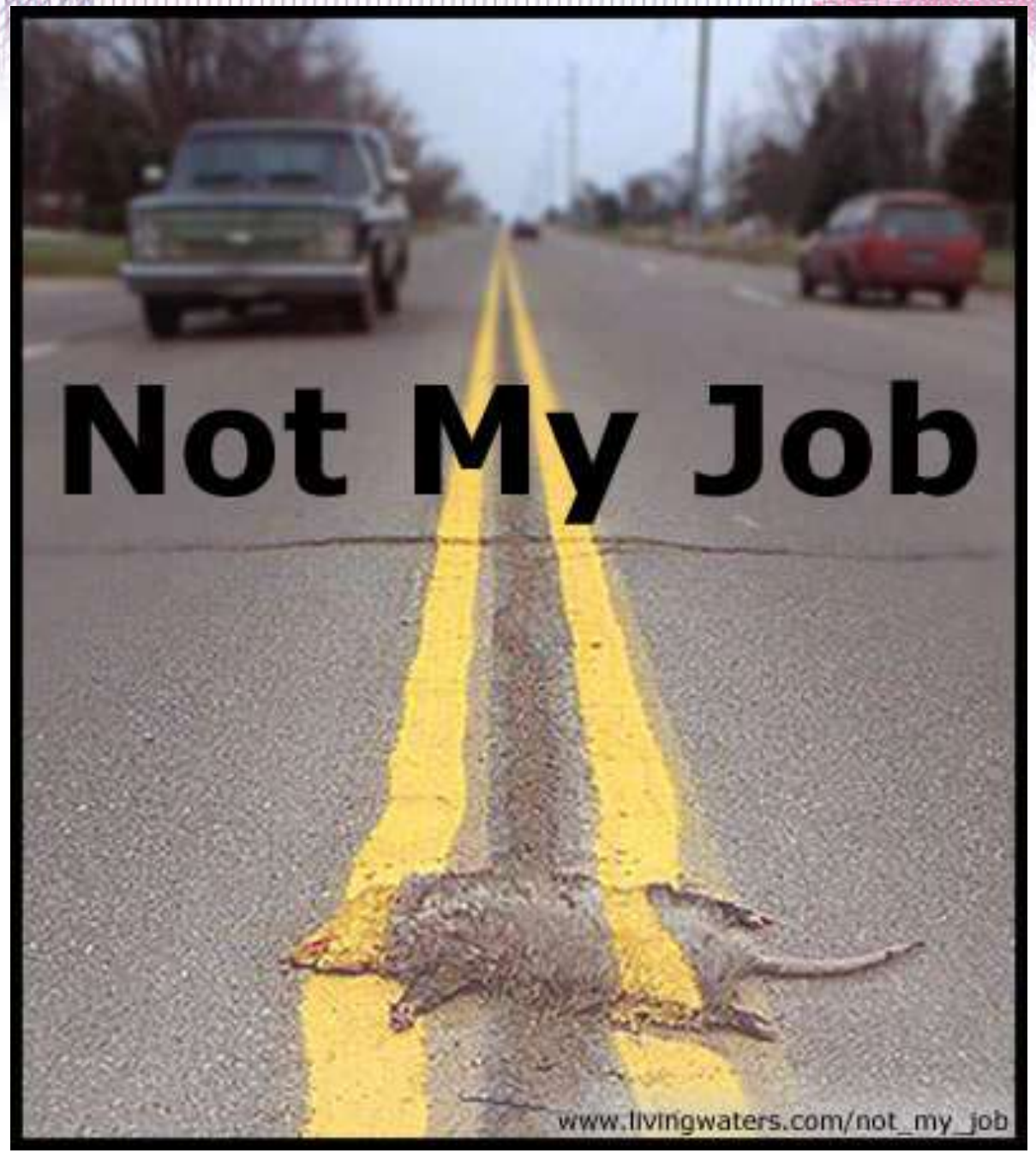
Cyber Security, Crimes, Forensics and law

(Ack- Internet Sources and police Investigations)

U.RAMAMOHAN – SP, CRIME SPOTS,CYBER CRIMES

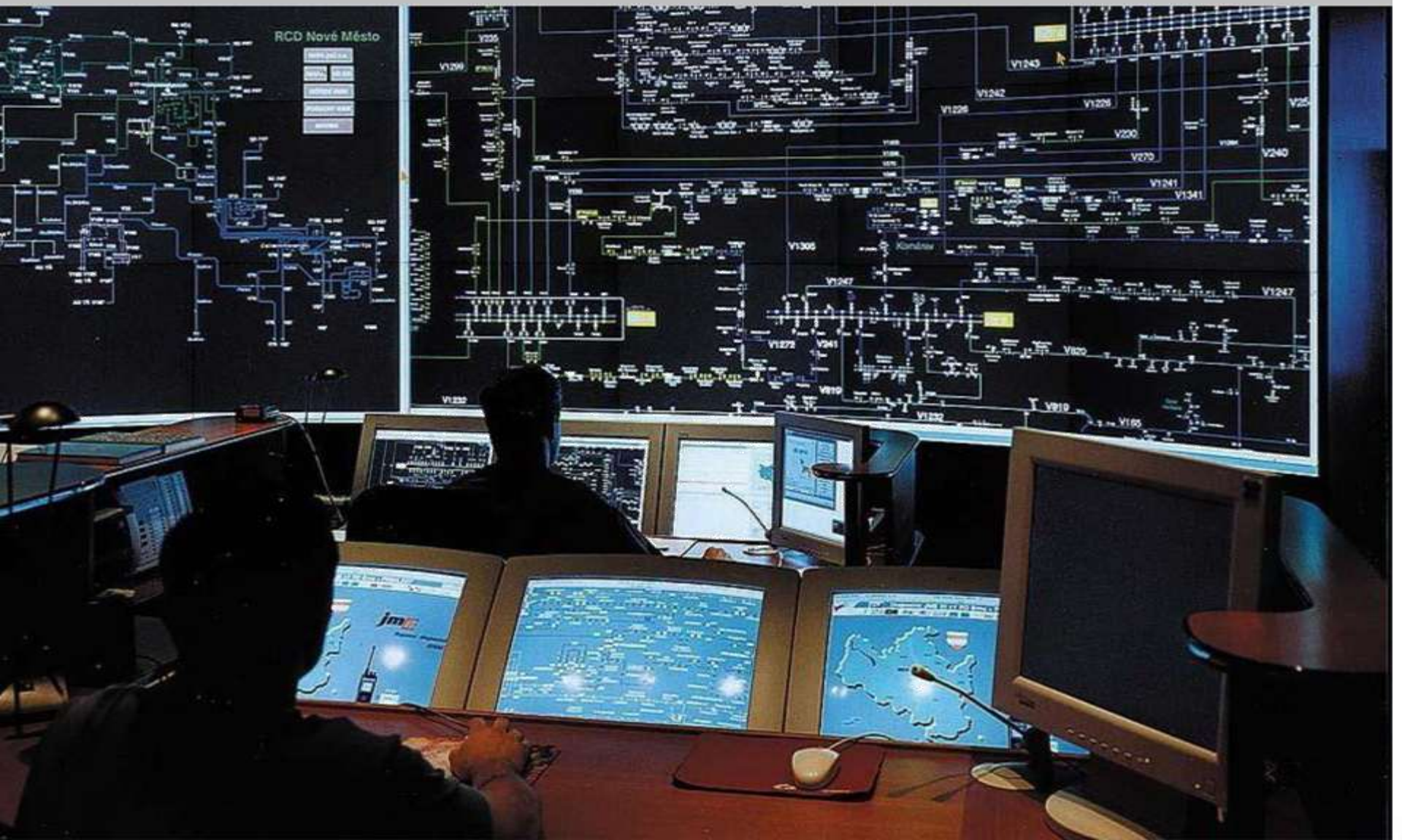
URM

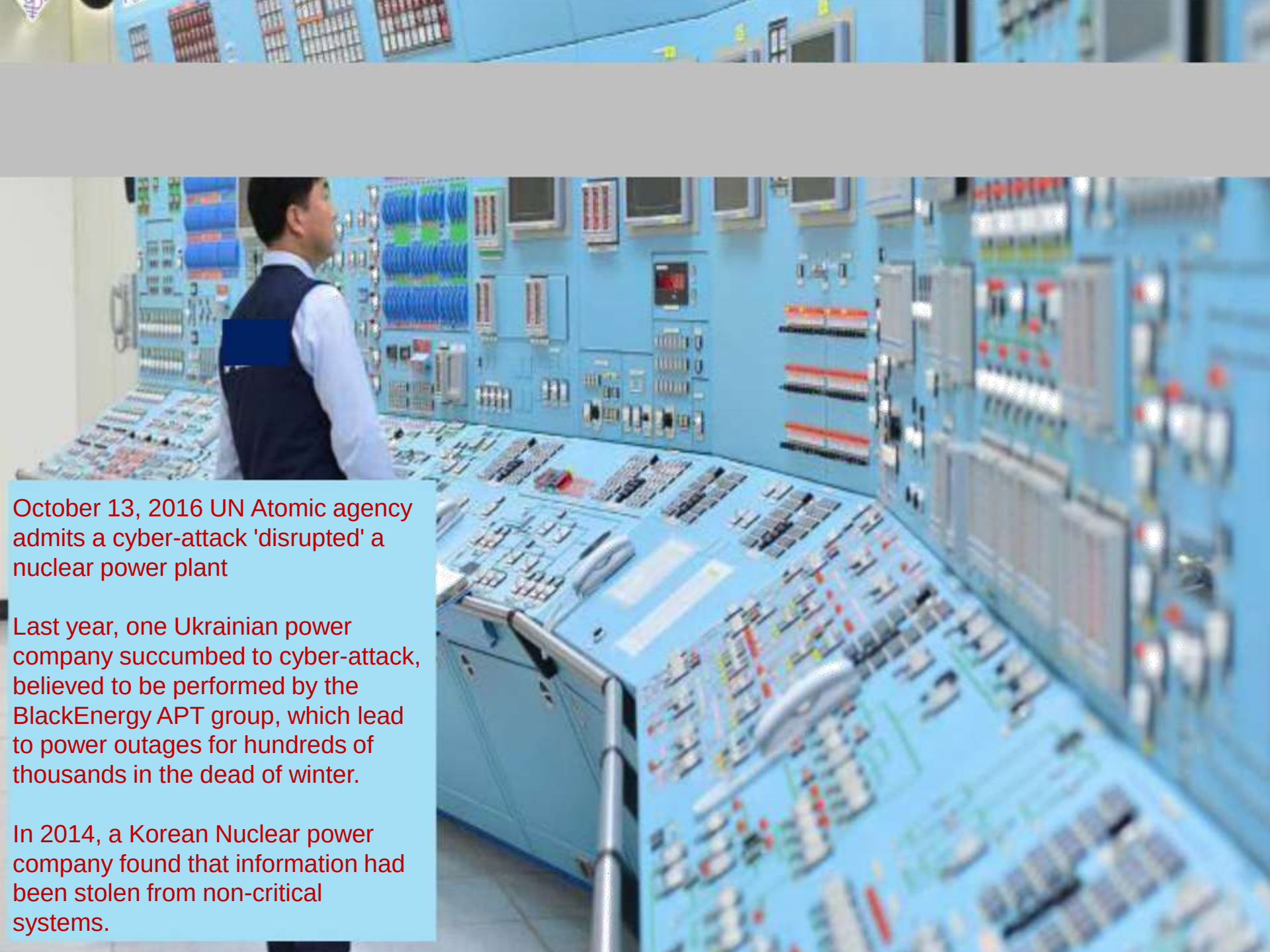

facebook
973,000
Logins
18 Million
Text
Messages
YouTube
4.3 Million
Videos Viewed
Google
3.7 Million
Search
Queries
NETFLIX
266,000
Hours
Watched
ANDROID APP ON
Google play
Available on the
App Store
375,000
Apps Downloaded
$862,823
Spent Online
174,000
Scrolling Instagram
60
SECONDS
2.4 Million
Snaps
Created
481,000
Tweets Sent


Not My Job
www.livingwaters.com/not_my_job


Z-PLUS SECURITY FOR SBI ATM

MAIN TARGETS – SCADA SYSTEMS



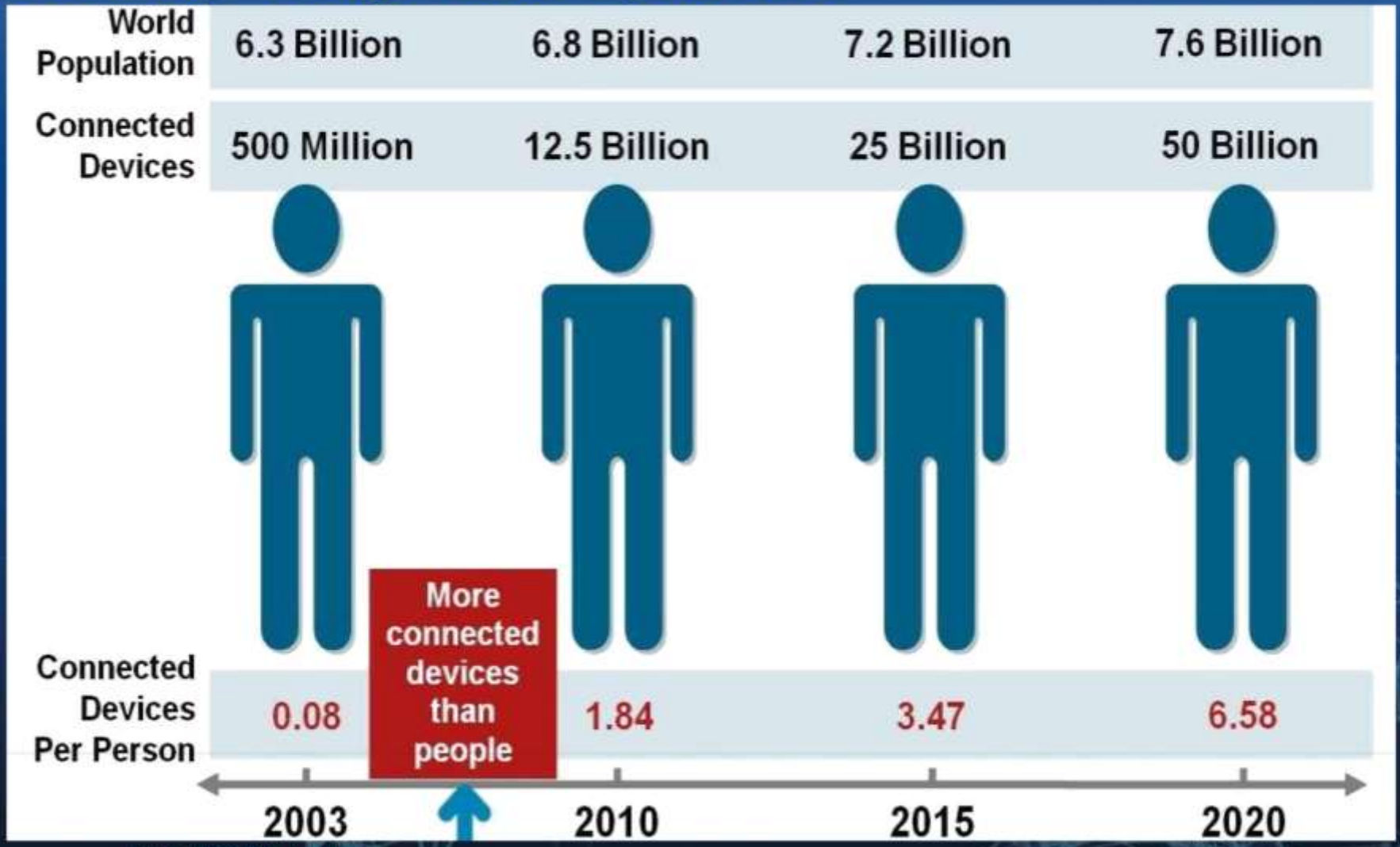


October 13, 2016 UN Atomic agency admits a cyber-attack 'disrupted' a nuclear power plant

Last year, one Ukrainian power company succumbed to cyber-attack, believed to be performed by the BlackEnergy APT group, which lead to power outages for hundreds of thousands in the dead of winter.

In 2014, a Korean Nuclear power company found that information had been stolen from non-critical systems.

How Many "Things" Make up the IoT?



Source : CUSCO IBSG , April 2011

- PAKISTAN BANK HACKS
- WannaCry had created scare in the banks and lots of them suspended their online / card banking transactions temporarily. It was just a ghost then, now its back again as a major hack in Pakistan, in which almost all the banks have been hacked. It is difficult to say that if this is in continuation of the City Union Bank, Cosmos Bank & State Bank of Mauritius hacks in India. They might have been the reconnaissance for this major hack, crippling the whole banking industry of a country. The details are yet to emerge. It's seems the banking heists would get bigger and bigger in the days to come.

- Might be for the first time the whole banking system of a country seems to have been compromised. The likely number of banks would be beyond 18 and the "the data of over 8000 account holders was sold," in a market by hackers. This accounts pertain to around 10 banks. Nobody knows the number of accounts compromised, the total number of fraudulent transactions, the nature of breach & the culprits thereof. The banking circles knew of this, the efforts to hide has messed up matters. This public disclosure comes after 10 banks had blocked all international transactions. This was a reaction to the concerns over breach of debit / credit card data.

- State Bank of Pakistan has been informed of this by various commercial banks. One bank has stopped online mobile banking services since Nov. 3, stating "technical grounds." The first cyber attack was reported by BankIslami on October 27th. Rs 2.6 million was was stolen from international payment cards. It then allowed only biometrically verified payments on ATM cards within Pakistan. Cyber is the ultimate war zone today, the amalgam of internal / external security, financial frauds & money laundering.

- WITH CYBER DEFENCES NOT IN PLACE, ALL OTHER DEFENCES ARE COSMETIC TODAY

- Banks security had been a major concern with the worsening cyber security scenario the world over. Recent big attacks started with the Bangladesh Bank Cyber Heist, which took place in Feb 2016. Of the 35 fraudulent instructions to withdraw close to US $1 billion via the SWIFT network, only 5 materialised, others were blocked on suspicion. In all $101 million was transferred, of which $38 million has been recovered. Since, then SWIFT is being compromised and so are the banks.

- 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 capabilities in hands of the hackers.

- '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.

- DIGITAL COLUMBUS

Reasons why people don’t report to Cyber Crimes

- Negative publicity
  – 70%

- Competitors would use to advantage
  – 61%

- Unaware that they could report
  – 53%

How can we secure ourselves?

Limit the amount of personal information you post - Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections.

Remember that the Internet is a public resource - Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and in blogs and other forums.

Be skeptical - Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, an exaggeration, or a joke. Take appropriate precautions, and try to verify the authenticity of any information before taking any action.

Contd..

- **Evaluate your settings** - Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you can customize your settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions, so don't post anything that you wouldn't want the public to see. Sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.
- **Use strong passwords** - Protect your account with passwords that cannot easily be guessed.
- **Check privacy policies** - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam.
- **Keep software, particularly your web browser, up to date** - Install software updates so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.
- **Use and maintain anti-virus software** - Anti-virus software helps protect your computer against known viruses, so you may be able to detect and remove the virus before it can do any damage. Because attackers are continually writing new viruses, it is important to keep your definitions up to date.
- *Children are especially susceptible to the threats that social networking sites present. Although many of these sites have age restrictions, children may misrepresent their ages so that they can join. By teaching children about Internet safety, being aware of their online habits, and guiding them to appropriate sites, parents can make sure that the children become safe and responsible users*.

Cyber Security Strategy in India

- **Security Policy, Compliance and Assurance – Legal Framework**
  - IT Act, 2000
  - IT (Amendment) Act 2008 – Data Protection & Computer crimes
  - Best Practice ISO 27001
  - Security Assurance Framework- IT/ITES/BPO Companies
- **Security Incident – Early Warning & Response**
  - CERT-In National Cyber Alert System
  - Information Exchange with international CERTs
- **Capacity building**
  - Skill & Competence development
  - Training of law enforcement agencies and judicial officials in the collection and analysis of digital evidence
  - Training in the area of implementing information security in collaboration with Specialised Organisations in US
- **Setting up Digital Forensics Centers**
  - Domain Specific training – Cyber Forensics
- **Research and Development**
  - Network Monitoring
  - Biometric Authentication
  - Network Security
- **International Collaboration**

Reporting of cyber incidents and vulnerability

The CERT Rules provide that in case of the following, wherein cyber security is

threatened, an individual, a company or an organisation must report the

incident to the Indian Computer Emergency Response Team (CERT-In)

- The **Indian Computer Emergency Response Team** (CERT-In) is an office within the Ministry of Electronics and Information Technology. It is the nodal agency to deal with cyber security threats like hacking and phishing. It strengthens security-related defence of the Indian Internet domain

What to be reported?

- Targeted scanning/probing of critical networks/systems
- Compromise of critical systems/information
- Unauthorised access of IT systems/data
- Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites, etc.
- Malicious code attacks such as spreading of virus / worm / Trojan / botnets / spyware

- Attacks on servers such as database, mail, and DNS and network devices such as routers
- Identity theft, spoofing and phishing attacks
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Attacks on critical infrastructure, Supervisory Control and Data Acquisition (SCADA) systems and wireless networks
- Attacks on applications such as e-governance, e-commerce etc.

Time period for reporting

- CERT Rules require cyber incidents to be reported within a reasonable time of occurrence. In our view, this should be at the earliest possible so that you can minimise your risks. Further, there is no time limit for reporting vulnerabilities by CERT-In. NCIIPC, on the other hand, requires incidents relating to Critical Information Infrastructure to be reported at the earliest.

Procedure for Reporting

- CERT-In and NCIIPC have incident reporting help desk that operates 24 hours a day and seven days a week. Both entities provide for their respective Cyber Incident Form and Vulnerability Form to report such incidents. The form can be sent by post to CERT-In at Electronics Niketan, CGO Complex, New Delhi - 110003 or emailed at **incident@cert-in.org.in**
- The NCIIPC vulnerability and incident reporting form can be emailed at **ir@nciipc.gov.in**

CERT-In

- Security Incident Reporting

  http://www.cert-in.org.in/PDF/certinirform.pdf

- Vulnerability Reporting Form

  http://www.cert-in.org.in/PDF/Vul_Report.pdf

NCIIPC

- Incident Reporting

  http://nciipc.gov.in/documents/Incidence_Report.pdf

- Vulnerability Disclosure
  http://nciipc.gov.in/documents/Vulnerability_Disclosure.pdf

Precaution is better!

1. Maintain regular Backups (P.s: Not on the same pc)
2. Turn Off Autoplay
3. Stay away from installing unnecessary **toolbars** in Browsers
4. Use a good and Licensed Anti-Virus Suite
5. Always use updated Browsers and install latest patches on Operating System
6. Say NO to Piracy. It kills your computer too, slowly
7. No! You are NOT that lucky visitor on someone's site. Believe me!

Create Frameworks and Policies for Secure IOT Infrastructure for Secure Smart Cities, Real-Time Sensor Data Networks for Agriculture and Home Land Security

- Institutionalize and provision a policy for securing IOT infrastructure to ensure the safety of the cyber-physical world.

- Set-up state and national Level R&D Centers in a PPP model to develop new security models and technologies will be required to be innovated.

- Identify critical infrastructure (smart cities, survey data, agriculture data, home land security/drones/surveillance) and secure them on highest priority in a time-bound manner.

Typically cyber space is made of a number of pipes, tubes and devices that are interconnect with each other, about which there is a fair degree of information and shared stake.

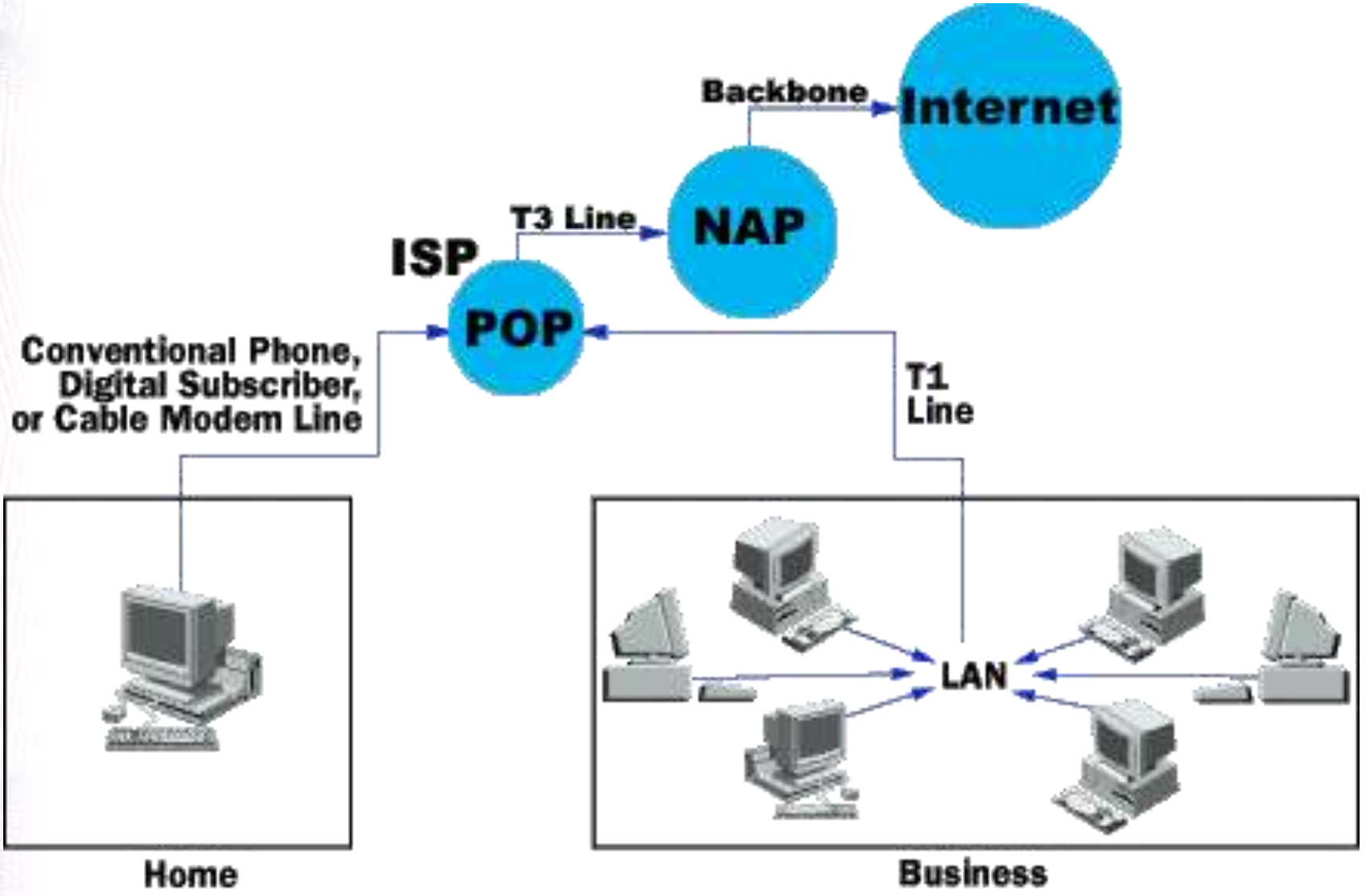
In India, the top five smart phone players are Samsung,ViVo, Oppo, Lenovo and Xiaomi. The top five Apps in India are Whatsapp, Facebook Messenger, SHAREit, UCBrowser and Truecaller which are from foreign players. The government, military, common users or the law enforcement agencies are unaware as to the terms of agreement based on which the license of the Android mobile operating system has been provided to the smart phone manufacturer. Neither is the user completely sure about the end user/privacy agreement which is the contract between a user and the App developer. Hence, it would be naïve for us to really believe that in a country dominated by Chinese and foreign players, it would be easy to protect or regulate the Indian cyber space.

Indigenous manufacture would be an ideal solution;

What if –

- A computer is effected with a Ransomware?
- A video with potential to cause disturbance to communal harmony gets viral?
- A picture with potential to cause disturbance to communal harmony gets viral?
- A movie is available on the internet even before it is released in theatres?
- An unknown user uploads and shares obscene videos of a victim?

When Connected to the Internet, the Computer Becomes Part of a Network.



