Gopi Krishna	Flat-201,I-block,Cp-srinivasa Heights,Hyderabad, Telangana, India	9963573272
K Gopi Krishna	Flat-201,I-block,Cp-srinivasa Heights,Hyderabad, Telangana, India	9963573272
K Gopi Krishna	Flat-201,I-block,Cp-srinivasa Heights,Hyderabad, Telangana, India	9963573272
K Gopi Krishna	Flat-201,I-block,Cp-srinivasa Heights,Hyderabad, Telangana, India	9963573272

Sec. 65B-Admissibility of Electronic Records

State (NCT of Delhi) Vs. Navjot Sandhu

(AIR 2005 SC 3820)

Electronic evidence can be made admissible by adducing secondary evidence under Section 63 & Section 65 of Evidence Act irrespective of compliance of Section 65B Evidence Act.

Overrule by the Supreme Court.

Sec. 65B-Admissibility of Electronic Records

Anvar P.V. Vs. P.K. Basheer and Others

The Supreme Court held:

Electronic Record can be produced in terms of Section 65B Evidence Act.

If no certificate under Section 65B, no oral evidence to prove the electronic record.

If there is a certificate under Section 65B, expert opinion can be rebutted under Section 45A of Evidence Act.

Section 65B being non-obstante clause shall prevail over general law.

Section 65B would prevail over Section 63/Section 65 of Evidence Act.

Overruled Navjot Sandhu Case to the extent of admissibility of electronic records.

Computer Print Outs

Admissible as per **Sec 65B EA**

- Banker Books :- *Require three certificate as per Sec 2A of Banker Books Of Evidence Act (**BBEA**)*

  A certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager.

  Authenticity certificate from person in-charge of computer system regarding:-

  Details of Computer System

  Process of Data Storage

  Safeguard to protect Computer System and Data

  such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question.

- The BBE Act being a special law will prevail over the Evidence Act which is a General law.

Admissibility of Hard Disk

Hon'ble Judge of Delhi High Court in the matter of Dharmabir Khattar Vs. CBI has held that :

A new Hard Disk is a storage device.

Once a blank hard disk is written it becomes a electronic record.

Even if the Hard Disk is formatted or wiped, it would contain Meta Data and as such it is a electronic record.

Through Forensic Software, it is possible to extract Meta Data and deleted data.

Section 65B Evidence Act would include:

Active accessible information – allocated data;

Data in subcutaneous memory – unallocated and unpartioned space.

Admissibility of Documents

SMS can be proved by:

SMS can be proved by:

Original mobile phone containing the SMS

Extracted copies of SMS along with Certificate ***U/s 65B Evidence Act****.*

Spoofed ***SMS*** is a challenge

Videos/Conferencing Admissibility

State of Maharashtra Vs. Dr. Praful B Desai (AIR 2003 SC 2053)

Amitabh Bagchi Vs. Ena Bagchi

(AIR 2005 Cal 11)

The presence of the witness does not mean actual physical presence.

There is no reason why the examination of a witness by video conferencing should not be an essential part of electronic evidence".

Email Admissibility

Require a Certificate U/s 65B of EA:

Server owned by the company

Data in e-mail clients

E-mail on Intermediary Server

Section 88A-Presumption as to Electronic Messages:

An electronic messages sent by the email

Message sent by the originator through email server is the same as received by the addressee.

Email Admissibility

ARK Shipping Co. Ltd. Vs. GRT Ship Management Pvt. Ltd. 2008(1)ARBLR317 (Bom)

"The high court while dealing with the admissibility of email accompanied by the affidavit of the witness as to the emails being the original reproduction of the content of the electronic record which are authored by him and exchange through the terminal used by him and as such admissible and is the sufficient compliance of section 65B of the evidence act".

Forged e-mail - - a challenge

Data in a Mobile

Syed Asifuddin & Ors. Vs. State of A.P [2005CriLJ4314]

A Cell Phone is a computer as envisaged under the IT Act.

Data in a CD/DVD

Mrs. Havovi Kersi Sethna Vs. Mr. Kersi Gustad Sethna [2011(3)BomCR100]

CD/DVD containing electronic records are copies and as such not admissible without certificate under Section 65B Evidence Act.

Forensics

Lab will analyze the storage media and provide opinion consisting of active data(saved by user in the system), deleted Data, unsaved data(emails, web access data), different log files and partial data.

Computer will have user generated data and system generated data.

User generated data requires more analysis for authentication where as system generated data doesn't require more authentication as user will not have control over the content.

1. What types of digital evidence have been collected? For example, in a cyber stalking case, is there a hard copy (printed) version of the e-mail? Is there an electronic copy? Does it contain full header information?

2. Who handled the evidence?

a. Document the name and job function of each individual who handled the digital evidence.

b. Identify everyone who had control of the digital evidence before it was seized.

3. How was the digital evidence collected and stored?

a. Identify any tools or methods used to collect the digital evidence.

b. Determine who had access to the digital evidence after it was collected

4. When was the evidence collected?
Document the date and time when the evidence was collected (including a reference to time zone if necessary).

Consider using a timeline to demonstrate the collection of evidence.

5. Where was the evidence when it was collected?

a. Geographical (e.g., 'In what room? On what desk?')

b. Hardware

1. What kind of machine/device held the digital evidence?
2. Who had access to the machine/device?
3. Who owned the machine/device?
4. Is a serial number present?
5. Was the machine/device a shared device?
6. Was information retrieved from a network?
7. Was information password-protected?
8. Who had access to password-protected information?

c. Offsite (e.g., servers – e- mail or remote – and web pages)

- **Use of Camera to capture and transmit images / video**
- **Transmission may be Point-to-Point (P2P), Wireless or through Internet**

CCTV Camera

DVR

LCD Monitor

- **Contains**
  - *Lenses*
  - *CMOS or CCD Chips*
- **Analog Vs Digital**
- **IP Camera Vs Wireless Camera**
- **Day/ Infrared Camera**
- **Manual or Auto Iris Camera**

Digital Video Recorder (DVR) is a Computer

- **Standalone / Embedded or PC Based**

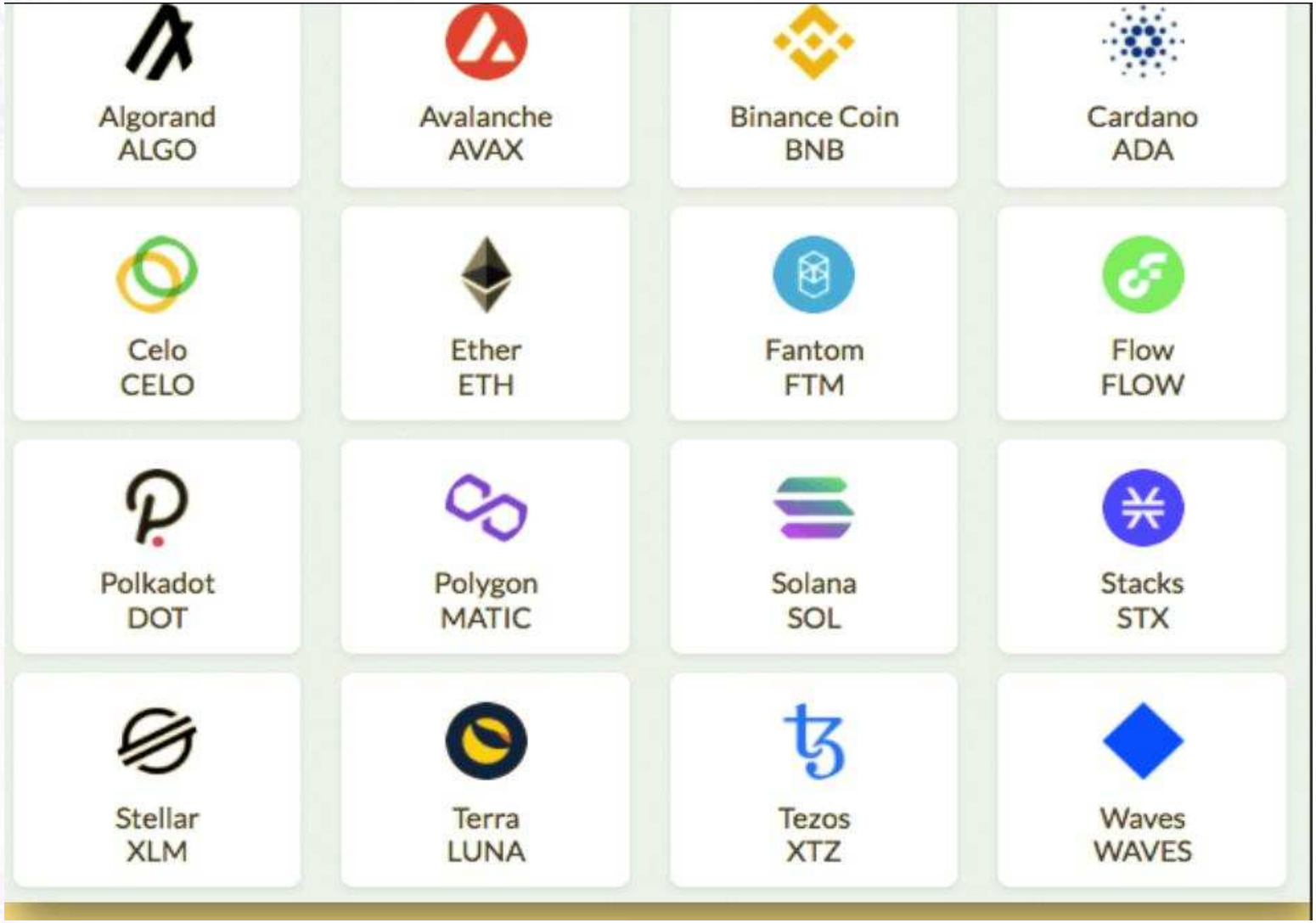
2. What Are Cryptos?

A Blockchain can have 1 or more “smart assets”. Calling these assets cryptocurrencies is not accurate because all blockchain smart assets do NOT work as currencies.

The Indian law calls them “virtual digital assets”. I prefer to simply call them “Cryptos”.

There are 9000+ Cryptos being actively traded in 450+ exchanges across 50,000+ market pairs.

Based on my analysis, Cryptos can be divided into 11 categories:


Algorand
ALGO
Avalanche
AVAX
Binance Coin
BNB
Cardano
ADA
Celo
CELO
Ether
ETH
Fantom
FTM
Flow
FLOW
Polkadot
DOT
Polygon
MATIC
Solana
SOL
Stacks
STX
Stellar
XLM
Terra
LUNA
Tezos
XTZ
Waves
WAVES

Mining- Minors

Miners validate new transactions and record them on the global ledger (blockchain).

Miners compete to solve a difficult mathematical problem based on a cryptographic hash algorithm.

The solution found is called the *Proof-Of-Work*. This proof proves that a miner did spend a lot of time and resources to solve the problem.

When a block is 'solved', the transactions contained are considered *confirmed*, and the crypto coin concerned in the transactions can be spend. So, if you receive some coin on your wallet, it will take approximately 10 minutes for your transaction to be confirmed as in case of bitcoin.

