Cyber Security (CPE-411)

BTech. CSE

Department of Computer Science and Engineering

Punjabi University

Section A

Part-I

Introduction to Internet

- Cyber Space and Threats,
- Computer Storage
- Cell Phone / Mobile Forensics
- Computer Ethics and Application Programs

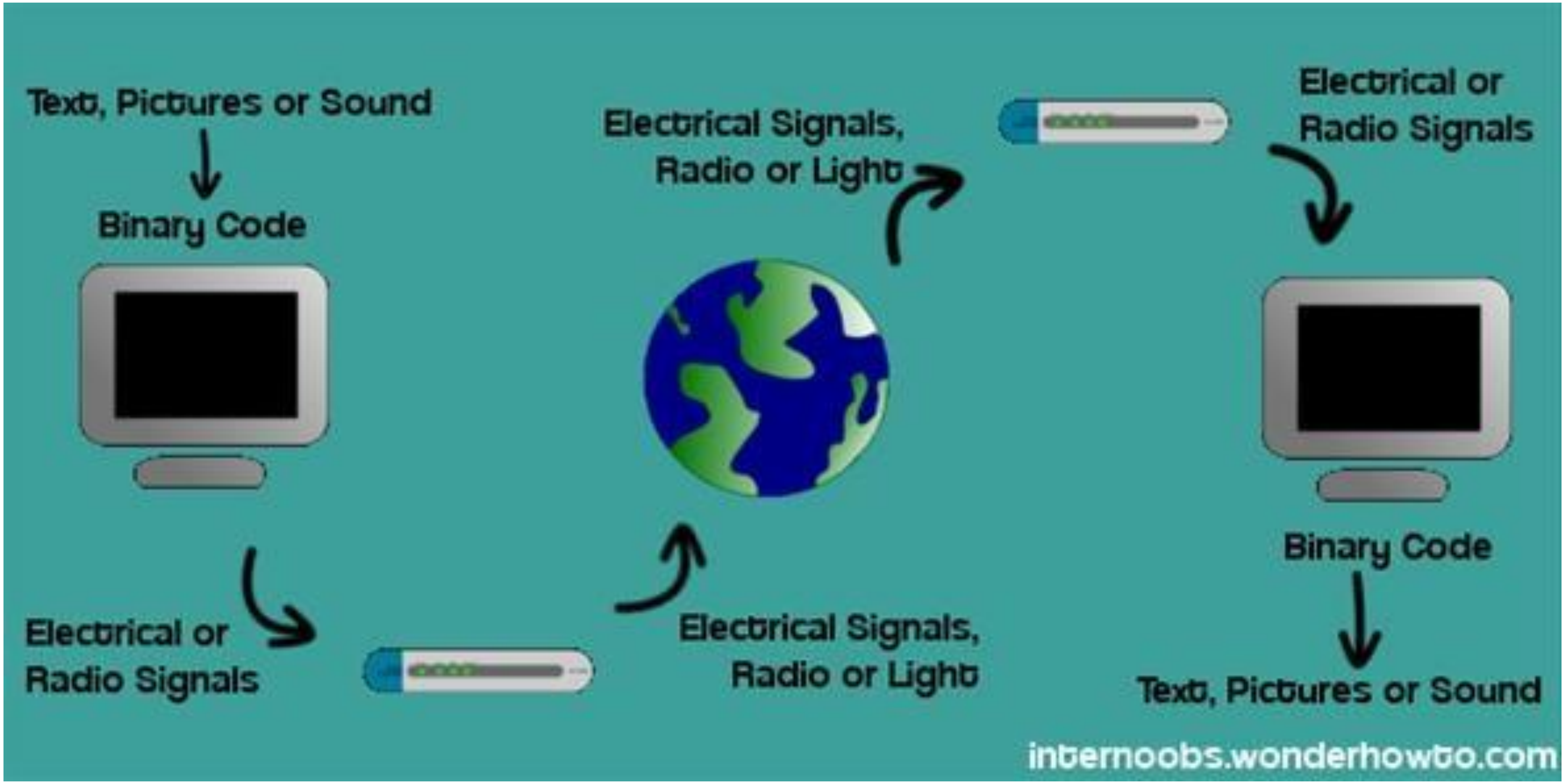
Introduction to Internet

A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

The Internet: Development History

- Development of this network, known as the ARPAnet after the Advanced Research Projects Agency (ARPA), began in 1969
- In the early 1980s, the current versions of the core Internet protocols, TCP and IP, were introduced across the network.
- In 1992, the Center for European Nuclear Research (CERN) released the first versions of World Wide Web software.

Internet is Heterogeneous Network


Text, Pictures or Sound
Binary Code
Electrical or Radio Signals
Electrical Signals, Radio or Light
Electrical Signals, Radio or Light
Electrical or Radio Signals
Binary Code
Text, Pictures or Sound
internoobs.wonderhowto.com

Different Types of Internet Connections

- Dial-Up (Analog 56K)

  Dial-up access is cheap but slow. A modem (internal or external) connects to the Internet after the computer dials a phone number. This analog signal is converted to digital via the modem and sent over a land-line serviced by a public telephone network.

- Digital Subscriber Line (DSL)

  It is an internet connection that is always "on". This uses 2 lines so your phone is not tied up when your computer is connected. There is also no need to dial a phone number to connect. DSL uses a router to transport data and the range of connection speed, depending on the service offered, is between 128K to 8 Mbps.

- Cable

  Cable provides an internet connection through a cable modem and operates over cable TV lines.

- Wireless

  Wireless, or Wi-Fi, as the name suggests, does not use telephone lines or cables to connect to the internet. Instead, it uses radio frequency. Speeds will vary, and the range is between 5 Mbps to 20 Mbps.

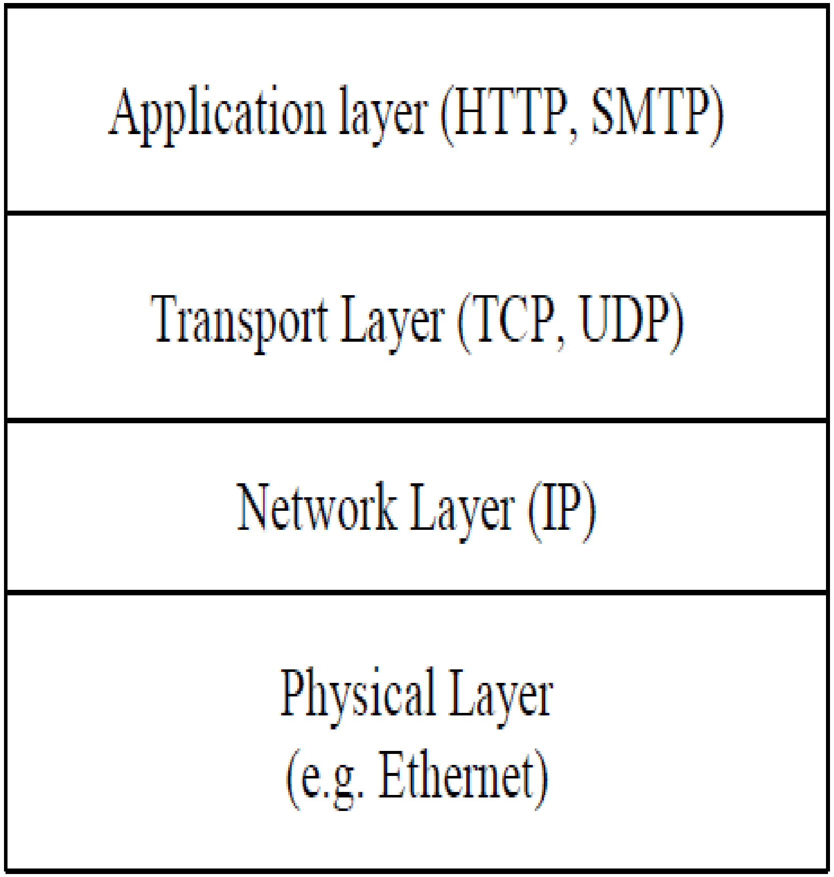
- Satellite

  Satellite accesses the internet via a satellite in Earth’s orbit. Satellite connection speeds are around 512K to 2.0 Mbps.

- Cellular

  Cellular technology provides wireless Internet access through cell phones. The speeds vary depending on the provider, but the most common are 3G and 4G speeds. A 3G is a term that describes a 3rd generation cellular network obtaining mobile speeds of around 2.0 Mbps. 4G is the fourth generation of cellular wireless standards. The goal of 4G is to achieve peak mobile speeds of 100 Mbps but the reality is about 21 Mbps currently.

The Internet Layered Architecture:

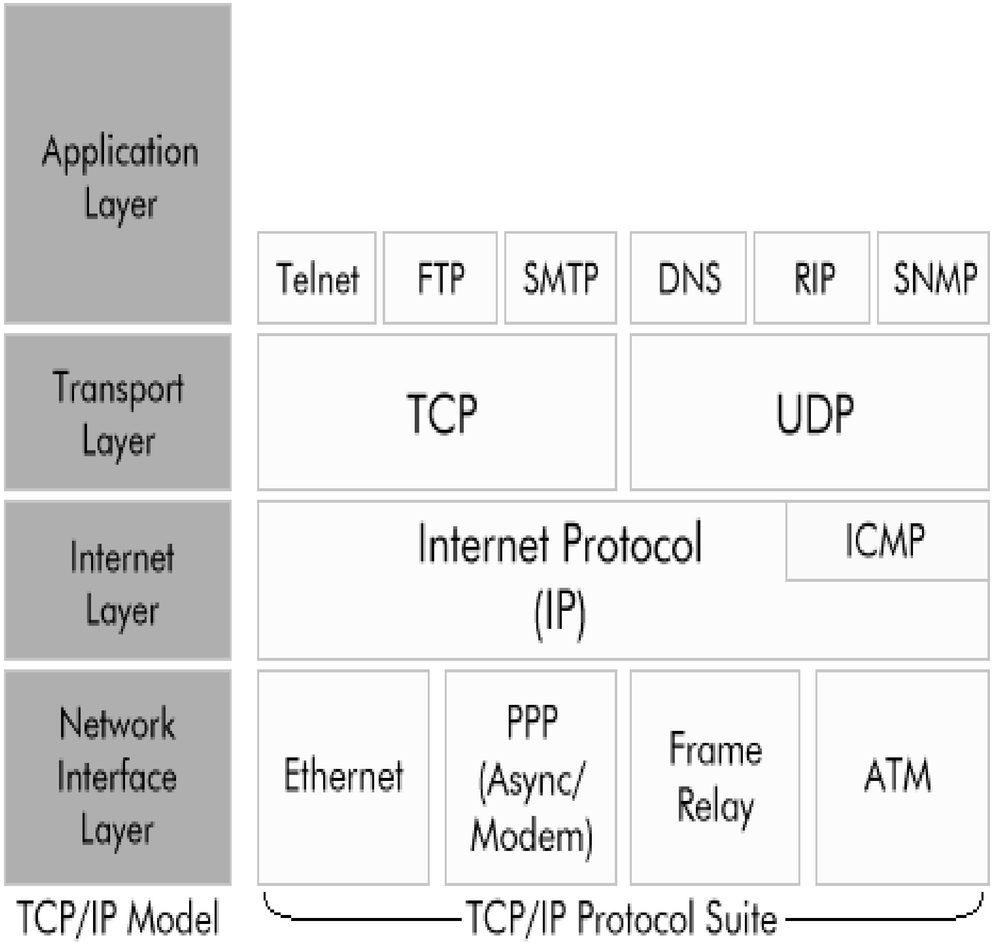


Application layer (HTTP, SMTP)

Transport Layer (TCP, UDP)

Network Layer (IP)

Physical Layer
(e.g. Ethernet)



Application Layer

Transport Layer

Internet Layer

Network Interface Layer

TCP/IP Model

Telnet, FTP, SMTP, DNS, RIP, SNMP

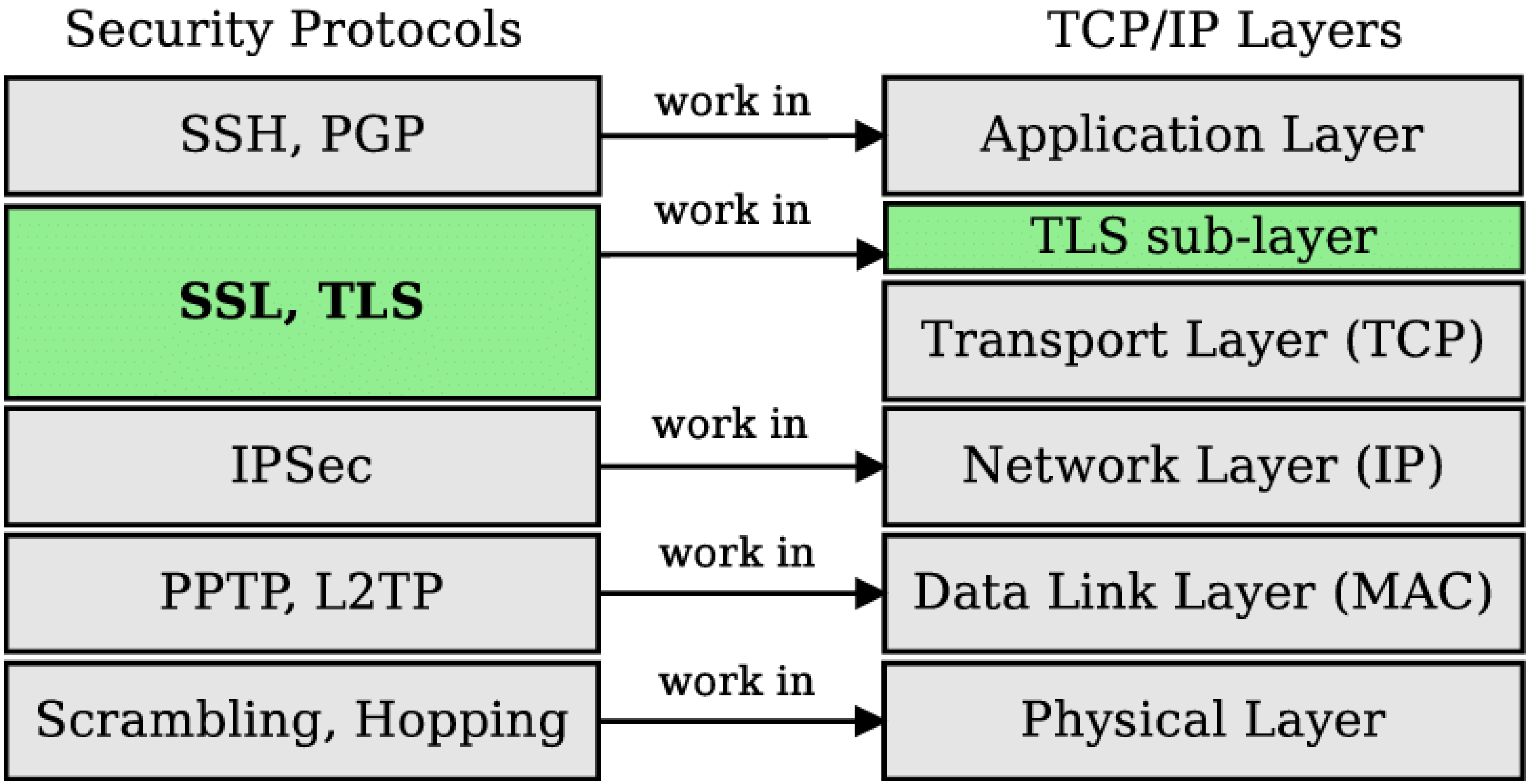
TCP, UDP

Internet Protocol (IP), ICMP

Ethernet, PPP (Async/ Modem), Frame Relay, ATM

TCP/IP Protocol Suite

Security in Internet Layered Architecture



Security Protocols

TCP/IP Layers

SSH, PGP work in Application Layer

SSL, TLS work in TLS sub-layer

Transport Layer (TCP)

IPSec work in Network Layer (IP)

PPTP, L2TP work in Data Link Layer (MAC)

Scrambling, Hopping work in Physical Layer

The Internet Layers Protocols

- The Internet, as a network of connecting many small networks, consists of four layers:
- - Application Layer (HTTP, FTP,SMTP)
- - Transport Layer (TCP, UDP)
- - Network Layer (IP)
- - Physical Layer

The Internet Protocols

- **FTP:(**File transfer protocol)- One of the most oldest and probably the most popular protocol to be used to move files on the Internet.