Cyber Security

Agenda

(Cyber Security) Perimeters of:

- Organization
- Data
- Application
- Network

- Securing National Digital Infrastructure
- Precautions

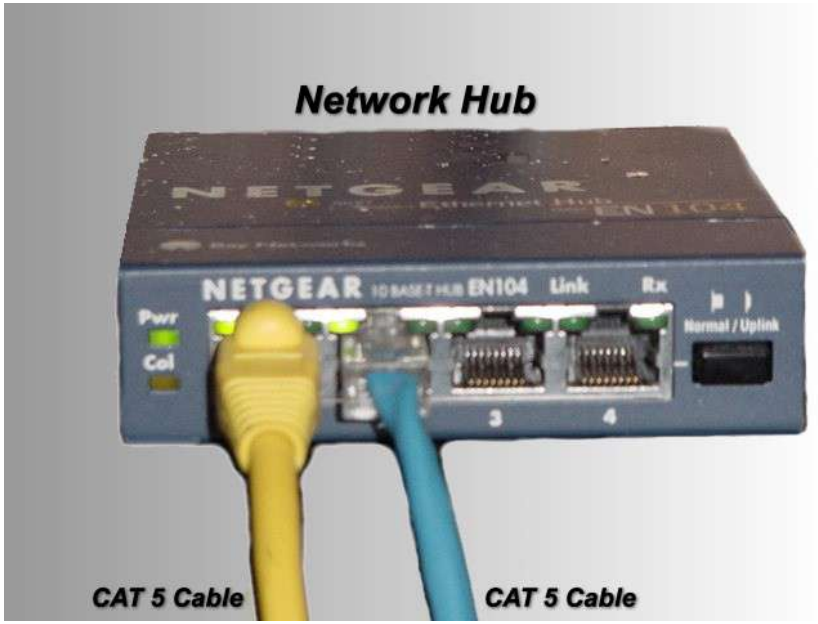
Organization

Organization

- Switches/Routers
- Firewalls
- IDS/IPS
- Proxy/Content Filtering
- Log Co-Relation/SIEM
  - Alerting
  - Monitoring
  - Auditing
- Website Security (SSL)

Network Hub

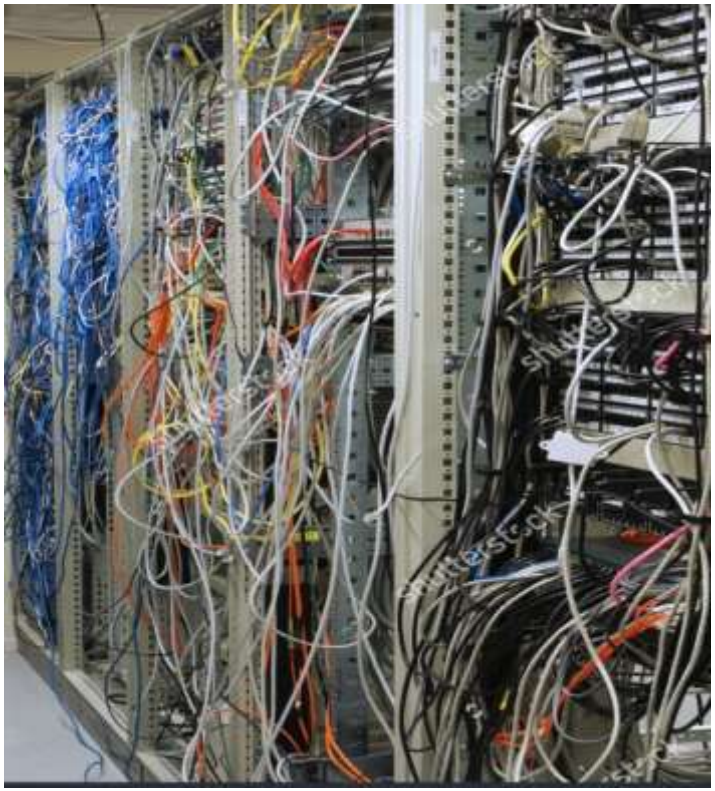
•Hub broadcasts all the data packets received from one port to all available ports. That means a packet sent via one computer to a certain destination computer goes to each and every computers which are connected to the same Network.
•The Hub has 4/8/16/24 ports (No of Computers connected)



Network Switch

A Switch is a Networking Device which has some intelligence as compared to Network Hub.
It binds IP with MAC in communication.
It doesn't broadcast the data packet to all the computer in the network but to the destination computer.
Switches also come with 52 Ports.

Which Switch?



Refer network Diagram

Switches maintain a **M**AC **A**ddress **T**able (MAT) which contains information of computers connected at different ports.

```
Switch#show mac-address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  10    0001.c7ad.e316    DYNAMIC     Fa0/24
  10    0002.4ab7.1701    DYNAMIC     Fa0/24
  11    0001.c7ad.e316    DYNAMIC     Fa0/24
  11    0002.4ab7.1701    DYNAMIC     Fa0/24
  12    0001.c7ad.e316    DYNAMIC     Fa0/24
  12    0002.4ab7.1701    DYNAMIC     Fa0/24
  12    000d.bd94.6b58    DYNAMIC     Fa0/1
  12    0060.3e5c.ba1d    DYNAMIC     Fa0/2
  12    00e0.f934.e3c4    DYNAMIC     Fa0/3
  13    0001.c7ad.e316    DYNAMIC     Fa0/24
  13    0002.4ab7.1701    DYNAMIC     Fa0/24
Switch#
```

Firewall Logs

```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info
path

2019-02-21 16:01:24 ALLOW UDP 172.16.22.236 172.16.27.2 63482 53 0 - - - - - - - - SEND
2019-02-21 16:01:34 DROP UDP 172.16.22.236 255.255.255.255 49152 1947 0 - - - - - - - - SEND
2019-02-21 16:01:35 ALLOW UDP fe80::21da:51ed:6054:e80c ff02::c 53872 1900 0 - - - - - - - - RECEIVE
2019-02-21 16:01:35 ALLOW UDP 172.16.22.236 172.16.27.2 56803 53 0 - - - - - - - - SEND
2019-02-21 16:01:35 ALLOW UDP fe80::ec72:4d7d:c643:ebe1 ff02::1:3 61291 5355 0 - - - - - - - - SEND
2019-02-21 16:01:35 ALLOW UDP 172.16.22.236 224.0.0.252 56607 5355 0 - - - - - - - - SEND
2019-02-21 16:01:36 ALLOW UDP 172.16.22.236 224.0.0.252 137 137 0 - - - - - - - - SEND
2019-02-21 16:01:38 DROP UDP 172.16.22.236 172.16.23.255 49152 1947 0 - - - - - - - - SEND
2019-02-21 16:01:40 ALLOW ICMP fe80::21da:51ed:6054:e80c fe80::ec72:4d7d:c643:ebe1 - - 0 - - - - 135 0 - RECEIVE
2019-02-21 16:01:40 ALLOW ICMP fe80::ec72:4d7d:c643:ebe1 ff02::1:ff54:e80c - - 0 - - - - 135 0 - SEND
2019-02-21 16:01:57 ALLOW UDP fe80::ec72:4d7d:c643:ebe1 ff02::1:3 58306 5355 0 - - - - - - - - SEND
2019-02-21 16:01:57 ALLOW UDP 172.16.22.236 224.0.0.252 57563 5355 0 - - - - - - - - SEND
2019-02-21 16:01:57 ALLOW UDP fe80::ec72:4d7d:c643:ebe1 ff02::1:3 64423 5355 0 - - - - - - - - SEND
2019-02-21 16:01:57 ALLOW UDP 172.16.22.236 224.0.0.252 51121 5355 0 - - - - - - - - SEND
2019-02-21 16:01:57 ALLOW UDP 172.16.22.236 255.255.255.255 68 67 0 - - - - - - - - SEND
2019-02-21 16:01:57 ALLOW UDP 172.16.22.236 172.16.23.255 137 137 0 - - - - - - - - SEND
2019-02-21 16:02:06 ALLOW UDP 172.16.22.236 172.16.27.2 52122 53 0 - - - - - - - - SEND
```

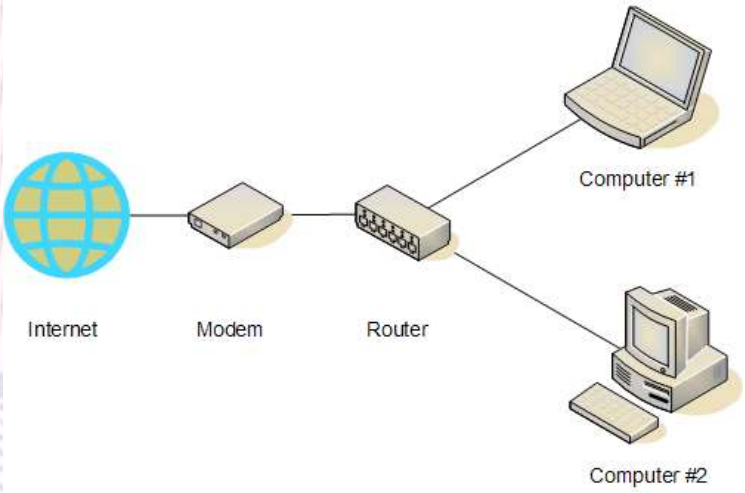
Router

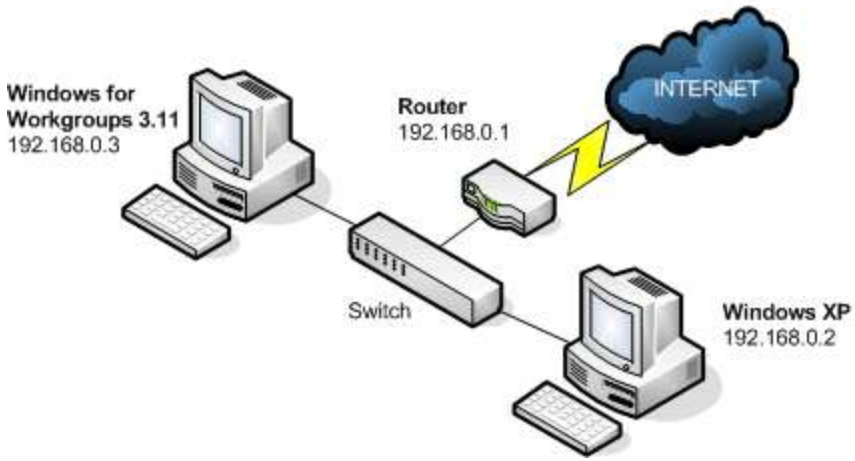
•Router is a Network device which sends the data packets from one network to another.

•In simple terms Routers is a bridge between two Networks.

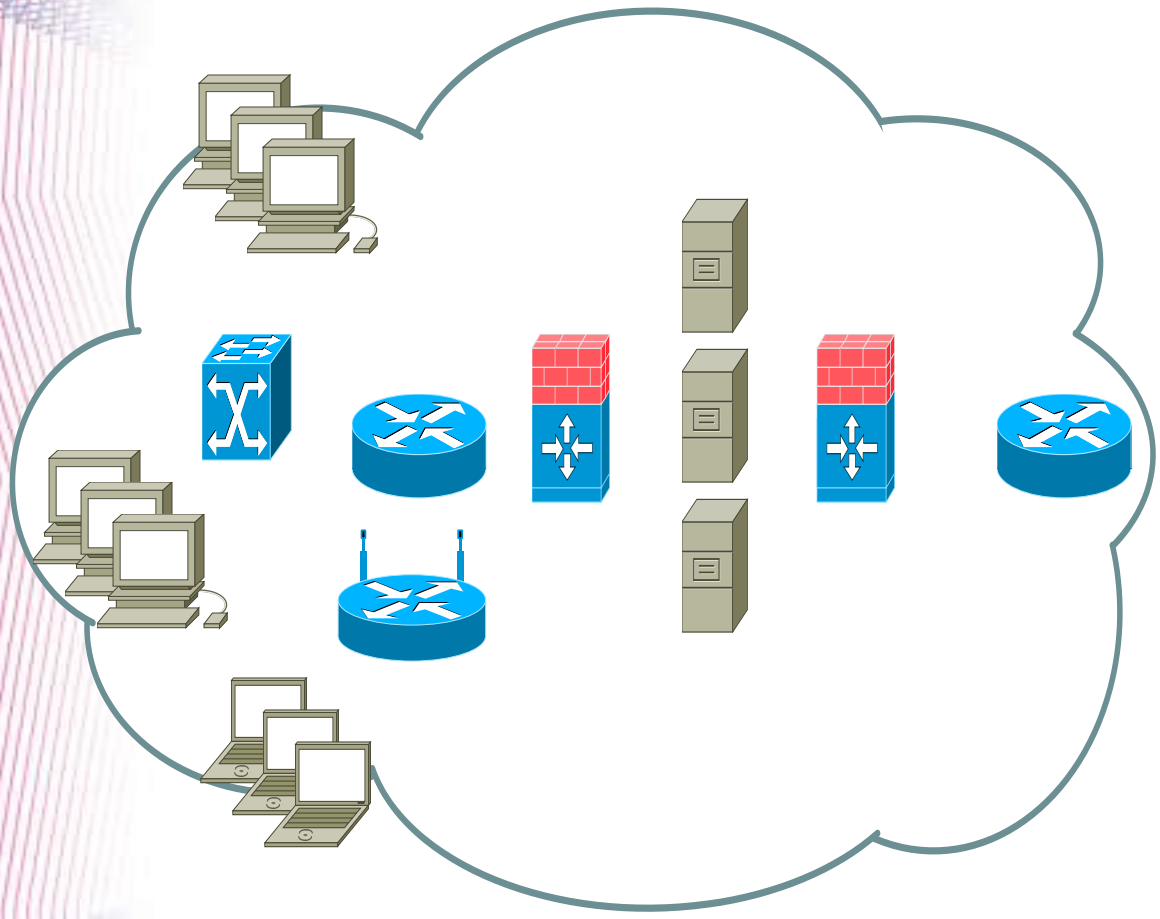
•It directs traffic over internet.

•Router reads the destination IP address of the data packet & accordingly transmit the data to the destination computer.





Network Elements



PC
Laptop

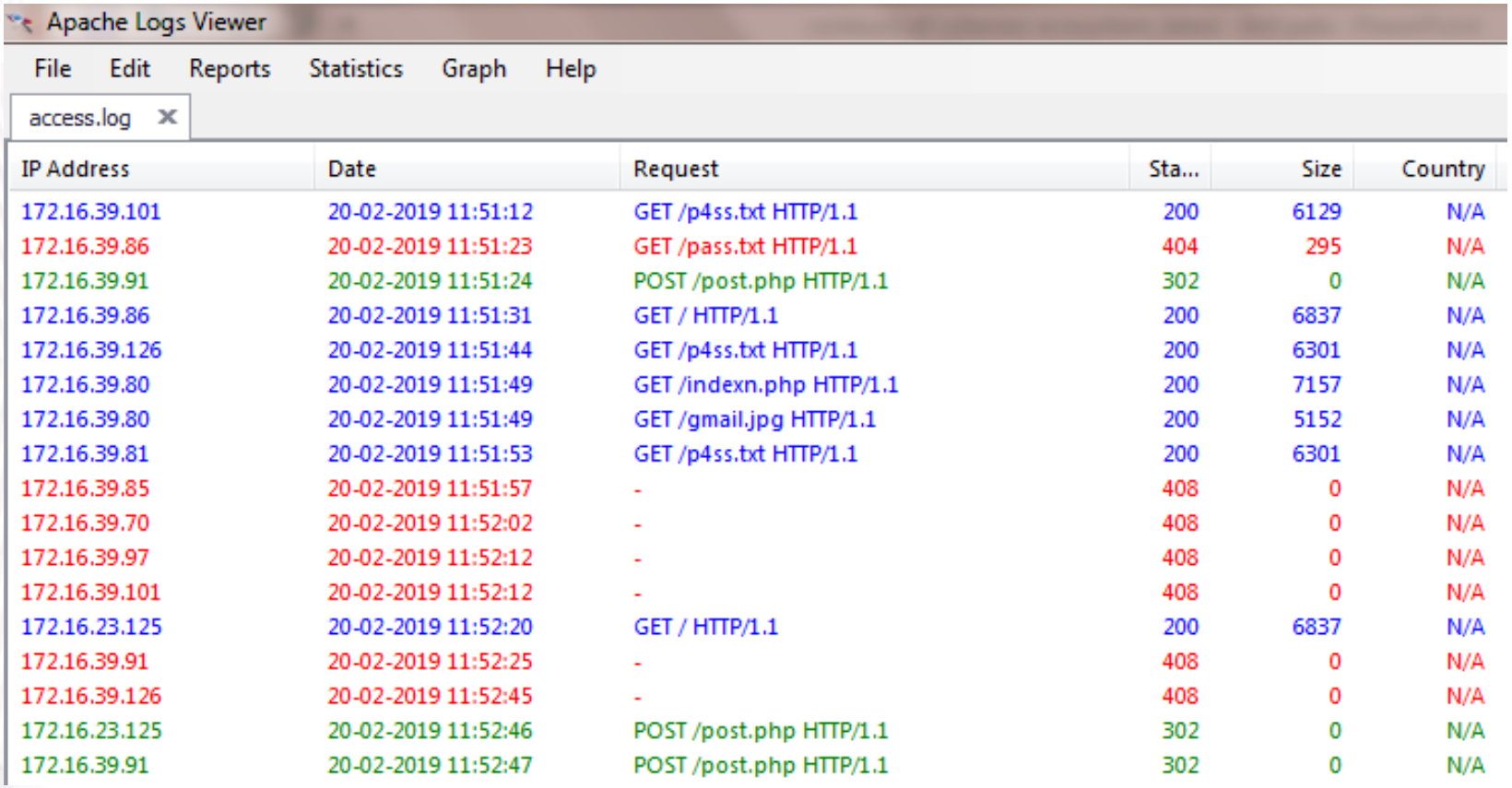
Firewall

Switch
Router
IDS / IPS
Wifi Router
Access Point

Proxy
Relay

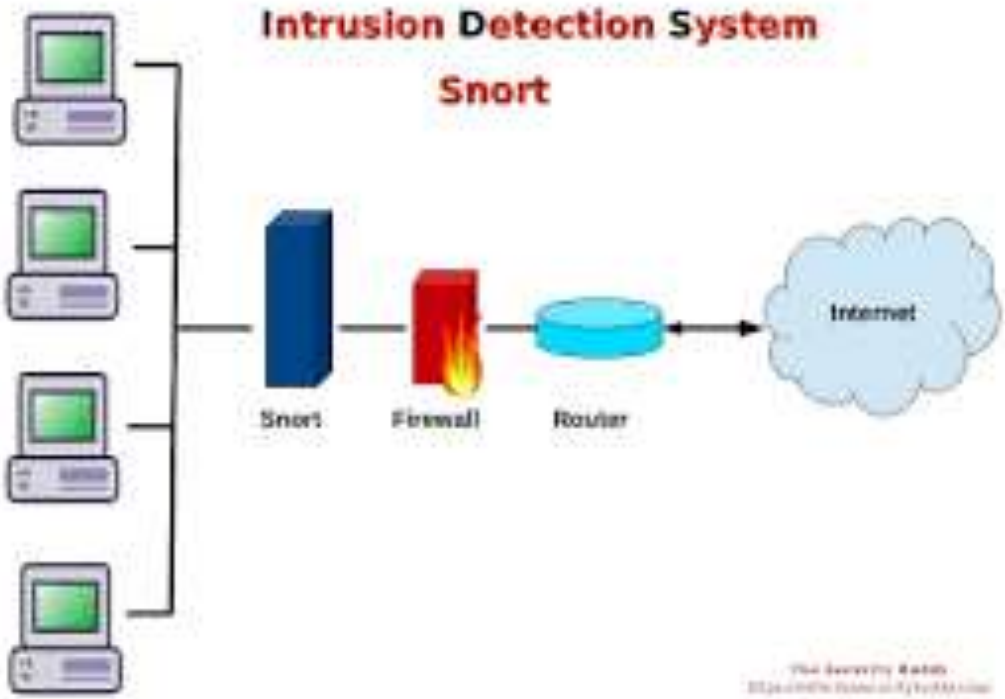
Web Server
Mail Server
DB Server

Server Access Logs



IP Address	Date	Request	Sta...	Size	Country
172.16.39.101	20-02-2019 11:51:12	GET /p4ss.txt HTTP/1.1	200	6129	N/A
172.16.39.86	20-02-2019 11:51:23	GET /pass.txt HTTP/1.1	404	295	N/A
172.16.39.91	20-02-2019 11:51:24	POST /post.php HTTP/1.1	302	0	N/A
172.16.39.86	20-02-2019 11:51:31	GET / HTTP/1.1	200	6837	N/A
172.16.39.126	20-02-2019 11:51:44	GET /p4ss.txt HTTP/1.1	200	6301	N/A
172.16.39.80	20-02-2019 11:51:49	GET /indexn.php HTTP/1.1	200	7157	N/A
172.16.39.80	20-02-2019 11:51:49	GET /gmail.jpg HTTP/1.1	200	5152	N/A
172.16.39.81	20-02-2019 11:51:53	GET /p4ss.txt HTTP/1.1	200	6301	N/A
172.16.39.85	20-02-2019 11:51:57	-	408	0	N/A
172.16.39.70	20-02-2019 11:52:02	-	408	0	N/A
172.16.39.97	20-02-2019 11:52:12	-	408	0	N/A
172.16.39.101	20-02-2019 11:52:12	-	408	0	N/A
172.16.23.125	20-02-2019 11:52:20	GET / HTTP/1.1	200	6837	N/A
172.16.39.91	20-02-2019 11:52:25	-	408	0	N/A
172.16.39.126	20-02-2019 11:52:45	-	408	0	N/A
172.16.23.125	20-02-2019 11:52:46	POST /post.php HTTP/1.1	302	0	N/A
172.16.39.91	20-02-2019 11:52:47	POST /post.php HTTP/1.1	302	0	N/A

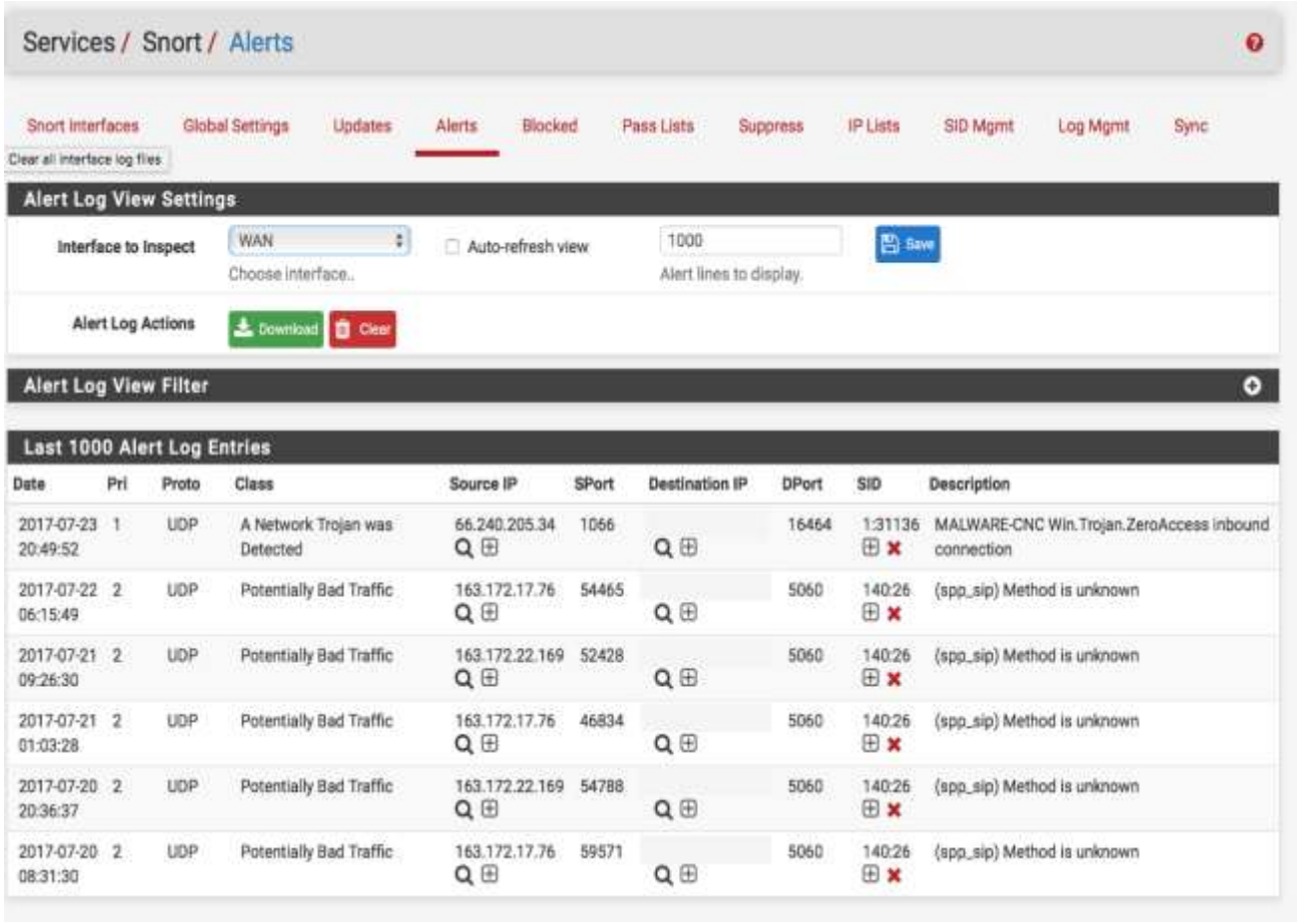
Intrusion Detection System



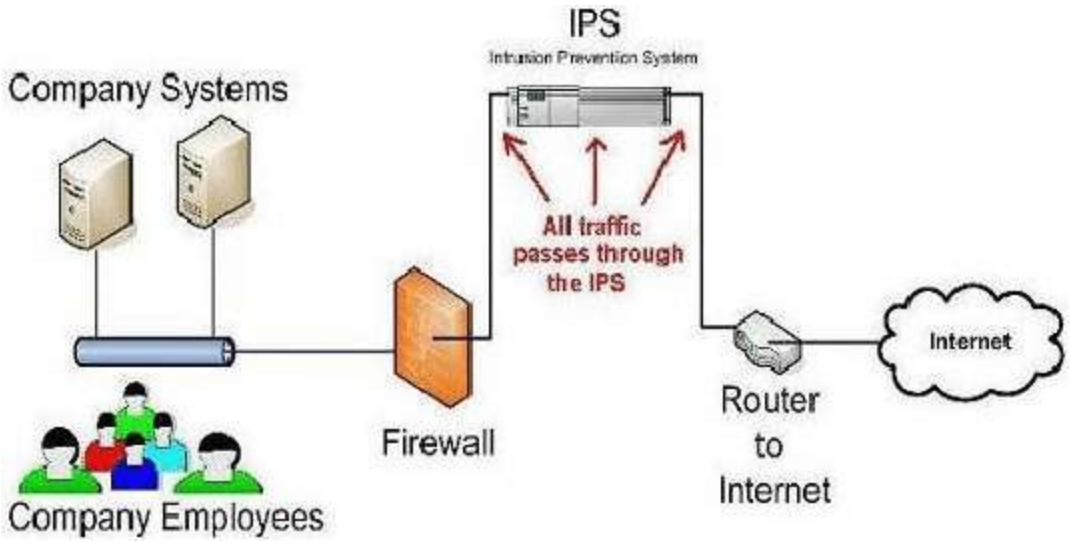
An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management system.