Miners receive a reward when they solve the complex mathematical problem.

There are two types of rewards: **new coins or transaction fees**.

The amount of coins created decreases every **n** number of blocks as defined in the protocol for the coin. This number will keep going down until no more coins will be issued

Miners can also receive rewards in the form of transaction fees. The winning miner can 'keep the change' on the block's transactions. As the amount of coins created with each block diminishes, the transactions fees received by the miner will increase. After no new coins are released, the winning miner will only receive transaction fees as his reward.

bitaddress

www.bitaddress.org is a JavaScript Client-Side Bitcoin Wallet Generator. It enables Bitcoin addresses and their corresponding private keys to be conveniently generated in a web browser.

Live site: https://www.bitaddress.org

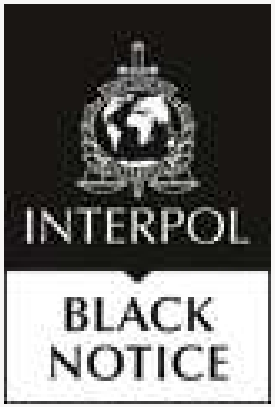
To generate a Bitcoin wallet (which is a Bitcoin address and its corresponding Bitcoin private key), simply move your mouse randomly on the bitaddress page.

Some of the features of Trust Wallet are:

- Buy Bitcoin in under 5 minutes.
- Easily earn interest on the crypto in your wallet.
- See your collectibles, art & non-fungible digital assets in one place.
- Exchange your crypto within the app.
- Track charts and prices within the wallet.

https://trustwallet.com

INTERPOL Notices

	**Red Notice** To seek the location and arrest of wanted persons with a view to extradition or similar lawful action. FORM		**Yellow Notice** To help locate missing persons, often minors, or to help identify persons who are unable to identify themselves.
	**Blue Notice** To collect additional information about a person's identity, location or activities in relation to a crime.		**Black Notice** To seek information on unidentified bodies.

	**Green Notice** To provide warnings and intelligence about persons who have committed criminal offences and are likely to repeat these crimes in other countries.		**Orange Notice** To warn of an event, a person, an object or a process representing a serious and imminent threat to public safety.
	**INTERPOL–United Nations Security Council Special Notice** Issued for groups and individuals who are the targets of UN Security Council Sanctions Committees.		**Purple Notice** To seek or provide information on modi operandi, objects, devices and concealment methods used by criminals.

Social Media Analysis

Social Media is being the most potential source for the cyber criminals to conduct any sort of crime (online harassment/ hacking/ phishing or cheating)

There is a challenge to trace these sophisticated cyber criminals as they grow with the evolving technology.

Further law enforcement cell(s) are being formed to help the local police to conduct their investigation with regards to the online crimes and investigations.

a. Automated AI Driven Collection Mechanism

i. Near Real Time Collection: from across networks for individual, group or topics

ii. Anonymous & Untraceable: ensuring security, latest updates & proactive intelligence

iii. Multiple Social Networks: enhancing ability to collect data across networks at once

iv. Volume of Data Collected: simultaneously for topics, individuals, and groups

v. Speed of Data Collection: across networks, social id's, groups, topics, and individuals.

vi. Private Accounts: collected with privacy compliance &referred as Inferred Data.

vii. Closed Groups: Semi Automated collection mechanism (3 Clicks)

viii. Ease of Use Interface: for investigators & analysts (basic computer operations)

ix. Security of Collection: maintained using End to End Encryption

x. Data Privacy Compliance: is maintained for the overall platform.

b. *Automated AI Based Analysis & In-depth Insights*

i. Relationships– Automatic 1st Level, 2nd Level, TNT& Hidden Connections

ii. Relationship Strengths – Automated showcase of closeness of individuals in a relationship

iii. Automated Discovery - Mediators, Top Connections, Identified & Ghosts

iv. Automated Analysis – Individual/s, Group, Across Groups and Topic/s

v. Fake Profiles, Propaganda Accounts& Bots – Single Click Identification

vi. Profile Insights – all details including automatic Collection of Likes & Comments

vii. Automated Impact Analysis of topics with auto identification of major Influencers & Contributors

viii. Automated Real Time Risk Assessment for millions of individuals at an instance

ix. Enhanced Profile Finder using only image, email id's, social idand/or phone numbers.

x. Analysis & Viewing of profile/s without Internet as well

xi. Visual Data Relationship Correlationwith Single Click Database &Watchlist creation

xii. Visual Data Acceptance from offline sources like Laptops, Phone, USB, CCTV, etc.

xiii. Offline to Online Visual Data Integration with Social Networks

xiv. Cross Topology Visual Images Correlation &Automated finding of Hidden Connections

Benefit:*Automated Precise AI Based In-depth Insights without need for manual intervention.*

c. Automated Detailed Reporting, Content Availability & Judicial Acceptability

i. Hash Value Generation& integrated for content

ii. Enhanced Reporting Functionality

iii. Automated Spotlight Reports

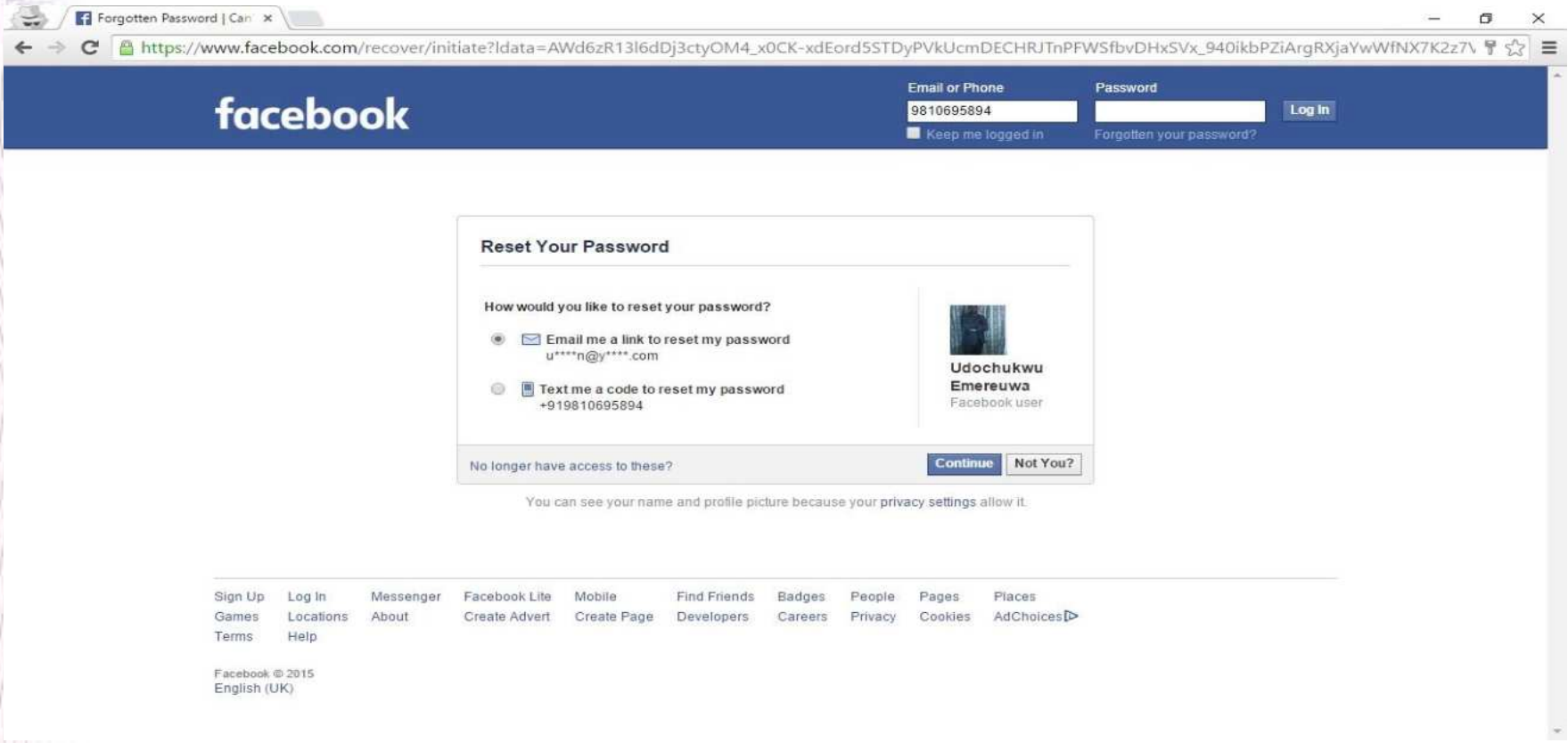
iv. Automated Alert Mechanism

v. Automated Download& Storage of Media &Content

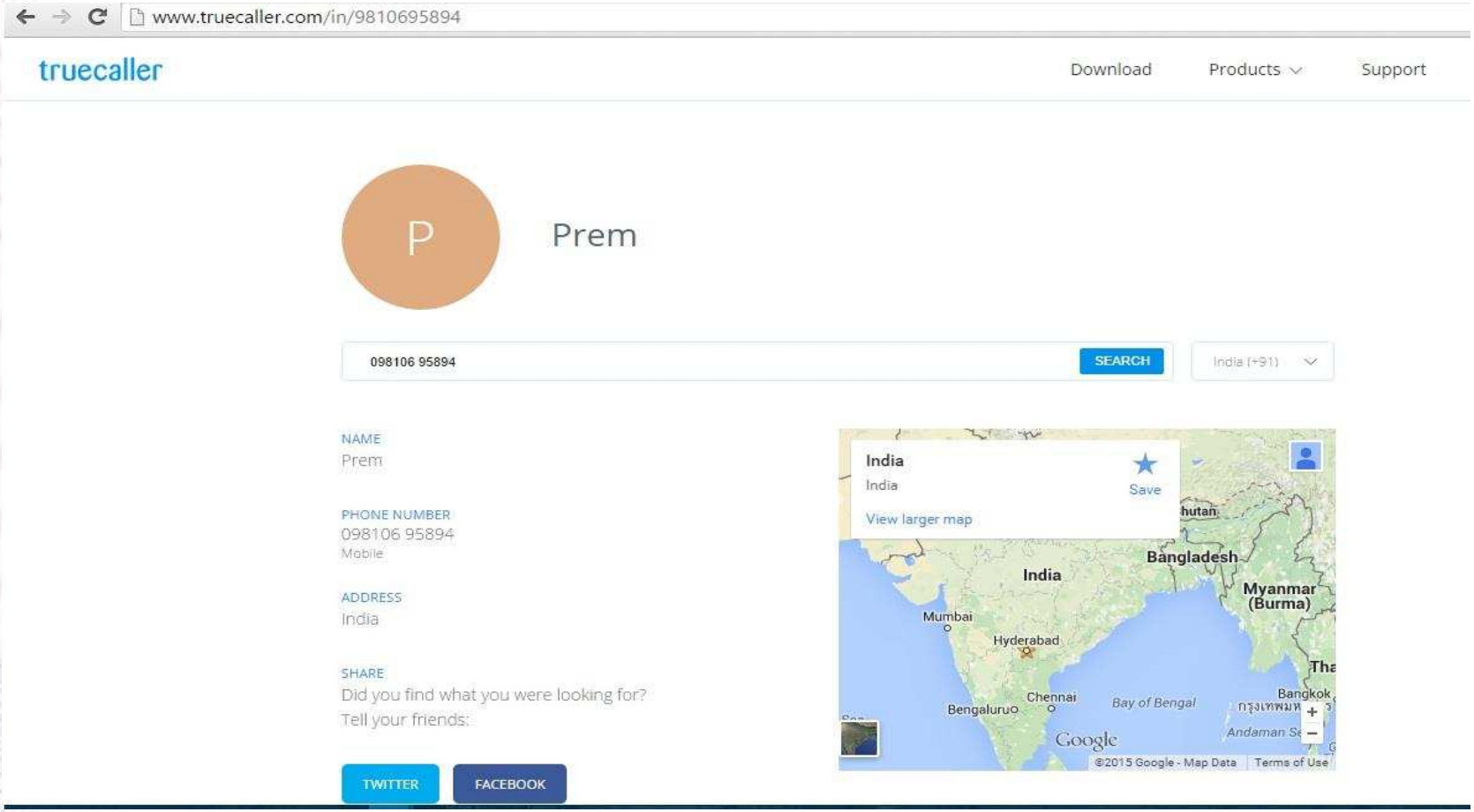
Benefit: *Legal Admissibility for Judicial Purposes*