- **TCP/IP:(**Transmission Control Protocol and Internet Protocol)

  - The low-level communications protocol that holds the Internet together.

  - It provides the essential service of making sure that each piece of data is transferred in the correct sequence and without error.

- **SMTP:** (the e-mail message protocol)- A protocol to allow two users to communicate through e-mail messages over the Internet.

- **NNTP:** (Net News Transfer Protocol)- A protocol, which can be used to access or transfer Usenet news over the Internet.

- **Simple Network Management Protocol (SNMP) :** is a set of protocols for network management and monitoring. These protocols are supported by many typical network devices such as routers, hubs, bridges, switches, servers, workstations, printers, modem racks and other network components and devices.
- **Routing Information Protocol (RIP):** is one of the oldest distance-vector routing protocols which employ the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support.
- **Telnet:** - The traditional teletype-style communications protocol for communicating with text-based information services

The Internet: Design Principles

- **Uniform Naming and Addressing:**

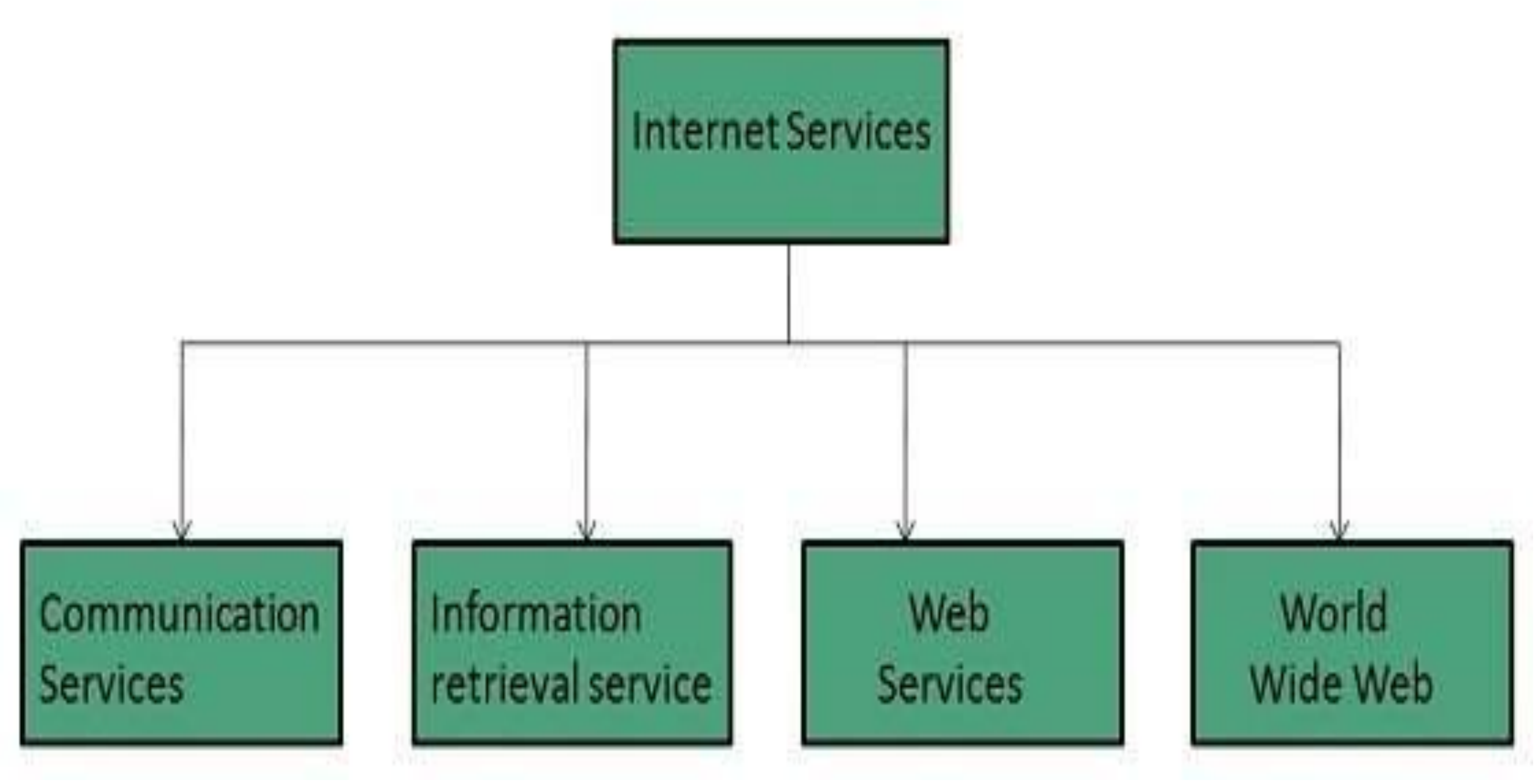
  The IP layer offers a uniform addressing structure that assigns a 32-bit address to each computer connected to the network.
- **Domain Name System (DNS)** offers a uniform way to translate human-readable names for computers, such as www.openmarket.com to the numeric address for that.
- **End-to-End protocols have several advantages:**

  - hide the internal structure of the network

  - provide simple abstractions to programmers

  - shielding them from such things as the messy details of recovering from lower-level errors.

Internet Services



The World Wide Web: History

- March, 1989, Tim Berners-Lee of Geneva European Particle Physics Laboratory (CERN) circulated a proposal to develop a hypertext system for global information sharing in High Energy Physics community.

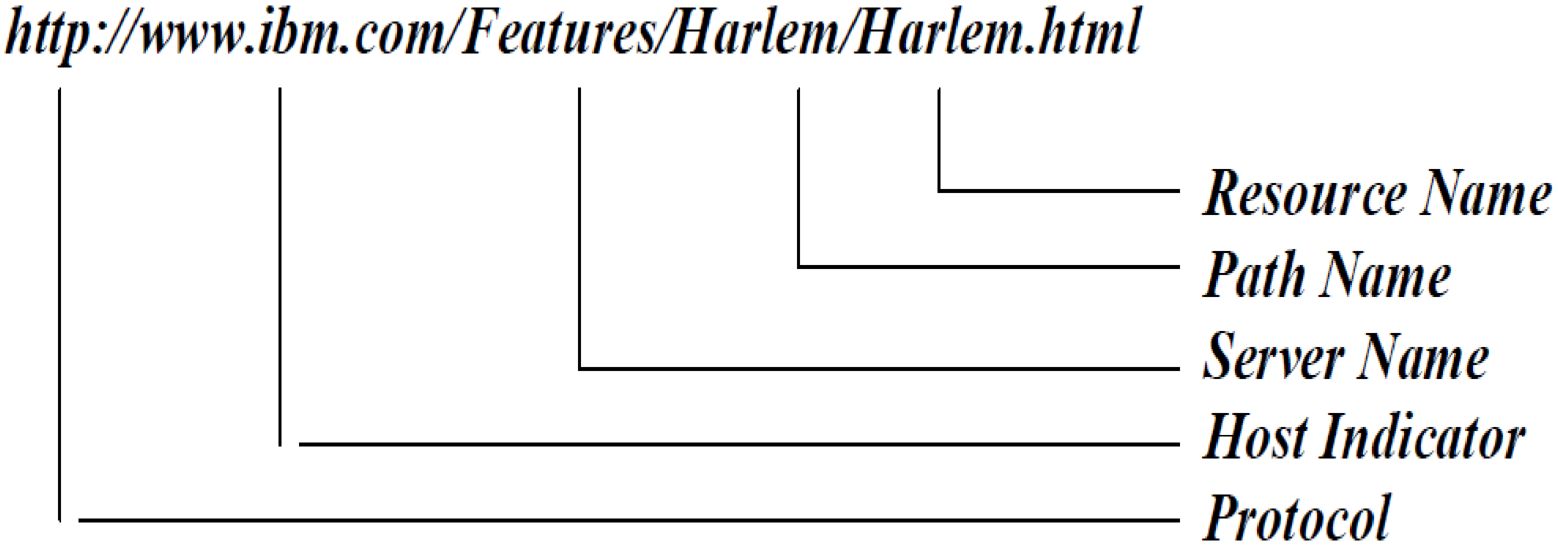
- The World Wide Web project began to take shape at the beginning of 1991

- In July of 1994, CERN began to turn over the Web project to a new group called the W3 organization, a joint venture between CERN and MIT to develop the Web further

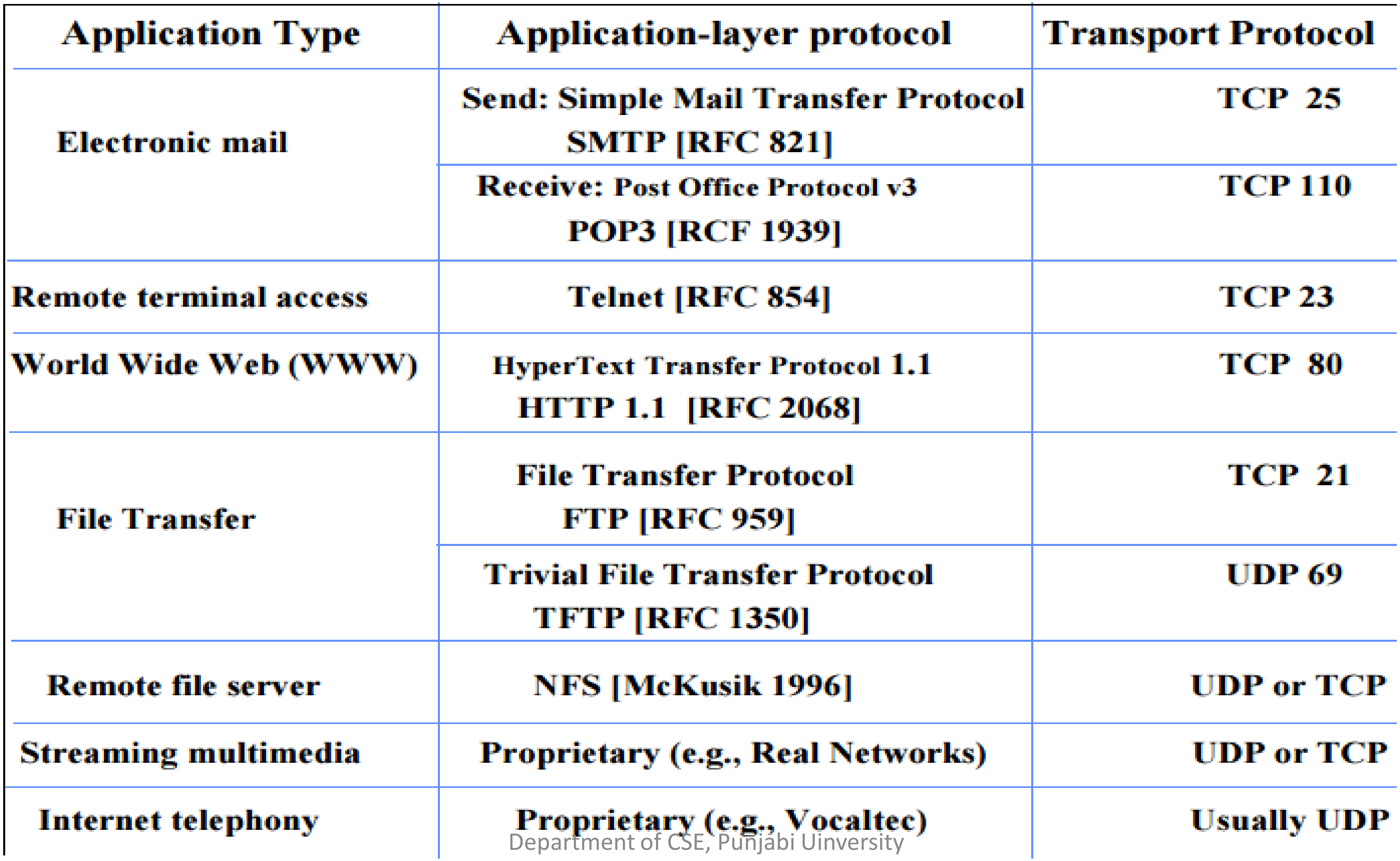
.

The World Wide Web: URL

- Usually, an URL leads to a file, but that s not always the case. A URL can point you to a single record in a database, the front-end of an Internet program, or a result of a query.