Intrusion Detection System Tools

- Snort
- OSSEC
- Suricata
- Bro
- Sagan
- Security Onion



Intrusion Prevention System



An Intrusion Prevention System (**IPS**) is a security solution that provides security against unauthorized access and malicious activities at the network level. ... The other functions that an Intrusion Prevention System can perform include: Blocks network traffic from the offending source IP addresses

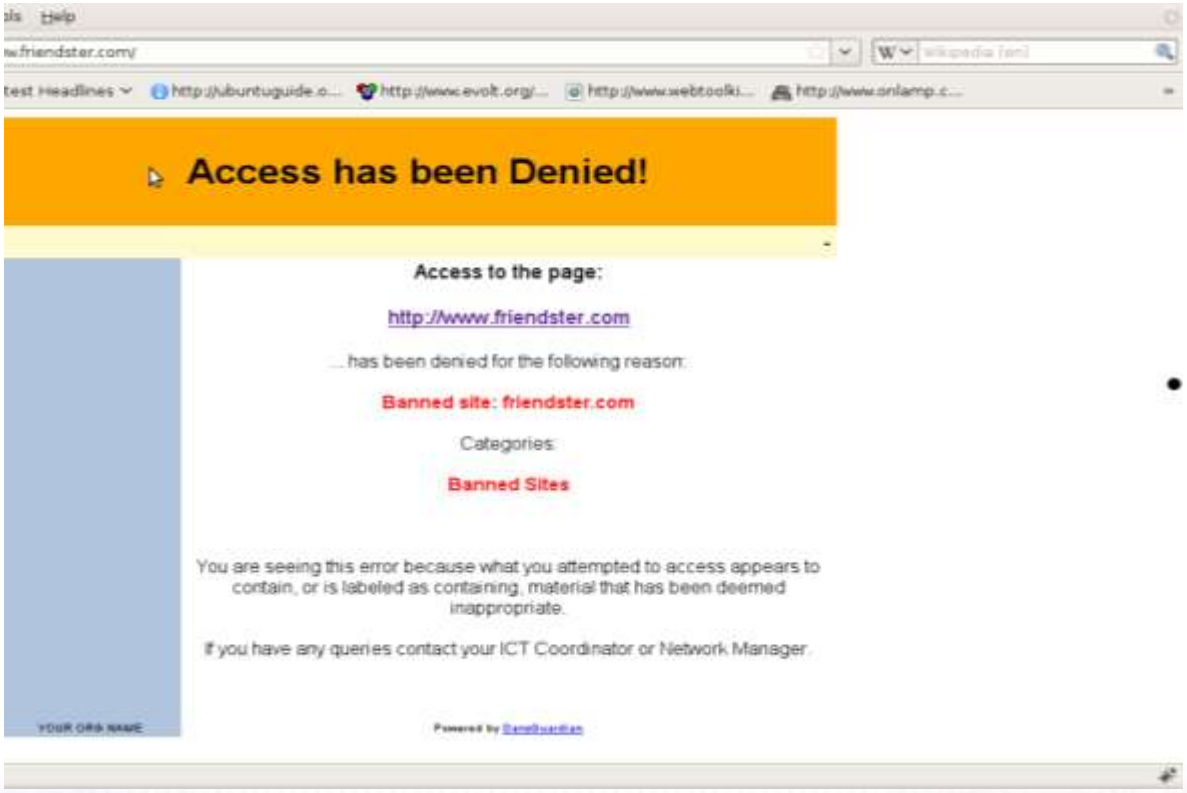
Features of Intrusion Prevention System

The IPS is able to perform actions to shut down the threat. These actions include –

- Restoring log files from storage
- Suspending user accounts
- Blocking IP addresses
- Killing processes
- Shutting down systems
- Starting up processes
- Updating firewall settings
- Alerting, recording, and reporting suspicious activities

Proxy Content-Filtering

A content-filtering web proxy server provides administrative control over the content that may be relayed through the proxy. It is commonly used in both commercial and non-commercial organizations to ensure that internet usage conforms to acceptable use policy



Proxy Content-Filtering Tools

SquidGuard

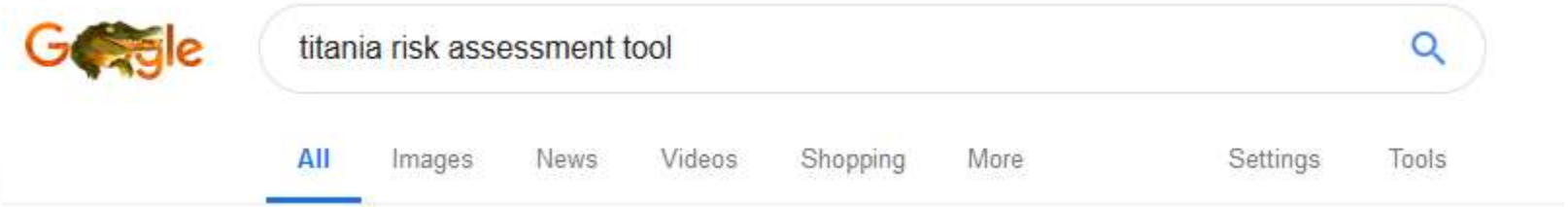
DansGuardian

OpenDNS

Security Information and Event Management

Security Audit!

https://tinyurl.com/risksvpnpa



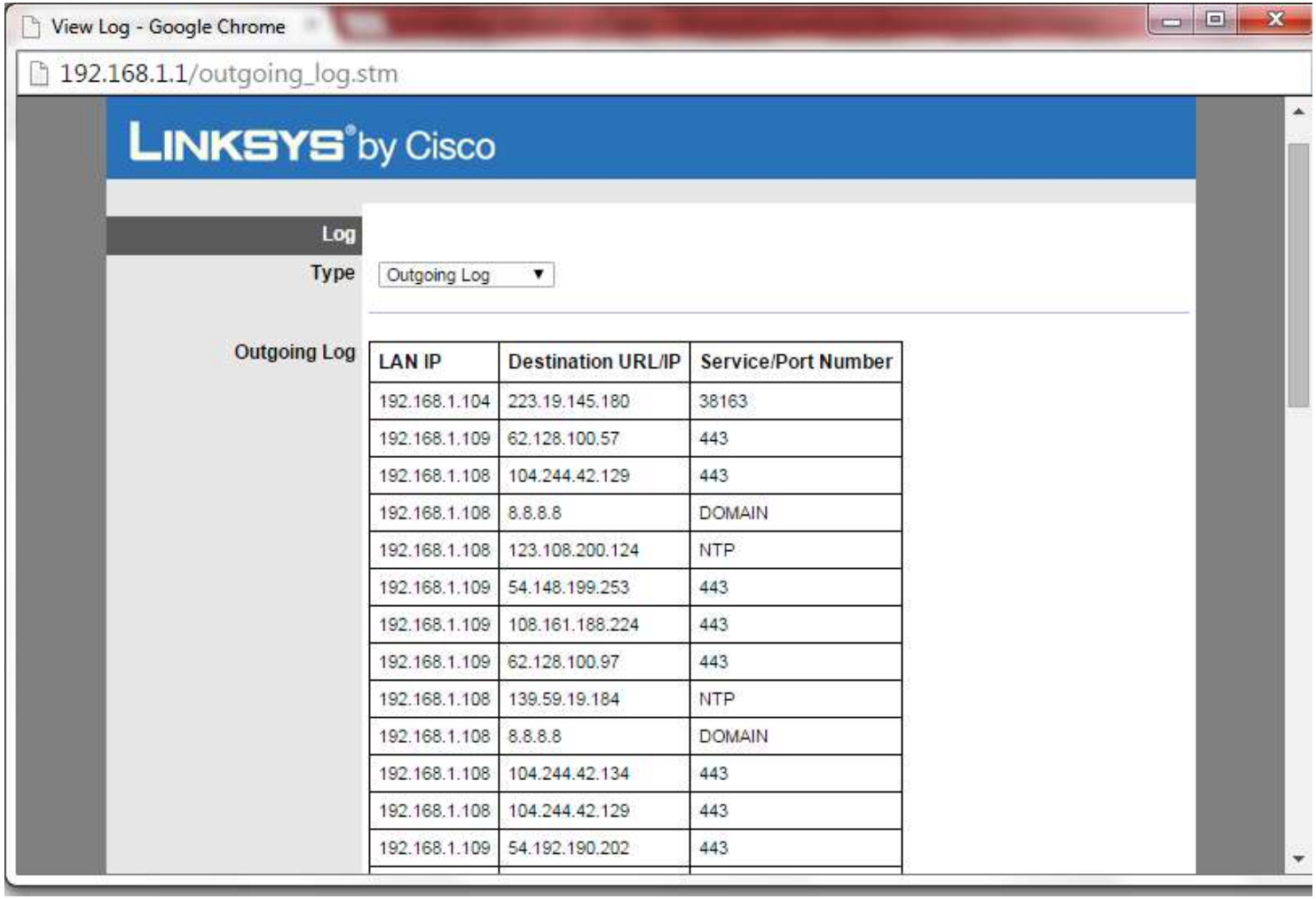
google.com?

What happens in those 2 seconds in which google’s homepage is loaded?

What information is stored at these nodes?

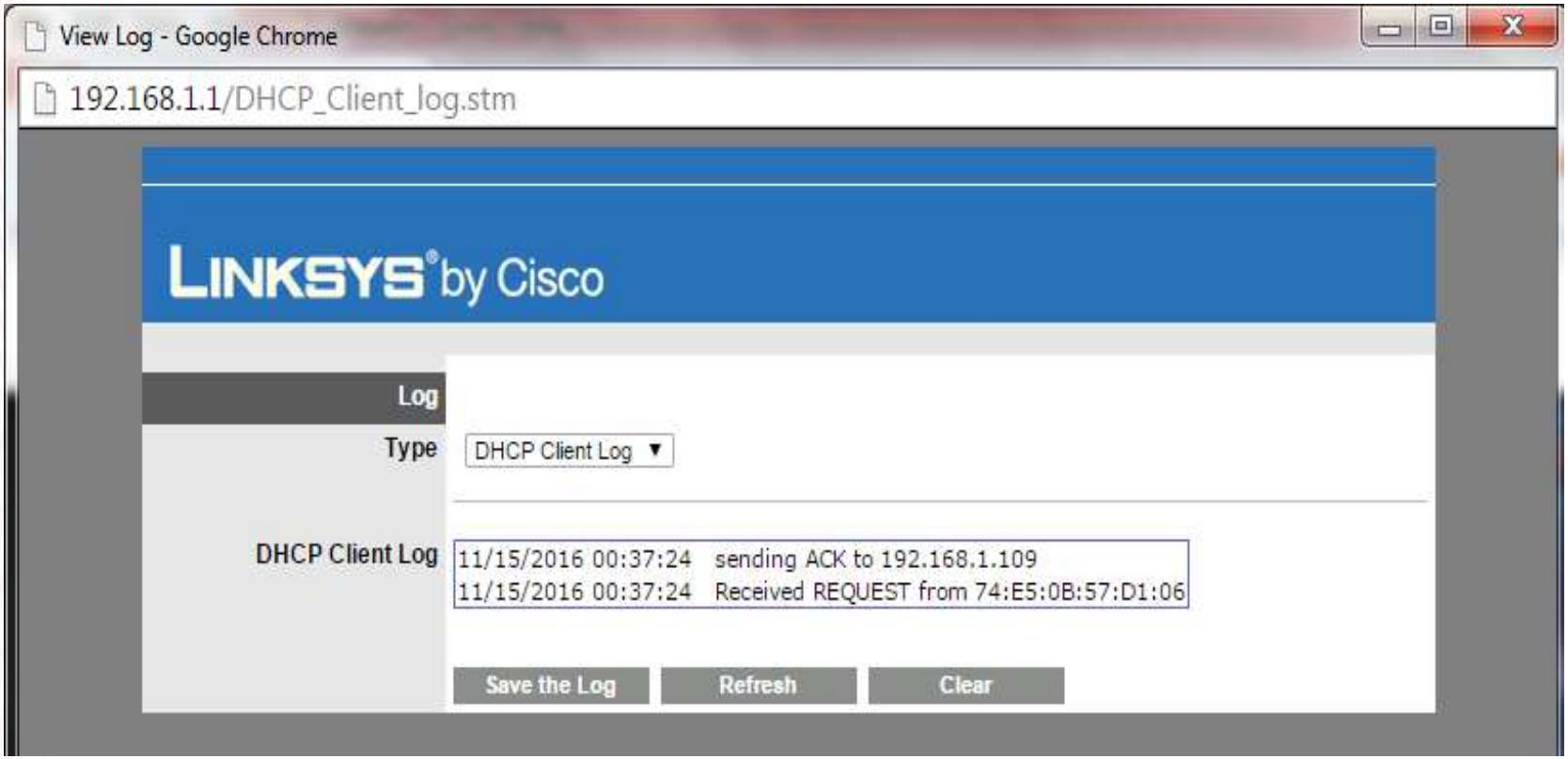
- system DHCP logs
- switch
- Router
- ISP
- DNS server
- target host

Router Logs – Outgoing traffic

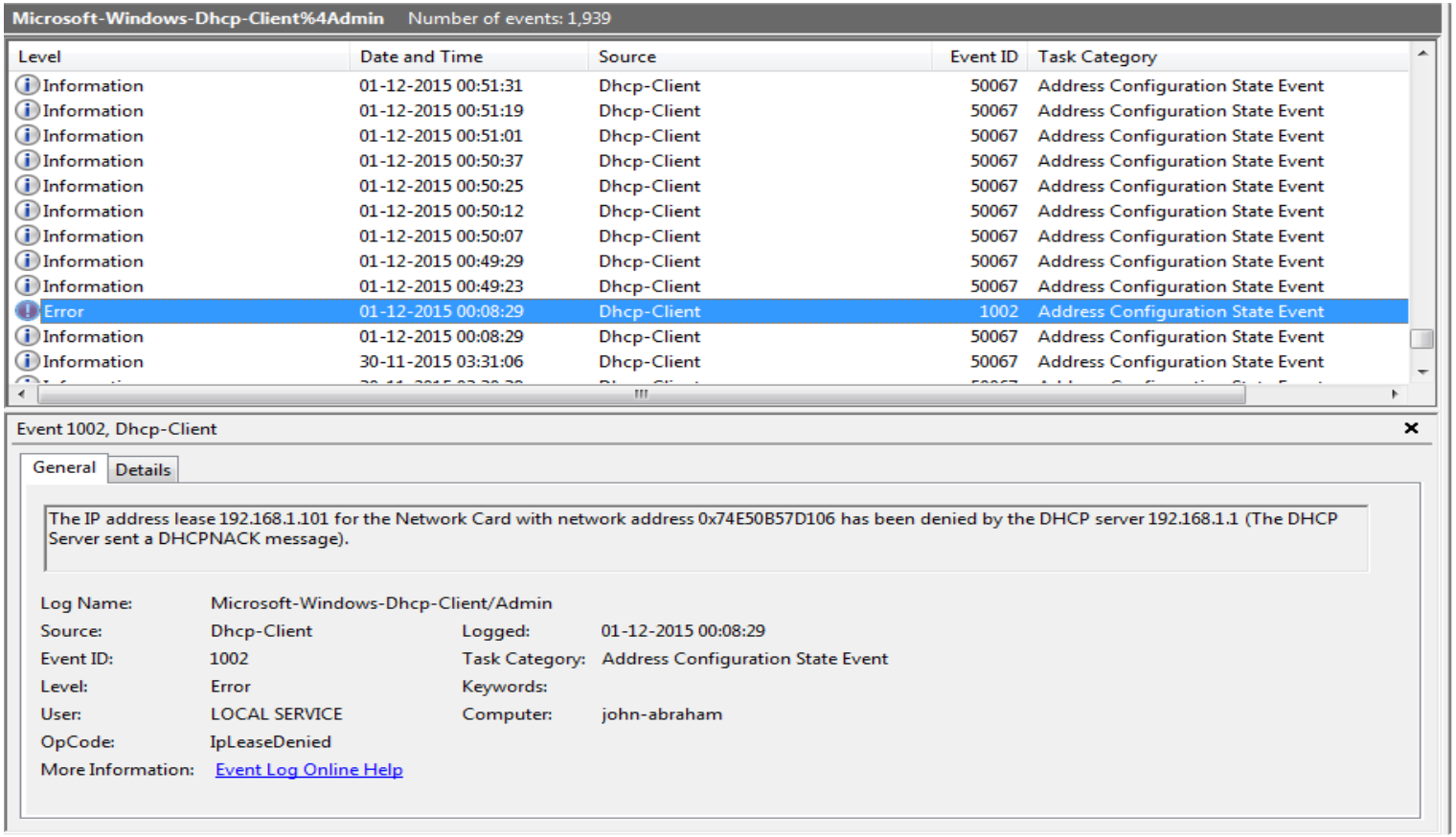


LAN IP	Destination URL/IP	Service/Port Number
192.168.1.104	223.19.145.180	38163
192.168.1.109	62.128.100.57	443
192.168.1.108	104.244.42.129	443
192.168.1.108	8.8.8.8	DOMAIN
192.168.1.108	123.108.200.124	NTP
192.168.1.109	54.148.199.253	443
192.168.1.109	108.161.188.224	443
192.168.1.109	62.128.100.97	443
192.168.1.108	139.59.19.184	NTP
192.168.1.108	8.8.8.8	DOMAIN
192.168.1.108	104.244.42.134	443
192.168.1.108	104.244.42.129	443
192.168.1.109	54.192.190.202	443

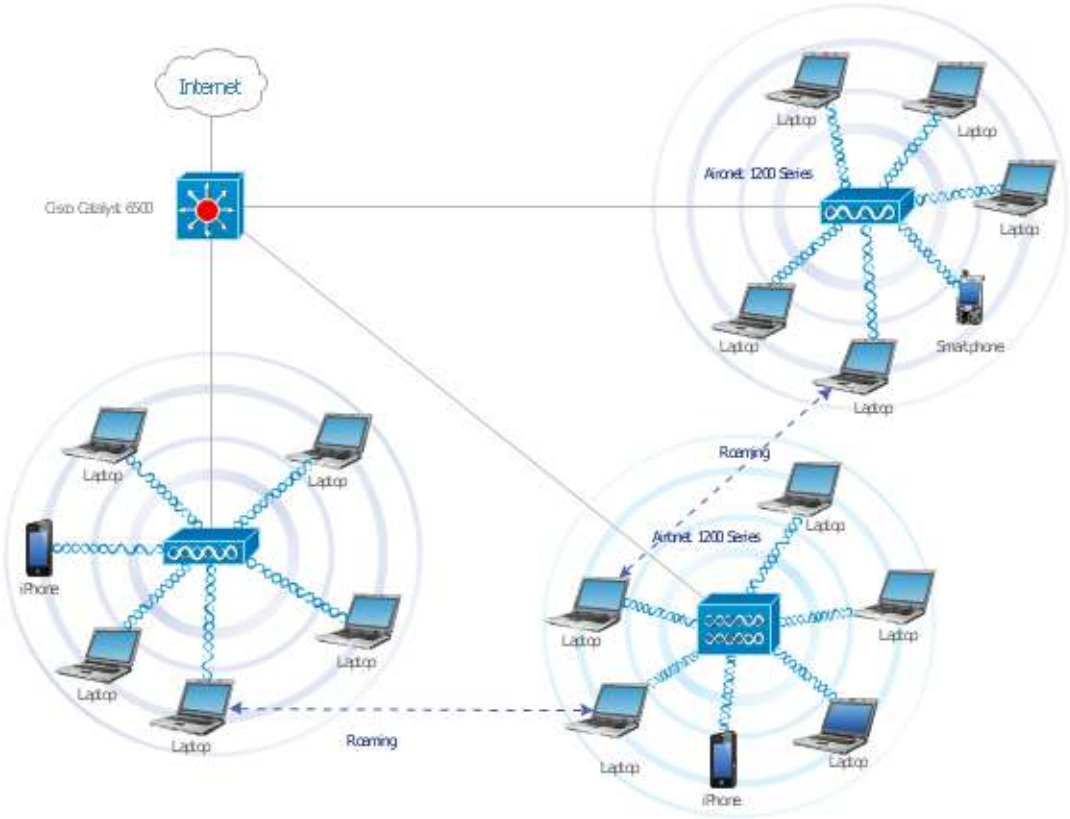
Router Logs – DHCP entries

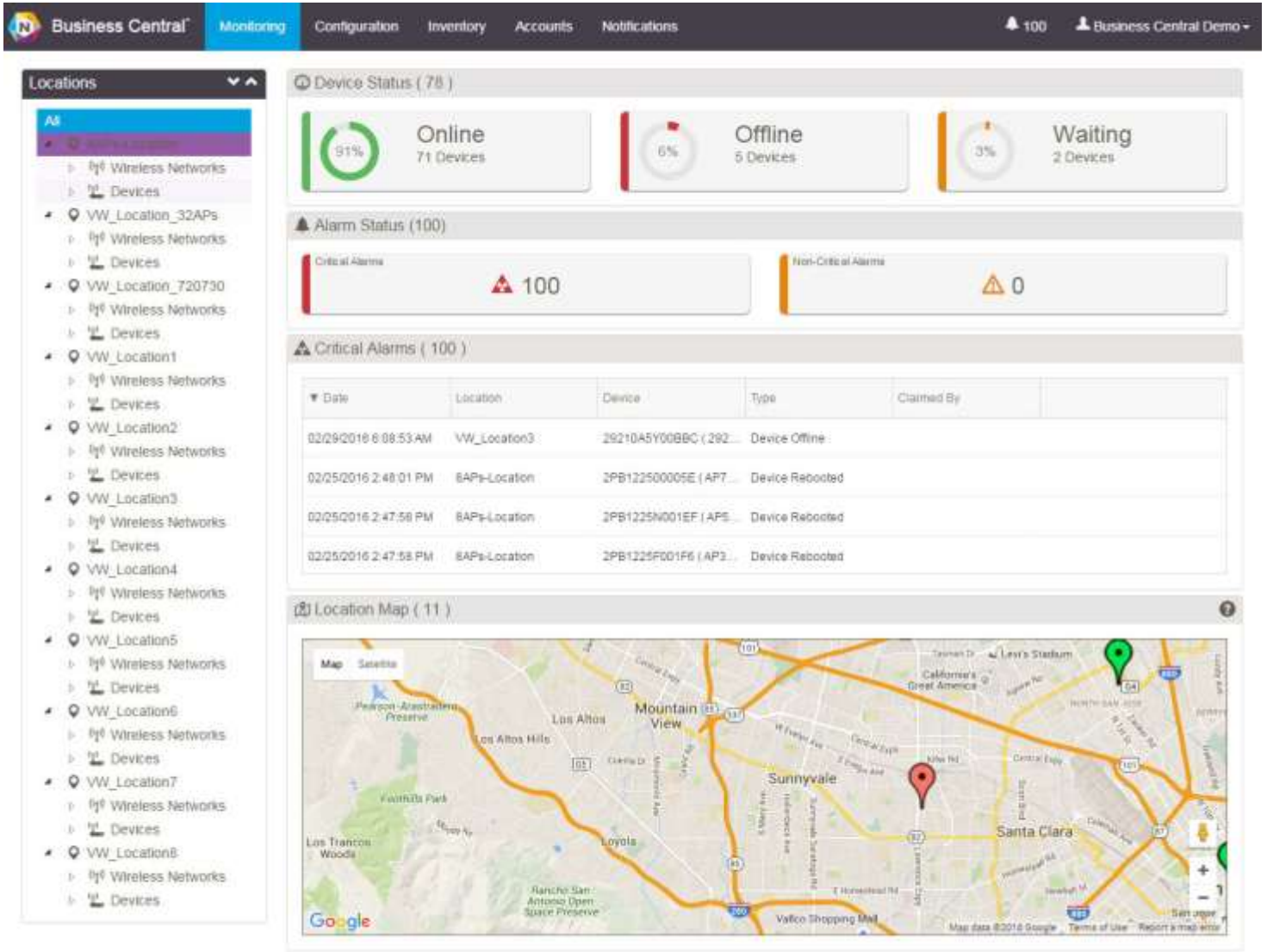


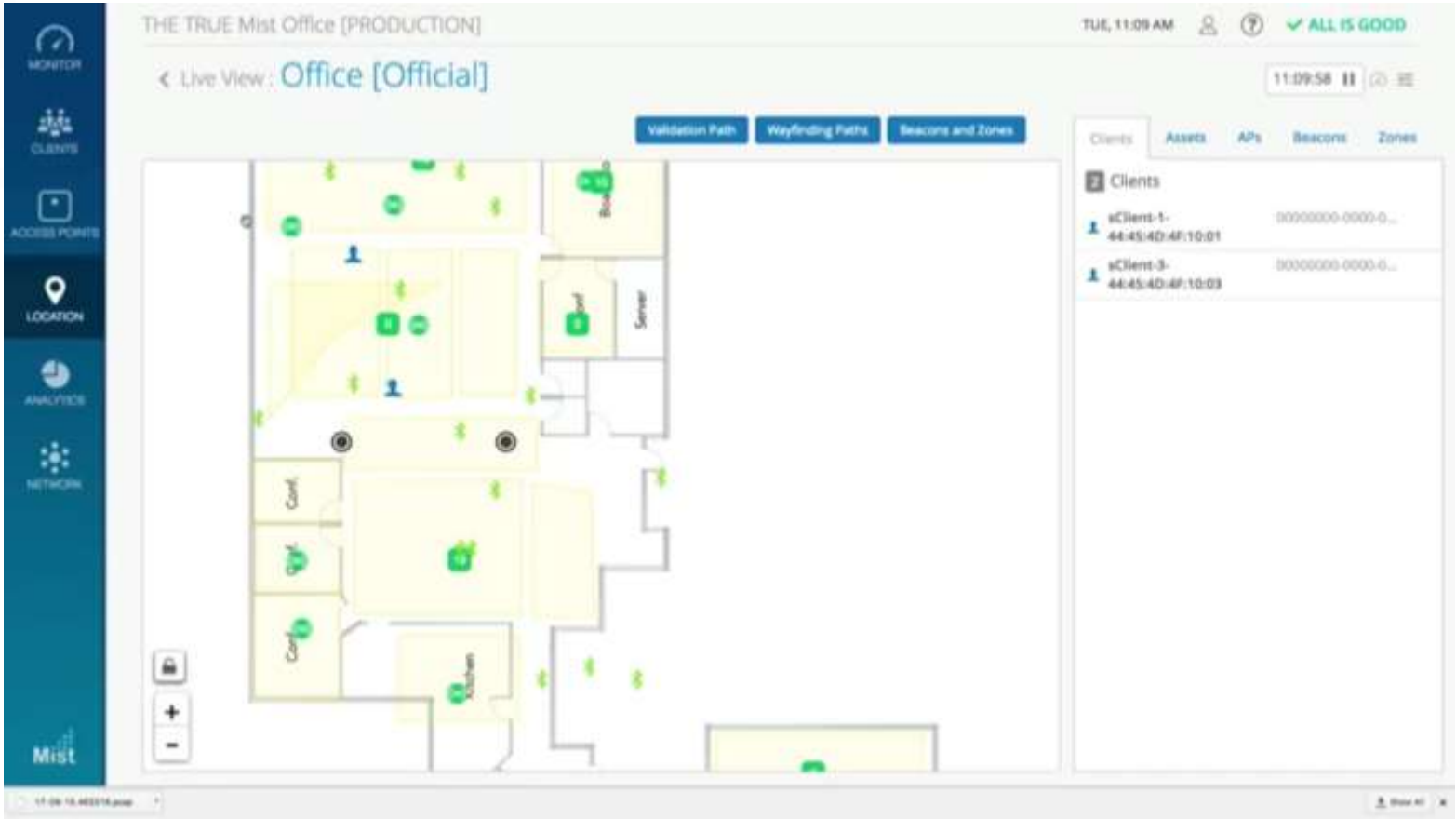
Windows also maintains DHCP logs at the following location:
C:\Windows\System32\winevt\Logs**Microsoft-Windows-Dhcp-Client%4Admin**



Access Points




Business Central
Monitoring
Configuration
Inventory
Accounts
Notifications
100
Business Central Demo
Locations
All
Wireless Networks
Devices
VW_Location_32APs
VW_Location_720730
VW_Location1
VW_Location2
VW_Location3
VW_Location4
VW_Location5
VW_Location6
VW_Location7
VW_Location8
Device Status (78)
91%
Online
71 Devices
6%
Offline
5 Devices
3%
Waiting
2 Devices
Alarm Status (100)
Critical Alarms
100
Non-Critical Alarms
0
Critical Alarms (100)
Date
Location
Device
Type
Claimed By
02/29/2016 6:08:53 AM
VW_Location3
29210A5Y00BBC (292...
Device Offline
02/25/2016 2:48:01 PM
6APs-Location
2PB122500005E (AP7...
Device Rebooted
02/25/2016 2:47:58 PM
6APs-Location
2PB1225N001EF (AP6...
Device Rebooted
02/25/2016 2:47:58 PM
6APs-Location
2PB1225F001F6 (AP3...
Device Rebooted
Location Map (11)
Map
Satellite
Mountain View
Los Altos
Los Altos Hills
Sunnyvale
Santa Clara
Levi's Stadium
Google


THE TRUE Mist Office [PRODUCTION]
TUE, 11:09 AM
ALL IS GOOD
Live View : Office [Official]
11:09:58
Validation Path
Wayfinding Paths
Beacons and Zones
Clients
Assets
APs
Beacons
Zones
2 Clients
sClient-1-
44:45:4D:4F:10:01
sClient-3-
44:45:4D:4F:10:03
MONITOR
CLIENTS
ACCESS POINTS
LOCATION
ANALYTICS
NETWORK
Mist
Server
Conf.
Kitchen

Data

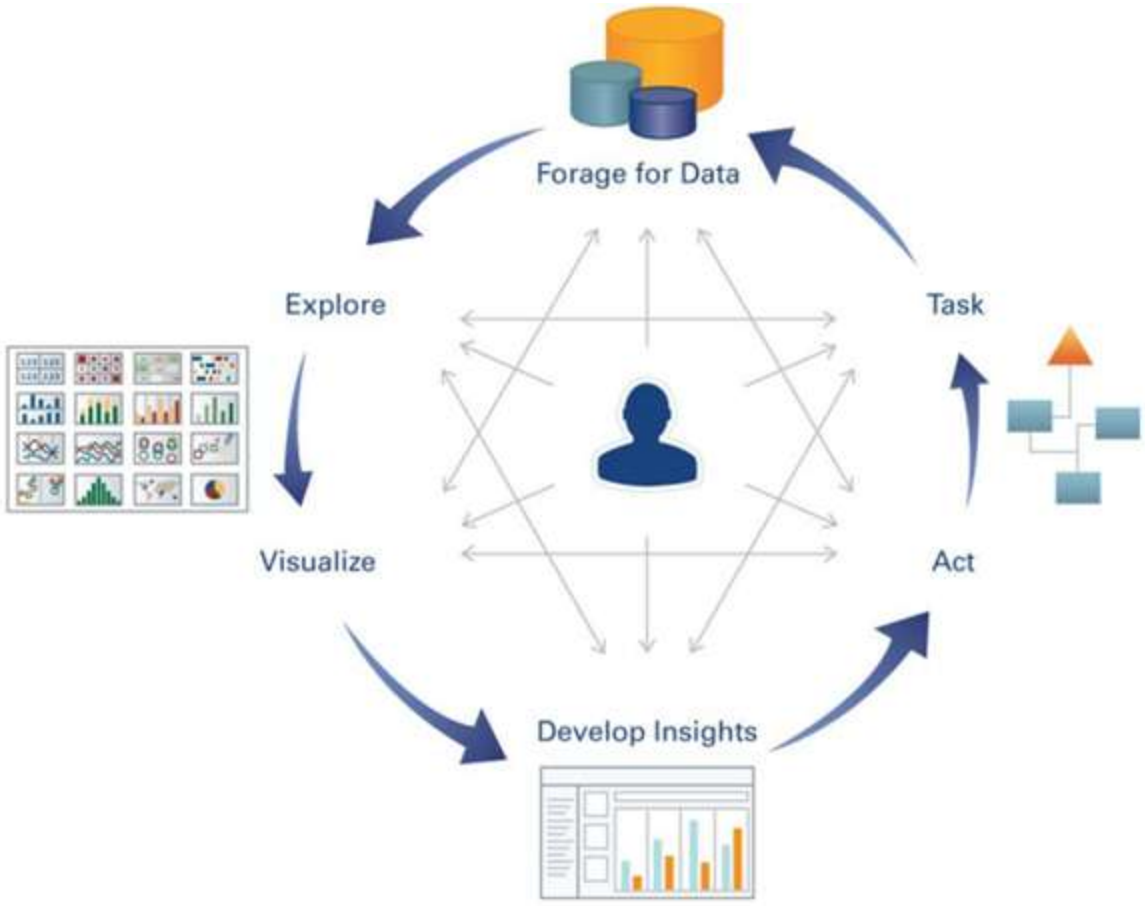
Data

- Data Discovery
- Data Classification
- Access Control
- Data Loss Prevention (DLP)
- Encryption
- Backup

Data Discovery

Data discovery is the collection and analysis of data from various sources to gain insight from hidden patterns and trends. It is the first step in fully harnessing an organization's data to inform critical decisions.