Open Source Intelligence

SOS – Search Our Suspect



Truecaller - ID Search

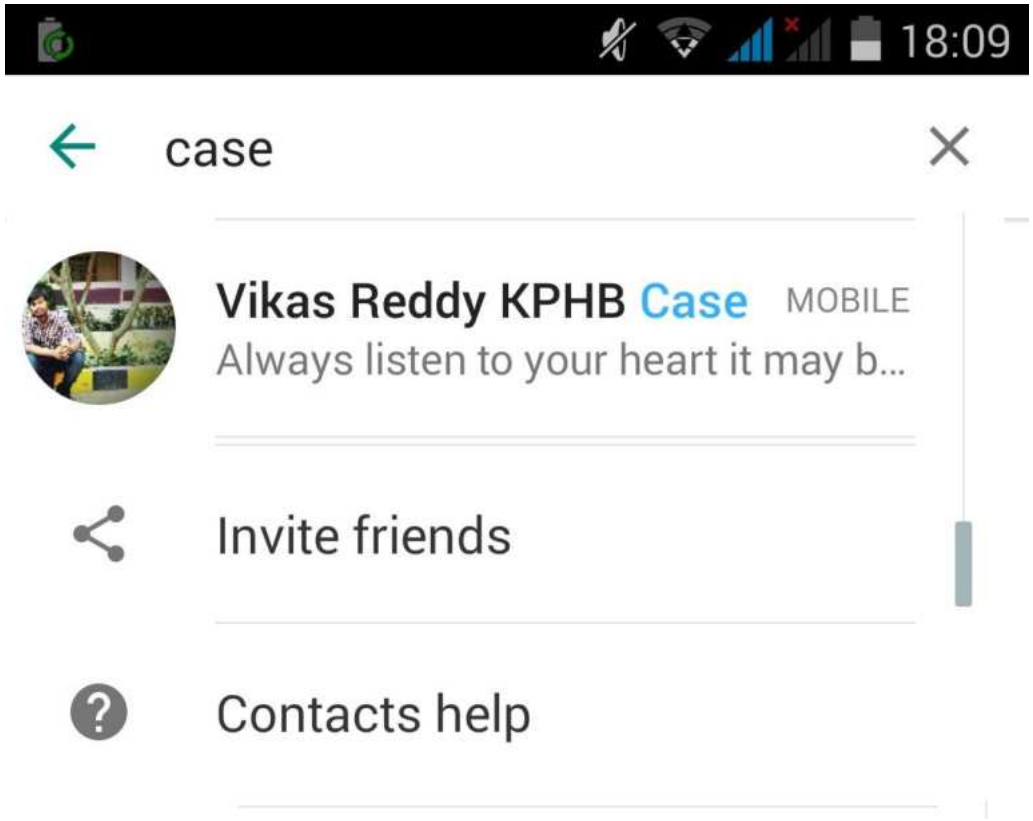


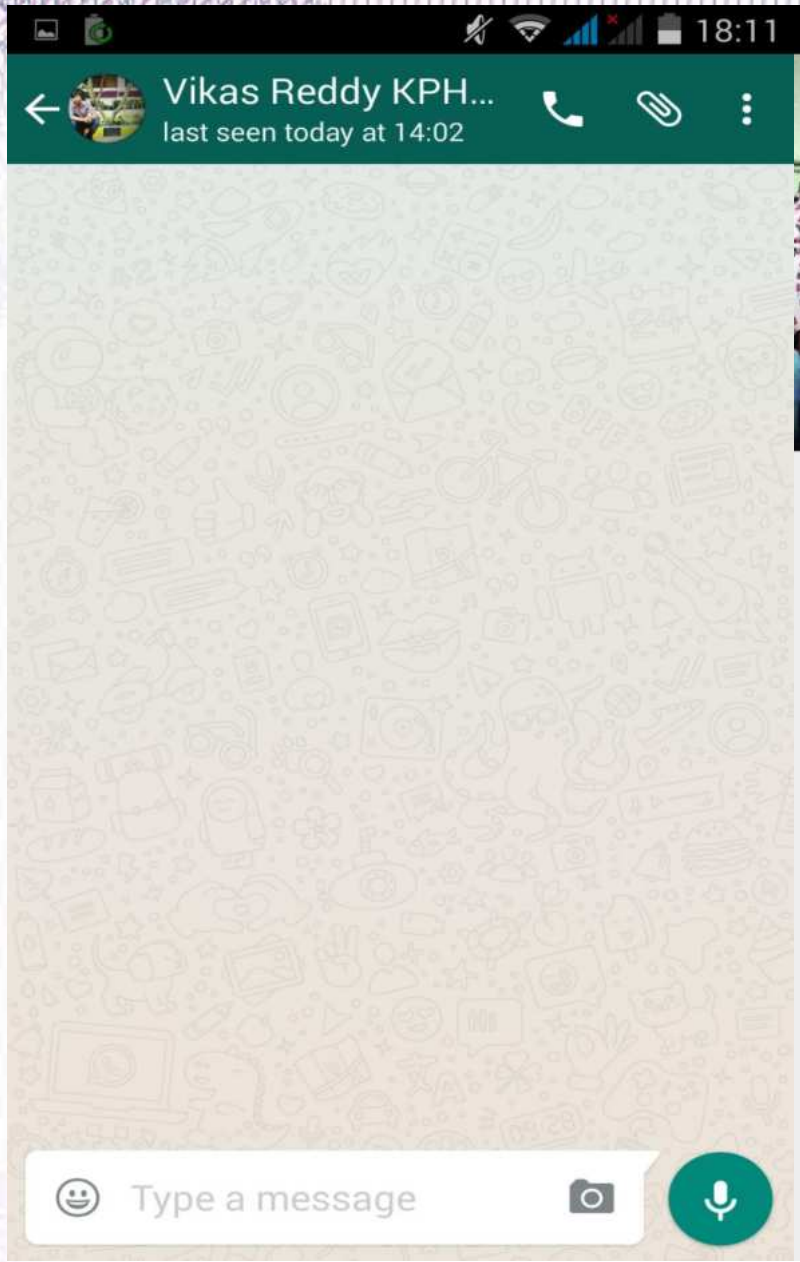
CEO- Election Commission Database Search

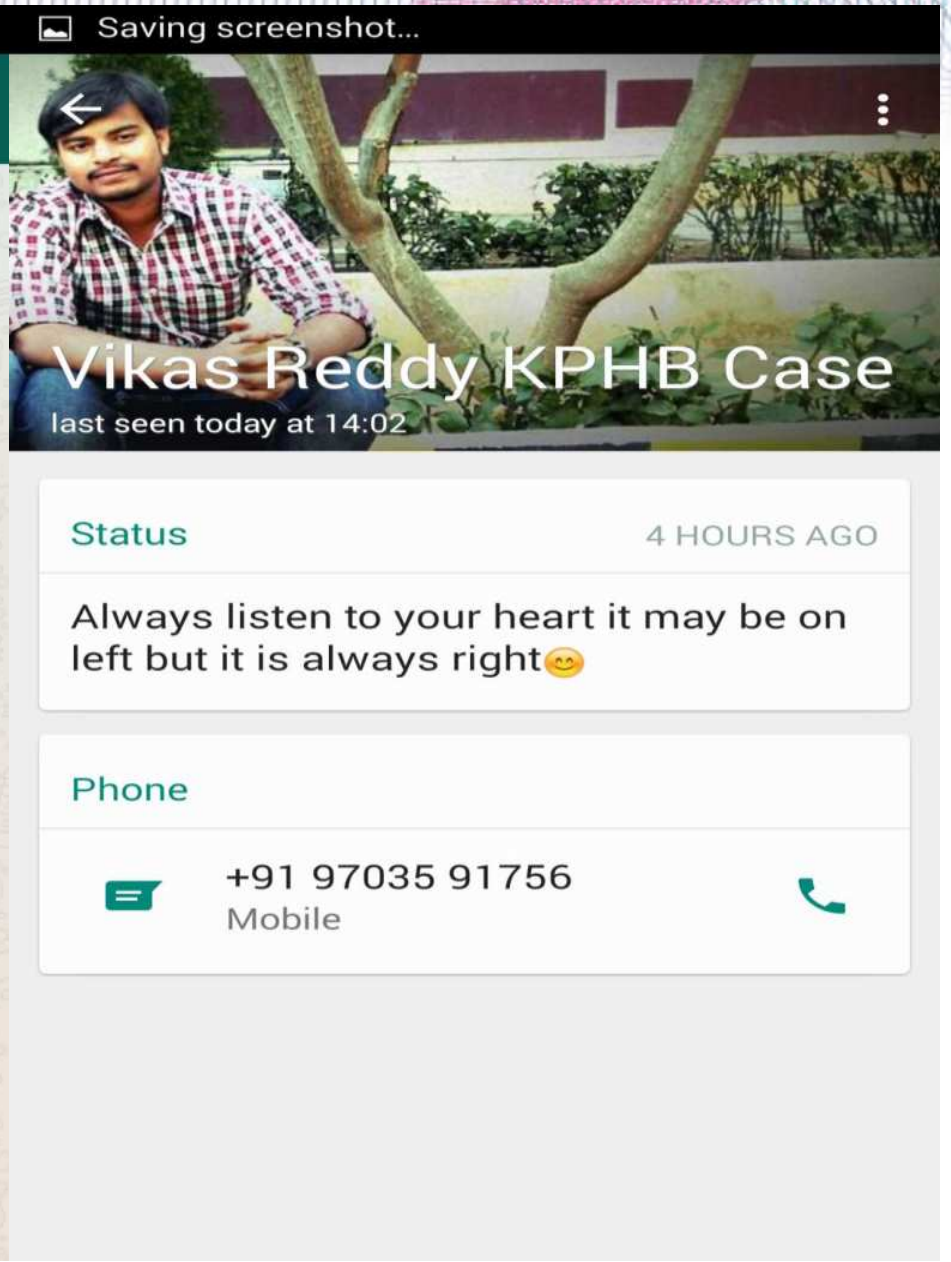
Name	Age	House Number	ID Card No.	Father/ Husband Name	Part Number & Polling station Location Name	Sl.No.in Part	Gender	
NAVEEN KUMAR MANDALOJU	37	11-4-322/20/35	CVG5619945	VEERA CHARY MANDALOJU	162-NETAJI HIGH SCHOOL	3	M	Print
KARNAKAR MANDALA	24	11-3-653	XDG0742644	KANAKAIAH MANDALA	76-Jai Bharath Seva Sangam, h.no. 11-3-604/398	16	M	Print
MANDALAPU CHANDRABABU	29	11-1-756/4	CVG1557503	M NAGAIAH	43-Chintabai Community Hall, P.No. 11-1-809/1	39	M	Print
CHANDRA BABU MANDALAPU	29	11-4-1/2/A	CVG3301033	NAGAIAH MANDALAPU	77-Municipal Ward Office,	50	M	Print
GEETHANJALI MANDALAPU	28	11-4-1/2/A	CVG3301132	NAGAIAH MANDALAPU	77-Municipal Ward Office,	51	F	Print
PRATYUSHA MANDALA	23	12-6-1100/21	XDG1050350	LATE VEERAIAH MANDALA	120-Railway Mixed High School,P.NO12-4-66,	75	F	Print
SURYA PRAKASH RAO MANDALIKA	74	12-7-295/A3	CVG5837067	SATYA NARAYANA MANDALIKA	126-MCH Community Hall, Mettuguda,	77	M	Print
NARSING RAO MANDALA	51	12-10-587/2/K/16	XDG0357939	PAPAIAH MANDALA	143-AMARAWATHI GARMMER SCHOOL, P.NO.12-10-587/88,	112	M	Print
JANA BAI MANDALOJU	58	11-4-322/20/35	XDG0932328	VEERA CHARY MANDALOJU	81-GOVTPRIMSCHFORGIRLS,NEWCONST SCHOOLBLD,DOOD BHAVI	133	F	Print