Internet Service and Port



Application Type	Application-layer protocol	Transport Protocol
Electronic mail	Send: Simple Mail Transfer Protocol SMTP [RFC 821]	TCP 25
	Receive: Post Office Protocol v3 POP3 [RCF 1939]	TCP 110
Remote terminal access	Telnet [RFC 854]	TCP 23
World Wide Web (WWW)	HyperText Transfer Protocol 1.1 HTTP 1.1 [RFC 2068]	TCP 80
File Transfer	File Transfer Protocol FTP [RFC 959]	TCP 21
	Trivial File Transfer Protocol TFTP [RFC 1350]	UDP 69
Remote file server	NFS [McKusik 1996]	UDP or TCP
Streaming multimedia	Proprietary (e.g., Real Networks)	UDP or TCP
Internet telephony	Proprietary (e.g., Vocaltec)	Usually UDP

The World Wide Web

The World Wide Web (abbreviated WWW or the Web) is an information space where documents and other web resources are identified by Uniform Resource Locators (URLs), interlinked by hypertext links, and can be accessed via the Internet.

The World Wide Web: HTTP

- **HTTP stands for HyperText Transfer Protocol.**

  - It is a simple data transfer protocol that binds the Web together.

  - It supports the communications between a web client (browser) and its web server.

  - It consists of a set of messages and replies for both servers and browsers.

  - It treats documents, files, menus, and graphics as objects.

  - It relies on the Universal resource identifier (URI), enclosed in the universal resource locator (URL), to identify files.

The World Wide Web: Applications

- **Distributing and Sharing Scientific Data:** Share scientific information (data, papers, databases)among scientists around the world
- **E-Commerce :** Electronic marketing and advertising, online shopping(order/purchase, payment), online trading, online customer services.
- **Online Education and Training :** On-line courses, training program and information, distance learning
- **Organization and Public Service :** Distributing public service information for organizations and government offices.
- **Online Publishing :** Online books, magazines and journals, newspapers, Video, CD .
- **Online Banking and Trading :** Support online bank transactions for banks and stockbrokerages

Cyberspace

Cyberspace refers to the virtual computer world in which electronic medium used to form a global computer network for online communication. It is a large computer network made up of many computer networks that employ TCP/IP protocol to aid in communication and data exchange activities.

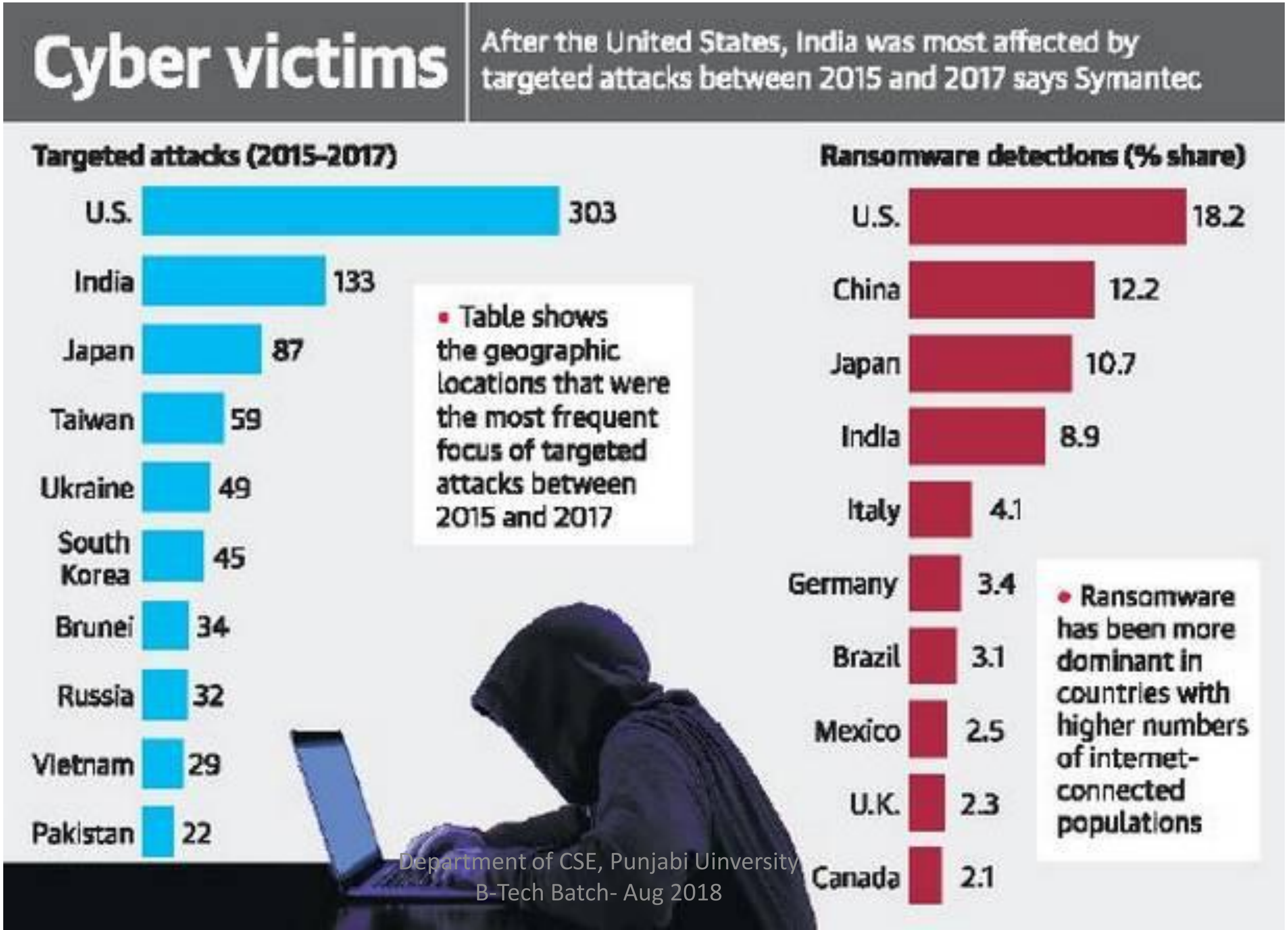
Or

Cyberspace is the imaginary environment in which communication over computer networks occurs using the Internet.

Cyber Threats

- According to ‘Internet Security Threat Report’ of 2017 by Symantec, The U.S. was most vulnerable to such attacks (26.61%) , followed by China (10.95%), and then India (5.09%) of global threats detected.
- The global threat ranking is based on eight metrics — Malware, Spam, Phishing, Bots, Network attacks, Web attacks, Ransomware and Cryptominers.

Threat Report 2017



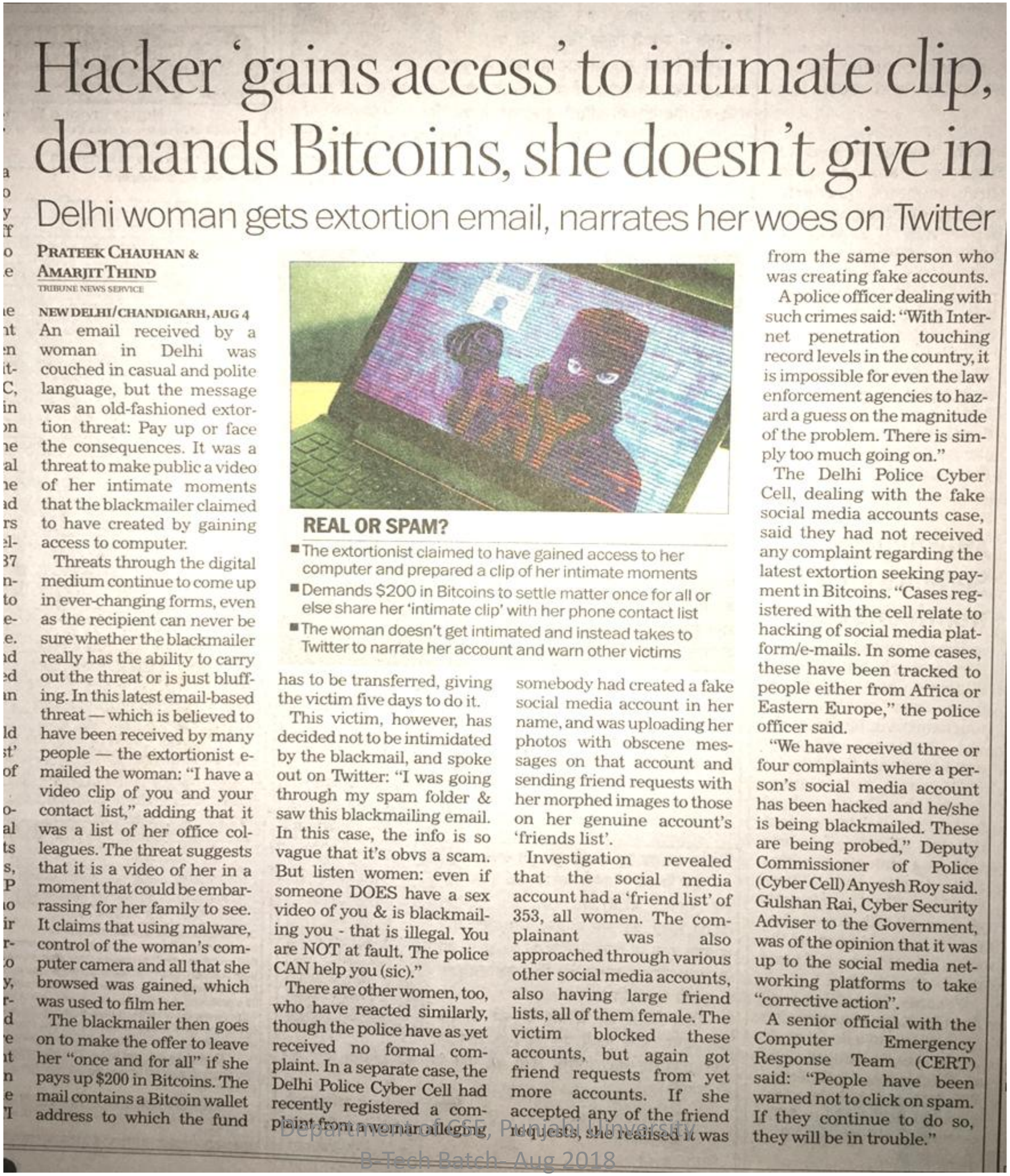
Cyber victims

After the United States, India was most affected by targeted attacks between 2015 and 2017 says Symantec

- Table shows the geographic locations that were the most frequent focus of targeted attacks between 2015 and 2017

- Ransomware has been more dominant in countries with higher numbers of internet-connected populations

The Tribune 4-8-2018



Hacker 'gains access' to intimate clip, demands Bitcoins, she doesn't give in

Delhi woman gets extortion email, narrates her woes on Twitter

PRATEEK CHAUHAN &
AMARJIT THIND
TRIBUNE NEWS SERVICE

NEW DELHI/CHANDIGARH, AUG 4

An email received by a woman in Delhi was couched in casual and polite language, but the message was an old-fashioned extortion threat: Pay up or face the consequences. It was a threat to make public a video of her intimate moments that the blackmailer claimed to have created by gaining access to computer.

Threats through the digital medium continue to come up in ever-changing forms, even as the recipient can never be sure whether the blackmailer really has the ability to carry out the threat or is just bluffing. In this latest email-based threat — which is believed to have been received by many people — the extortionist e-mailed the woman: "I have a video clip of you and your contact list," adding that it was a list of her office colleagues. The threat suggests that it is a video of her in a moment that could be embarrassing for her family to see. It claims that using malware, control of the woman's computer camera and all that she browsed was gained, which was used to film her.

The blackmailer then goes on to make the offer to leave her "once and for all" if she pays up $200 in Bitcoins. The mail contains a Bitcoin wallet address to which the fund has to be transferred, giving the victim five days to do it.

This victim, however, has decided not to be intimidated by the blackmail, and spoke out on Twitter: "I was going through my spam folder & saw this blackmailing email. In this case, the info is so vague that it's obvs a scam. But listen women: even if someone DOES have a sex video of you & is blackmailing you - that is illegal. You are NOT at fault. The police CAN help you (sic)."

There are other women, too, who have reacted similarly, though the police have as yet received no formal complaint. In a separate case, the Delhi Police Cyber Cell had recently registered a complaint from a woman alleging somebody had created a fake social media account in her name, and was uploading her photos with obscene messages on that account and sending friend requests with her morphed images to those on her genuine account's 'friends list'.

Investigation revealed that the social media account had a 'friend list' of 353, all women. The complainant was also approached through various other social media accounts, also having large friend lists, all of them female. The victim blocked these accounts, but again got friend requests from yet more accounts. If she accepted any of the friend requests, she realised it was from the same person who was creating fake accounts.

A police officer dealing with such crimes said: "With Internet penetration touching record levels in the country, it is impossible for even the law enforcement agencies to hazard a guess on the magnitude of the problem. There is simply too much going on."

The Delhi Police Cyber Cell, dealing with the fake social media accounts case, said they had not received any complaint regarding the latest extortion seeking payment in Bitcoins. "Cases registered with the cell relate to hacking of social media platform/e-mails. In some cases, these have been tracked to people either from Africa or Eastern Europe," the police officer said.