Data Discovery



Data Classification

Data classification in information security services involve **classifying data** into various groups based on its sensitivity.

Data Classification Scheme

Public	Internal Only	Confidential	Restricted
Data that may be freely disclosed to the public For example: marketing materials, contact information, price lists, etc.	**Internal data not meant for public disclosure** For example: battlecards, sales playbooks, organizational charts, etc.	**Sensitive data that if compromised could negatively affect operations** For example: contracts with vendors, employee reviews, etc.	**Highly sensitive corporate and customer data that if compromised could put the organization at financial or legal risk** For example: IP, credit card information, social security numbers, PHI)

Access Control

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control:

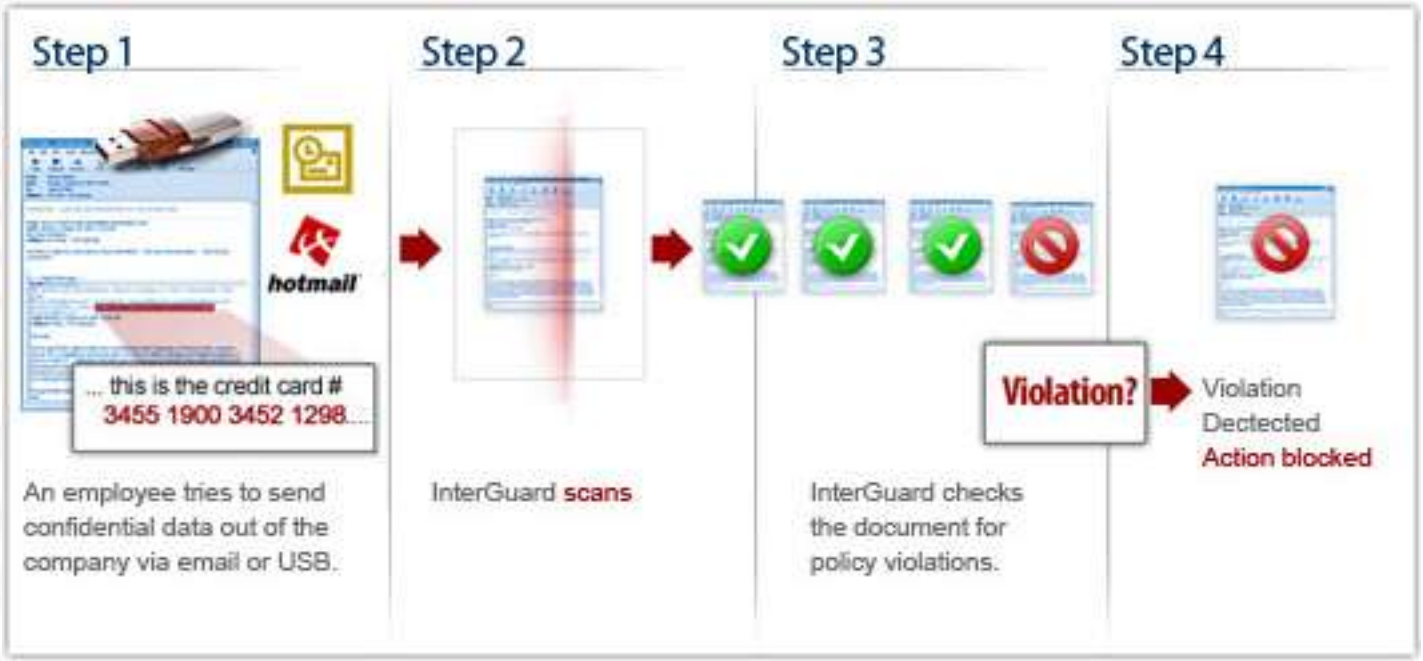
- Physical
- Logical

Access Control

Data Loss/Leak Prevention

Data loss prevention (**DLP**) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

How DLP works?



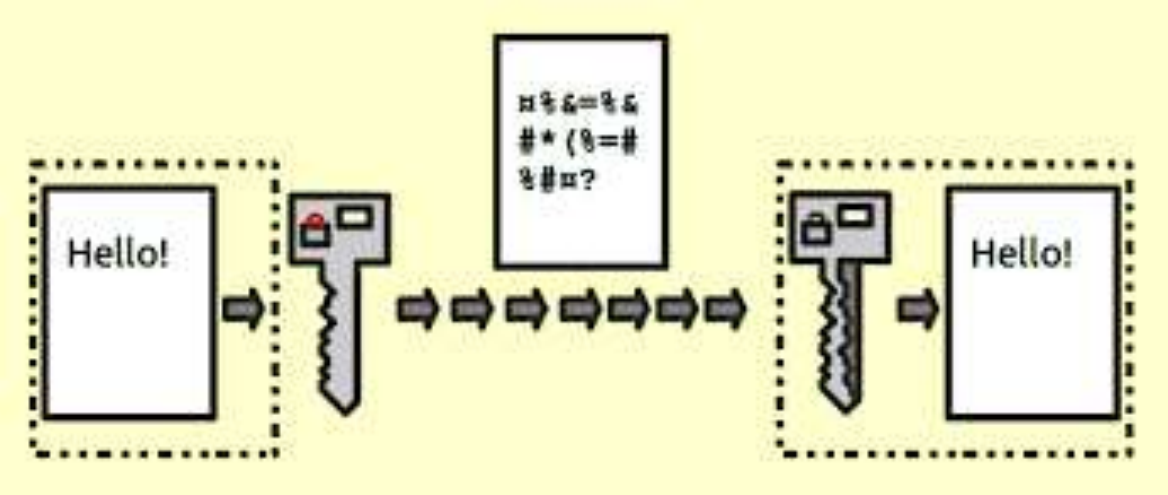
DLP tool: InterGuard

DLP Tools

Symantec Data Loss Prevention
Empulse
McAfee DLP Endpoint
My Endpoint Protector
Forcepoint DLP
Curtain e-locker

Data Encryption

In cryptography, **encryption** is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.



What-If

- Your official pendrive is stolen
- Your official laptop is stolen
- Your official mobile is stolen

Use Data Encryption Tools in advance

- EncryptRight
- Bitlocker
- VeraCrypt

Encryption for e-mails?

- Enigmail for Mozilla Thunderbird

- OpenPGP for Microsoft Outlook

Application Security

Application Security

- Application Development Standards
- Secure Coding
- Application Vulnerability Testing

Application Testing

How is it Performed?

Step #1 It starts with a list of Vulnerabilities/potential problem areas that would cause a security breach for the system.

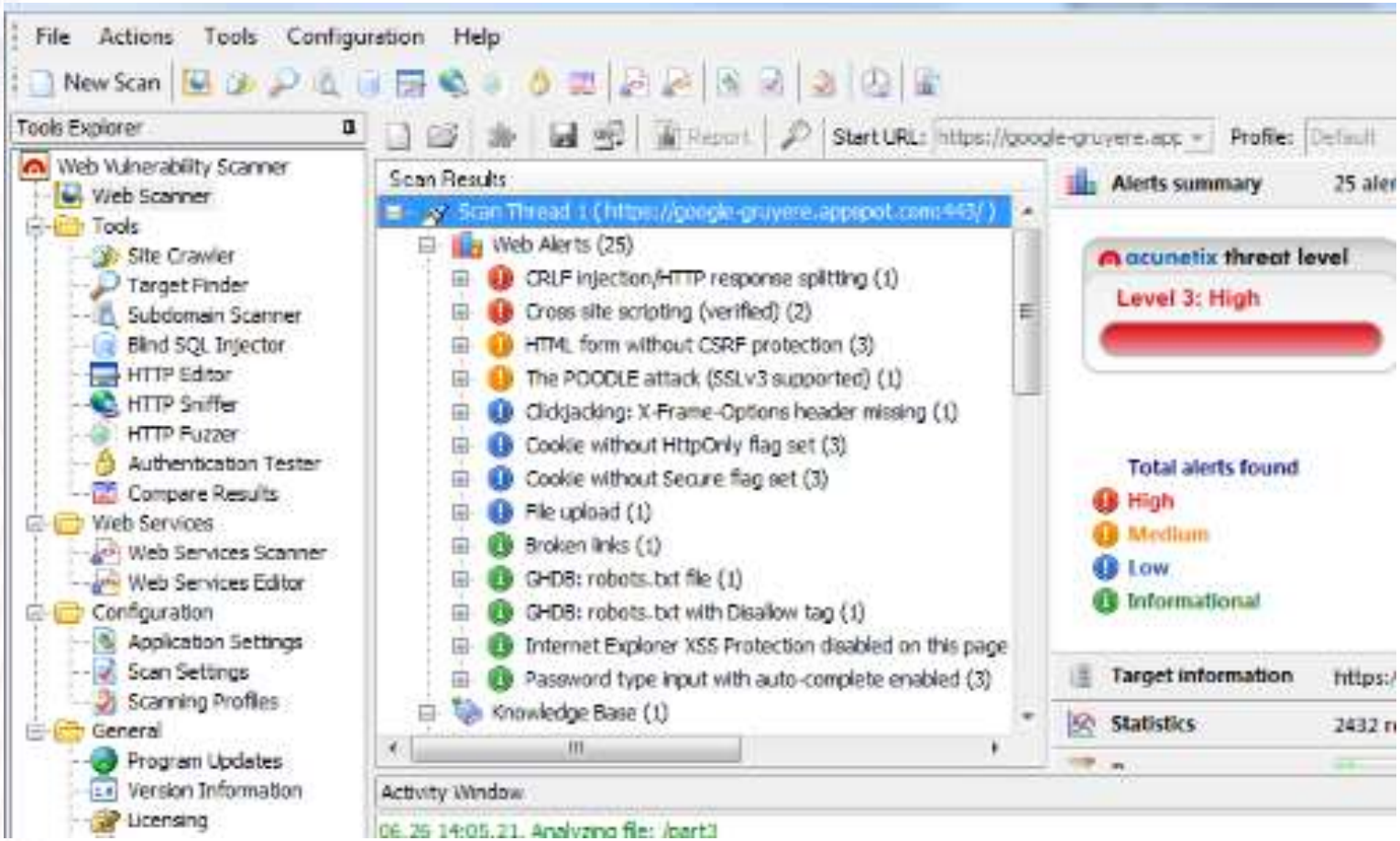
Step #2 If possible, this list of items is ranked in the order of priority/criticality.

Step #3 Devise penetration tests that would work (attack your system) from both within the network and outside (externally) are done to determine if you can access data/network/server/website unauthorized.

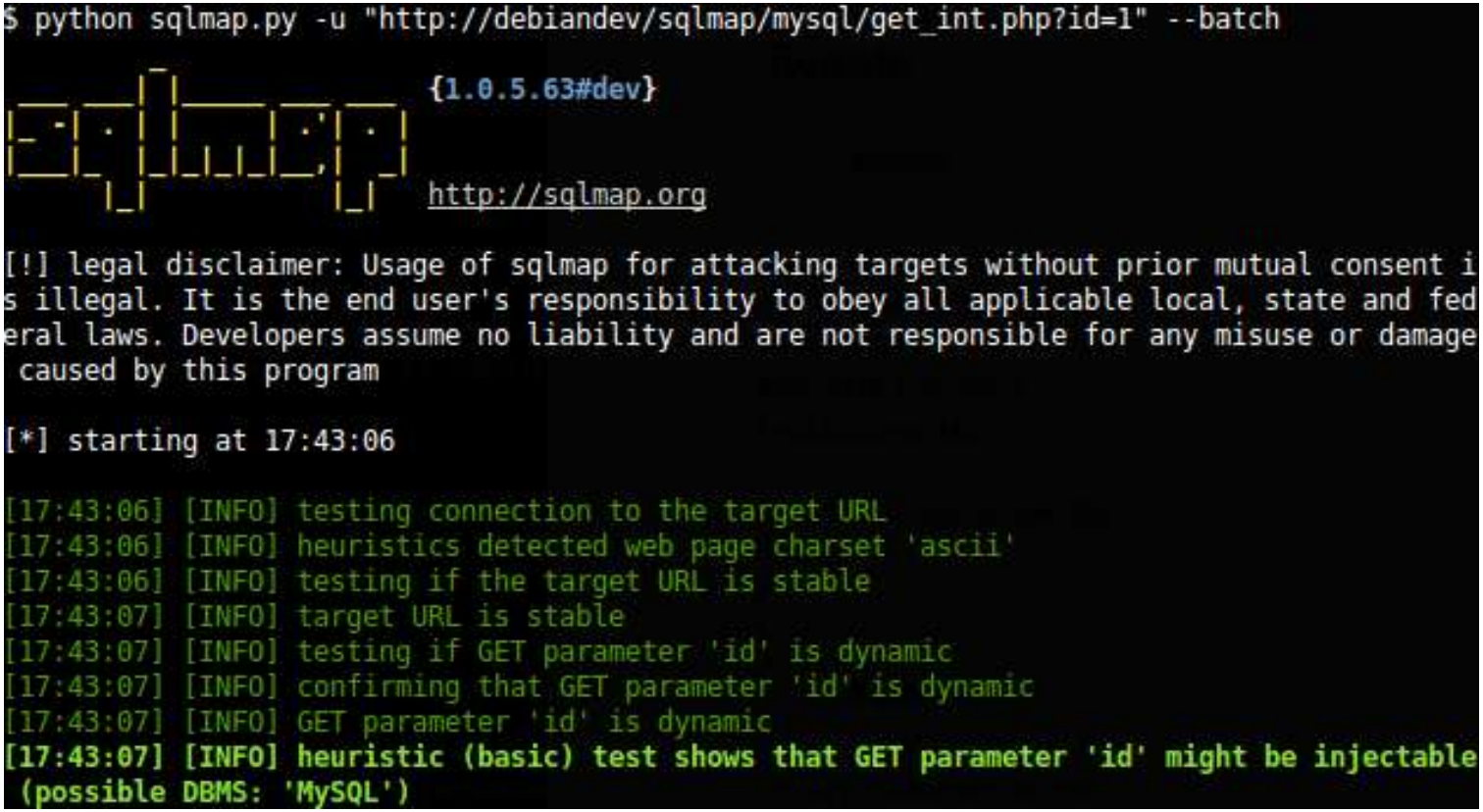
Step #4 If unauthorized access is possible, then the system has to be corrected and the series of steps need to be re-run until the problem area is fixed.

Tools for Testing Applications

- SQL based applications
  - SQLMap
  - Havij
- Fully Automated Web Apps Vulnerability Scanners
  - Vega
  - Acunetix
  - Nessus



Acunetix Vulnerability Scanner


$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
{1.0.5.63#dev}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent i
s illegal. It is the end user's responsibility to obey all applicable local, state and fed
eral laws. Developers assume no liability and are not responsible for any misuse or damage
caused by this program
[*] starting at 17:43:06
[17:43:06] [INFO] testing connection to the target URL
[17:43:06] [INFO] heuristics detected web page charset 'ascii'
[17:43:06] [INFO] testing if the target URL is stable
[17:43:07] [INFO] target URL is stable
[17:43:07] [INFO] testing if GET parameter 'id' is dynamic
[17:43:07] [INFO] confirming that GET parameter 'id' is dynamic
[17:43:07] [INFO] GET parameter 'id' is dynamic
[17:43:07] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
(possible DBMS: 'MySQL')

SQLMap

Securing the Network

What data can your Internet Service Provider see?

Tools of the Trade

Wireshark 

and

NetworkMiner 

How to Define your Network perimeter?

1. Any network owner is required to know the full layout of the enterprise network. But if every node is the perimeter itself, then the layout of the network is less of an issue with regard to the perimeter boundaries.

2. Because the network has become extremely dynamic, you must ensure a vigilant exploration of this ever-changing network. Scanning and assessment must be continuous and ensure that you can identify misuse and abuse of the network and its IT resources.

3. The key to successfully defining the network perimeter is a combination of automated network tools and the ability to globally enforce host-based security software deployed to the mobile systems that you know access the network.

4. Scanning and the discovering of unknown devices also must be considered because by definition, these unknown entities may constitute a perimeter breach.

Securing the National Digital Infrastructure

A Four Step Process

Step 1: Map all the critical National digital (and sometimes non-digital) assets with regard to the threat vectors.

This might include security procedures, data stores, network architecture, physical offices, central servers, portable devices.

Step 2: Conduct a detailed/comprehensive national level threat landscape survey

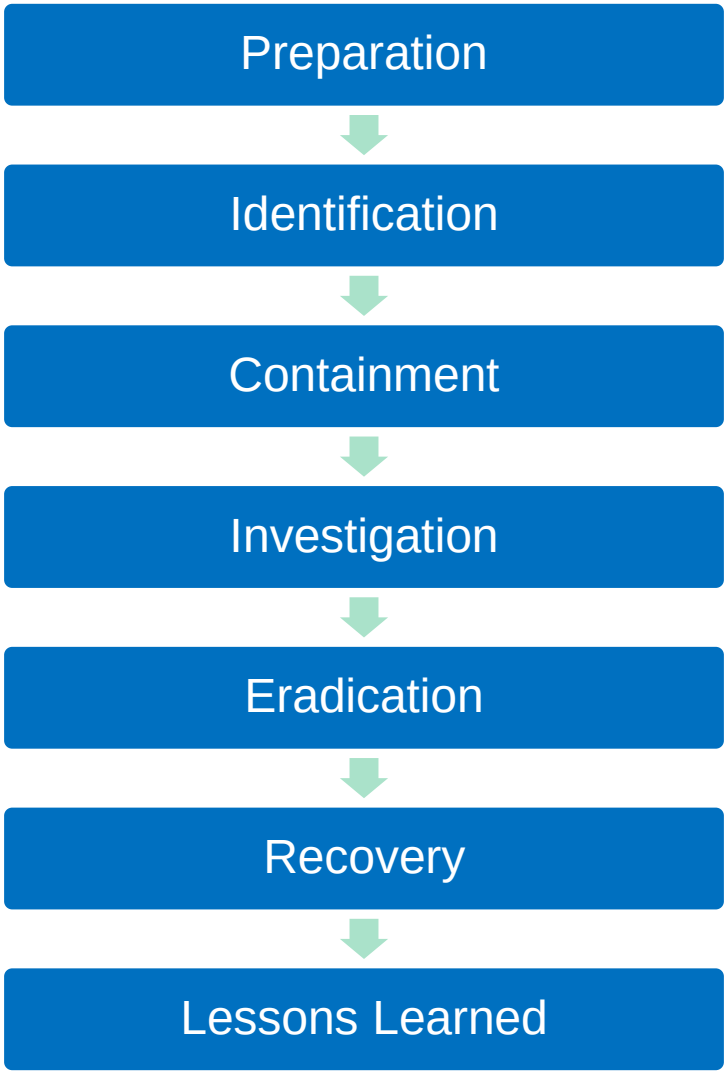
This analysis will help create a coherent risk map that enables controls, and security measures to be put into place in an intelligent manner while taking into consideration the true nature of the exposure.

Step 3: **Identify all the contours/perimeters of defense/attack**

This analysis should cover all the users, devices, applications, servers,
network, and data center (hardware and software).

Step 4: **Define**, **Provision and Enforce Policies and relevant security technologies** for each of the assets in the contours in relation to the cyber threats.

The Process


Preparation
Identification
Containment
Investigation
Eradication
Recovery
Lessons Learned

Preparation

- Bootable USB or Live CD (up to date tools, anti malware, static linked binaries)
- Laptop with forensic tools (EnCase/FTK), anti malware utilities, internet access
- Computer and network toolkits (components, network cables, network switches, network hubs, network taps, hard drives etc.)
- Drive duplicators with write blocking (for forensically sound images)

Identification

These include but are not limited to:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

- Review system logs, error messages, firewall alerts, IPS alerts, Antivirus alerts etc.

- If it is an incident, report it as soon as possible so that the incident response team can start collecting evidence

Containment

•Limit and prevent any further damage from occurring

•Image systems to preserve evidence
- Take a forensic image of the systems in question
- Use known forensic tools (FTK, EnCase etc.)

•Limit the incident E.g. Isolating network segment, removing servers etc.

Eradication

- ❑ Ensure that proper measures have been taken to remove malicious content from the affected systems
- ❑ A complete reimage, or restore from a known good/clean backup
- ❑ Improve the defences of the system to ensure that it will not be compromised again (e.g. patching to remove a vulnerability etc.)

Recovery

- Bring the system back in to normal use

- Key decisions (including, but not limited to)
  - How to test and verify the system is clean and fully functional
  - What tools to use to test, monitor and validate the system behaviour
  - How long to monitor for signs of abnormal activities

- When to restore the system (system owners to make decision based upon advice of the CERT team

Responding to Security Incidents

- Preserving Digital evidence that can be used to track and identify and intruder

- Identifying perpetrators after a cyber incident to help determine the appropriate Governmental response (eg. Prosecution)

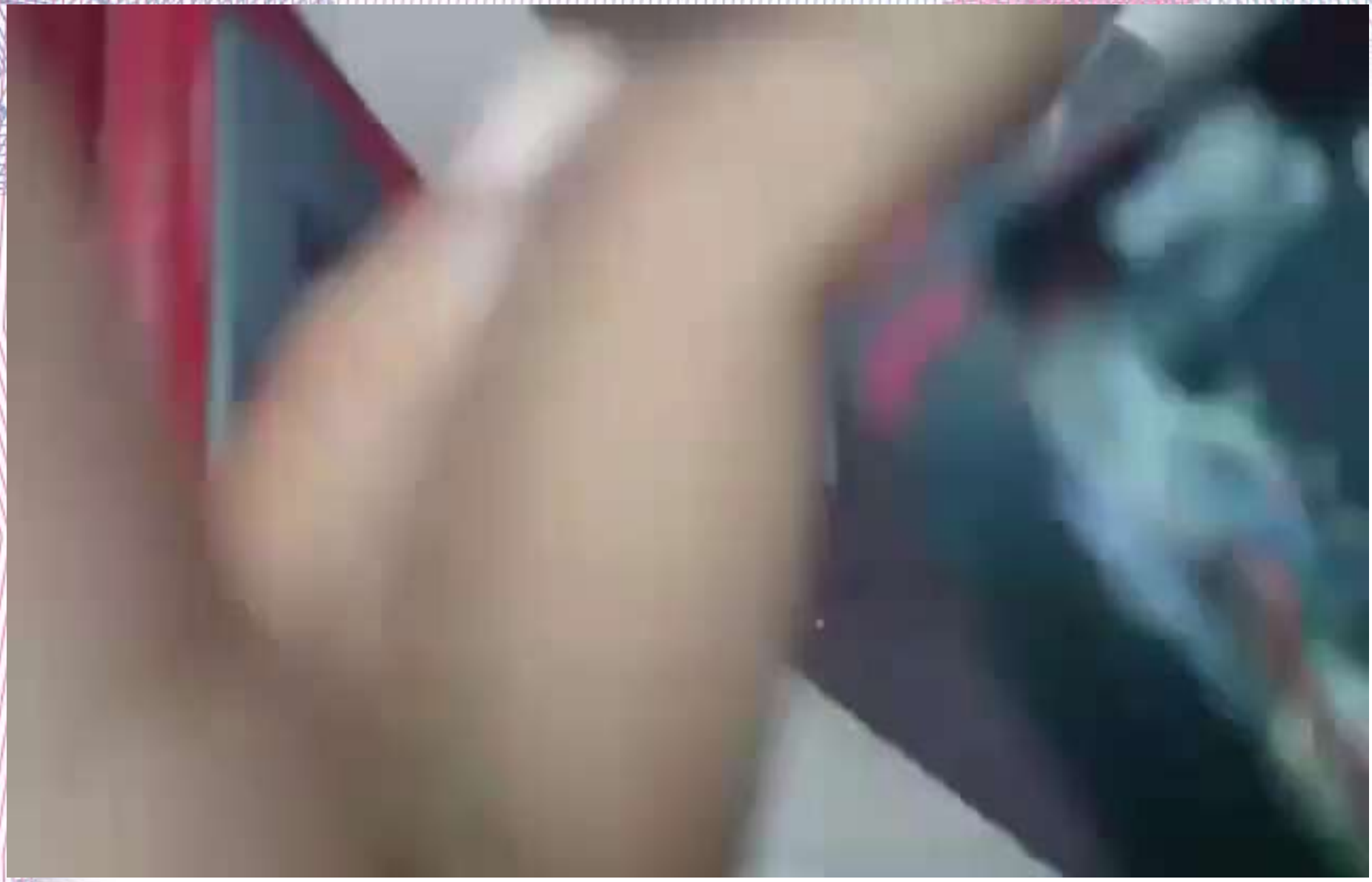
Preventing future security incidents

•Prosecuting computer intrusion cases to discourage would-be intruders

•Training prosecutors and investigators

•Co-ordinating with companies to improve their security and intrusion detection capabilities.


Know When to
Stop.