Property Tax Public Search

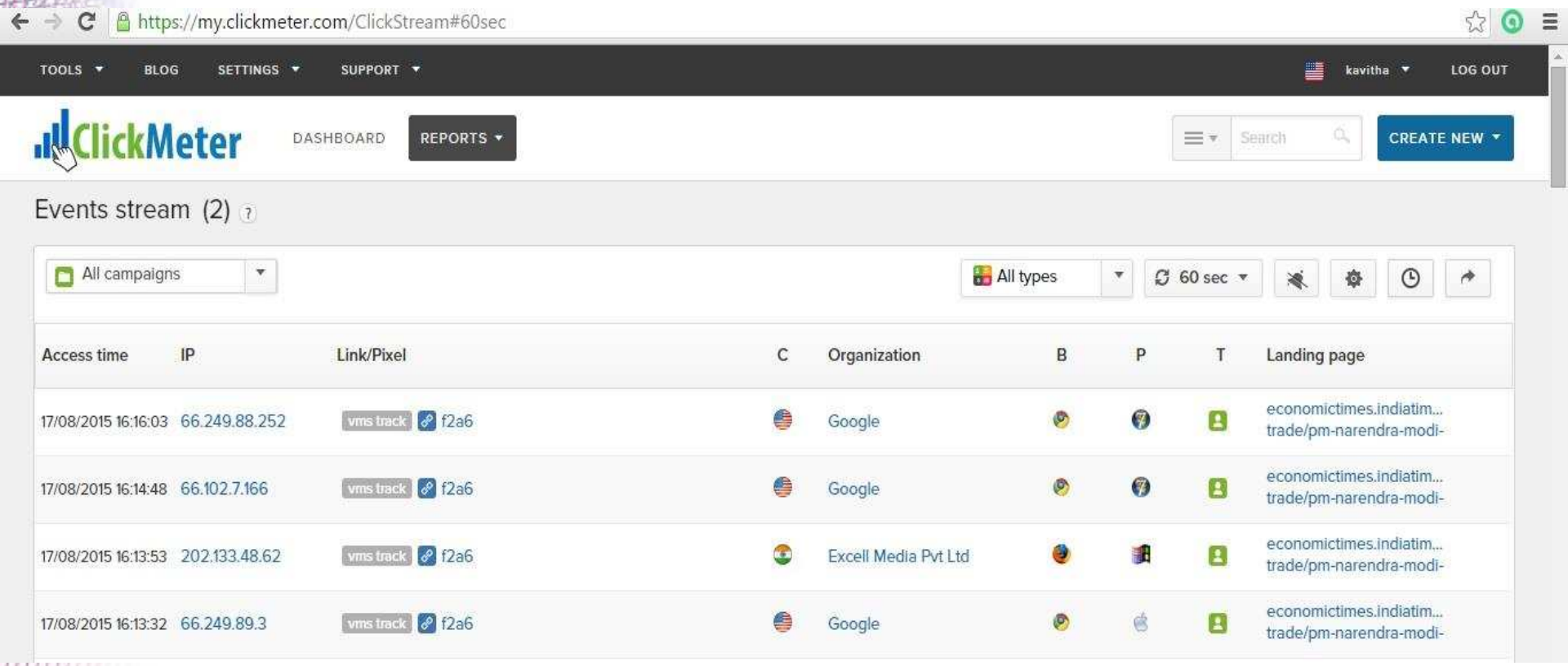
Whatsapp Search




18:11
Vikas Reddy KPH...
last seen today at 14:02
Type a message


Saving screenshot...
Vikas Reddy KPHB Case
last seen today at 14:02
Status
4 HOURS AGO
Always listen to your heart it may be on left but it is always right
Phone
+91 97035 91756
Mobile

Social Media Tracking



ClickMeter is one such method of grabbing the user IP address / Browser Details and Operating System Type.

Social Media Tracking

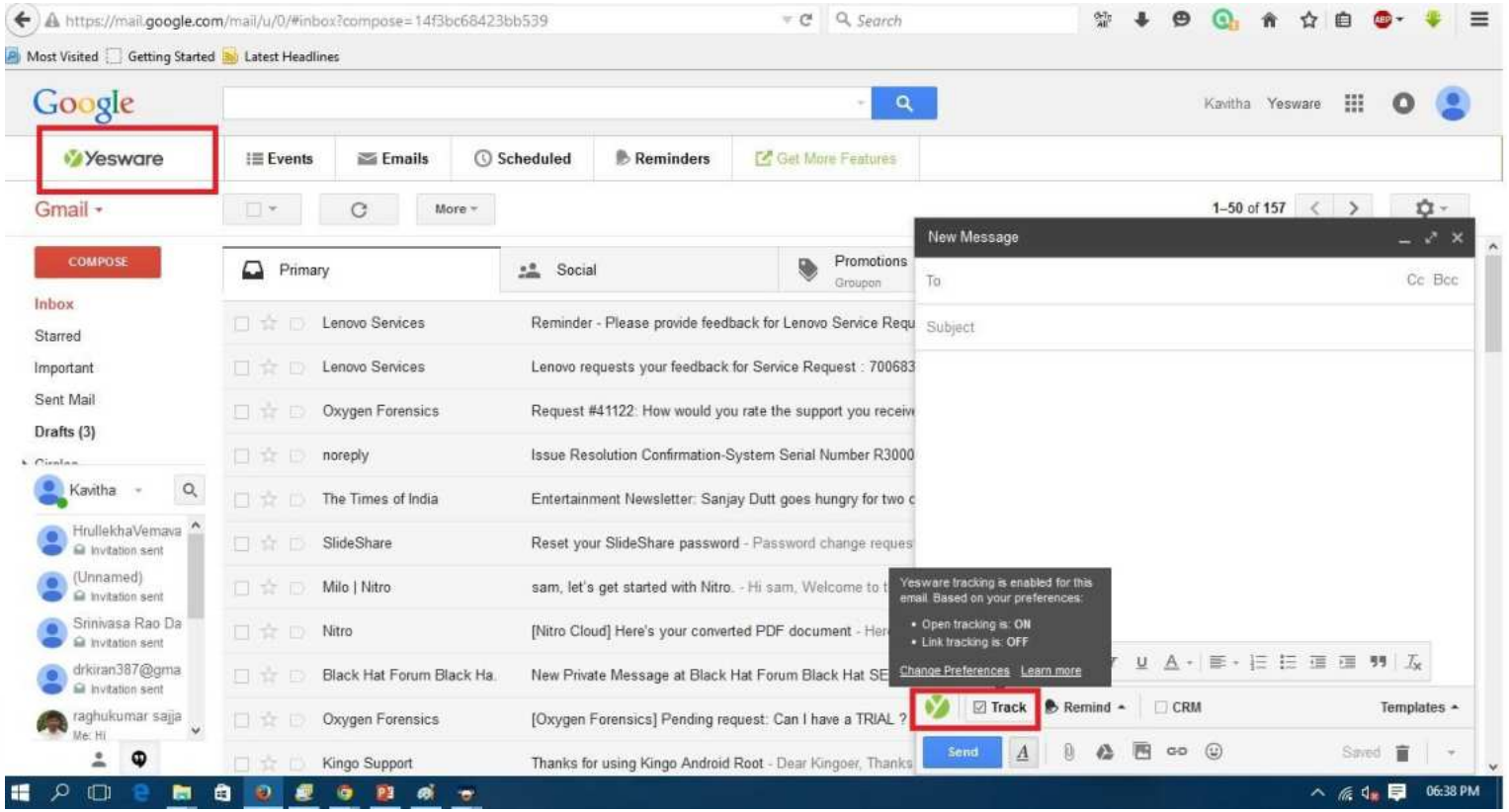
GPS Location tracking through Website(s)