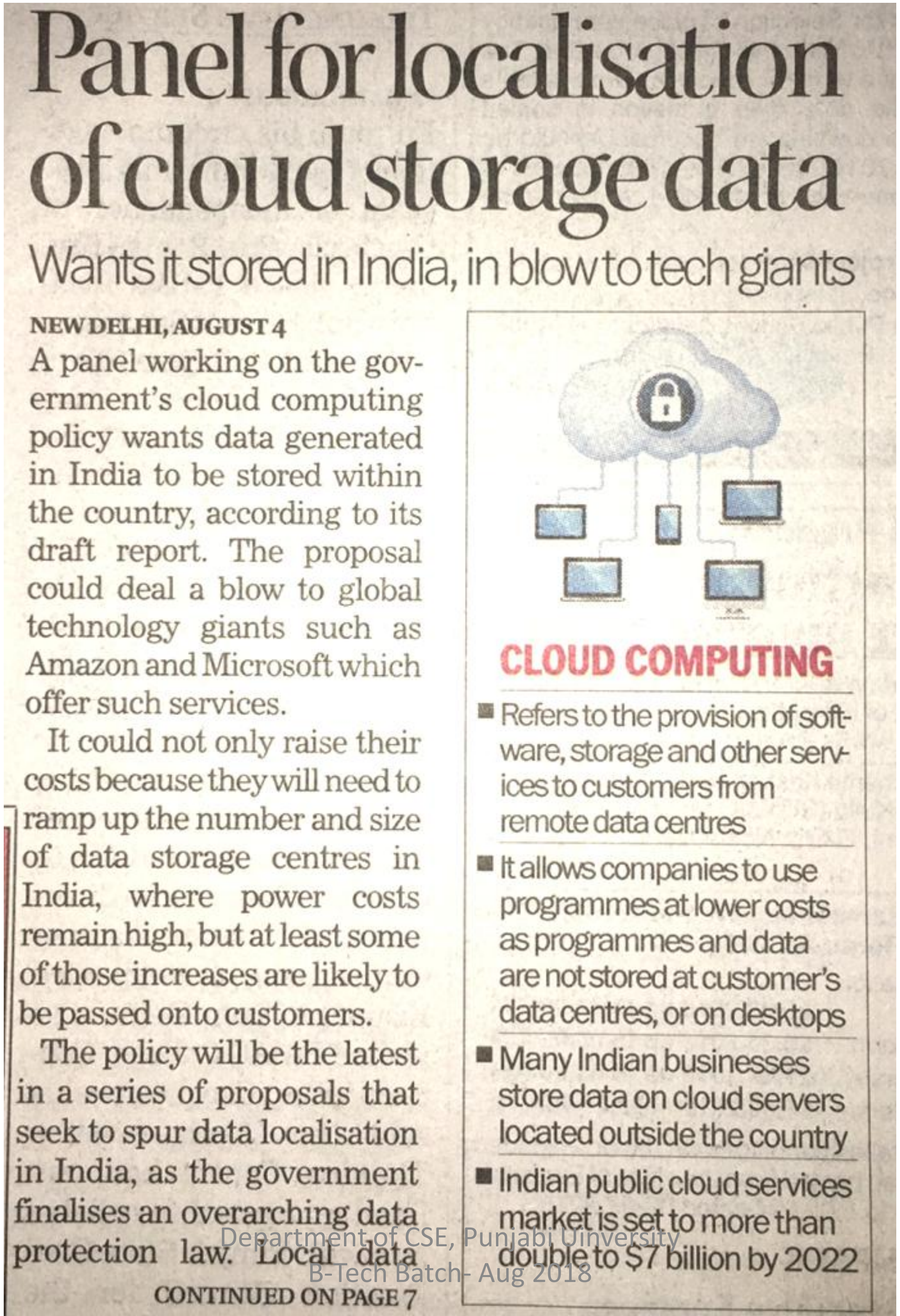
"We have received three or four complaints where a person's social media account has been hacked and he/she is being blackmailed. These are being probed," Deputy Commissioner of Police (Cyber Cell) Anyesh Roy said. Gulshan Rai, Cyber Security Adviser to the Government, was of the opinion that it was up to the social media networking platforms to take "corrective action".

A senior official with the Computer Emergency Response Team (CERT) said: "People have been warned not to click on spam. If they continue to do so, they will be in trouble."

REAL OR SPAM?

- The extortionist claimed to have gained access to her computer and prepared a clip of her intimate moments
- Demands $200 in Bitcoins to settle matter once for all or else share her 'intimate clip' with her phone contact list
- The woman doesn't get intimated and instead takes to Twitter to narrate her account and warn other victims

The Tribune 4-8-2018



Panel for localisation of cloud storage data

Wants it stored in India, in blow to tech giants

NEW DELHI, AUGUST 4

A panel working on the government's cloud computing policy wants data generated in India to be stored within the country, according to its draft report. The proposal could deal a blow to global technology giants such as Amazon and Microsoft which offer such services.

It could not only raise their costs because they will need to ramp up the number and size of data storage centres in India, where power costs remain high, but at least some of those increases are likely to be passed onto customers.

The policy will be the latest in a series of proposals that seek to spur data localisation in India, as the government finalises an overarching data protection law. Local data

CONTINUED ON PAGE 7

CLOUD COMPUTING

- Refers to the provision of software, storage and other services to customers from remote data centres
- It allows companies to use programmes at lower costs as programmes and data are not stored at customer's data centres, or on desktops
- Many Indian businesses store data on cloud servers located outside the country
- Indian public cloud services market is set to more than double to $7 billion by 2022

Cyberspace is facing a variety of other dangerous Threats

- **Cyber invasion**

(Cyber invasion is referred to the intrusion into networks to collect information, but neither add or modify data or interfere with the networks)

- **Cybercrime**

(Cybercrime is referred to the use of networks to carry out criminal activities such as selling illegal products)

- **Malware**

(Malware usually includes computer virus and worm, Trojan horse, spam and phishing)

- **Cyber attack**

(An attempt by hackers to damage or destroy a computer network or system)

- **Cyber vulnerabilities**

(Vulnerability is a weakness in the system (software and hardware components)) that can be exploited by attackers and impact to loss confidentiality, integrity, OR availability.)

Computer storage

Computer data storage, often called storage or memory, is a technology consisting of computer components and recording media that are used to retain digital data. It is a core function and fundamental component of computers.

Computer storage is measured in bytes, kilobytes (KB), megabytes (MB), gigabytes (GB) and increasingly terabytes (TB), PetaByte (PB). These will comprise the storage necessary to keep files internally on their computer, as well as those media required to back-up, transfer and archive data.

Types of Computer storage

- HARD DISK STORAGE

 (Spinning hard disk (HD) drives are today the most common means of high capacity computer storage)

- RAID

(Redundant Array of Independent Disks used on servers and high-end PC workstations)

- EXTERNAL HARD DISKS / DIRECT ATTACHED STORAGE (DAS)

(DAS external hard disks connect via a USB, firewire or an E-SATA interface)

- OPTICAL DISK STORAGE

(These are compact disk (CD), digital versatile disk (DVD)and Blu-Ray disk (BD))

- SOLID STATE DRIVES

(Solid state storage devices store computer data on non-volatile "flash" memory chips)

- NETWORK AND ONLINE STORAGE

(The disk is located remotely to your computer, can be accessed from anywhere using network)

- CLOUD DATA STORAGE

(An online file space can be thought of as a hard disk in the cloud that can be accessed with a web browser to upload or download files)

Mobile Phone

A mobile phone is a wireless handheld device that allows users to make and receive calls and to send text messages, among other features. The earliest generation of mobile phones could only make and receive calls. Today’s mobile phone with advanced features similar to a computer is called a smartphone, however, are packed with many additional features, such as web browsers, games, cameras, video players and even navigational systems.

Mobile phones belonging to the Global System for Mobile Communications (GSM) Network. A mobile phone may also be known as a cellular phone or simply a cell phone typically operates on a cellular network, which is composed of cell sites scattered throughout cities.

Mobile Device Forensics Overview

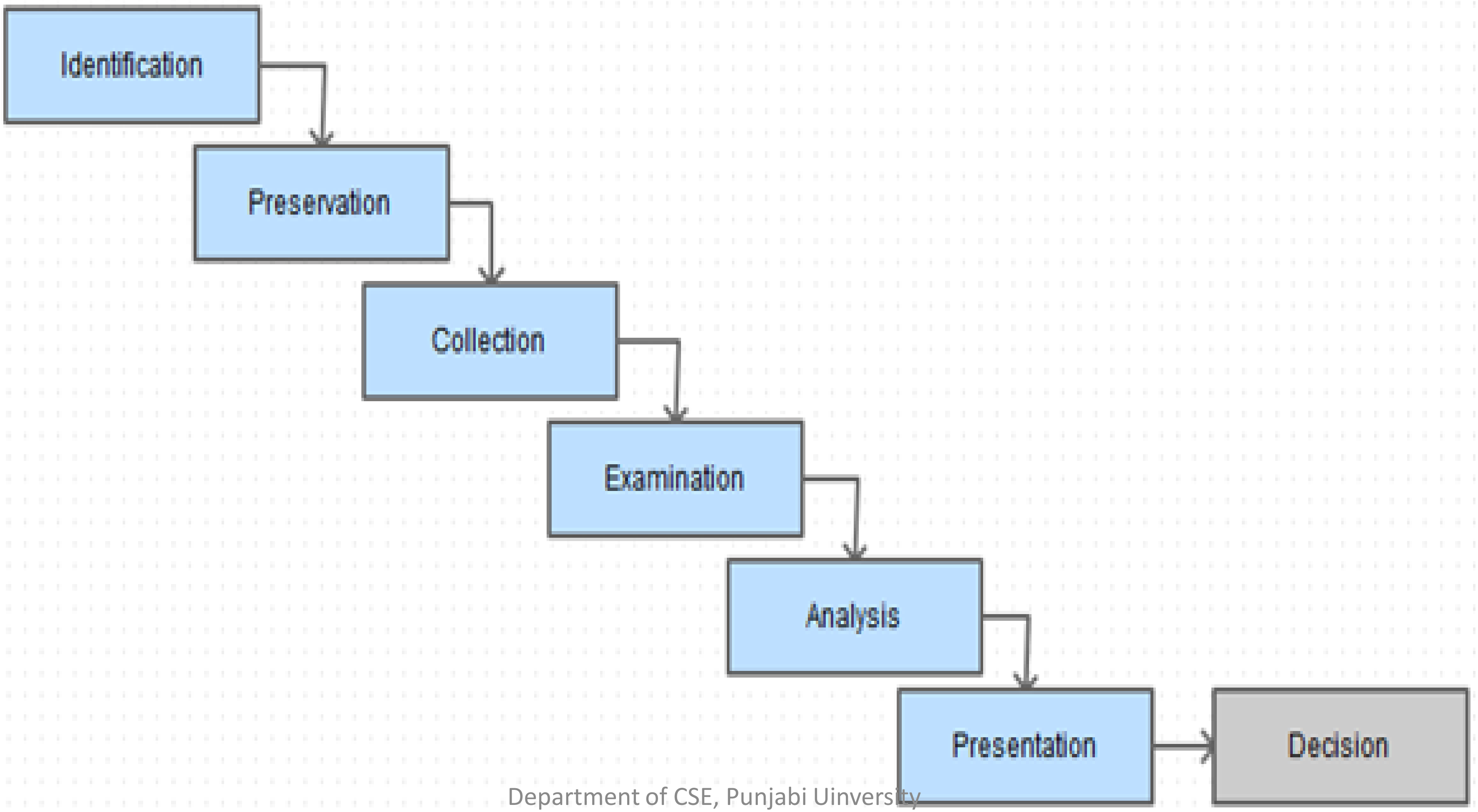
- Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes, SMS and MMS messages.

- There is growing need for mobile forensics due to several reasons are:
  - Use of mobile phones to store and transmit personal and corporate information
  - Use of mobile phones in online transactions
  - Law enforcement, criminals and mobile phone devices

Mobile Forensics

- Mobile forensics is the process to analyses the mobile phone to detect and collect the evidences related to the crime. A method is proposed to analyze the mobile phone to detect crime, main focus of the method is to analyze mobile phone internal and external memory and SIM card. Mobile forensic process of mobile devices

Digital Forensic



Mobile Device Forensics Overview

Today’s Cellular Standards:

CDMA code code divison multiple access, GSM Global System for mobile communication , iDEN(integrated Digital Enhanced Network), (TDMA, AMPS almost gone)

CDMA

Worldwide: +500 Million Subscribers

CDMA is largely in U.S., Asia Pacific (155 Mil), Latin America (71.5 Mil)

source: cdg.org

Major CDMA Network Operators: Verizon, Sprint, Alltel, Leap, U.S. Cellular.

GSM / 3G GSM (UMTS (Universal Mobile Telecommunication System))

Worldwide: +4.5 Billion Subscribers (including 3G, WCDMA, HSPDA)

source: gsmworld.com

Major U.S. GSM Network Operators: AT+T, T-Mobile, Alltel, SunCom, Dobson, CellularOne.

SIM Card

iDEN – 7 Operators – +30 Million subscribers

Major iDen Operators: Nextel, SouthernLINC Wireless, Boost (MVNO) Telus (Canada)

A Motorola Technology – Only Motorola Phones!

GSM and iDEN Both Use The SIM Card: Subscriber Identity Module

Mobile Device Forensics Overview

Cell Phone Forensics Short History

- **Working in Mobile Forensics since 2003**
- **Originated in Europe and focused on the GSM SIM card.** Roaming of Devices from Network and Spectrum Required - I.D. Info on SIM – Also SMS, Phonebooks, and Last Numbers Dialed on SIM
- **Terrorist use of phones as IED detonators** Increased the demand for mobile forensics. Mobile device forensics is making a real impact in the war on terror.
- **Adoption Has Moved Quickly From Federal to Local Level and Now Enterprise, Prisons, Schools, etc.**

Mobile Device Forensics Overview

The Big Difference:

- **Computer Forensics:** – **Only a Few Major Operating System Standards:** Windows, Mac, Linux. Standard practice is to image the Harddrive and Examine Data.

- **Cell Phone Forensics:** – **Multiple Operating Systems**. Various Communication Standards. Each manufacturer has their own: Nokia, Samsung, Motorola, Palm, Blackberry, etc., etc. Communication Standards Evolving. **Started this way but is consolidating to four or five. Mobile Forensics is becoming more like computer forensics in some ways.**

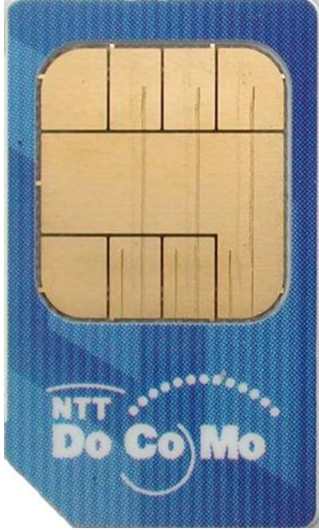
- **Mobility Aspect:** - **Phones are Live Things Roaming Around**. It's not just about what's on the device, but where has it been and what connections have been made?

Networks Are Managing The Massive Data in Different Ways – Lots There.

What's retained by the network varies from carrier to carrier, but apart from the billing essentials, not much data is saved after 30 days. Some Exceptions.

Mobile Device Forensics Overview

Start with the SIM on GSM Phones



FROM GSM and iDEN Phone SIM Cards (Partial List):

- IMSI: International Mobile Subscriber Identity
- ICCID: Integrated Circuit Card Identification (SIM Serial No.)
- MSISDN: Mobile Station Integrated Services Digital Network (phone number)
- Network Information
- LND: Last Number Dialled (sometimes, not always, depends on the phone)
- ADN: Abbreviated Dialled Numbers (Phonebook)
- SMS: Text Messages, Sent, Received, Deleted, Originating Number, Service Center (also depends on Phone)
- SMS Service Center Info: GPRS Service Center Info:
- Location Information: The GSM channel (BCCH) and Location Area Code (LAC) when phone was used last.