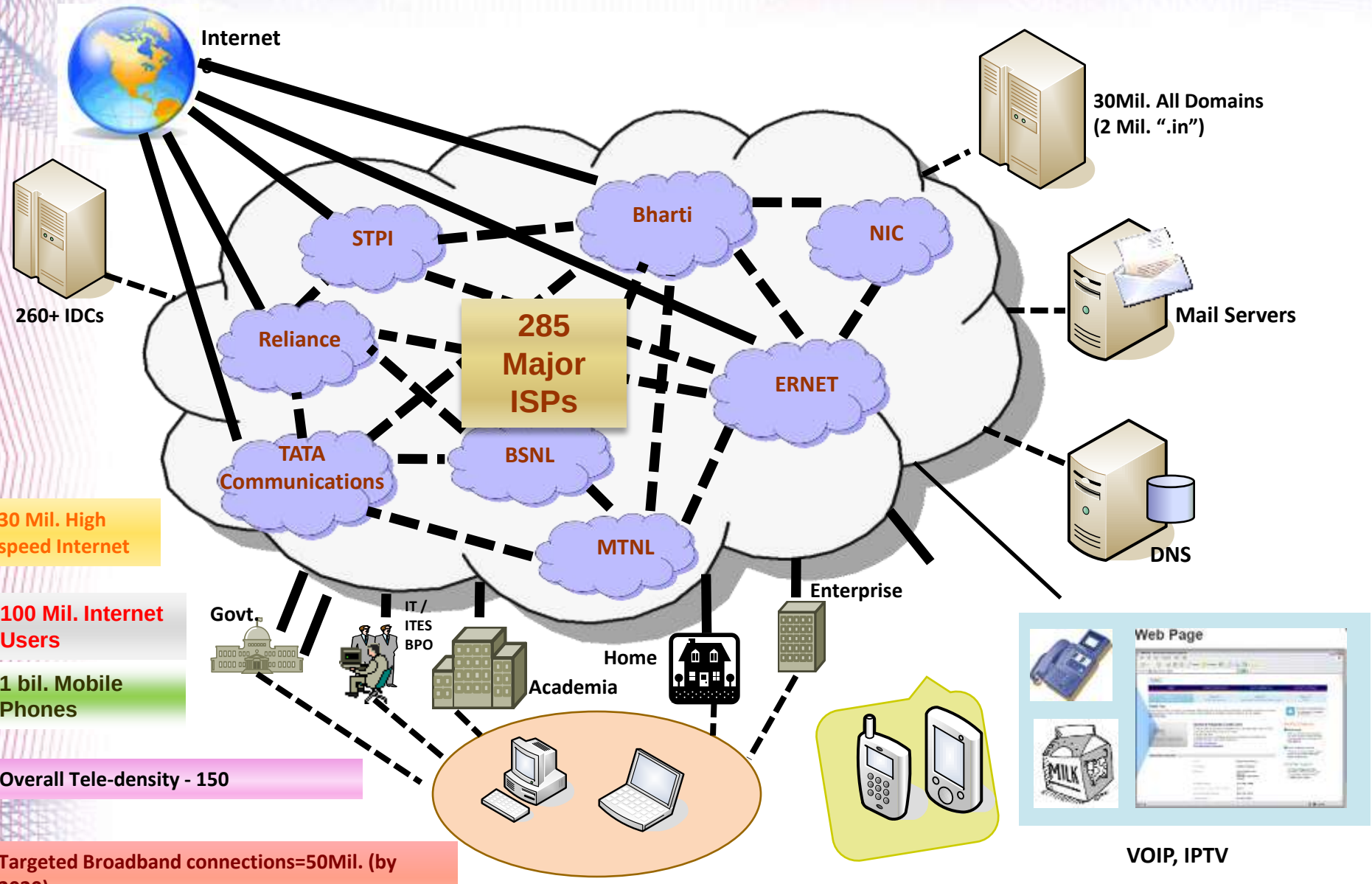


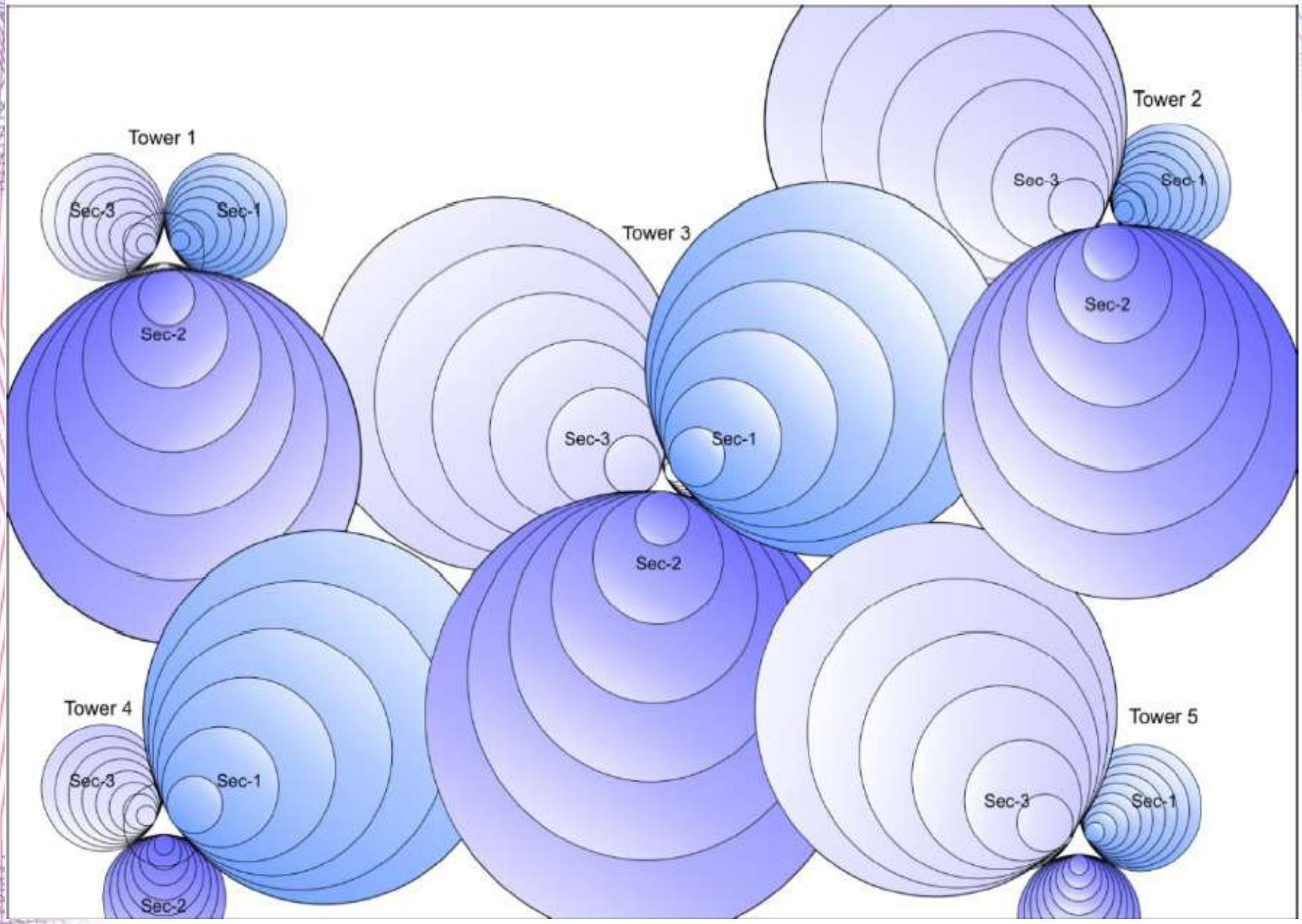

24-06-2017 22:52:27

- VISHING
- PHISHING
- SMISHING
- SKIMMING
- BUGGING
- STEALING ONLINE CREDENTIALS FROM INMATES
- COLLECTING CREDENTIALS FROM ONLINE SITES
- E MAIL SPOOFING/ HACKING

- Mobile
- ATM images and CCTV clippings
- Bank AC details/KYC
- E-Mails
- Websites
- Payment Gateways
- Bank server details
- Online Investigation
- LR based investigation

INDIA Internet Infrastructure:2016




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

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.


POLICE COMMISSIONERATE

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

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.

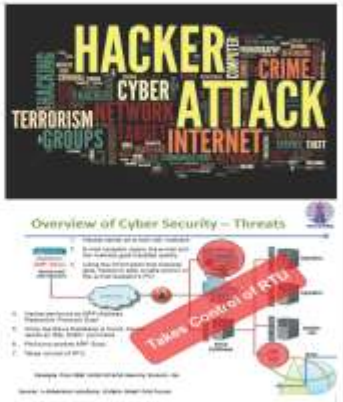
SECTION - 72 DISCLOSURE OF INFORMATION

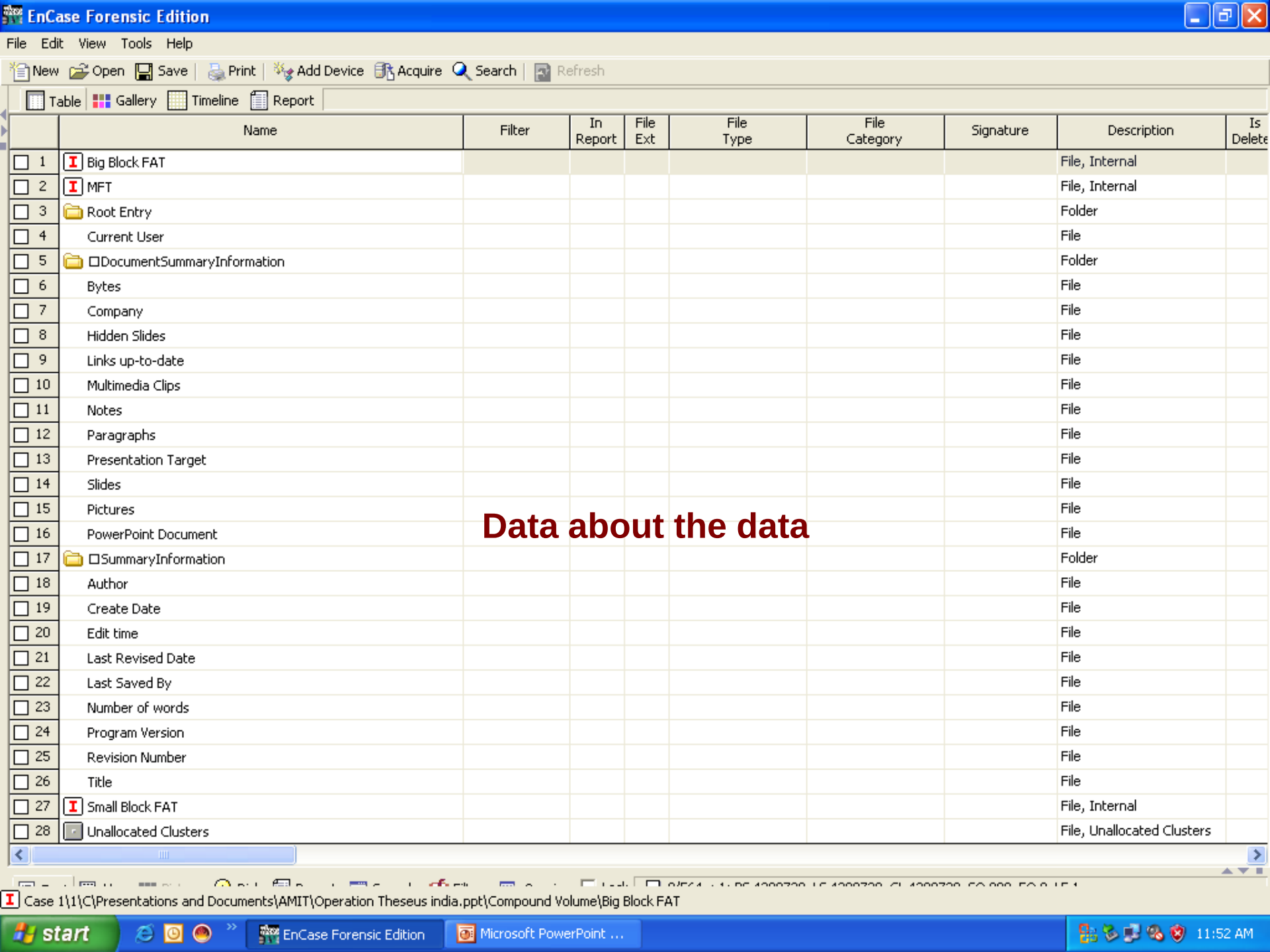
PUNISHABLE WITH IMPRISONMENT UPTO 2 YEARS,

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




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

Traditionally All Records Paper Based Found in Files, Desks etc.

Records Are Likely to be on A Computer

On a Computer the Volume of Information Can be Very High

100000x 4 Drawer Filing Cabinets Full of Documents

Definition of the Science of Computer Forensics

Computer forensics is the scientific examination and analysis of data held on or retrieved from computer storage media for the purposes of presentation in a court of law, together with the study of the legal aspects of computer use and misuse

- The secure collection of computer data
- The examination of data to determine details
- The collation and presentation of information about computer data and computer systems to courts of law
- The application of a country’s laws to computer practice

Why is computer forensics necessary?

- Data can be altered or lost as soon as the computer is booted
- Evidential integrity must not be compromised

- Special procedures, techniques and tools are required to ensure that any information that is retrieved can be presented as evidence in a court

A Legal/Forensic Problem

- **Rules of Evidence**
- **Legal Processes**
- **Computer Law**
- **Forensic Principles**

What is Computer Crime?

A criminal act in which a computer is essential to the crime.

Examples:

Credit card fraud, electronic funds transfer, distribution of pornography via the Internet, hacking, virus writing etc.

A criminal act where a computer, non-essential to perpetration of the crime, acts as a store of information, concerning the crime.

Examples:

Murder, Fraud, Terrorism, Theft, Forgery, Rape etc.

Investigator-Forensic Analyst Relationship

- A confidential partnership involving exchange of relevant information
- Investigator advises on the nature of the case and the information/evidence sought
- Forensic analyst advises on computer aspects and interprets computer based evidence
- Both collaborate to present case in court

Forensic Objectives and Principles

The Forensic Objective

The objective of the computer forensic investigator is to analyze the contents of a computer in such a way that any information obtained is suitable and acceptable for use as evidence in a court of law

The Two Most Important Concepts in the Field of Computer Forensics

Evidential Integrity

Evidential Continuity

Key Concepts

- Evidential Integrity
  - Nothing must be changed on the original
  - Proof of integrity must be available
- Evidential Continuity
  - Must be able to account for all actions at all times involving any and all suspect materials
  - Must maintain accurate handling, record keeping and reporting

The Three Computer Forensic Tasks

- Collection of Data
- Analysis of Data
- Presentation of Data

Collection of Data

- Everything on the hard drive *must* be copied
- The original copy *must not* be altered in any way

We must prove to the court, beyond doubt, that we have conducted our work according to these principles

Analysis of Data

1. Accuracy vs. Speed

We never sacrifice accuracy for speed

2. Volume of Data

The average computer can contain 50,000+ files

The Forensic Priority

ACCURACY

Doing things EFFICIENTLY:

that is as fast as possible without sacrificing accuracy

Presentation of Data

- Evidence must be presented in a way that the court can accept and understand
- We must do this with due regard to any legal requirements and within the budget

General Computing Principles

Hardware

- *It is the ‘hard’ equipment*

Software

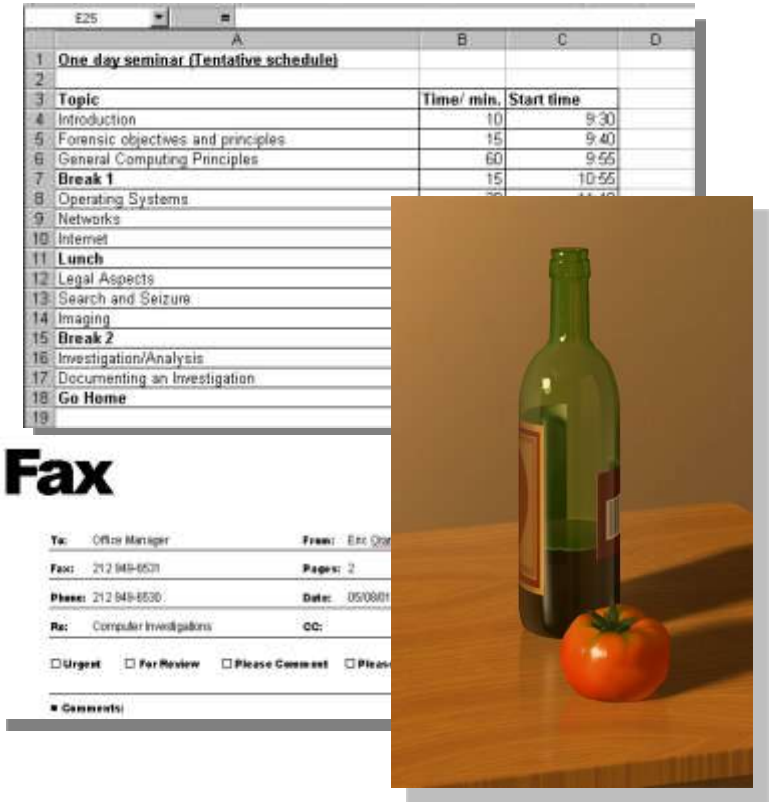
- *Software is intangible*

Information exists on the computer in the form of data.

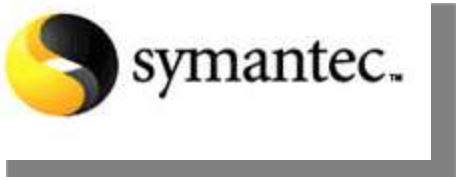
Data is processed by the computer to produce items such as letters, images or spreadsheets

001010110101
0100111101011
011101000100
1101 10

Processor



Other useful information exists on the computer in the form of sets of instructions or programs which are used to manipulate data



Sometimes the presence of a certain type of software can be used as evidence e.g. credit card fraud, currency/document forgery

From a forensic viewpoint we are interested in the parts of the computer that store information.

- Hard Disks
- Floppy Disks
- CD's/DVD's
- Memory Cards

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.

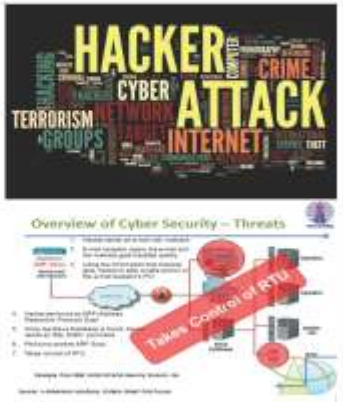
SECTION - 72 DISCLOSURE OF INFORMATION

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

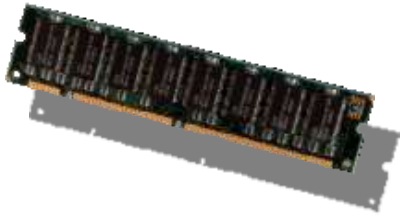
PUNISHABLE WITH IMPRISONMENT WHICH MAY EXTEND TO LIFE



Three Common Types of Storage

Magnetic

Silicon



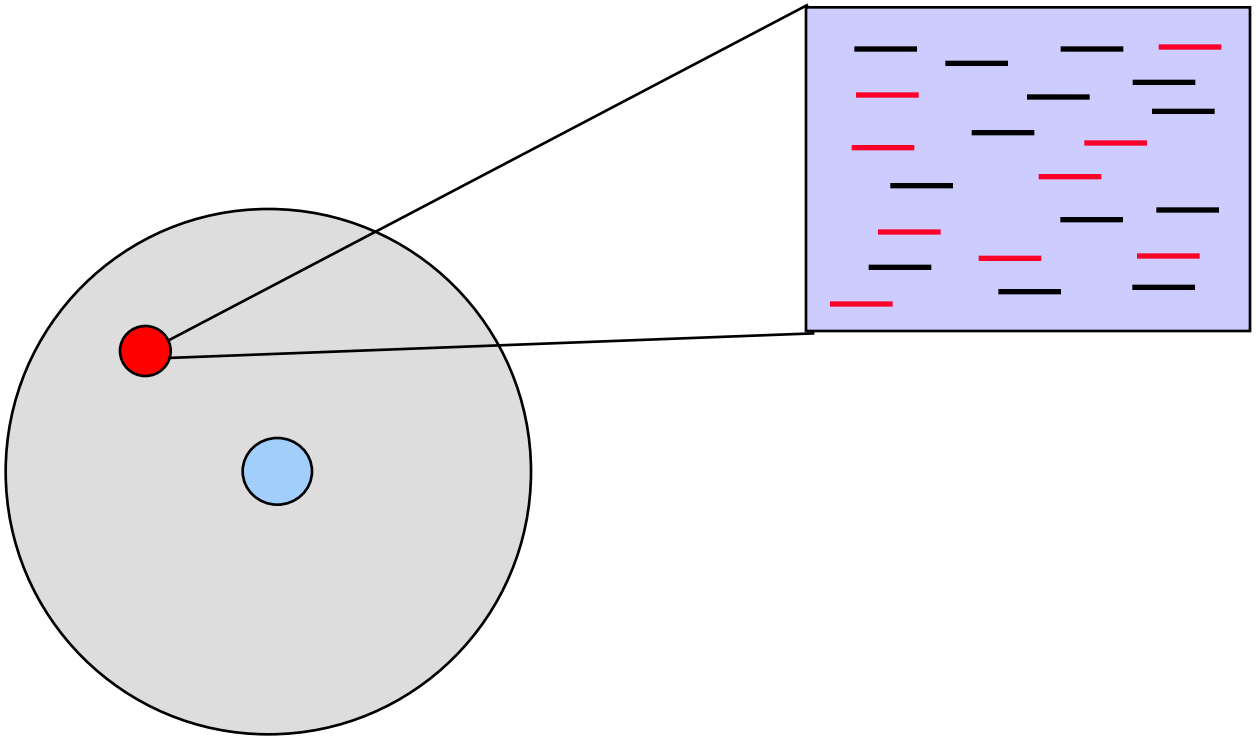
Optical

Magnetic Storage

- Data is recorded as a series of disturbances on an otherwise uniform magnetic surface
- Magnetic particles are arranged in a pattern
- The orientation of the particles can be altered by the application of an electric current
- This pattern of particles can be read and interpreted as data

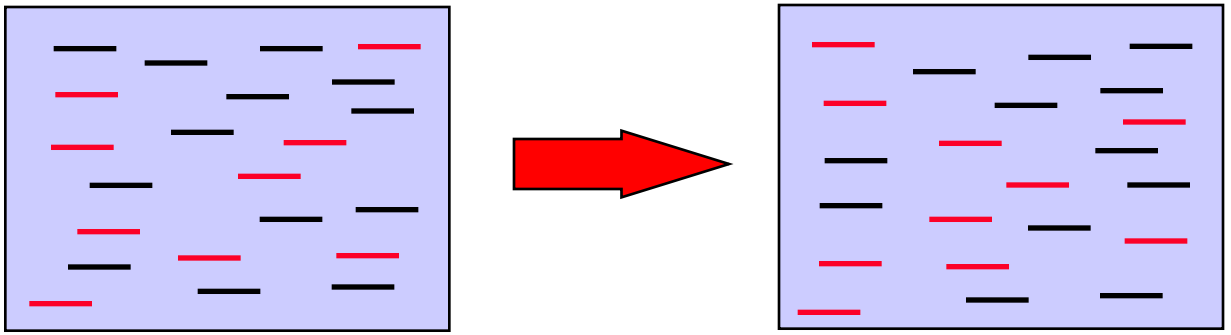
Magnetic Storage – Hard Disks

Information Stored as a Pattern of Magnetic Particles



Magnetic Storage – Hard Disks

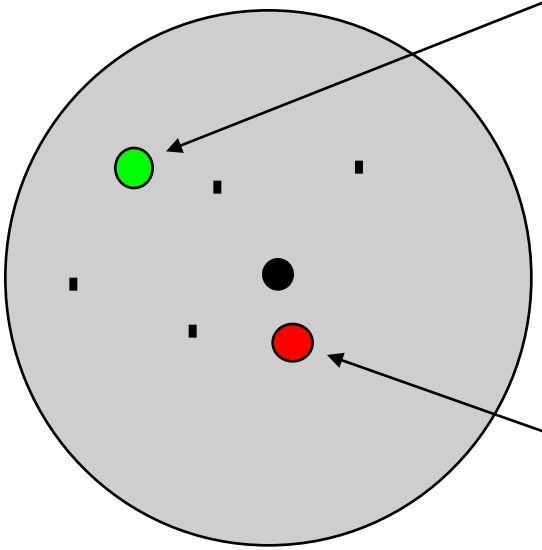
When Computer Turned on Pattern Can Change



Change Irreversible and Undetectable

Magnetic Storage – Hard Disks

If Change Occurs Evidential Integrity is Compromised



This is a log file and it has changed during the boot procedure

If the log file has changed how can you prove that the evidence contained in this file has not also changed?

Hard Drives

- The disk is made of aluminum, or some other non-magnetic material
- It has a fine magnetic coating to increase the amount of storage
- Usually there is more than one disk within a hard disk drive
- The disks are stacked co-axially one upon the other with a spacer in-between and each side of each disk has a reader/writer head which records and retrieves information from the surface

Typical Hard Drive Construction

Read/Write head

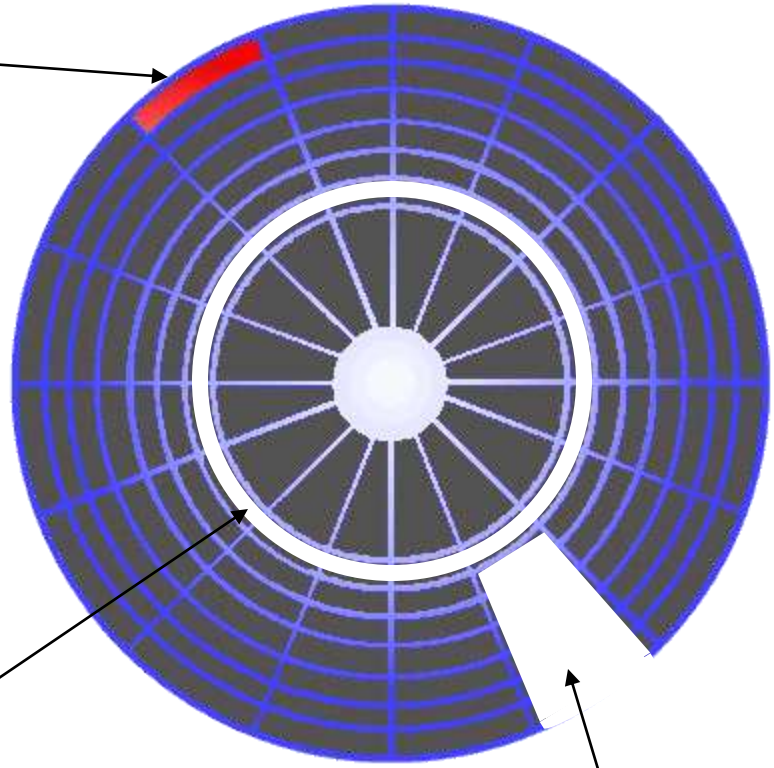
Platters

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

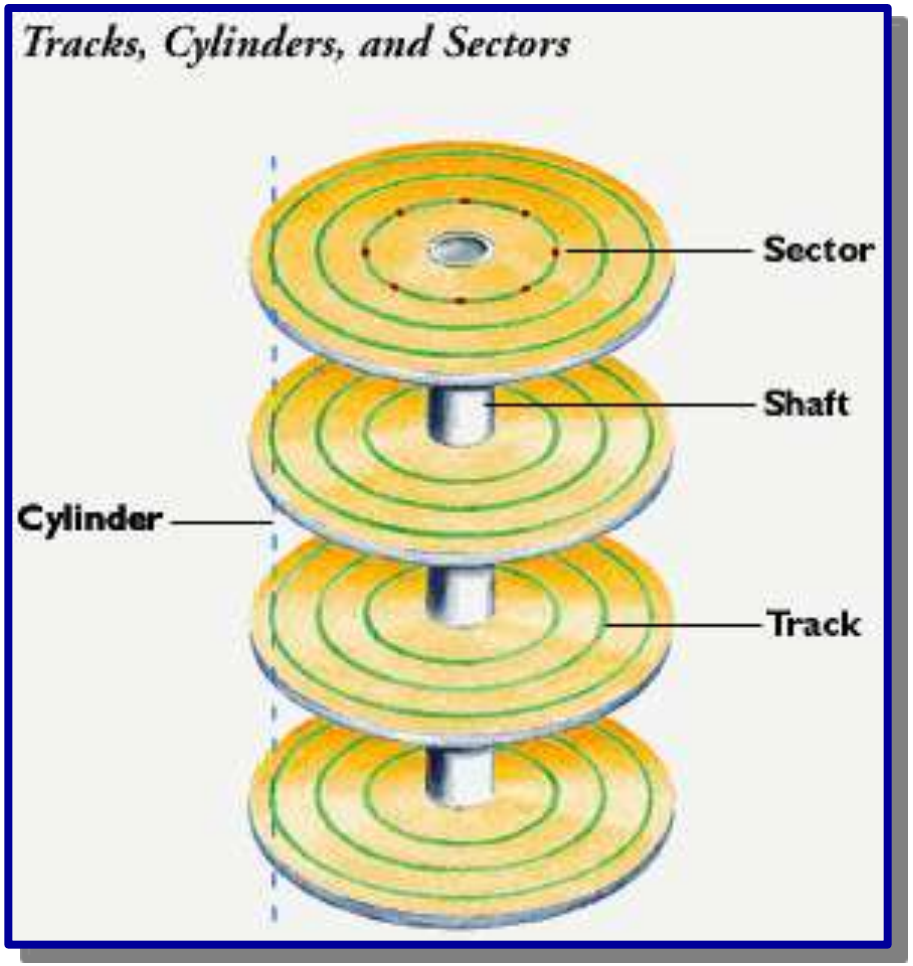
The disk is therefore divided into:



Tracks

Sectors

Accessing Information on a Hard Drive

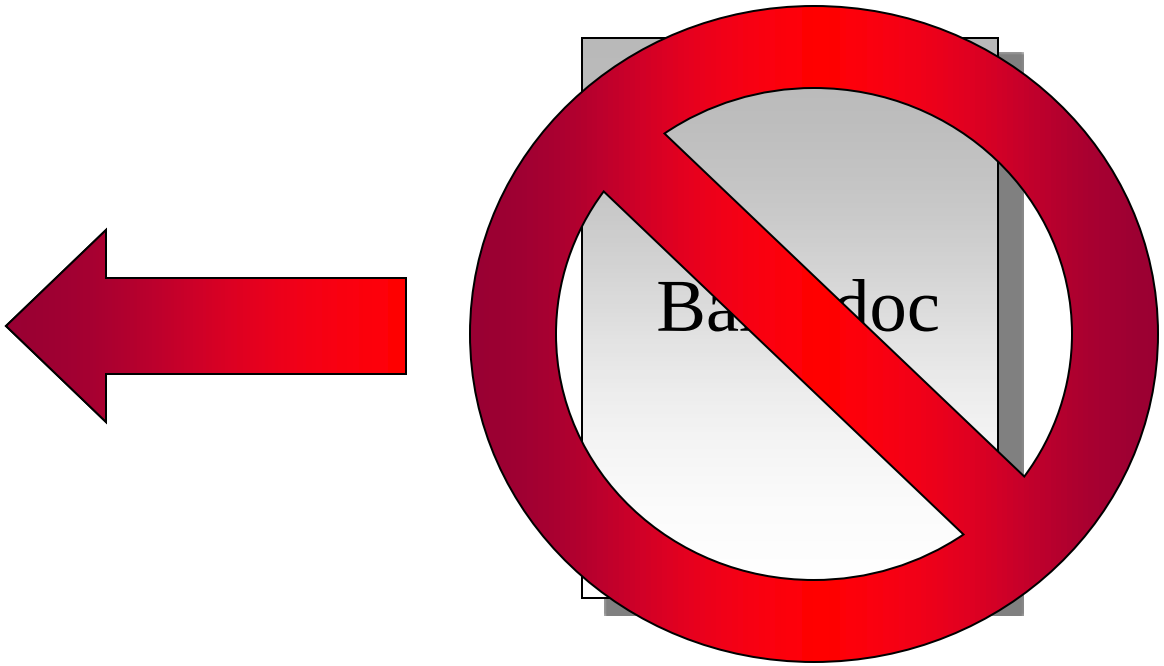


Deleted Files

- **Deleted files are not erased by the operating system**
- **The first character in the reference in the FAT is written over**
- **The cluster is marked as being available for use by another file**
- **As long as another file is not written to the cluster the information remains**