Email Tracking

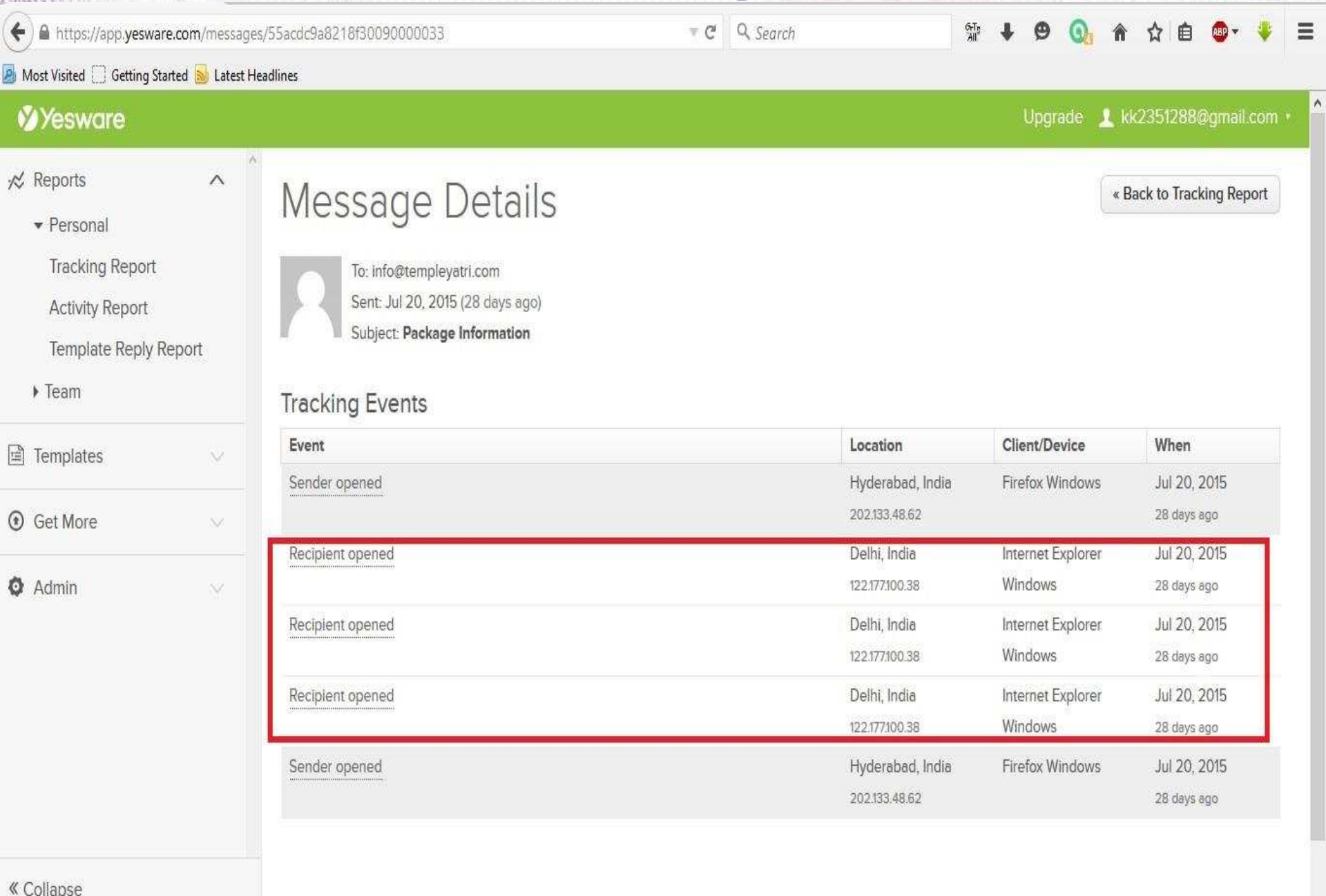
Email tracking is the most efficient method of tracking the offenders back.

The method involves tracking of email via a tracker sent though email. This tracker could tack the IP address/system information of the user who open(s) it.
The other method is gaining access to the target(offender) computer via attachment.

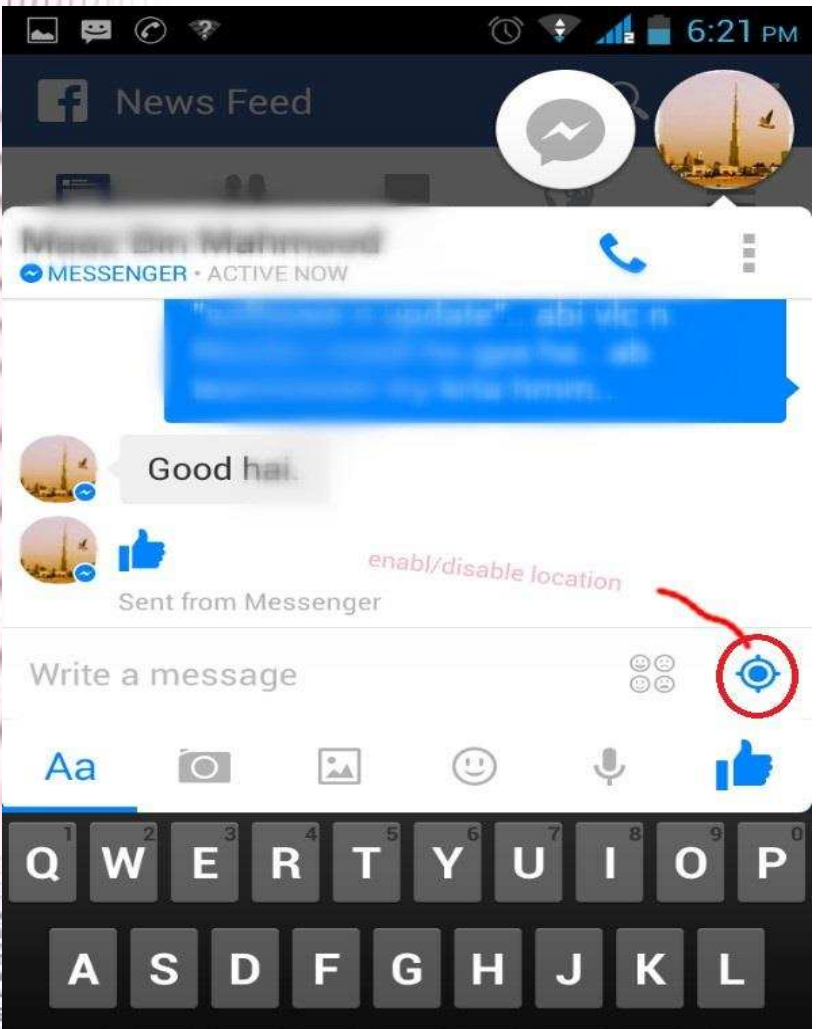
Email Tracking - Yesware

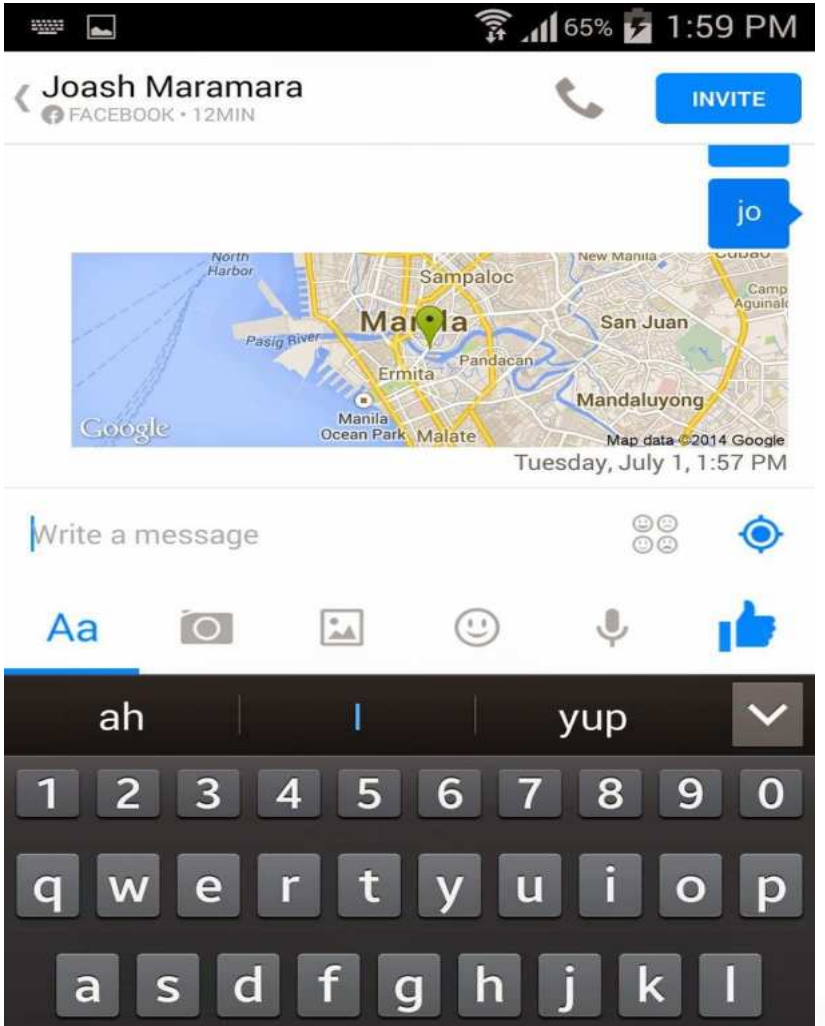


Email Tracking - Yesware

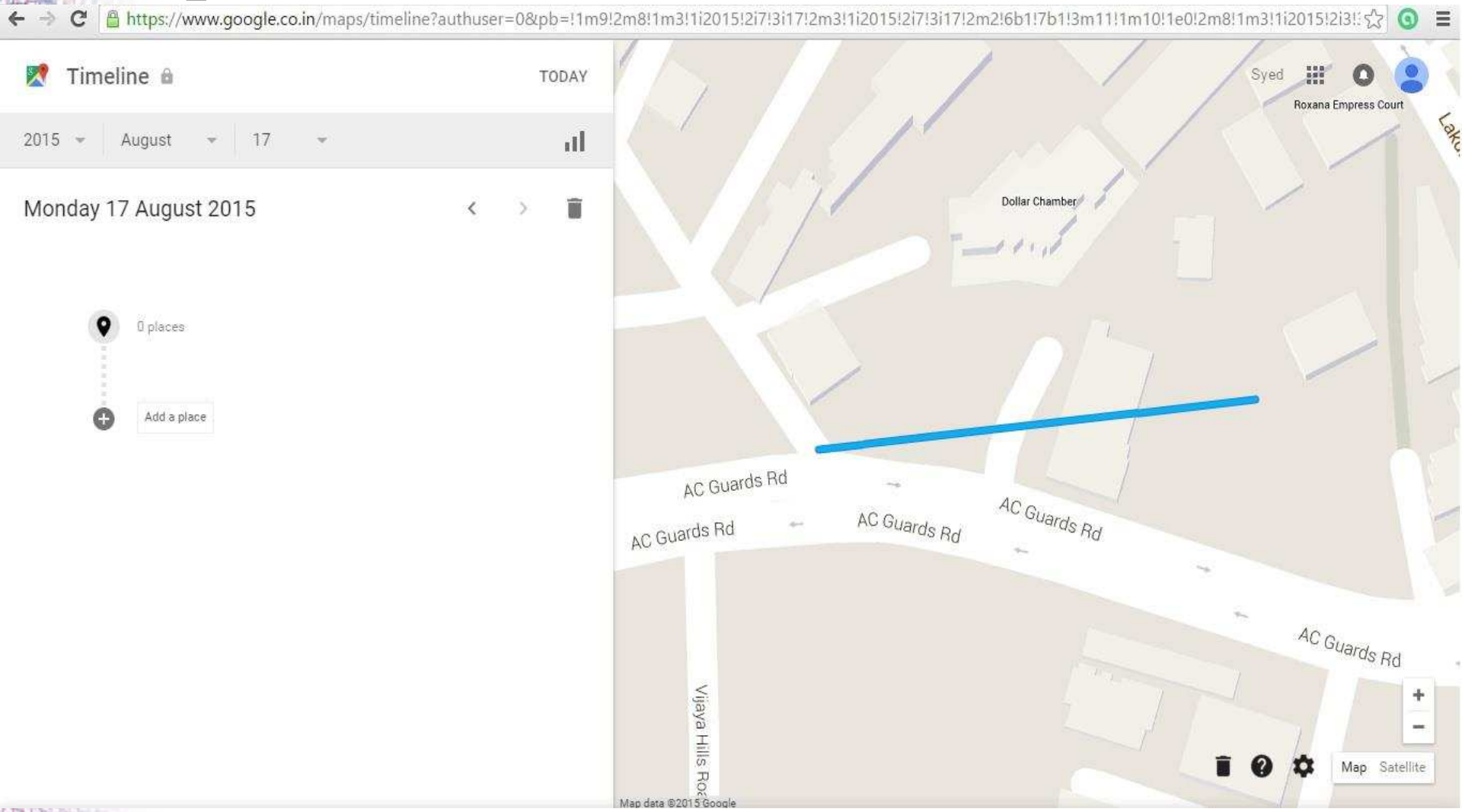


Facebook GPS secret : If your GPS is Turned ON then Facebook chat can track your GPS Location.