* When SIM Locked – Cannot Be Cracked without Network Operator Assistance.

Not on SIM, but Exclusive To GSM Devices

- IMEI: International Mobile Equipment Identity. - To Find IMEI,

  Type #*06#. IMEI is on the Device, registers with the network, along with IMSI. IMSI+IMEI+MSISDN the most detailed identity information of user.

Remember… Only GSM and Nextel Phones have SIMs. Not in CDMA (Verizon, Sprint)

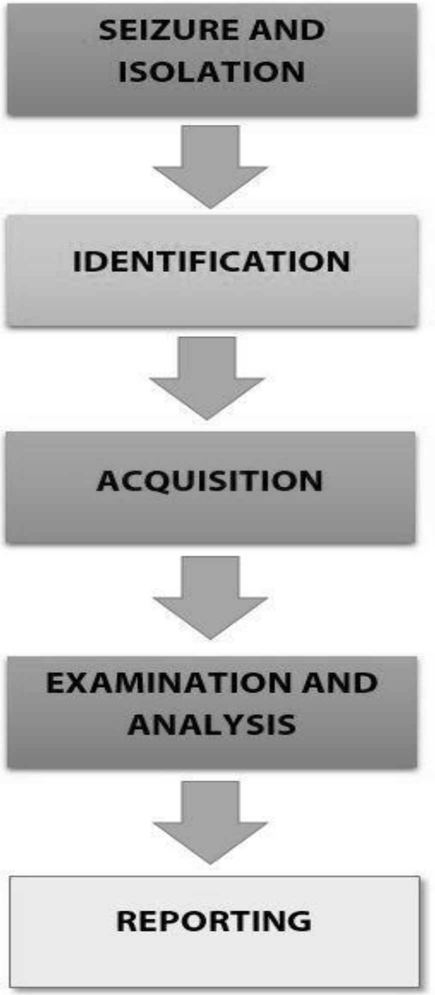
A PIN Locked SIM is Not Accessible Without PIN – Requires PUK From Carrier

Mobile Device Forensics Overview

What Can Be Pulled from the Device (Best case scenario from Logical Tools)

- Phonebook
- Call History and Details (To/From)
- Call Durations
- Text Messages with identifiers (sent-to, and originating) Sent, received, deleted messages
- Multimedia Text Messages with identifiers
- Photos and Video (also stored on external flash)
- Sound Files (also stored on external flash)
- Network Information, GPS location
- Phone Info (CDMA Serial Number)
- Emails, memos, calendars, documents, etc. from PDAs.
- Today with Smartphones – GPS Info, Social Networking Data

Mobile Forensics Process



Seizure:

Prior to the actual examination digital media will be seized. This phase is very important in mobile forensics; It Collects the digital evidence provided in the mobile device. In this phase the investigator preserve the device in its original stage. As in this phase the cell phones are seized that are involved in the activity, so that there should not be any change in the evidences. Seize the mobile device means to cut off all the wireless networks. Any failure in this stage will result in the failure of all the rest stages. The goal of seizure is to preserve the evidence as it avoids shut down the device.

Acquisition:

Once exhibits have been seized an exact sector level duplicate of the media is created, usually via a write blocking device, a process referred to as Imaging or Acquisition. The duplicate is created using a hard-drive duplicator or software imaging tools such as DCFLdd, IXimager, Guymager, TrueBack, EnCase. The original drive is then returned to secure storage to prevent tampering.

The acquired image is verified by using the SHA-1 or MD5 hash functions. At critical points throughout the analysis, the media is verified again, known as "hashing", to ensure that the evidence is still in its original state.

The second phase is acquisition phase after the preservation on the device is done. This phase chooses a right method and approach for analysis phase and the phase starts when the device is received at the forensic lab. In this phase the model and type of device is identified. After this the right tool for the acquisition is to be choose as this is very difficult because there are many no of devices in the market.

Analysis:

After acquisition the contents of (the HDD) image files are analysed to identify evidence that either supports or contradicts a hypothesis or for signs of tampering (to hide data).

During the analysis an investigator usually recovers evidence material using a number of different methodologies (and tools), often beginning with recovery of deleted material. Examiners use specialist tools (EnCase, ILOOKIX, FTK, etc.) to aid with viewing and recovering data. The type of data recovered varies depending on the investigation; but examples include email, chat logs, images, internet history or documents. The data can be recovered from accessible disk space, deleted (unallocated) space or from within operating system cache files.

Various types of techniques are used to recover evidence, usually involving some form of keyword searching within the acquired image file; either to identify matches to relevant phrases or to parse out known file types. Certain files (such as graphic images) have a specific set of bytes which identify the start and end of a file, if identified a deleted file can be reconstructed. Many forensic tools use hash signatures to identify notable files or to exclude known (benign) ones; acquired data is hashed and compared to pre-compiled lists such as the Reference Data Set (RDS) from the National Software Reference Library On most media types including standard magnetic hard disks, once data has been securely deleted it can never be recovered. SSD Drives are specifically of interest from a forensics viewpoint, because even after a secure-erase operation some of the data that was intended to be secure erased persists on the drive. Once evidence is recovered the information is analyzed to reconstruct events or actions and to reach conclusions, work that can often be performed by less specialist staff. Digital investigators, particularly in criminal investigations, have to ensure that conclusions are based upon data and their own expert knowledge.

Reporting:

Presentation phase shows the result of the analysis phase. The forensic examiner should know the expectations of the audience as different audience have different expectations. As when investigator come to know about the expectations of the audience it is easy for him to prepare the presentation. Whatever data is collected is presented in the presentation phase. When an investigation is completed the information is often reported in a form suitable for nontechnical individuals. Reports may also include audit information and other meta-documentation.

When completed reports are usually passed to those commissioning the investigation, such as law enforcement (for criminal cases) or the employing company (in civil cases), who will then decide whether to use the evidence in court. Generally, for a criminal court, the report package will consist of a written expert conclusion of the evidence as well as the evidence itself.

Computer Ethics

Ethics is a set of moral principles that govern the behavior of a group or individual. Therefore, computer ethics is set of moral principles that regulate the use of computers. Some common issues of computer ethics include intellectual property rights (such as copyrighted electronic content), privacy concerns, and how computers affect society. As technology advances, computers continue to have a greater impact on society.

Types of Computer Ethics

- Basic Netiquette
- Plagiarism
- Copyright
- Privacy

Basic Netiquette

- Don't use a computer to harm other people.
- Don't interfere with other people’s computer work.
- Don't use a computer to steal.
- Don't copy or use proprietary software for which you have not paid.
- Don't use other people’s computer resources without authorization or proper compensation.
- Use a computer in ways that show consideration and respect for your fellow humans.

Plagiarism

Plagiarism is presenting someone else’s work as your own; this includes work represented in hard copy, on disk, or on the Internet. Make sure you summarize, or at least change the order of the words when using someone else’s work as a reference. Also be sure to cite that work as something you have used to gain the information you are presenting. Anything that is directly quoted from any source must be put in quotation marks and cited as well.

Copyright infringements can get you sued. They encompass anything that anyone has expressed in any way. A person does not need to express their copyright or even actually register it, a person’s ideas are their own and it is illegal to pretend that they are yours.

Copyright

- **Software Piracy**

  Public Domain
- Some software is free to use, copy, and/or change, but only do so if there is written notice that the software is in the public domain. Look for this notice in the “read me” files that accompany programs.

  General Public License
- GPL software has the same restrictions as public domain software, but cannot be sold for profit.

  Shareware
- Using shareware programs is free, but it is illegal to copy or modify them without permission since they are copyrighted. Most shareware programs are really trial versions of the software, which must be paid for after the trial period has expired

Privacy

The right to privacy is a multidimensional concept. In modern society right to privacy has been recognized both in the eye of the law and in common parlance. **Article 21 protects the right to privacy and promotes the dignity of the individual.**

In recent years there has been a growing fear about the large amount of information about individuals held in computer files. The right to privacy refers to the specific right of an individual to control the collection, use and disclosure of personal information. Personal information could be in the form of personal interests, habits and activities, family records, educational records, communications (including mail and telephone) records, medical records and financial records.

Section A

Part-II

- Cyber Law
- Digital Signature
- Intellectual property
- Need for cyber law and forensics
- Jurisprudence of Cyber Law

Cyber Law

Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

Cyber Law encompasses laws relating to:

1. Cyber Crimes

2. Electronic and Digital Signatures

3. Intellectual Property

4. Data Protection and Privacy

Cyber Crimes

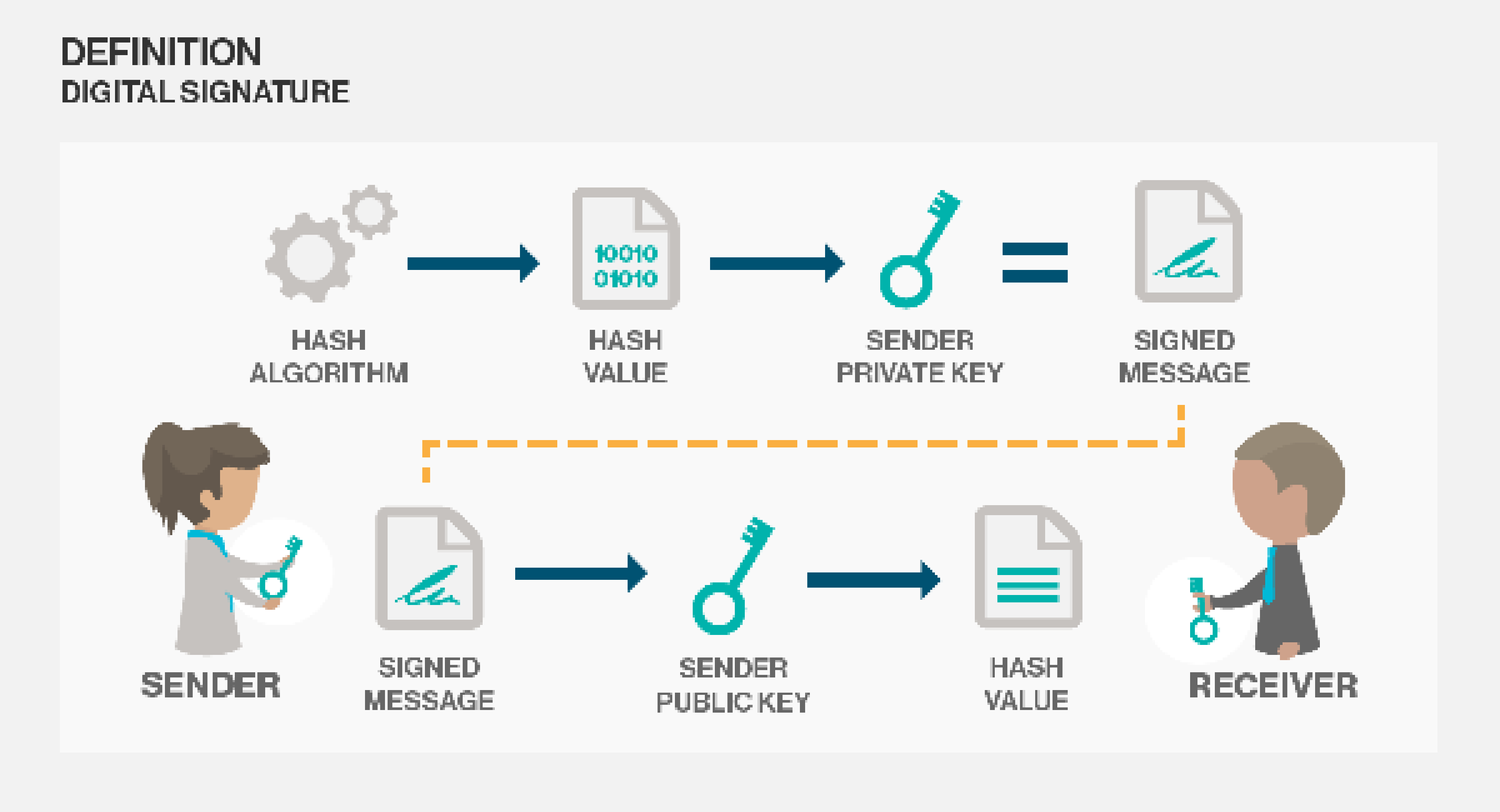
Cyber crimes are unlawful acts where the crime done with the use of computer either computer being the tool or target or both. The huge growth in electronic commerce (e-commerce) and online share trading has led to a exceptional explode in incidents of cyber crime.

To protect the citizens from cyber crime Indian Cyber laws i.e., Information Technology Act, 2000 was enacted. The act provides for the types of cyber crime and punishment for the same.

Digital Signature

A digital signature is a technique to validate the authenticity of a digital message or a document.

A valid digital signature provides the surety to the recipient that the message was generated by a known sender, such that the sender cannot deny having sent the message. Digital signatures are mostly used for software distribution, financial transactions, and in other cases where there is a risk of forgery.