File Deletion

Cluster



σank.doc

Slack Space

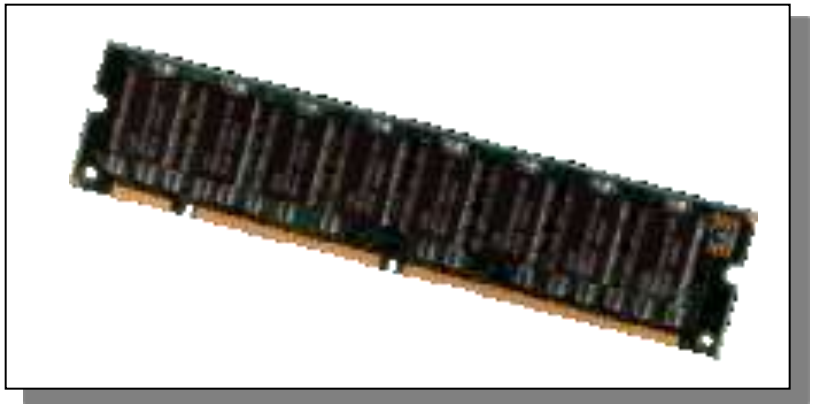
1. Slack space is the unused space remaining in a cluster when the rest of the space is occupied by a file
2. Slack space can contain the remains of previous files that occupied the cluster
3. The contents of slack space cannot be overwritten as long as the cluster they occupy is owned by a file
4. Will generally predate the creation date of the file whose slack space it is in, and must predate the date of last access
5. Slack space can be very important for the preservation of evidence

Silicon Storage

- Electronic form of storage
- Electrically dependent
- Many times faster than magnetic storage
- RAM and ROM

Random Access Memory

- **RAM works only while the PC is turned on.**
- **Fast, short-term storage**
- **Temporary files swap between the hard drive and RAM.**



Temporary Files

- The more memory available the faster and more efficient the system will operate
- As the memory stack fills up the operating system will transfer information to the hard drive
- When the information is needed again it is transfered back to the stack and the clusters it occupied on the disk are marked as being available for use
- Clusters that have been occupied by temporary files can contain evidential material

Read Only Memory

- CMOS- Complementary Metal Oxide Semiconductor
- BIOS- Basic Input Output System
- POST- Power On Self Test

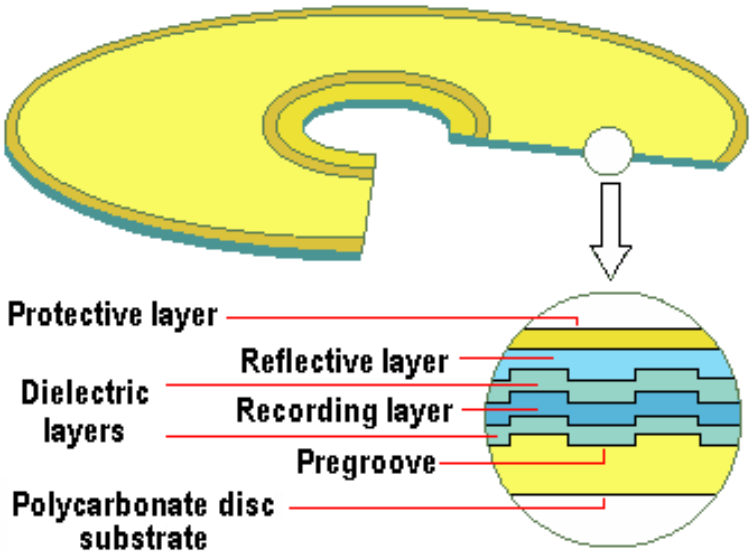
Optical Storage

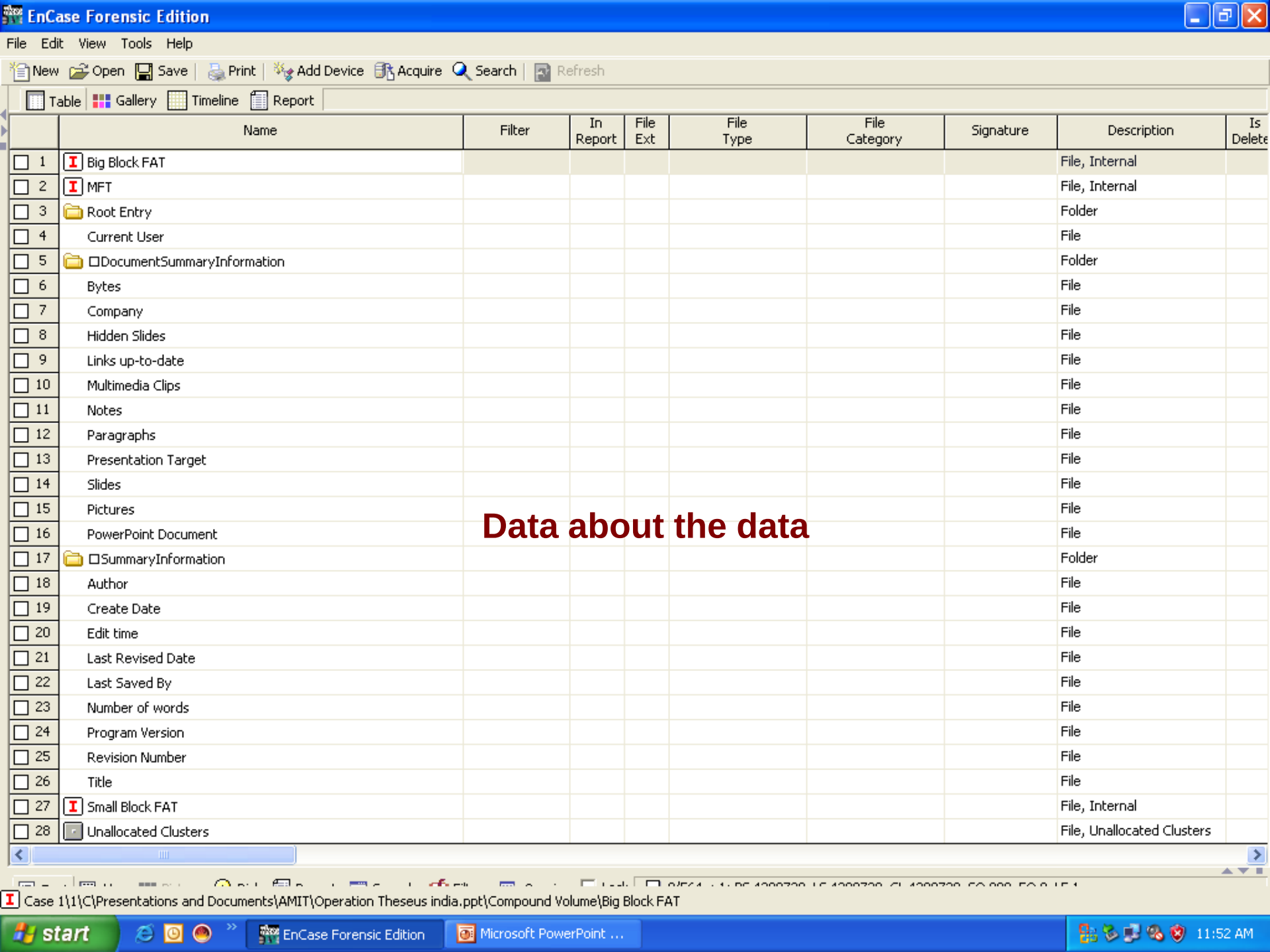
- Includes CD's and magneto optical cartridges.
- Uses a laser to "etch" the surface of the medium.
- CD's are a good storage medium for evidence to be presented.
- Magneto optical cartridges are preferred for image copies of suspect drives.

CD/RW Technology

The CD-Rewritable recorder uses three different laser powers to sore data It is essentially a chemical process.

1. The highest laser power, which is called "Write Power", creates a non-crystalline (absorptive) state on the recording layer
2. the middle power, also known as "Erase Power", melts the recording layer and converts it to a reflective crystalline state
3. the lowest power, which is "Read Power", does not alter the state of the recording layer, so it can be used for reading the data.




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

The Internet

Internet Problems

- Vast with no boundaries
- Outside of international control
- Largely unpoliced
- Anonymous
- Vast range of subjects
- Like can meet like
- Impossible to trace origins of material

Internet Crimes

- Pornography - implications for companies
- Intellectual property theft
- Credit card fraud
- Emails ‘scams’
- Terrorism
- Banking online – security issues
- Sophistication of the perpetrators
- The ‘Spam’ problem

Sources of Internet 'Evidence'

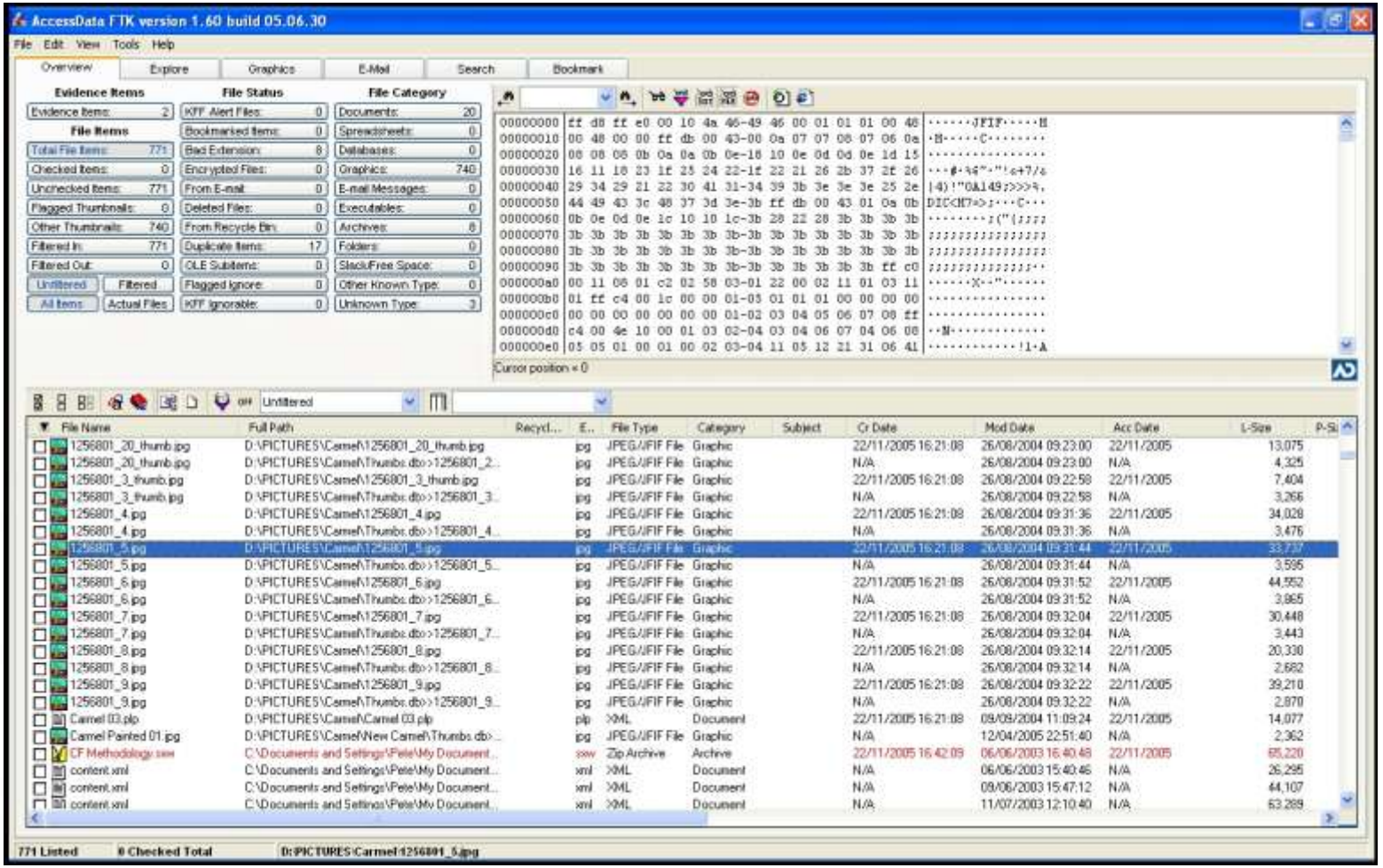
- Log files
- Browser history
- Telephone records
- Emails
- ISP records
- Chat rooms

Obtain specialist help.

Collecting the Data

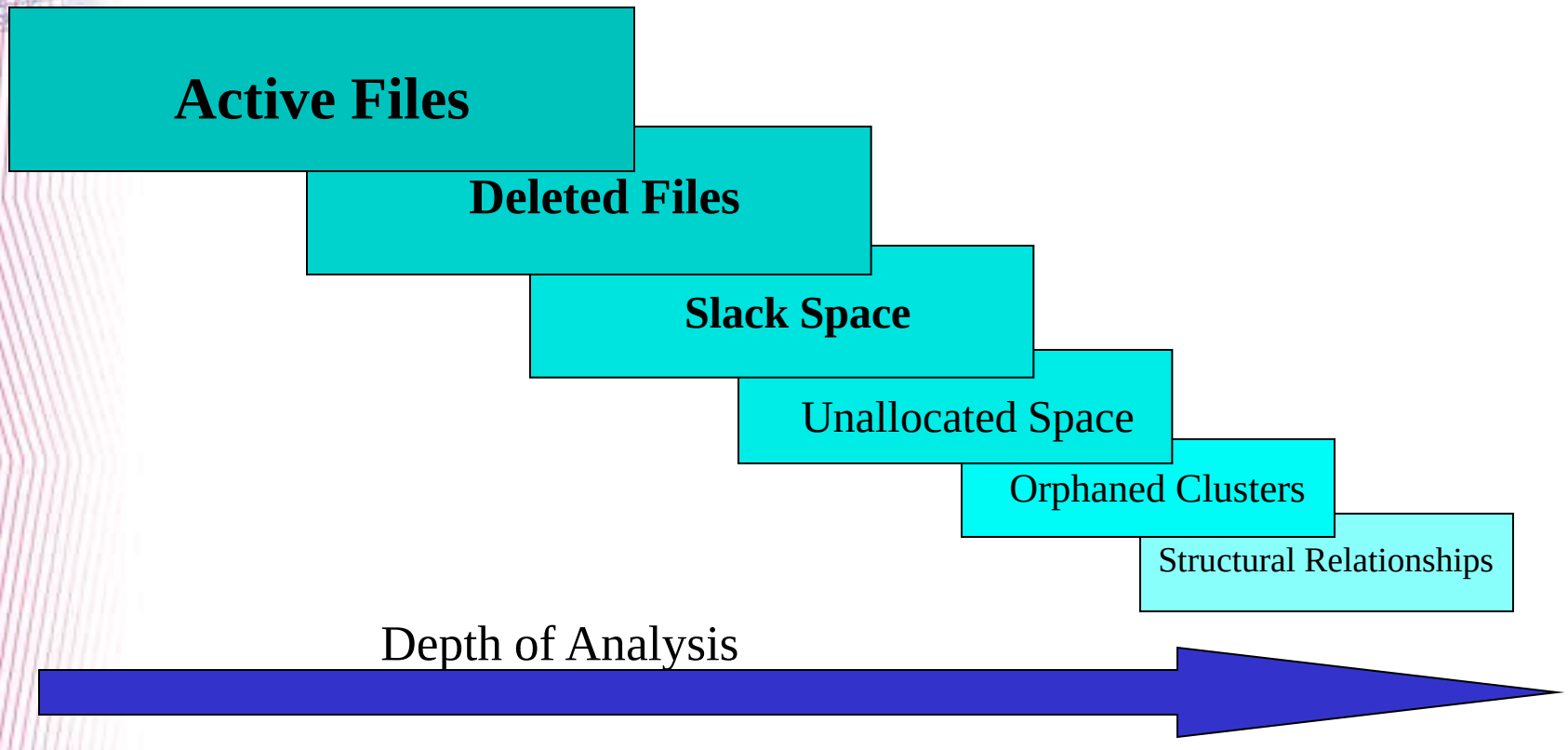
Imaging

Forensic Analysis Software



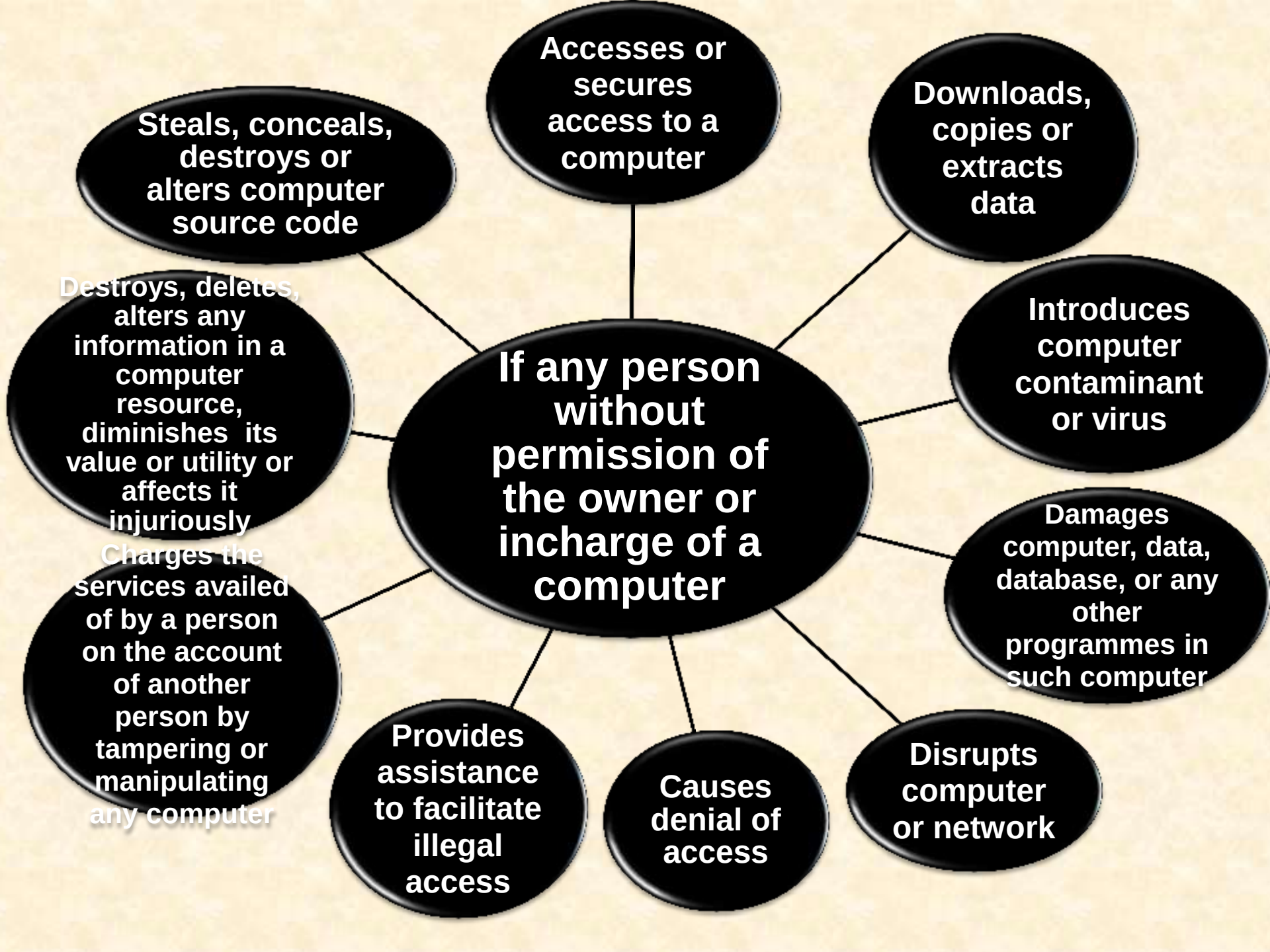
Hierarchical Structured Investigati

Level of Forensic Analysis




Know When to
Stop.

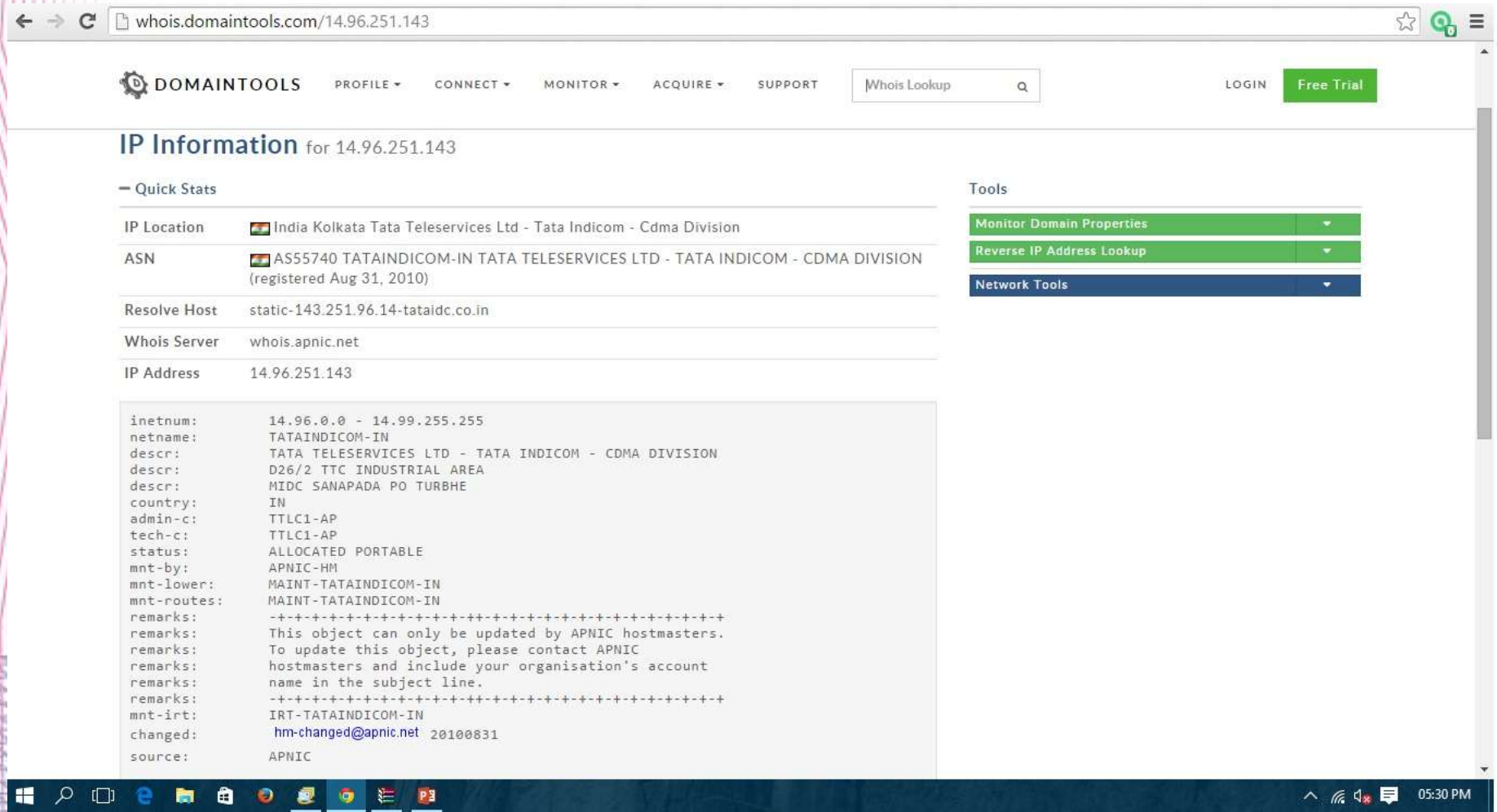

Surface Web - ClearNet
Facebook
Bing
Yahoo
Wikipedia
Google
YouTube
Deep Web
Represents anywhere from 90-96% of all content available on the internet
Legal Documents
Medical Records
Science Journals
Academic Information
Subscriptions
Government Resources
Financial Records
Organizational Repositories
DarkNet
Only 30,000 to 50,000 websites thought to exist
Hitmen
Classified Communication
Leaked Material
Drug Sales
Passport Forging
Encrypted.onion sites
Alternative Medi4