Google GPS Track : Your Google account keeps an EYE on YOU!!



Payment GATEWAY(s)

Gateway: A **payment gateway** is an e-commerce application service provider service that authorizes credit card **payments** for e-businesses, online retailers, bricks and clicks, or traditional brick and mortar. It is the equivalent of a physical point of sale terminal located in most retail outlets.

Most of the times we request the logs relating to the debit/credit card. But when we look/seek entire logs for the user/wallet then ??

Payment GATEWAY(s)
Oxigen Wallet

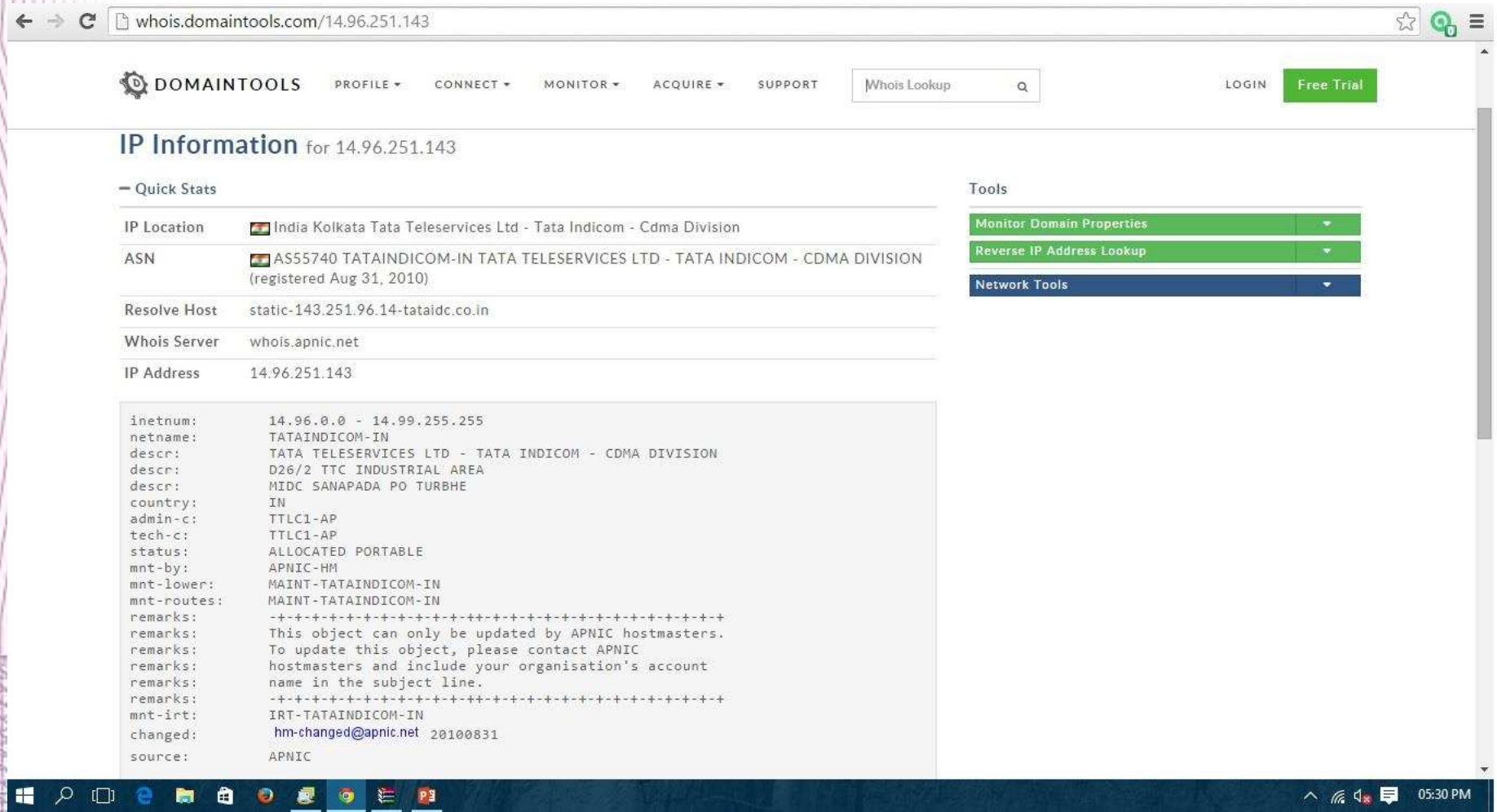
DNS LOOKUP

DNS - hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.

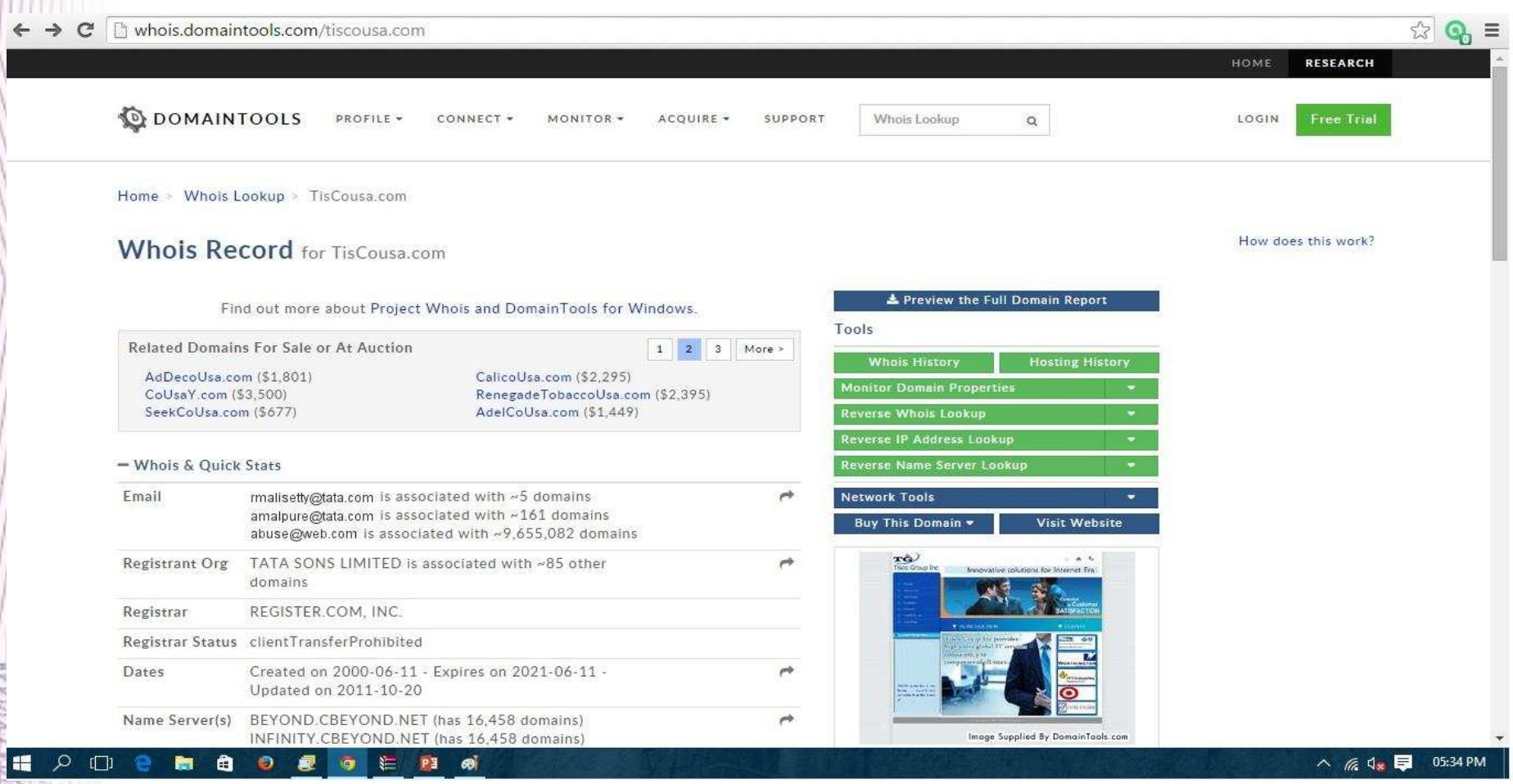
The Process help in identifying:

- Server IP address
- Service based area(USA,INDIA)
- Other Domains associated with IP