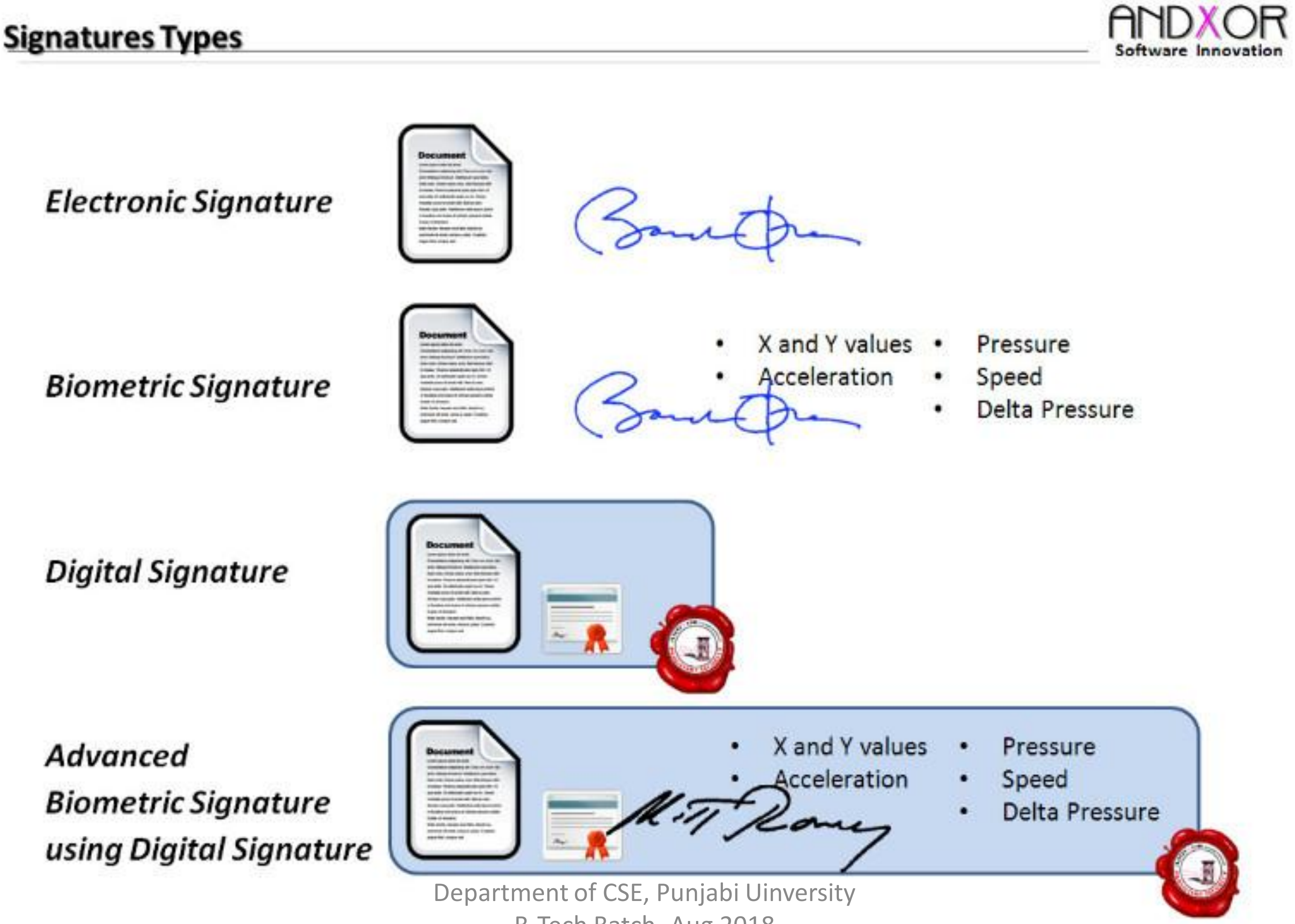

DEFINITION
DIGITAL SIGNATURE
HASH ALGORITHM
10010 01010
HASH VALUE
SENDER PRIVATE KEY
SIGNED MESSAGE
SENDER
SIGNED MESSAGE
SENDER PUBLIC KEY
HASH VALUE
RECEIVER

Electronic Signature

An E-signature can be defined as a schematic script related with a person. A signature on a document is a sign that the person accepts the purposes recorded in the document. In many engineering companies digital seals are also required for another layer of authentication and security. Digital seals and signatures are same as handwritten signatures and stamped seals.

Digital Signature was the term defined in the old I.T. Act, 2000. Electronic Signature is the term defined by the amended act (I.T. Act, 2008). The concept of Electronic Signature is broader than Digital Signature.

Types of Signature



Signatures Types

Electronic Signature

Biometric Signature

- X and Y values
- Acceleration
- Pressure
- Speed
- Delta Pressure

Digital Signature

Advanced Biometric Signature using Digital Signature

- X and Y values
- Acceleration
- Pressure
- Speed
- Delta Pressure

Digital and E-Signature

Electronic signatures are used to authenticate electronic records. Digital signatures are one type of electronic signature. Digital signatures satisfy three major legal requirements – signer authentication, message authentication and message integrity. The technology and efficiency of digital signatures makes them more trustworthy than hand written signatures.

Intellectual property rights

- Intellectual property rights are the legal rights that cover the privileges given to individuals who are the owners and inventors of a work, and have created something with their intellectual creativity. Individuals related to areas such as literature, music, invention, etc., can be granted such rights, which can then be used in the business practices by them.
- The creator/inventor gets exclusive rights against any misuse or use of work without his/her prior information. However, the rights are granted for a limited period of time to maintain equilibrium.

Types of Intellectual Property Rights

Intellectual Property Rights can be further classified into the following categories:

- Copyright
- Patent
- Trademark
- Trade Secrets, etc.

Intellectual property

Intellectual property is refers to creations of the human mind e.g. a story, a song, a painting, a design etc. The facets of intellectual property that relate to cyber space are covered by cyber law.

These include:

- Copyright law in relation to computer software, computer source code, websites, cell phone content etc,
- Software and source code licenses
- Trademark law with relation to domain names, meta tags, mirroring, framing, linking etc
- Semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts,
- Patent law in relation to computer hardware and software.

Privacy

The appropriate use of personal information under the circumstances: What is appropriate Will depend on context, law and the individual's expectations, also the right of an individual to control the collection use and disclosure of information.

Data Protection

The management of personal information and assurance that data not corrupted and accessible only for authorized purpose

Or

The implementation of appropriate administrative technical or physical means to guard against unauthorized intentional or accidental disclosure, modification or destruction of data

Data protection and privacy

Data protection and privacy laws aim to achieve a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, email service providers etc. These laws seek to address the challenges to privacy caused by collecting, storing and transmitting data using new technologies.

Need Cyber Law

Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber laws is a very technical field and that it does not have any bearing to most activities in Cyberspace.

Cyber Forensics

Cyber forensics, also called computer forensics or digital forensics, is the process of extracting information and data from computers to serve as digital evidence - for civil purposes or, in many cases, to prove and legally prosecute cyber crime.

New court rulings are issued that affect how Cyber/Computer forensics is applied. Increasingly, laws are being passed that require organizations to safeguard the privacy of personal data.

Jurisprudence of Cyber Law

Jurisprudence studies the concepts of law and the effect of social norms and regulations on the development of law.

Jurisprudence refers to two different things.

1. The philosophy of law, or legal theory

   Legal theory does not study the characteristics of law in a particular country (e.g. India or Canada) but studies law in general i.e. those attributes common to all legal systems.

2. Case Law

   Case law is the law that is established through the decisions of the courts and other officials. Case law assumes even greater significance when the wordings of a particular law are ambiguous. The interpretation of the Courts helps clarify the real objectives and meaning of such laws.

Section A

Part-III

- Footprinting
- DNS Enumeration
- WHOIS
- Network Reconnaissance
- Email Spoofing
- Internet Time theft

Footprinting

Footprinting is a part of exploration process which is used for gathering possible information about a target computer system or network by hackers as first step for intrude into system.

Foot printing could be both passive and active. Reviewing a company's website is an example of passive foot printing, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.

DNS Enumeration

DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. A company may have both internal and external DNS servers that can yield information such as usernames, computer names, and IP addresses of potential target systems. There are a lot of tools that can be used to gain information for performing DNS enumeration. The examples of tool that can be used for DNS enumeration are NSlookup, DNSstuff, American Registry for Internet Numbers (ARIN), and Whois. To enumerate DNS, you must have understanding about DNS and how it work

DNS Enumeration

Domain Name Server (DNS) is like a map or an address book. In fact, it is like a distributed database which is used to translate an IP address 192.111.1.120 to a name www.example.com and vice versa.

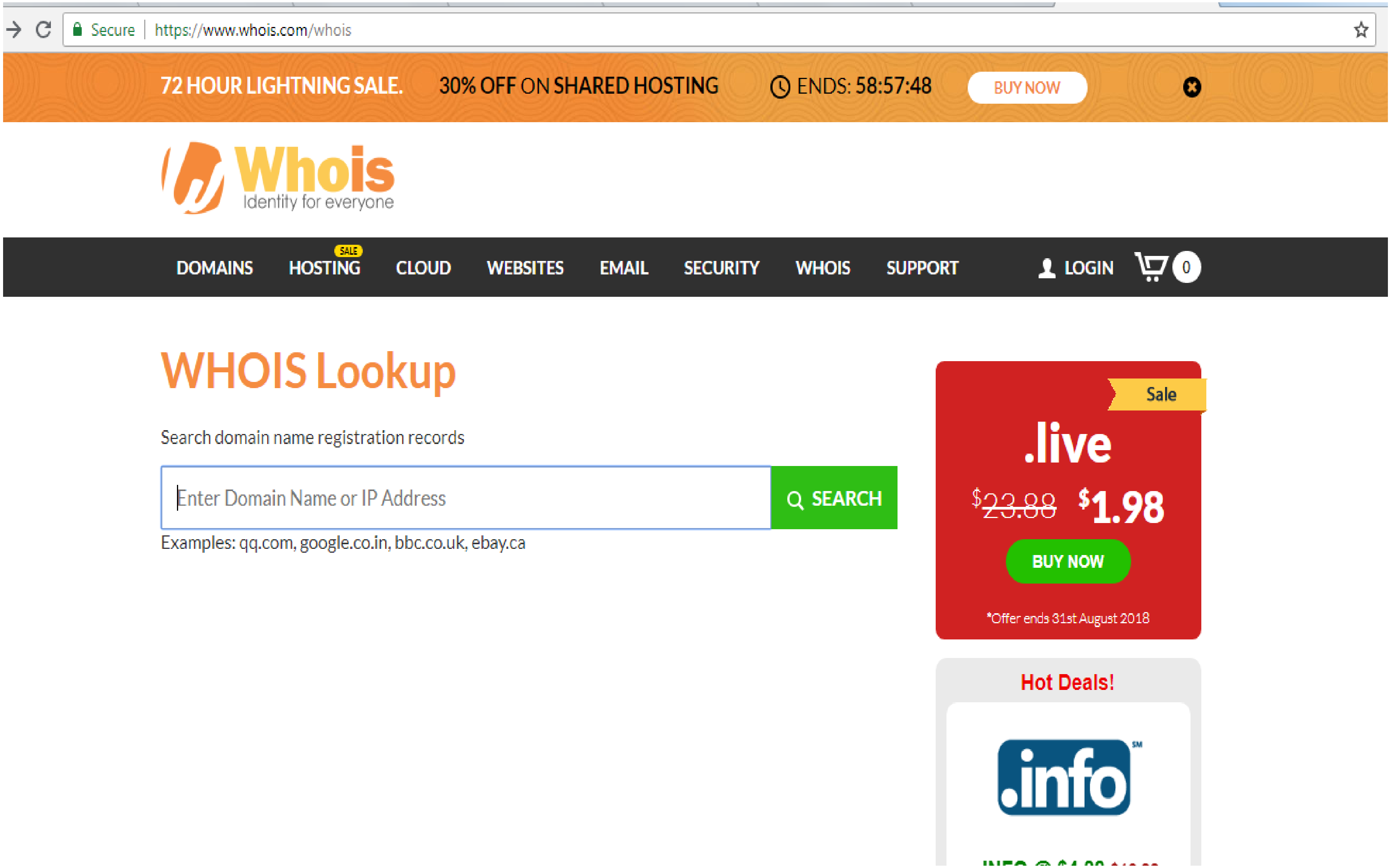
DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. The idea is to gather as much interesting details as possible about your target before initiating an attack.

You can use nslookup command available on Linux to get DNS and host-related information. In addition, you can use the following DNSenum script to get detailed information about a domain:

WHOIS

WHOIS (pronounced as the phrase who is) is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information.

You can use http://www.whois.com/whois website to get other detailed information about a domain name information including its owner, its registrar, date of registration, expiry,name server, owner's contact information, etc



Secure | https://www.whois.com/whois

72 HOUR LIGHTNING SALE. 30% OFF ON SHARED HOSTING ENDS: 58:57:48 BUY NOW

Whois
Identity for everyone

DOMAINS | HOSTING SALE | CLOUD | WEBSITES | EMAIL | SECURITY | WHOIS | SUPPORT | LOGIN | 0

WHOIS Lookup

Search domain name registration records

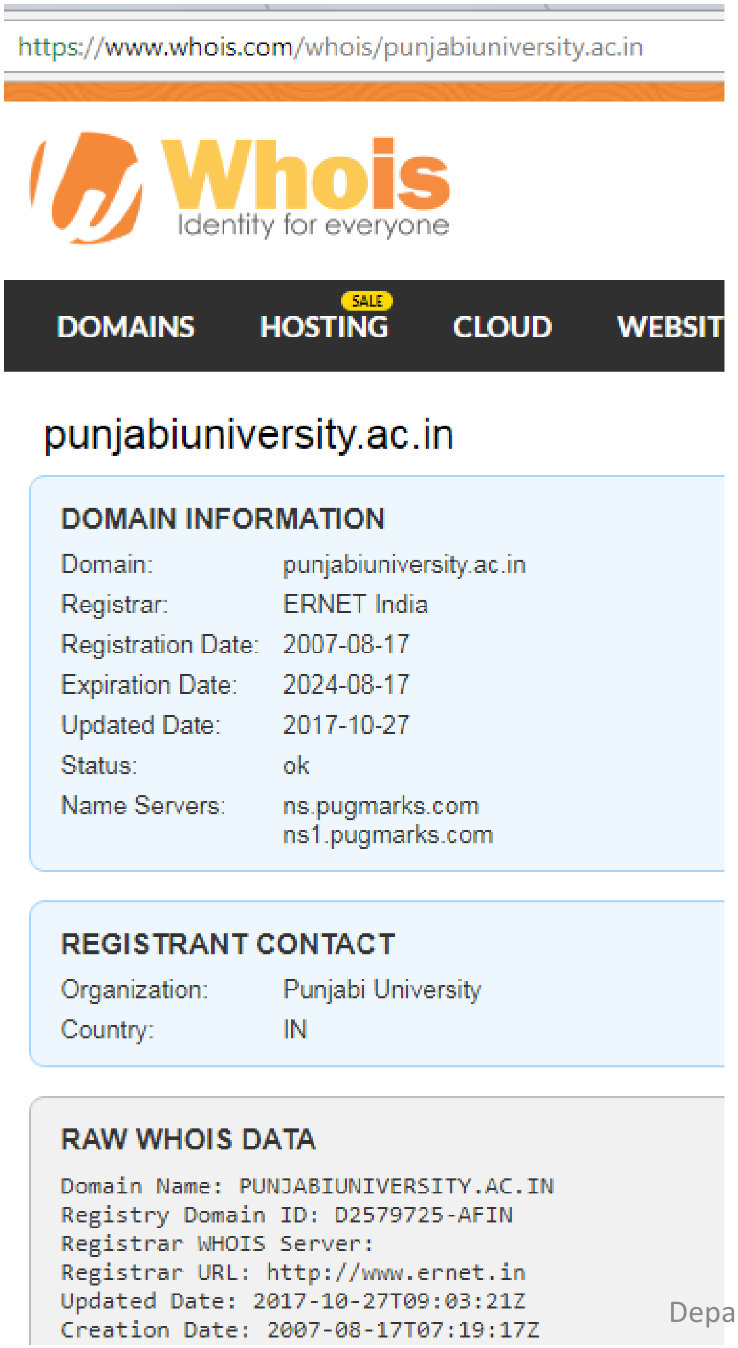
Enter Domain Name or IP Address | SEARCH

Examples: qq.com, google.co.in, bbc.co.uk, ebay.ca

Sale
.live
$~~23.88~~ $1.98
BUY NOW
*Offer ends 31st August 2018

Hot Deals!