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

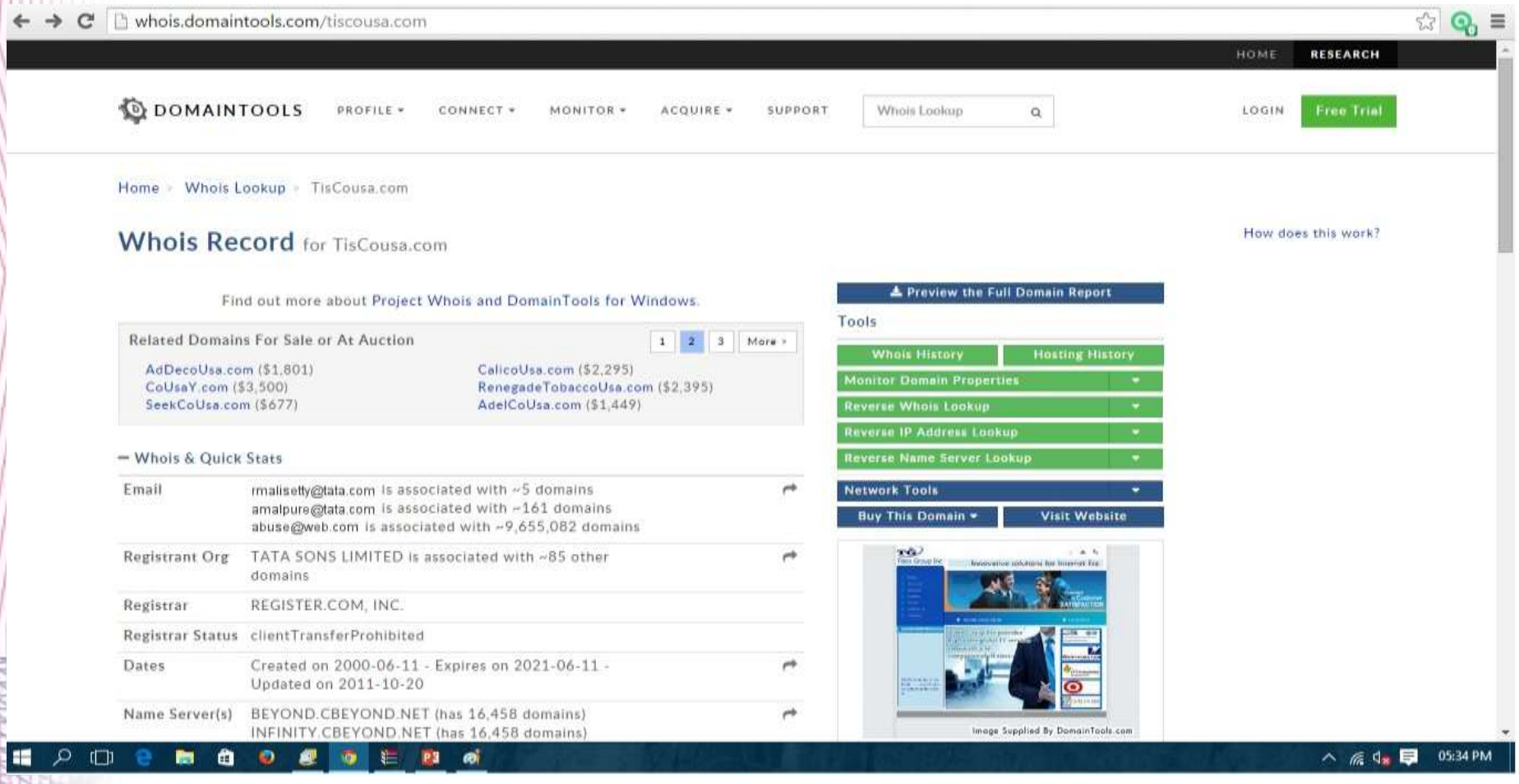
DNS LOOKUP

- 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

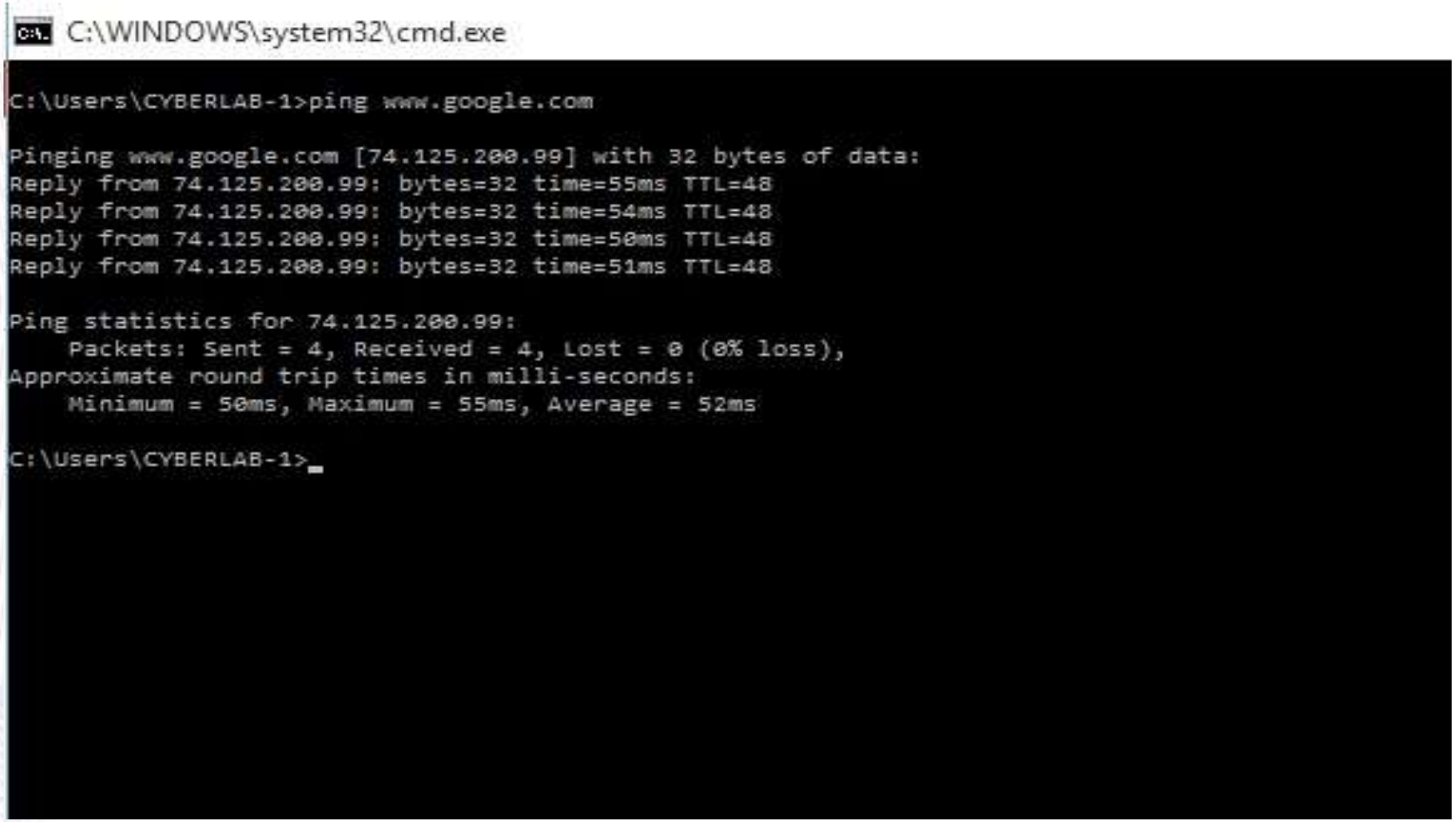


PING – Identify IP address of the Service

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)

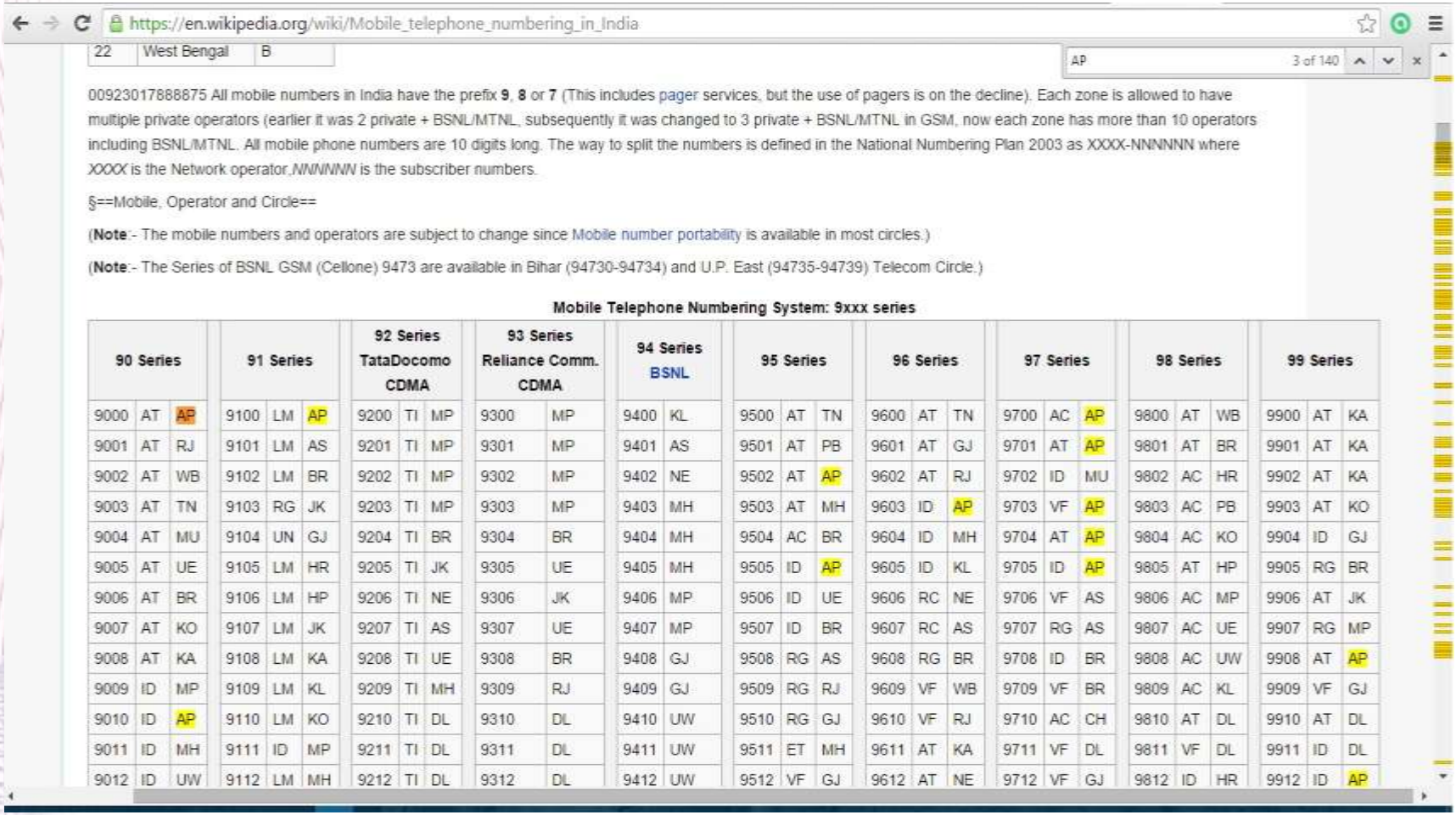
- To find out the Service Provider of any phone number. Visit the link:

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==

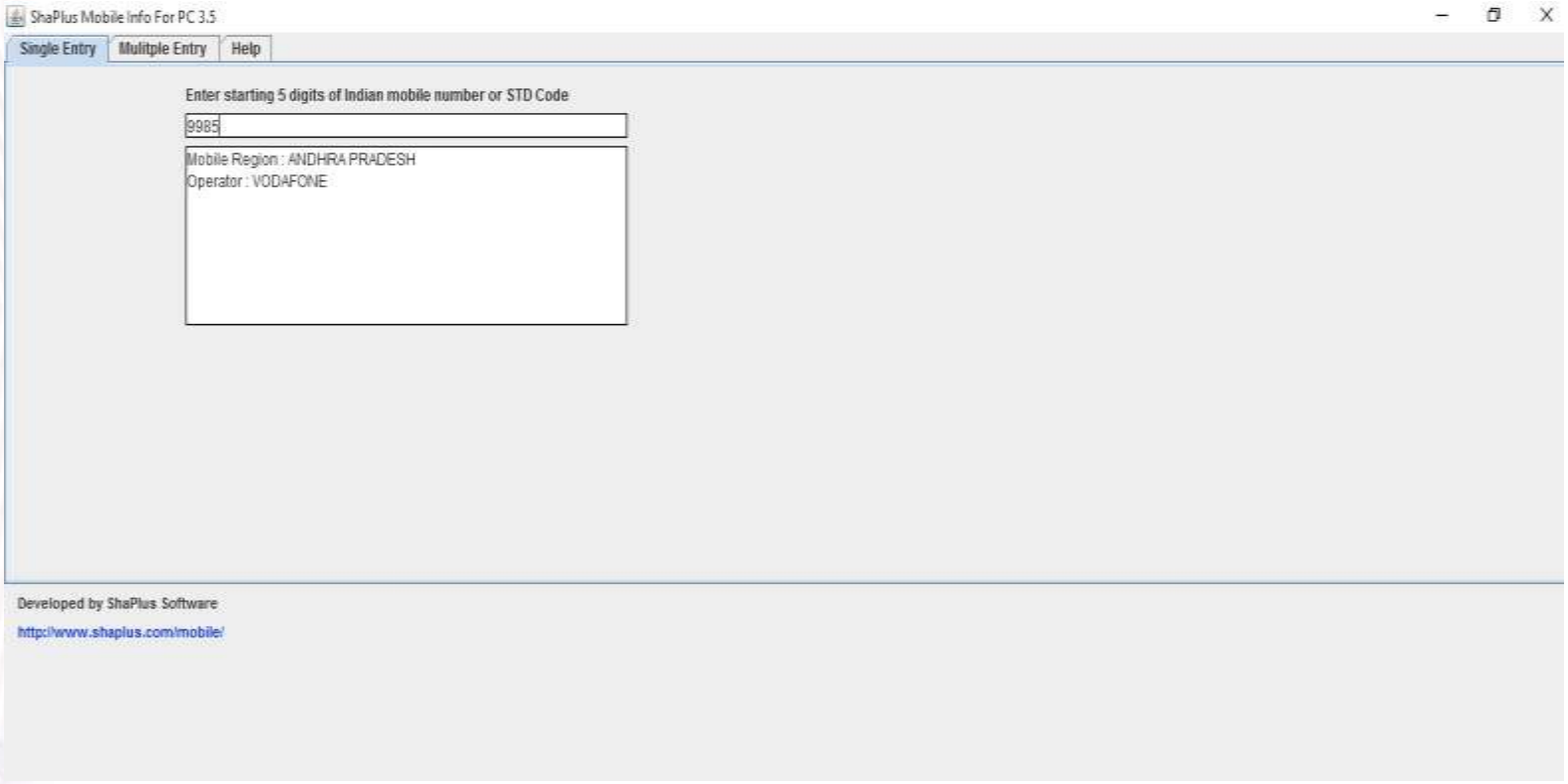
(**Note**:- The mobile numbers and operators are subject to change since Mobile number portability is available in most circles.)

(**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

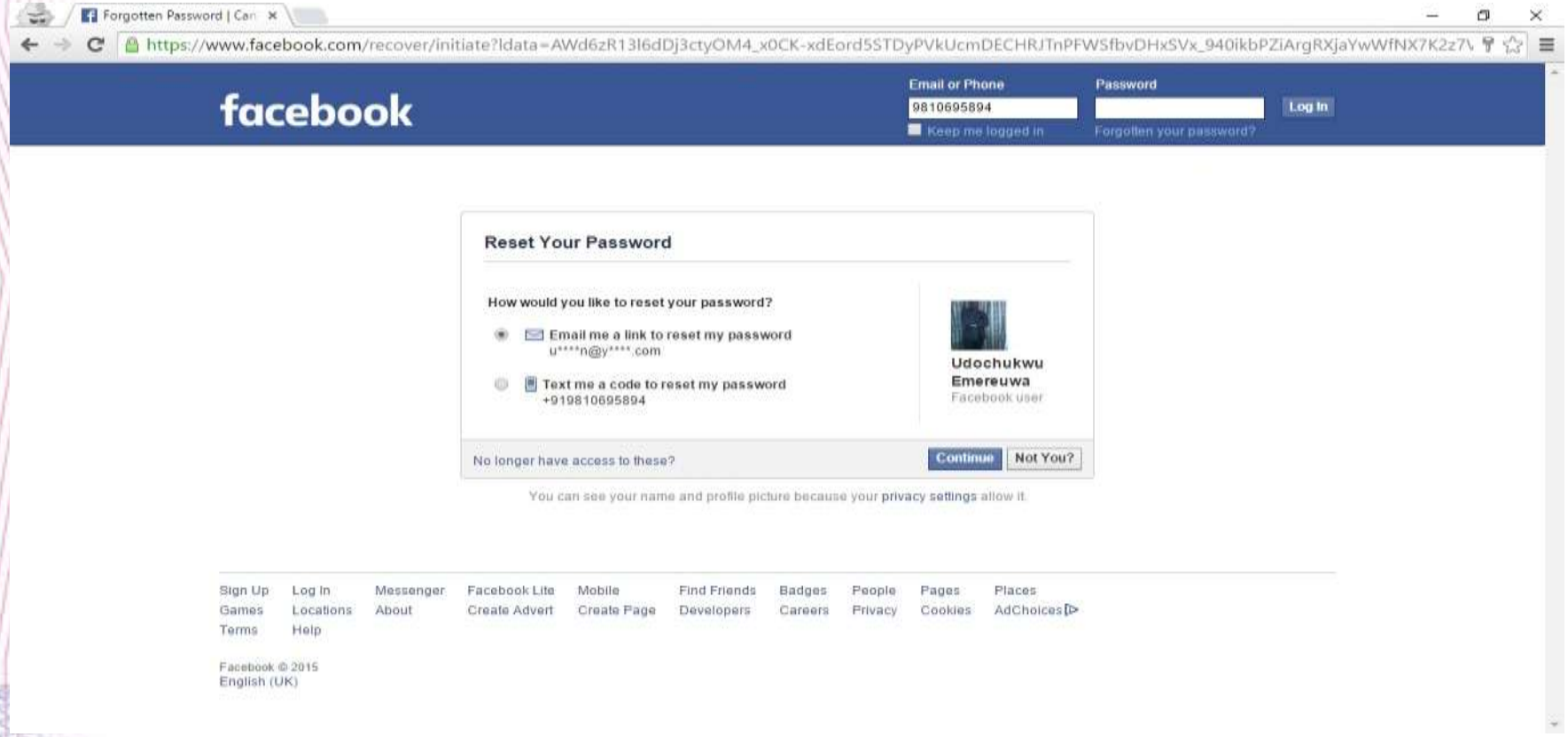
Mobile Service Provider



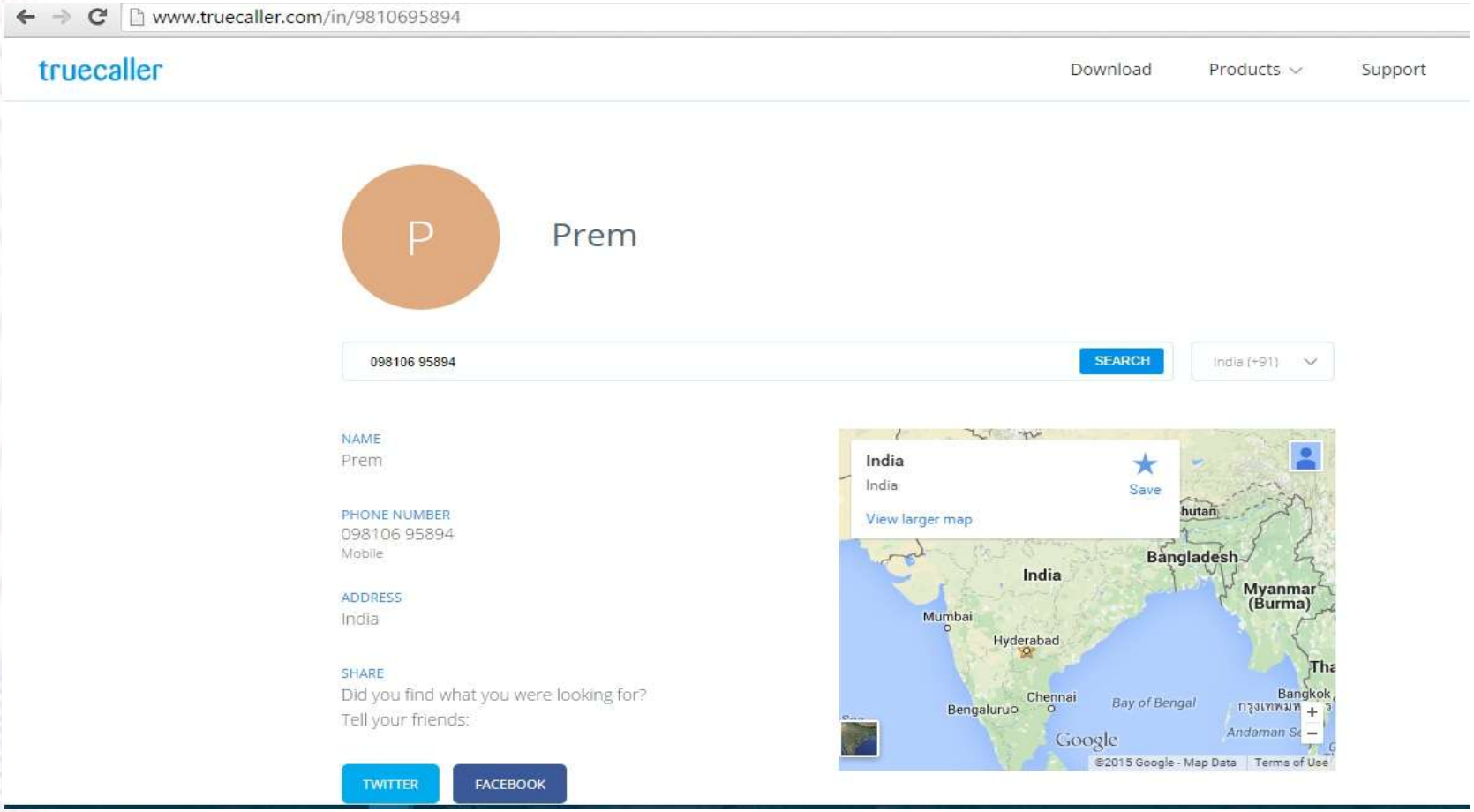
Social Media Analysis

- 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.

SOS – Search Our Suspect



Truecaller - ID Search

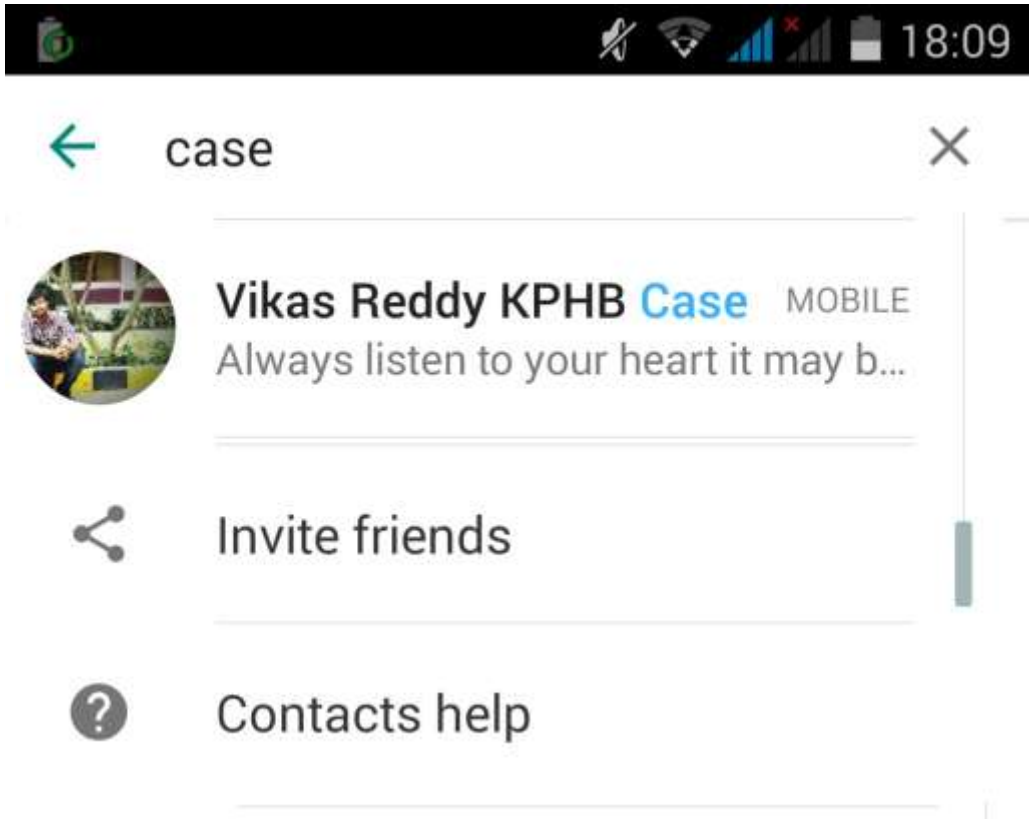


CEO- Election Commission Database Search

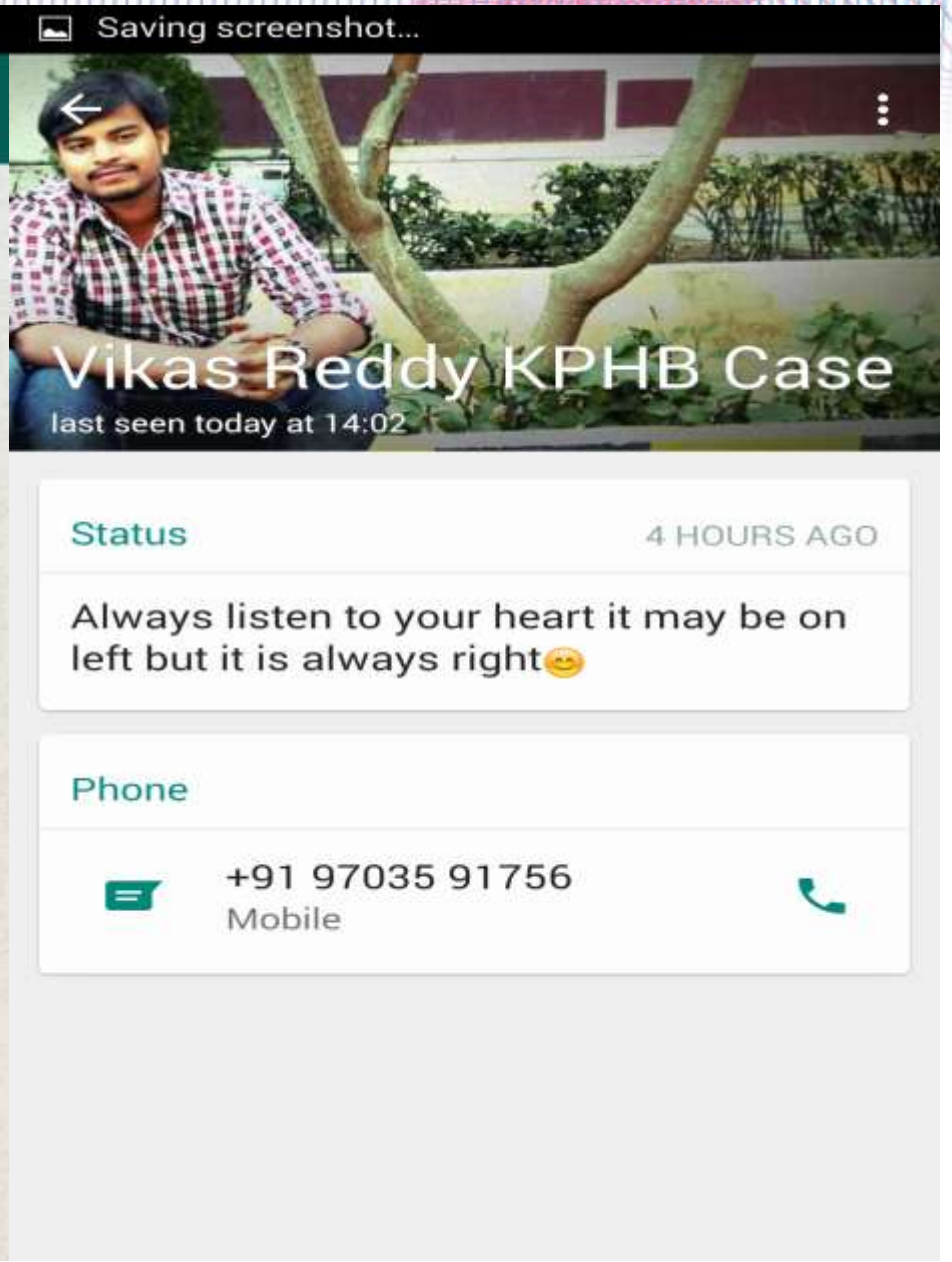
Name	Age	House Number	ID Card No.	Father/ Husband Name	Part Number & Polling station Location Name	Sl.No.in Part	Gender	
NAVEEN KUMAR MANDALOJU	37	11-4-322/20/35	CVG5619945	VEERA CHARY MANDALOJU	162-NETAJI HIGH SCHOOL	3	M	Print
KARNAKAR MANDALA	24	11-3-653	XDG0742644	KANAKAIAH MANDALA	76-Jai Bharath 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

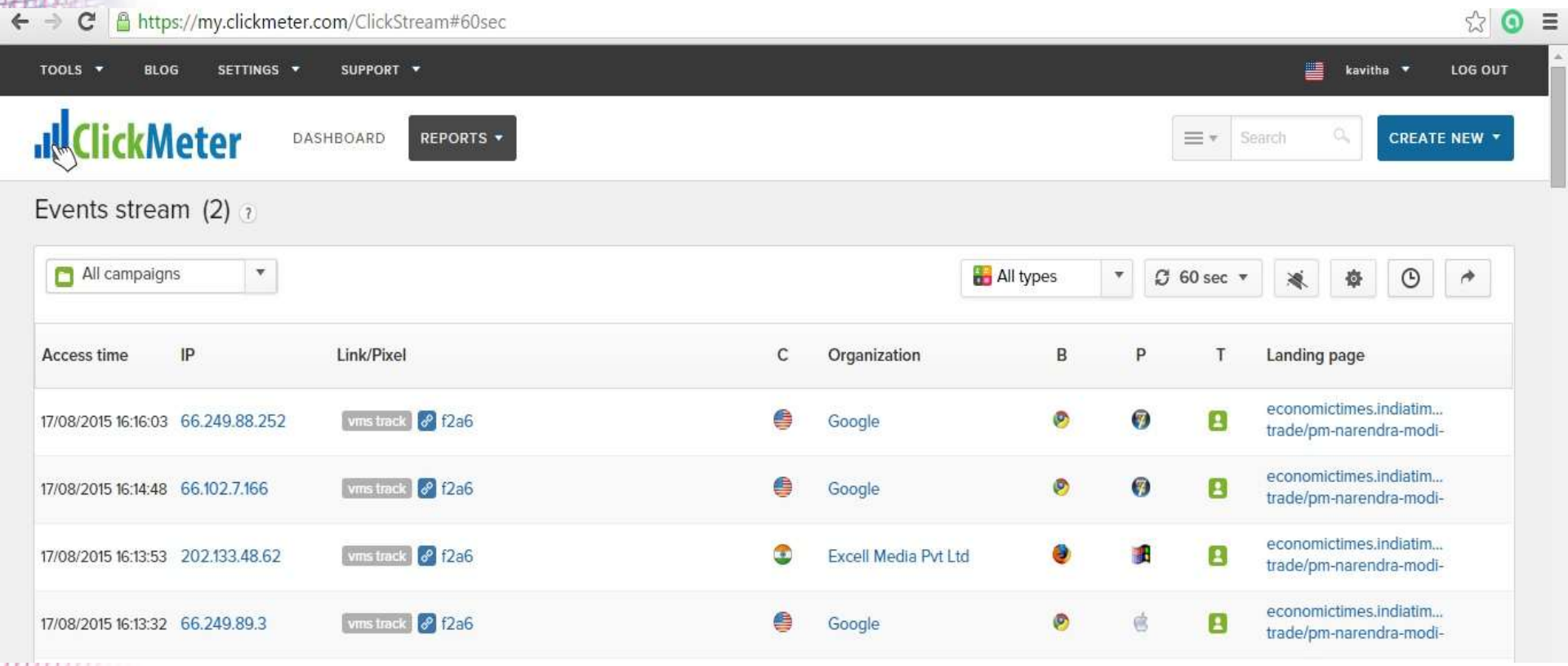
Whatsapp Search




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

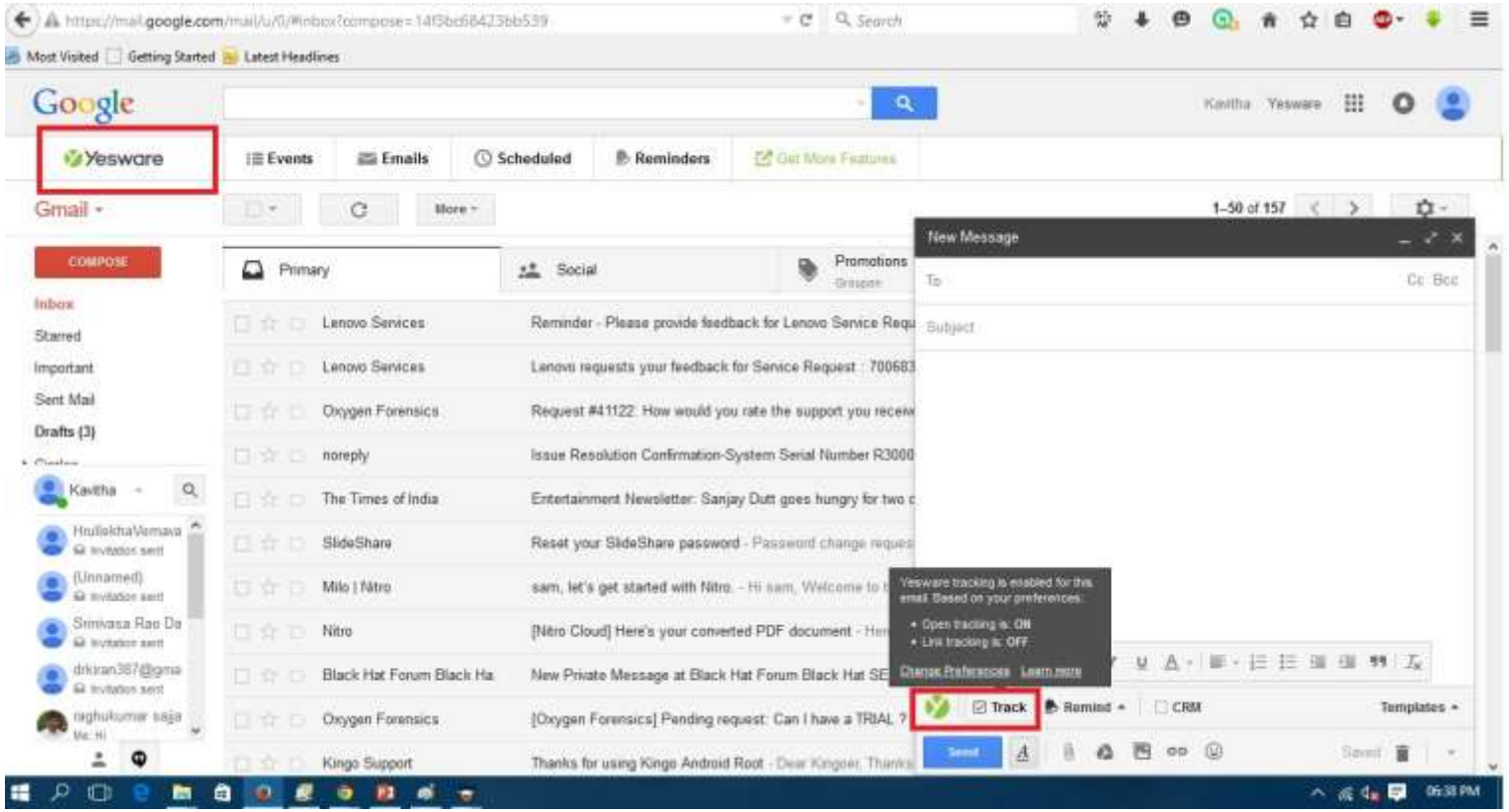


ClickMeter is one such method of grabbing the user IP address / Browser Details and Operating System Type.