WHOIS LOOKUP- IP Based



WHOIS LOOKUP- Domain Name Based

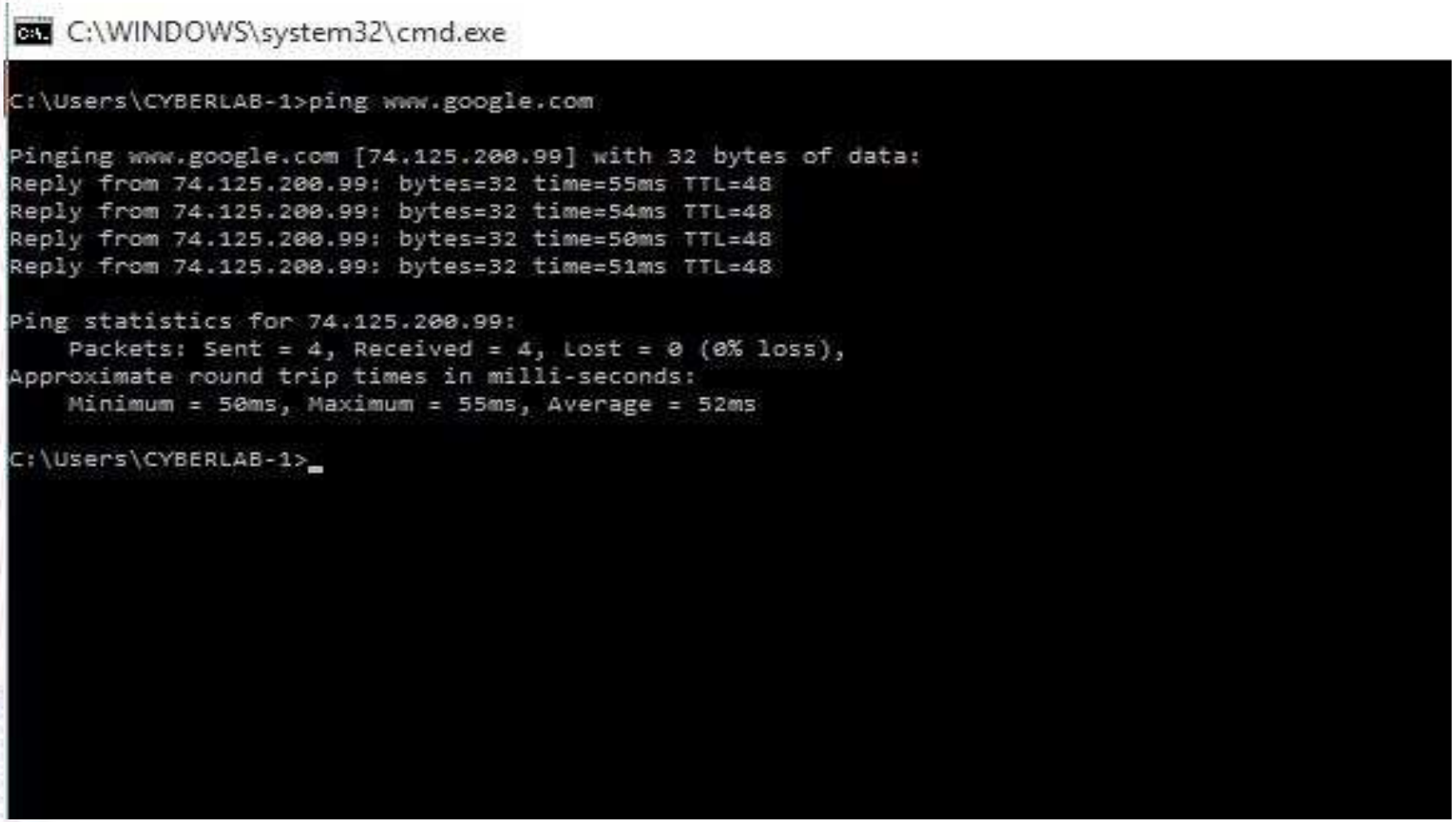


PING – Identify IP address of the Service

PING : Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol network and to measure the round-trip time for messages sent from the originating host to a destination computer and back.

Open command prompt and type the domain name: ping www.google.com

PING – Identify IP address of the Service



Who is your MSP?
(Mobile Service Provider)

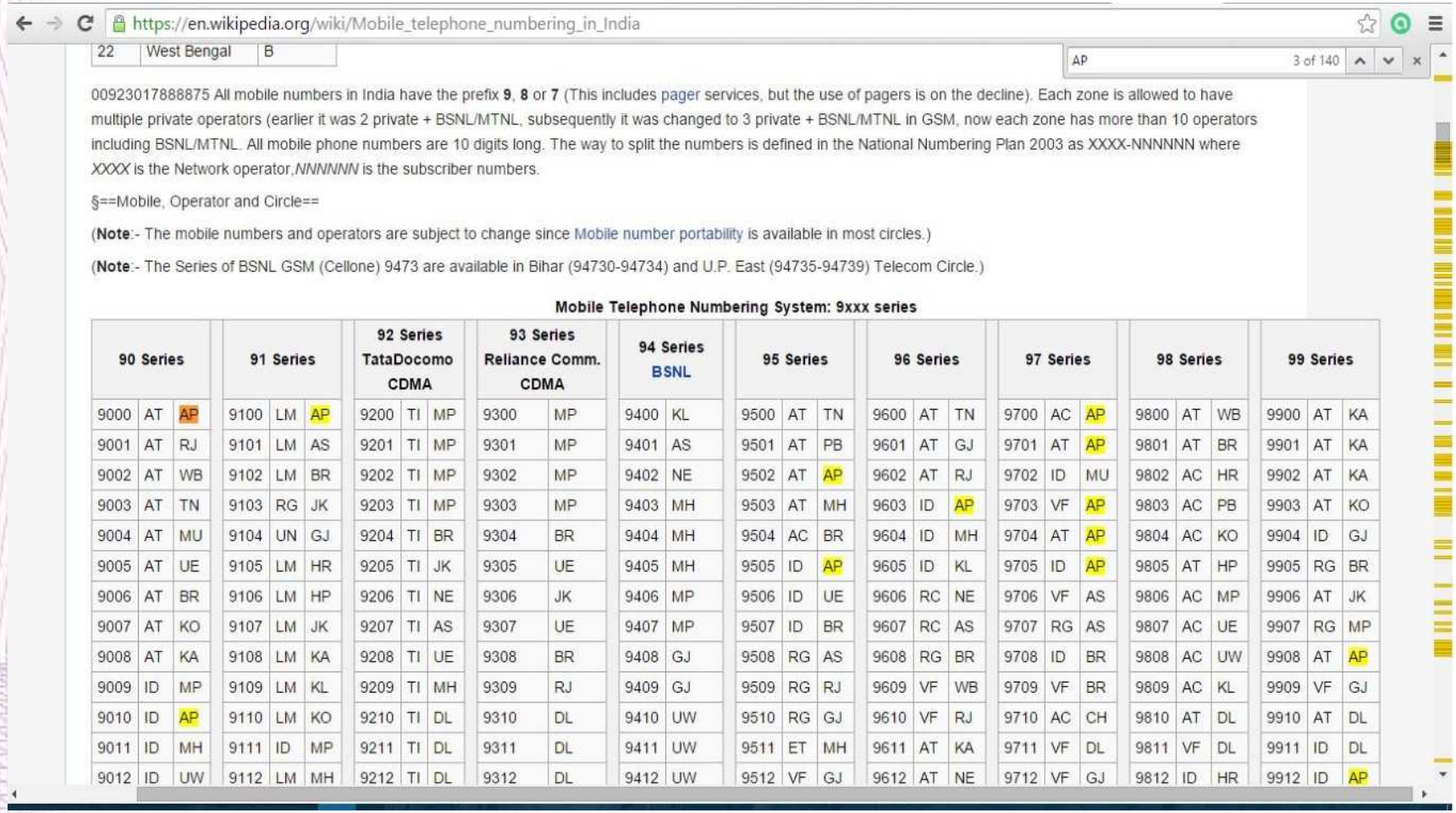
- To find out the Service Provider of any phone number. Visit the link:

http://en.wikipedia.org/wiki/Mobile_telephone_numbering_in_India

- Install this software on your computer system as well as mobile phones based on android and Java

http://www.shaplus.com/mobile/

Mobile Service Provider



https://en.wikipedia.org/wiki/Mobile_telephone_numbering_in_India

22	West Bengal	B

AP 3 of 140

00923017888875 All mobile numbers in India have the prefix **9**, **8** or **7** (This includes pager services, but the use of pagers is on the decline). Each zone is allowed to have multiple private operators (earlier it was 2 private + BSNL/MTNL, subsequently it was changed to 3 private + BSNL/MTNL in GSM, now each zone has more than 10 operators including BSNL/MTNL. All mobile phone numbers are 10 digits long. The way to split the numbers is defined in the National Numbering Plan 2003 as XXXX-NNNNNN where *XXXX* is the Network operator,*NNNNNN* is the subscriber numbers.

§==Mobile, Operator and Circle==

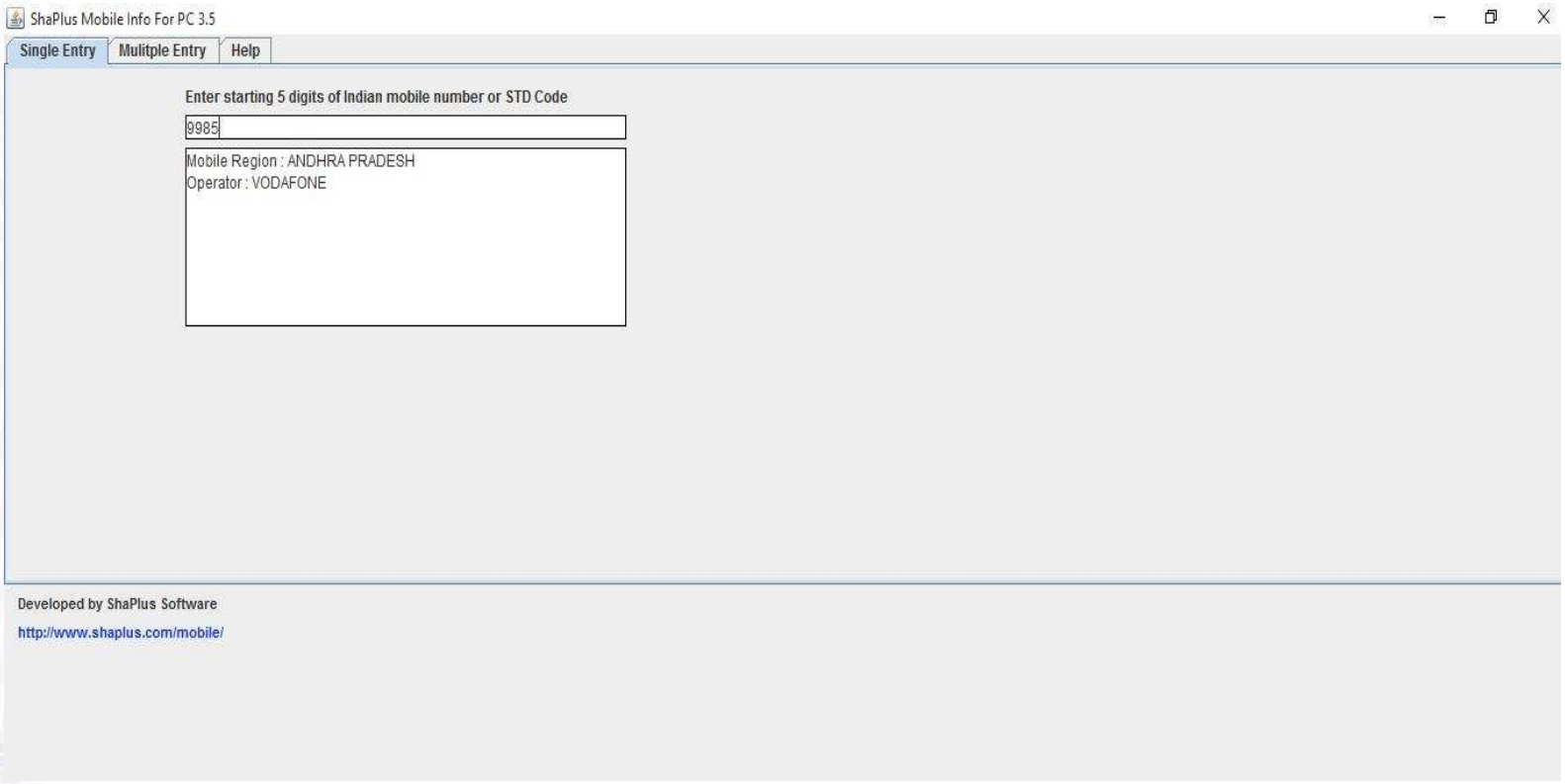
(**Note**:- The mobile numbers and operators are subject to change since Mobile number portability is available in most circles.)