.info SM



https://www.whois.com/whois/punjabiuniversity.ac.in

punjabiuniversity.ac.in

DOMAIN INFORMATION

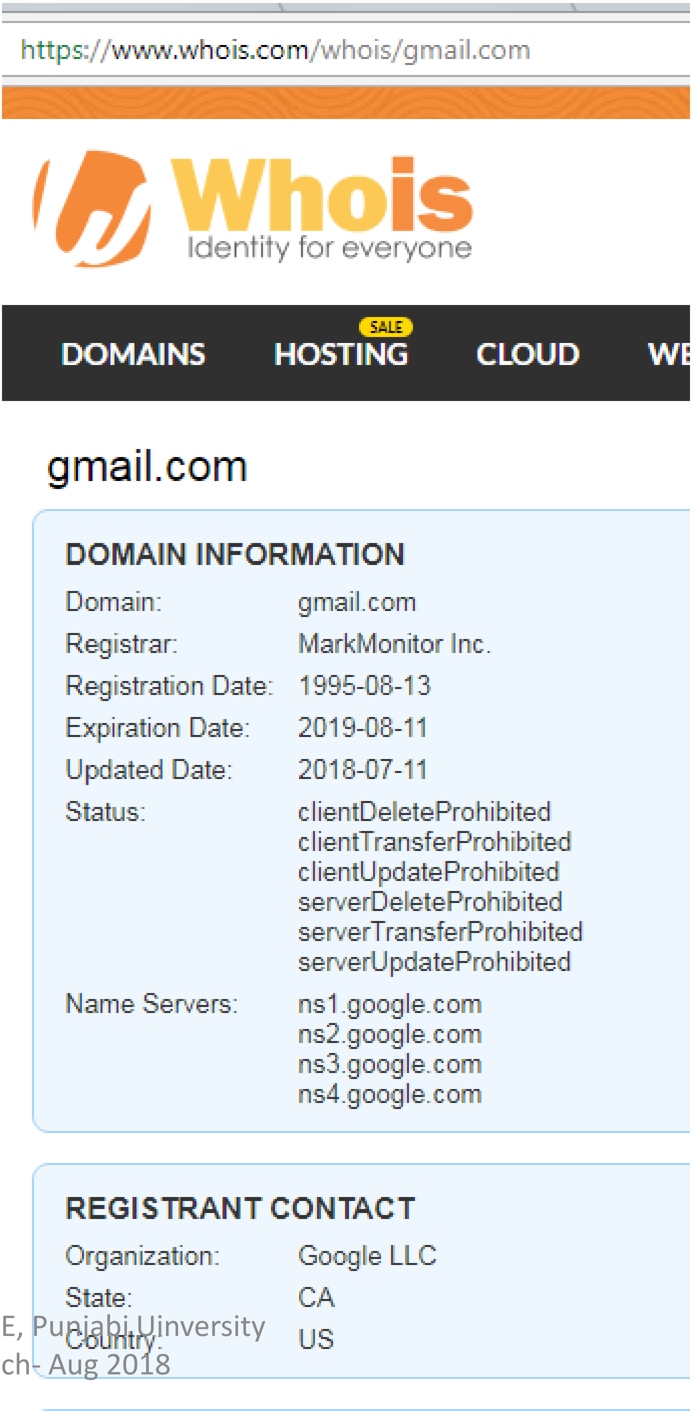
Domain:	punjabiuniversity.ac.in
Registrar:	ERNET India
Registration Date:	2007-08-17
Expiration Date:	2024-08-17
Updated Date:	2017-10-27
Status:	ok
Name Servers:	ns.pugmarks.com ns1.pugmarks.com

REGISTRANT CONTACT

Organization:	Punjabi University
Country:	IN

RAW WHOIS DATA

```
Domain Name: PUNJABIUNIVERSITY.AC.IN
Registry Domain ID: D2579725-AFIN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2017-10-27T09:03:21Z
Creation Date: 2007-08-17T07:19:17Z
```



https://www.whois.com/whois/gmail.com

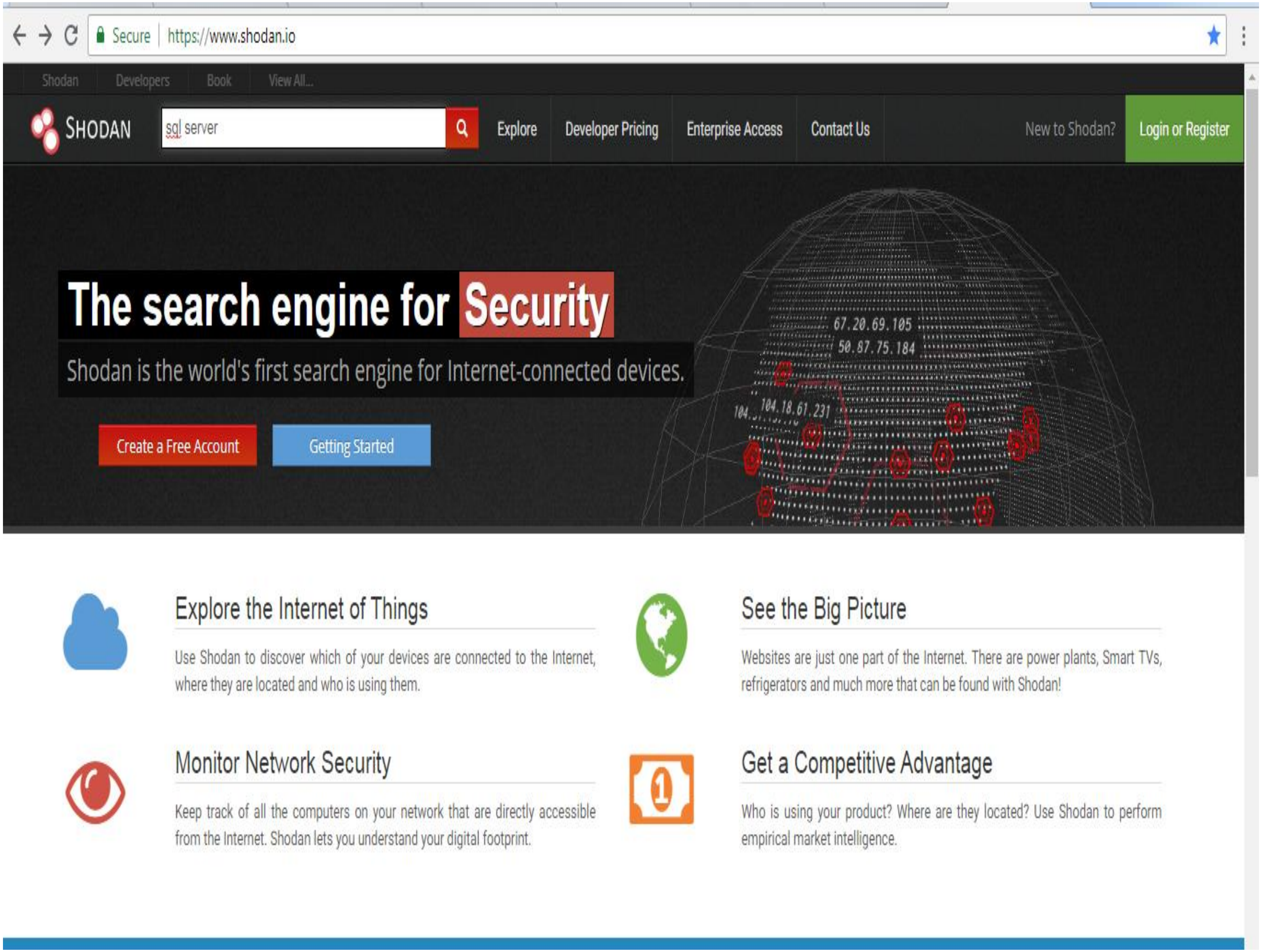
gmail.com

DOMAIN INFORMATION

Domain:	gmail.com
Registrar:	MarkMonitor Inc.
Registration Date:	1995-08-13
Expiration Date:	2019-08-11
Updated Date:	2018-07-11
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1.google.com ns2.google.com ns3.google.com ns4.google.com

REGISTRANT CONTACT

Organization:	Google LLC
State:	CA
Country:	US



The search engine for Security

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

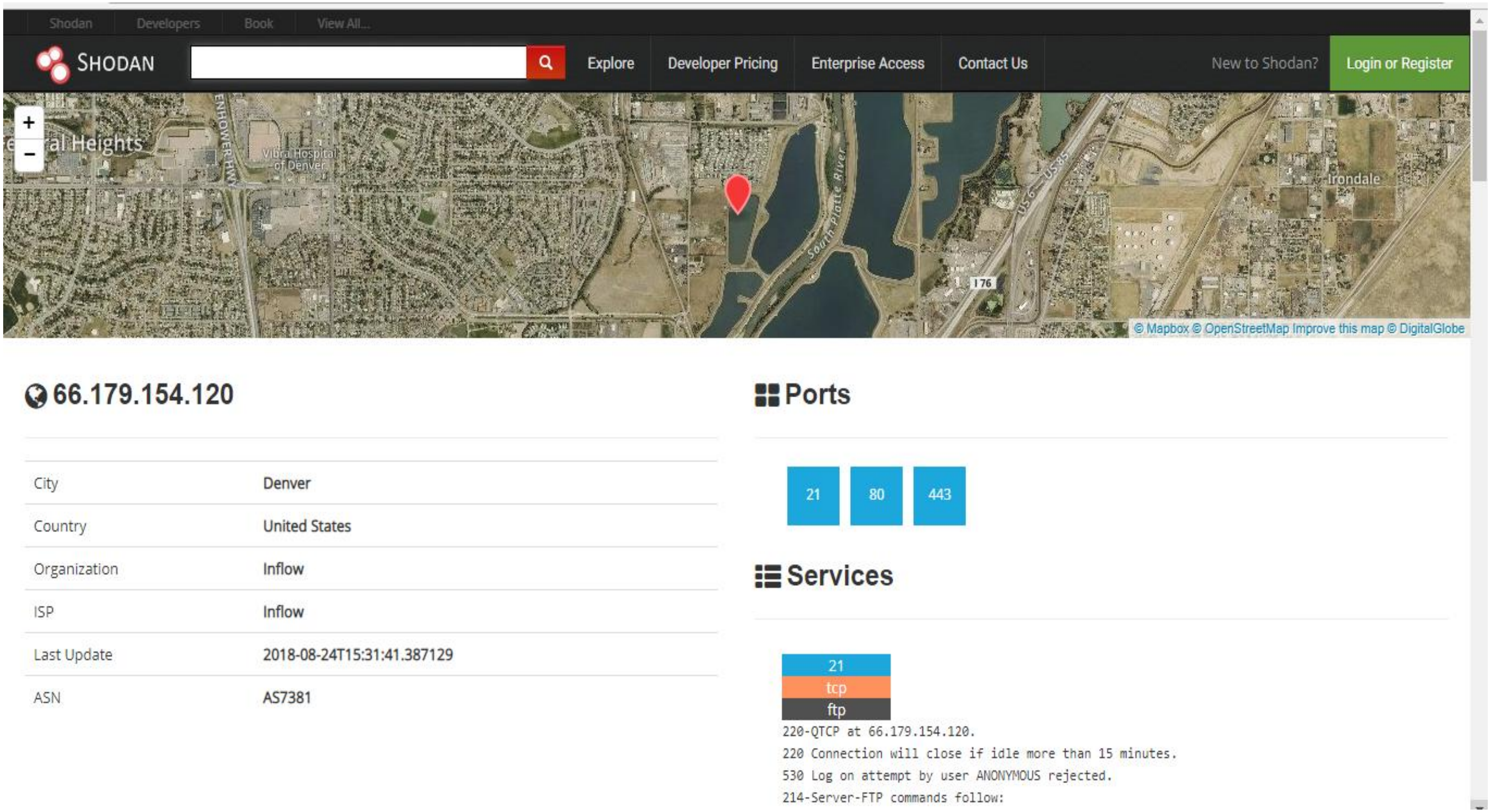
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.



66.179.154.120

City	Denver
Country	United States
Organization	Inflow
ISP	Inflow
Last Update	2018-08-24T15:31:41.387129
ASN	AS7381

Ports

21 80 443

Services

21
tcp
ftp

```
220-QTCP at 66.179.154.120.
220 Connection will close if idle more than 15 minutes.
530 Log on attempt by user ANONYMOUS rejected.
214-Server-FTP commands follow:
```

Network Reconnaissance

Network reconnaissance is a term for testing for potential vulnerabilities in a computer network. This may be a legitimate activity by the network owner/operator, seeking to protect it or to enforce its acceptable use policy. It also may be a precursor to external attacks on the network.

Passive reconnaissance is an attempt to gain information about targeted computers and networks without actively engaging with the systems.

In active reconnaissance, in contrast, the attacker engages with the target system, typically conducting a port scan to determine find any open ports.

Email Spoofing

Email Hijacking, or email hacking, is a widespread menace nowadays. It works by using the following three techniques which are email spoofing, social engineering tools, or inserting viruses in a user computer.

Email spoofing is the creation of email messages with a forged sender address. Because the core email protocols do not have any mechanism for authentication, it is common for spam and phishing emails to use such spoofing to mislead the recipient about the origin of the message.

Email Bombing

In Internet usage, an email bomb is a form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.

Data Diddling

Data Diddling (also called false data entry) is the unauthorized changing of data before or during their input to a computer system. Examples are forging or counterfeiting documents and exchanging valid computer tapes or cards with prepared replacements.