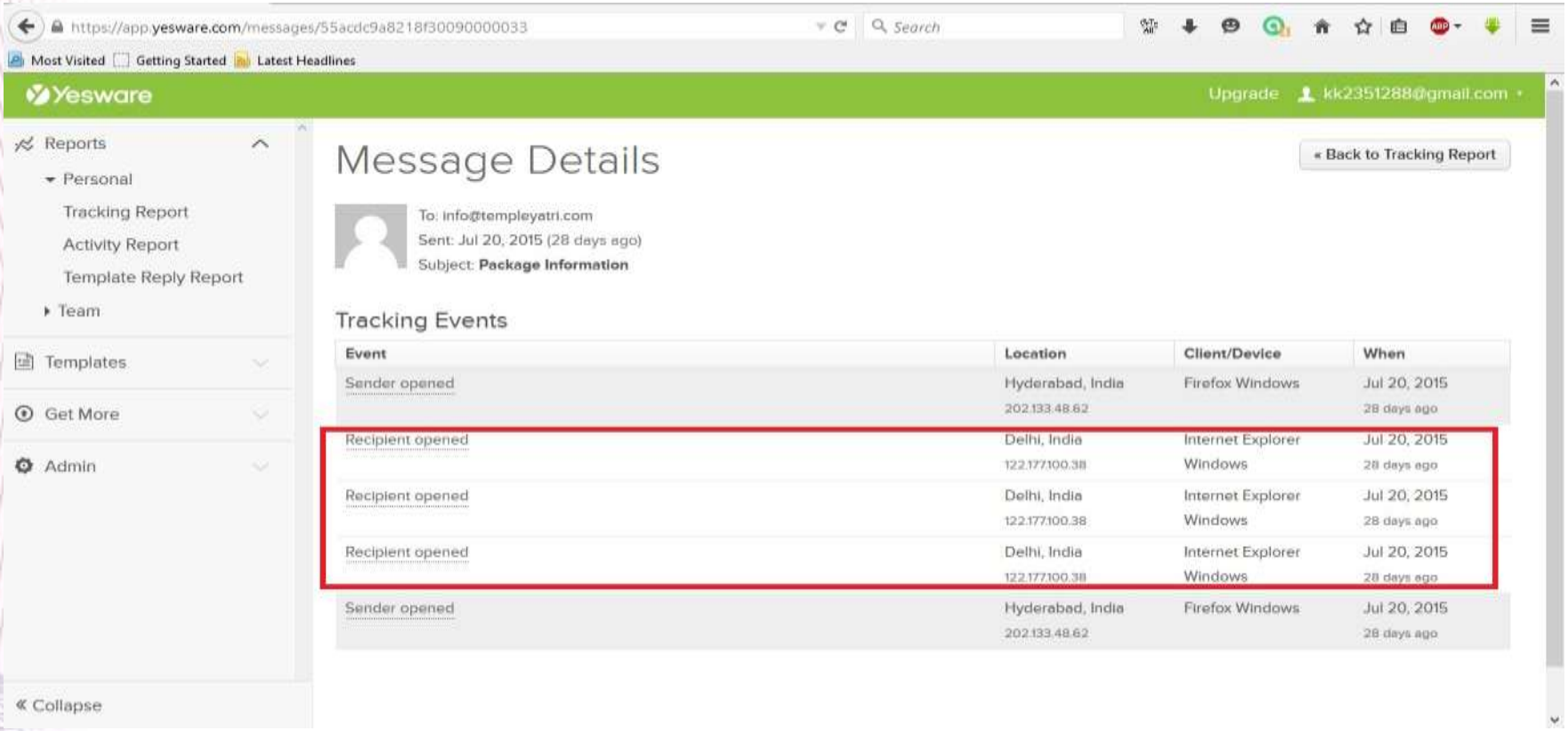
Email Tracking

- 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

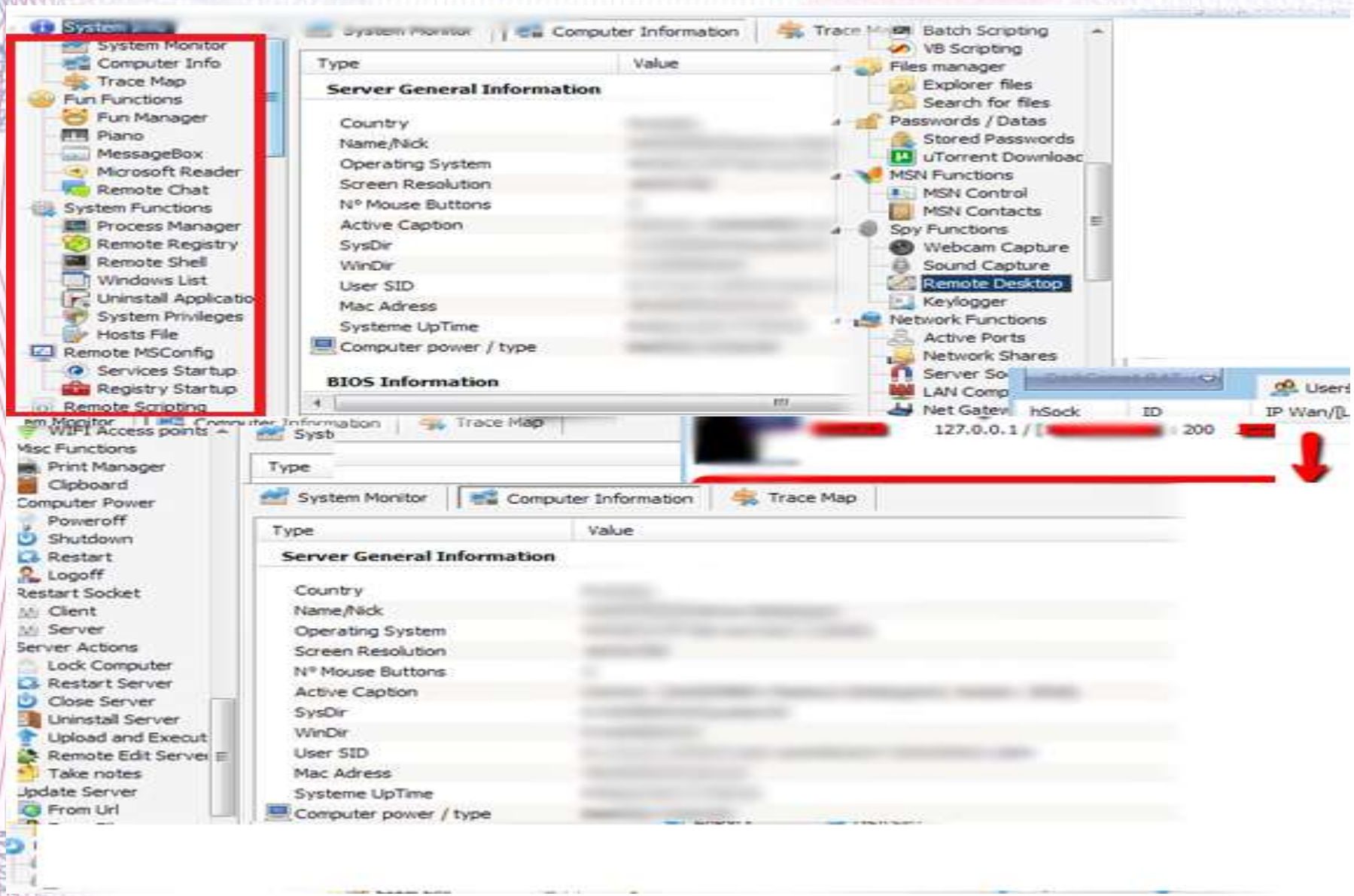


RAT

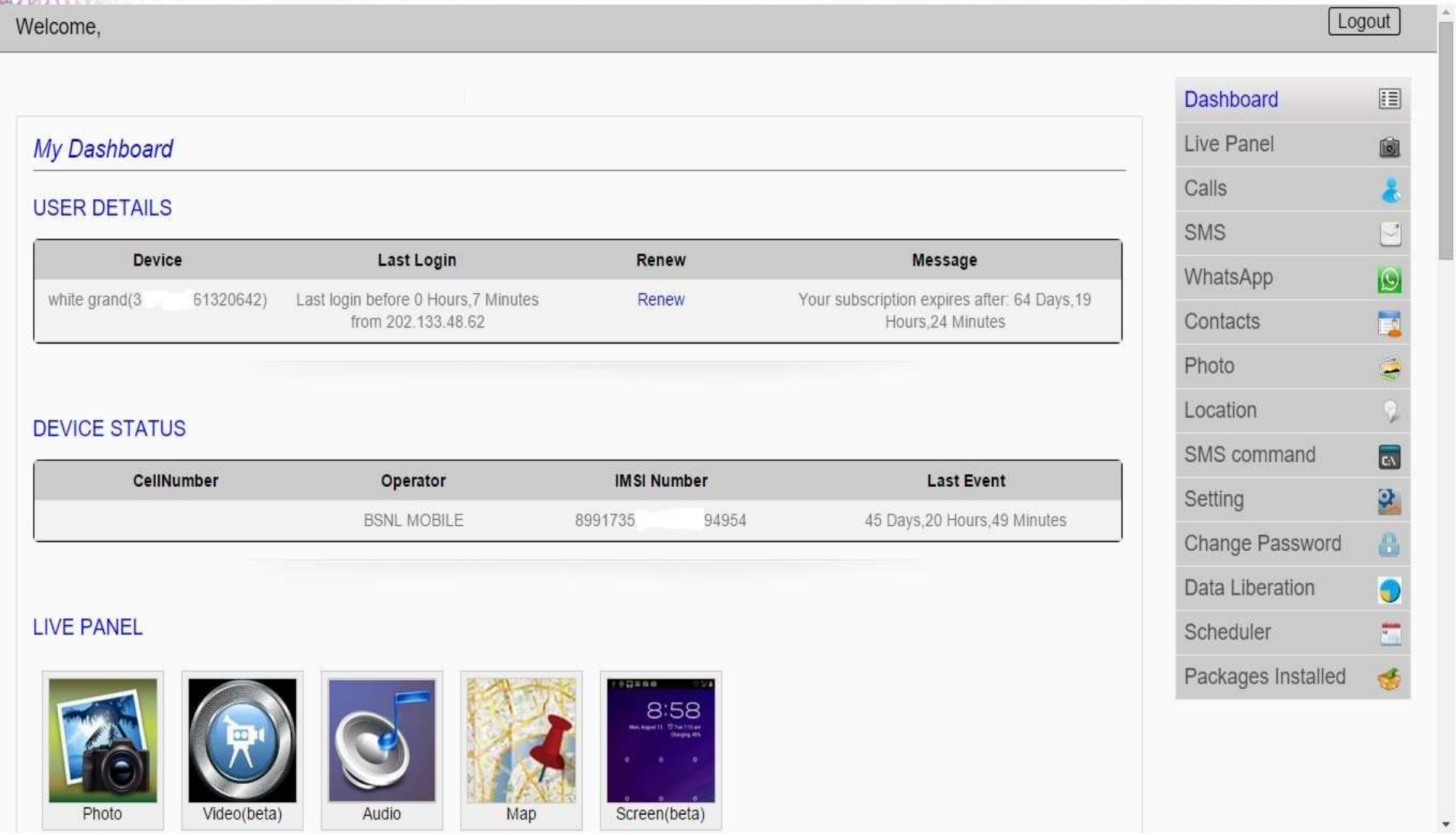
A **remote administration tool** (RAT) is a piece of software that allows a **remote** "operator" to control a system as if he has physical access to that system. While desktop sharing and **remote administration** have many legal uses, "RAT" software is usually associated with criminal or malicious activity.

This RAT can be anything Document/PDF/Excel/Photo/Video and executable file which a system can run/open.

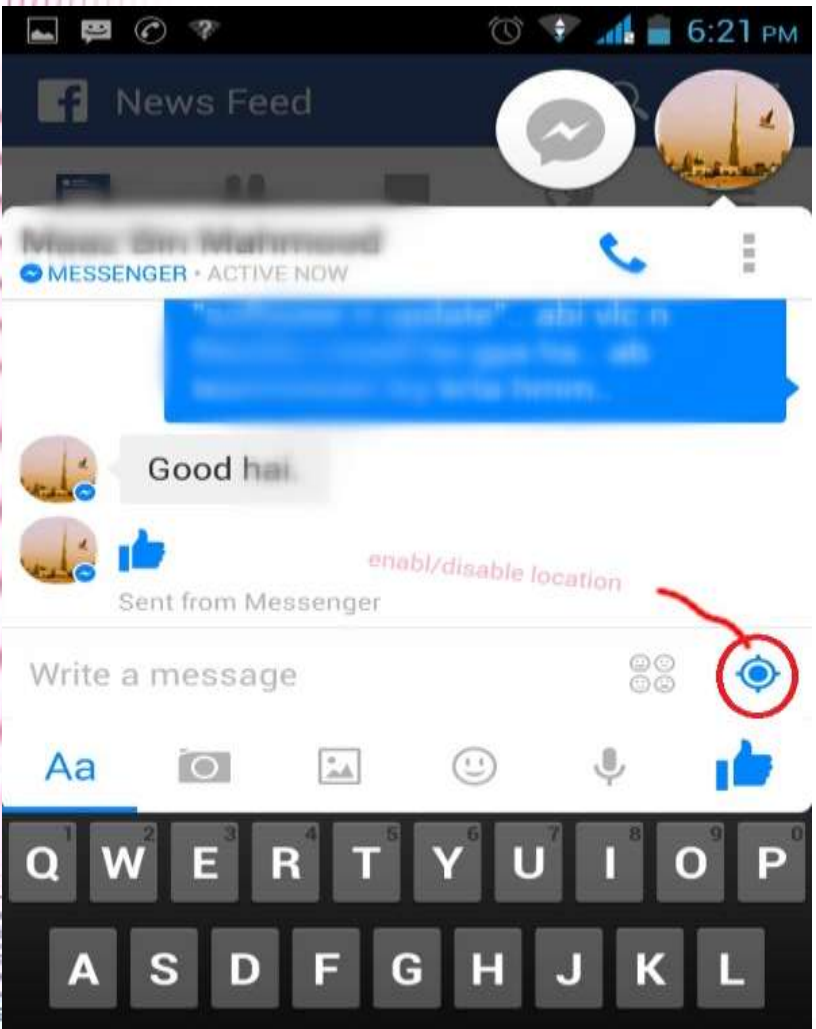
System based RAT - DarkCommet

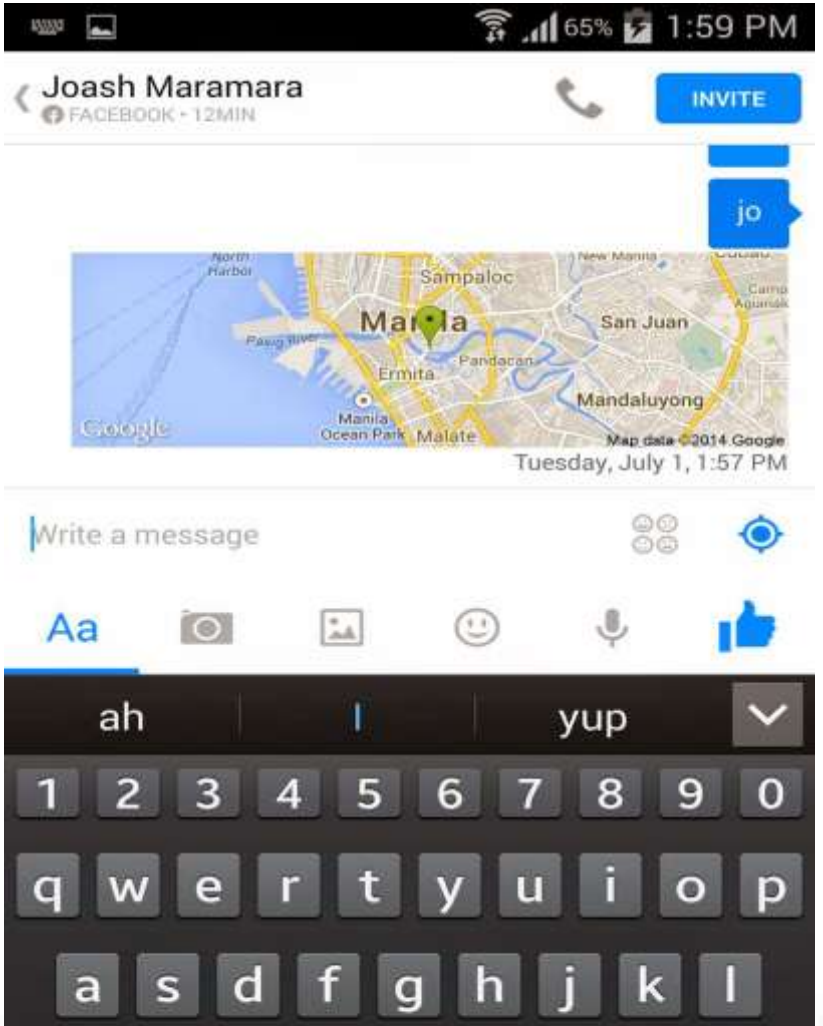


Mobile based RAT – AndroRAT

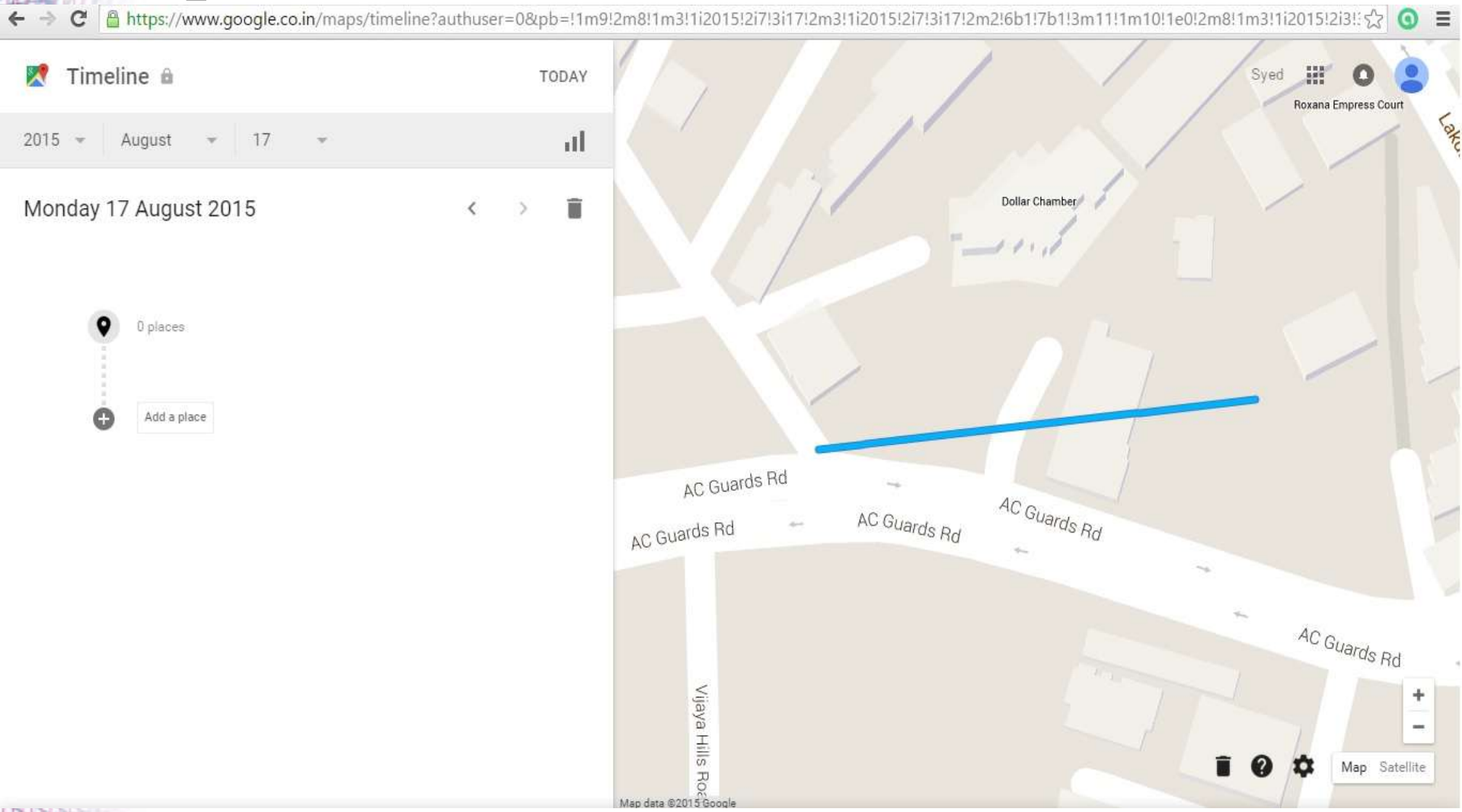


Facebook GPS secret : If your GPS is Turned ON then Facebook chat can track your GPS Location.





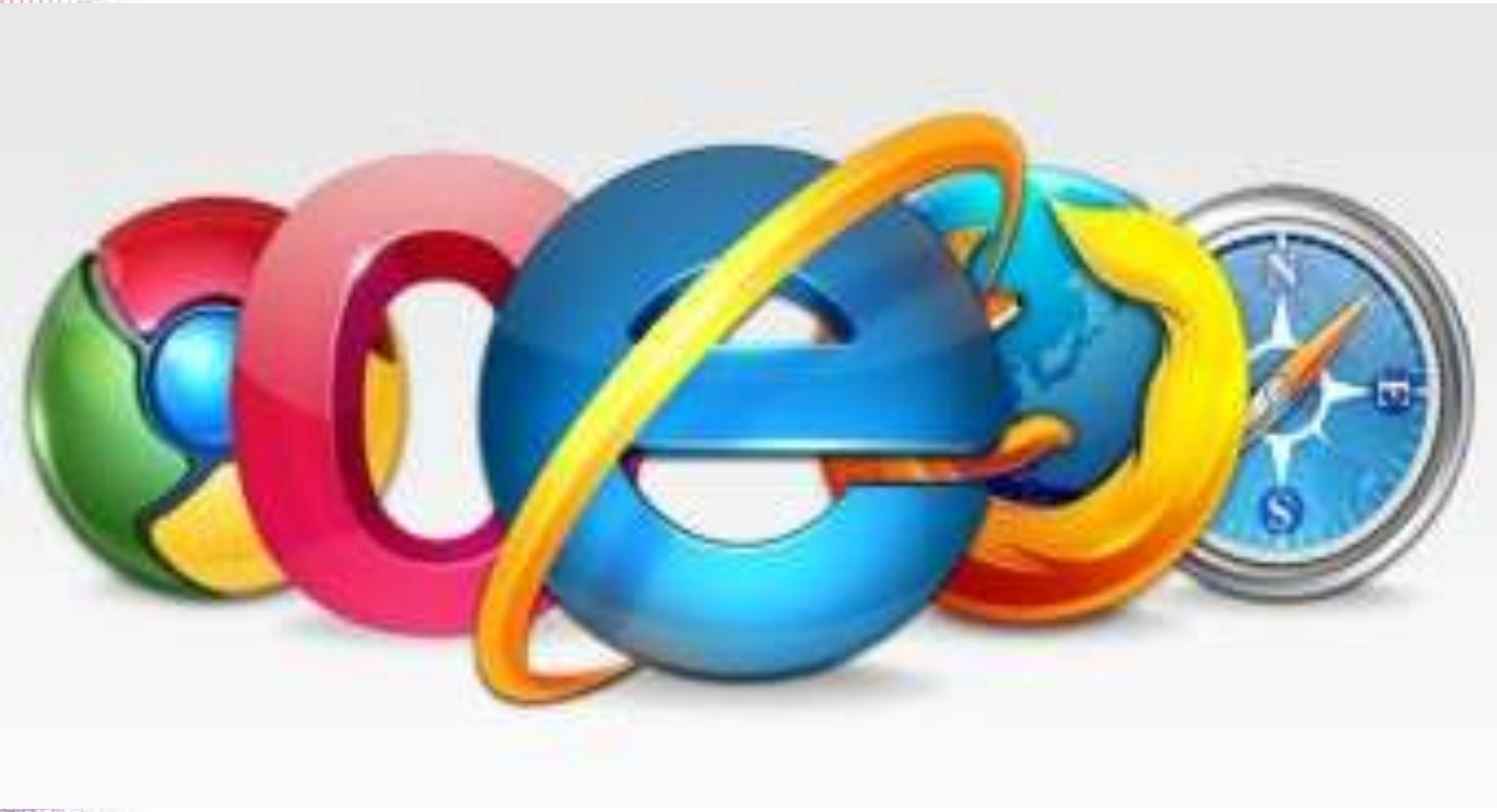
Google GPS Track : Your Google account keeps an EYE on YOU!!



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 ??**

Follow these internet safety tips for avoiding spyware and fortify your computer security right away




Know When to
Stop.


Thank you ...