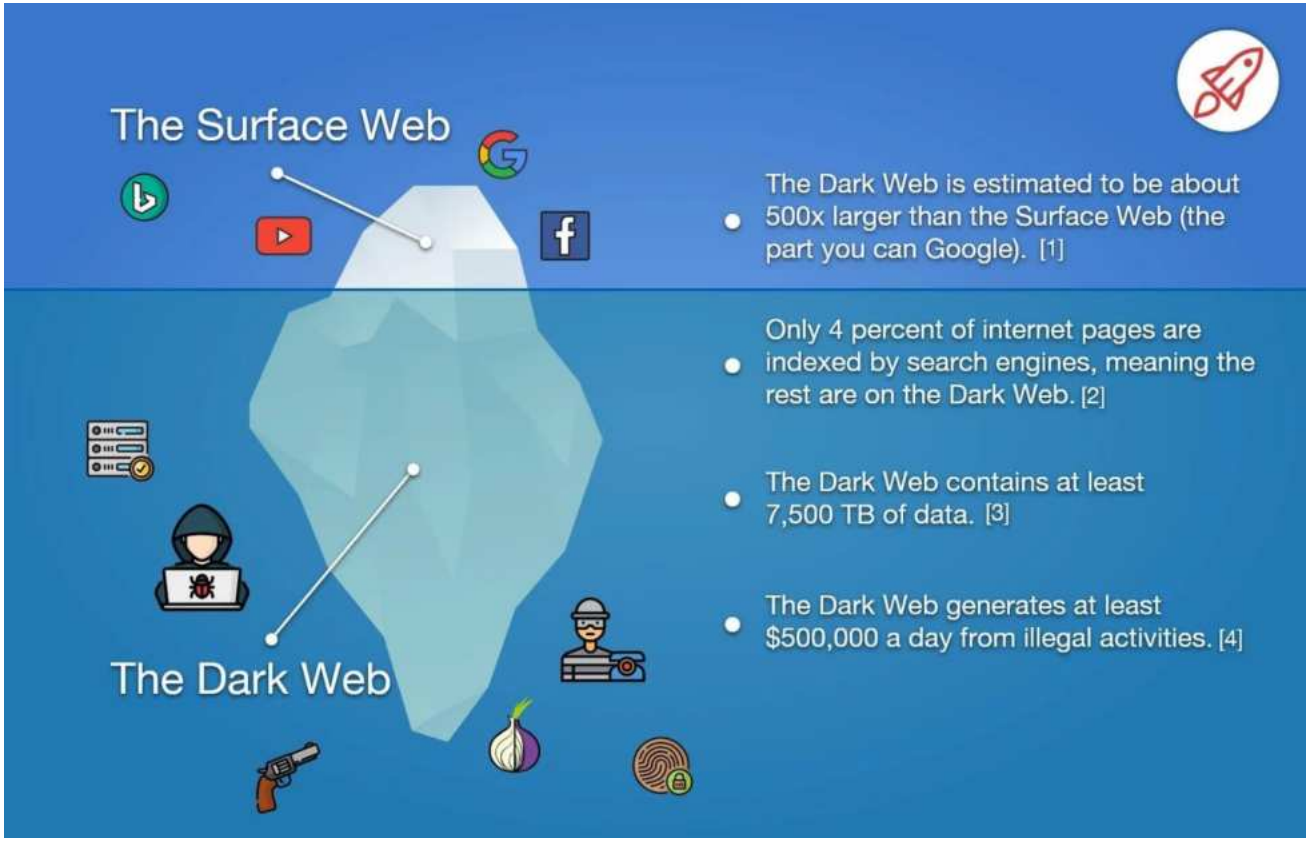
(**Note**:- The Series of BSNL GSM (Cellone) 9473 are available in Bihar (94730-94734) and U.P. East (94735-94739) Telecom Circle.)

Mobile Telephone Numbering System: 9xxx series

90 Series			91 Series			92 Series TataDocomo CDMA			93 Series Reliance Comm. CDMA		94 Series BSNL			95 Series			96 Series			97 Series			98 Series			99 Series		
9000	AT	AP	9100	LM	AP	9200	TI	MP	9300	MP	9400	KL		9500	AT	TN	9600	AT	TN	9700	AC	AP	9800	AT	WB	9900	AT	KA
9001	AT	RJ	9101	LM	AS	9201	TI	MP	9301	MP	9401	AS		9501	AT	PB	9601	AT	GJ	9701	AT	AP	9801	AT	BR	9901	AT	KA
9002	AT	WB	9102	LM	BR	9202	TI	MP	9302	MP	9402	NE		9502	AT	AP	9602	AT	RJ	9702	ID	MU	9802	AC	HR	9902	AT	KA
9003	AT	TN	9103	RG	JK	9203	TI	MP	9303	MP	9403	MH		9503	AT	MH	9603	ID	AP	9703	VF	AP	9803	AC	PB	9903	AT	KO
9004	AT	MU	9104	UN	GJ	9204	TI	BR	9304	BR	9404	MH		9504	AC	BR	9604	ID	MH	9704	AT	AP	9804	AC	KO	9904	ID	GJ
9005	AT	UE	9105	LM	HR	9205	TI	JK	9305	UE	9405	MH		9505	ID	AP	9605	ID	KL	9705	ID	AP	9805	AT	HP	9905	RG	BR
9006	AT	BR	9106	LM	HP	9206	TI	NE	9306	JK	9406	MP		9506	ID	UE	9606	RC	NE	9706	VF	AS	9806	AC	MP	9906	AT	JK
9007	AT	KO	9107	LM	JK	9207	TI	AS	9307	UE	9407	MP		9507	ID	BR	9607	RC	AS	9707	RG	AS	9807	AC	UE	9907	RG	MP
9008	AT	KA	9108	LM	KA	9208	TI	UE	9308	BR	9408	GJ		9508	RG	AS	9608	RG	BR	9708	ID	BR	9808	AC	UW	9908	AT	AP
9009	ID	MP	9109	LM	KL	9209	TI	MH	9309	RJ	9409	GJ		9509	RG	RJ	9609	VF	WB	9709	VF	BR	9809	AC	KL	9909	VF	GJ
9010	ID	AP	9110	LM	KO	9210	TI	DL	9310	DL	9410	UW		9510	RG	GJ	9610	VF	RJ	9710	AC	CH	9810	AT	DL	9910	AT	DL
9011	ID	MH	9111	ID	MP	9211	TI	DL	9311	DL	9411	UW		9511	ET	MH	9611	AT	KA	9711	VF	DL	9811	VF	DL	9911	ID	DL
9012	ID	UW	9112	LM	MH	9212	TI	DL	9312	DL	9412	UW		9512	VF	GJ	9612	AT	NE	9712	VF	GJ	9812	ID	HR	9912	ID	AP

Mobile Service Provider




The Surface Web
The Dark Web
The Dark Web is estimated to be about 500x larger than the Surface Web (the part you can Google). [1]
Only 4 percent of internet pages are indexed by search engines, meaning the rest are on the Dark Web. [2]
The Dark Web contains at least 7,500 TB of data. [3]
The Dark Web generates at least $500,000 a day from illegal activities. [4]

5 BEST ANONYMOUS BROWSERS

1] TOR

2] IRON

3] BRAVE

4] WATER FOX

5] COMODO DRAGON

Do you often charge your mobile device from public ports while travelling? Did you know this can lead to "**Juice Jacking**" ?

Beware of Juice Jacking

Attackers use USB charging ports available at public places to install malware, steal data or even take complete control of your device.

Tips to stay safe

- Disable data transfer feature on your mobile phone while charging
- Get a charge only cable instead of cable supporting charging and data transfer capabilities
- Try to carry a power bank
- If possible, switch off the device while charging from public ports


7mm
9mm
9mm


WiFi


Camera
1080p 3.0MP FHD video

WHAT DO YOUR DEVICES KNOW ABOUT YOU?

Whether it's a computer on your desk or a phone in your pocket, your devices retain a lot of personal data. And all of that information may be vulnerable to cybercriminals.

WINDOWS PCs | MACS | ANDROID TABLETS | SMART PHONES

Passwords
- Web browser autofill
- Stored in the file system

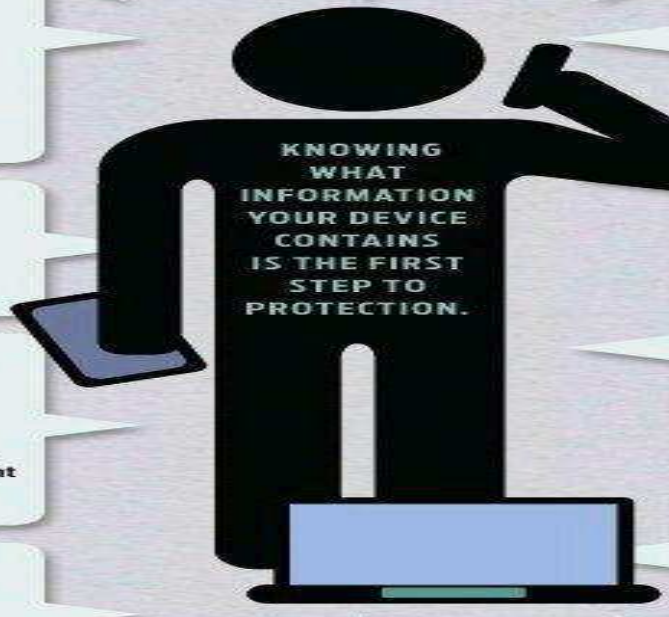
Credit Card Numbers
- Web browser autofill
- Downloaded credit card statements

Social Security Number
- Downloaded tax documents

Deleted Files
- All deleted files, including ones no longer in recycle bin or trash, can be recovered until physical storage space overwritten.

Text Messages
- Text log stored on phone

Phone Calls
- Call log stored on phone



Bank Account Info
- Downloaded bank statements

Name and Address
- Web browser autofill
- Windows Contacts
- Address Book
- Contact manager

Recent Files
- List kept by operating system
- Various applications keep their own recent file lists

Recently Visited Sites
- Browser's cache
- Browser's history
- Cookies

Contacts
- Windows Contacts
- Address Book
- Contact manager

Current Location
- Readable off your GPS

Recent Locations
- Photos
- Navigation apps

CYBER CRIME STATISTICS

Average monetary cost to victim of cyber crime:

Email scams sent daily:

75 MILLION

Daily victims of scam emails:

2,000

Percent of Americans who have experienced cyber crime:

73%

Percentage of Americans who believe that cyber-criminals will not be brought to justice:

78%

Percentage of Americans who expect to escape cyber crime in their lifetime:

2%

SOURCE: CYBER CRIME WATCH