DoS Attack

In computing, a denial-of-service attack (DoS attack) is a cyber-attack where the executor seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Virus

A computer virus is a type of malicious software program ("malware") that, when executed, replicates itself by modifying other computer programs and inserting its own code. Infected computer programs can include, as well, data files, or the "boot" sector of the hard drive.

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate.

Types of Viruses

- File infector viruses

  Examples are Jerusalem and Cascade.

- Boot sector viruses

  Examples are Disk Killer, Michelangelo, and Stoned.

- Master boot record viruses

  MBR infectors are NYB, AntiExe, and Unashamed.

- Macro viruses

  Macro are W97M.Melissa, WM.NiceDay, and W97M.Groov.

Worms

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate.

Although worms generally exist inside of other files, often Word or Excel documents. The entire document will travel from computer to computer, so the entire document should be considered the worm. PrettyPark. Worm is a particularly prevalent example.

Trojan horses

Trojan horses are impostors--files that claim to be something desirable but, in fact, are malicious. A very important distinction from true viruses is that they do not replicate themselves, as viruses do. Trojans contain malicious code, that, when triggered, cause loss, or even theft, of data. In order for a Trojan horse to spread, you must, in effect, invite these programs onto your computers--for example, by opening an email attachment.

Phishing, Vishing, Smishing, & Pharming

Phishing (email), vishing (phone), smishing (text message) and pharming (redirect web site) are all methods used by criminals to fraudulently obtain personal information such as a social security number, bank account information, or credit card information. Each method has its own distinguishing characteristics, but they all have the same goal: stealing your money.

Blended Threat

A blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan horses and malicious code into one single threat. Blended threats can use server and Internet vulnerabilities to initiate, then transmit and also spread an attack

Keyloggers

A keylogger is a type of surveillance software (considered to be either software or spyware) that has the capability to record every keystroke you make to a log file, usually encrypted. A keylogger recorder can record instant messages, e-mail, and any information you type at any time using your keyboard. The log file created by the keylogger can then be sent to a specified receiver. Some keylogger programs will also record any e-mail addresses you use and Web site URLsyou visit.

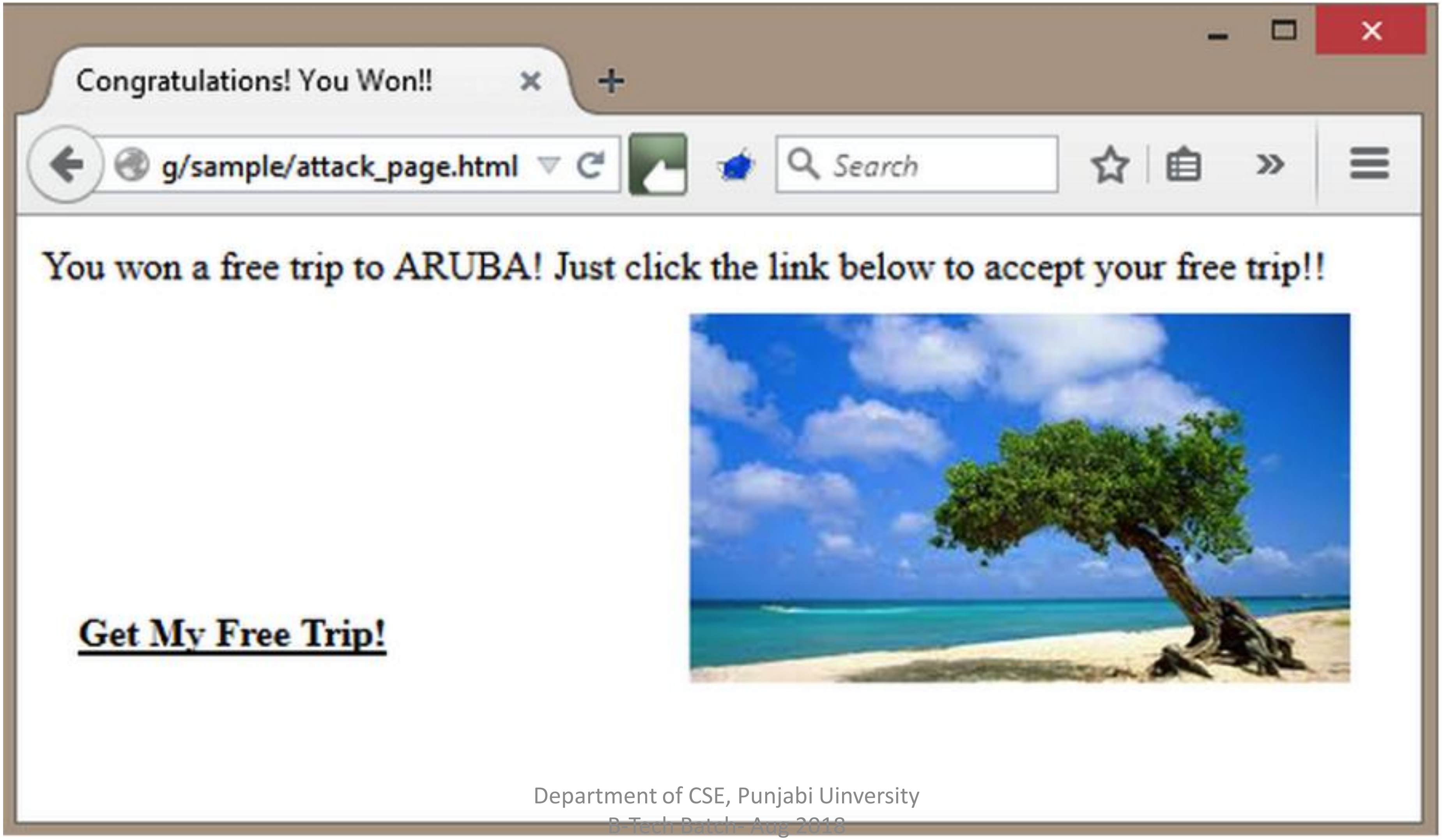
Keylogger, as a surveillance tool, are often used by employers to ensure employees use work computers for business purposes only. Unfortunately, keylogger can also be embedded in spyware allowing your information to be transmitted to an unknown third party.

Internet Time theft

Internet Time theft is connotes the usage by an unauthorized person of the internet hours paid for by another person. These are also known as computer crimes or violations of cyberspace laws. Since the internet is a relatively new phenomenon, the laws governing internet usage may vary widely according to region or state.

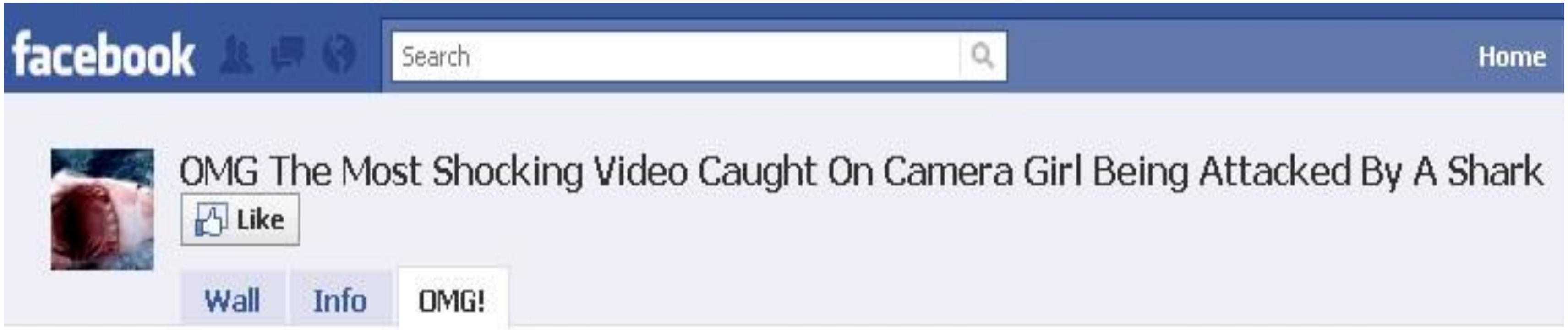
Web Jacking

The Web Jacking Attack Vector is another phishing technique that can be used in social engineering engagements. Attackers that are using this method are creating a fake website and when the victim opens the link a page appears with the message that the website has moved and they need to click another link. If the victim clicks the link that looks real he will redirected to a fake page.



You won a free trip to ARUBA! Just click the link below to accept your free trip!!

Get My Free Trip!



OMG The Most Shocking Video Caught On Camera Girl Being Attacked By A Shark

Use of Encryption by Terrorists

As powerful encryption increasingly becomes embedded in electronic devices and online messaging apps, Islamist terrorists are exploiting the technology to communicate securely and store information.

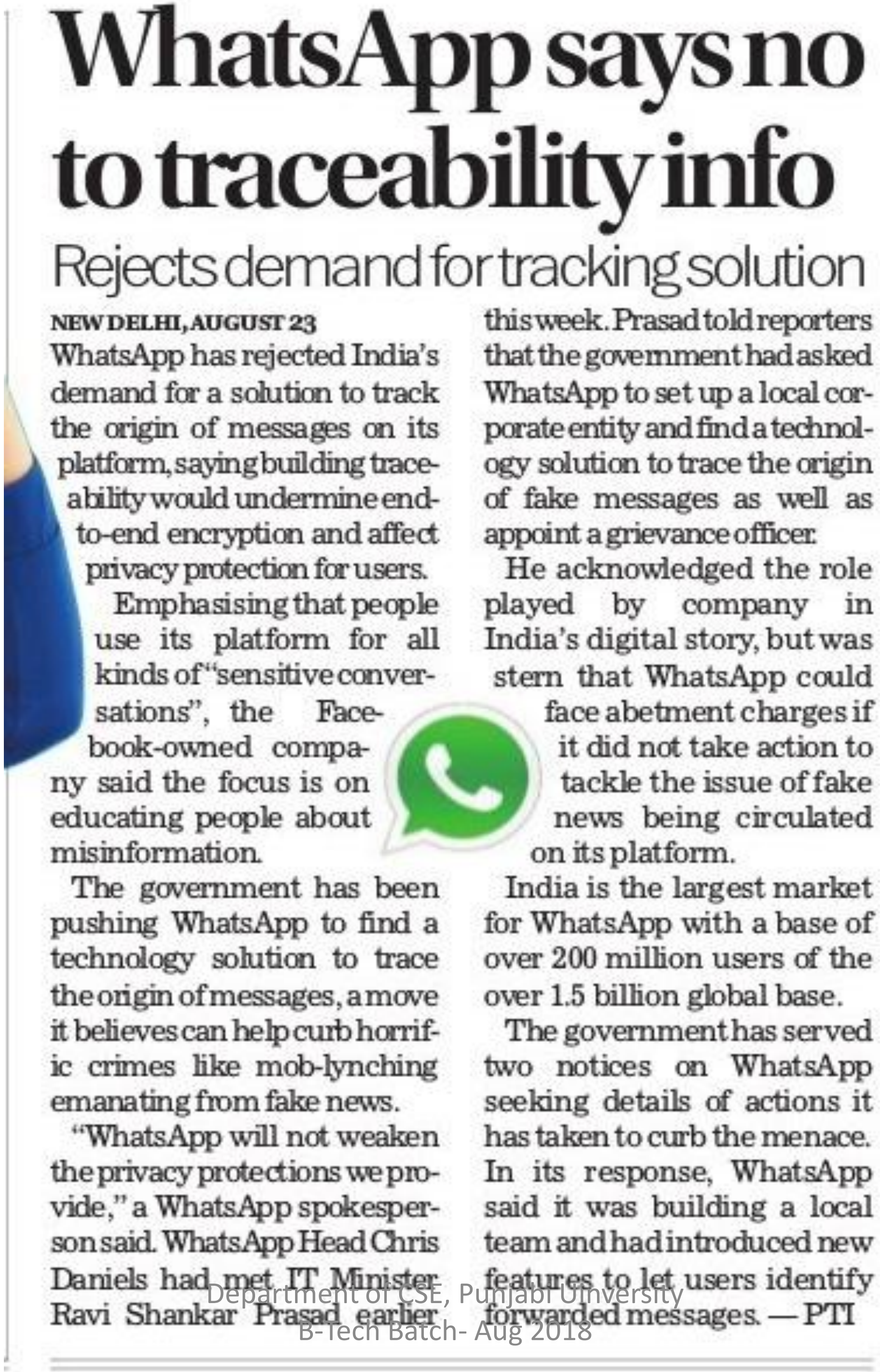
End-to-End Encryption

End-to-End encryption now widely available, unbreakable encryption newer chat apps, instead of encrypting the messages only as far as the server, encrypt the message all the way to the other end, to the recipient's phone. Only the recipients, with a private key, are able to decrypt the message. Service providers can still provide the "metadata" to police (who sent messages to whom), but they no longer have access to the content of the messages.

Full Device Encryption

If an individual loses his iPhone, for example, his data should be safe from criminals. The reason an iPhone is secure from criminals is because of full device encryption, also full disk encryption. Not only is all of the data encrypted, it is done in a way that is combined or entangled with the hardware. Thus, the police cannot clone the encrypted data, then crack it offline using supercomputers to “brute-force” guess all possible combinations of the passcode. Instead, they effectively have to ask the phone to decrypt itself, which it will do but slowly, defeating cracking.

The Tribune 24-8-2018



WhatsApp says no to traceability info

Rejects demand for tracking solution

NEW DELHI, AUGUST 23

WhatsApp has rejected India's demand for a solution to track the origin of messages on its platform, saying building traceability would undermine end-to-end encryption and affect privacy protection for users.

Emphasising that people use its platform for all kinds of "sensitive conversations", the Facebook-owned company said the focus is on educating people about misinformation.

The government has been pushing WhatsApp to find a technology solution to trace the origin of messages, a move it believes can help curb horrific crimes like mob-lynching emanating from fake news.

"WhatsApp will not weaken the privacy protections we provide," a WhatsApp spokesperson said. WhatsApp Head Chris Daniels had met IT Minister Ravi Shankar Prasad earlier this week. Prasad told reporters that the government had asked WhatsApp to set up a local corporate entity and find a technology solution to trace the origin of fake messages as well as appoint a grievance officer.

He acknowledged the role played by company in India's digital story, but was stern that WhatsApp could face abetment charges if it did not take action to tackle the issue of fake news being circulated on its platform.

India is the largest market for WhatsApp with a base of over 200 million users of the over 1.5 billion global base.

The government has served two notices on WhatsApp seeking details of actions it has taken to curb the menace. In its response, WhatsApp said it was building a local team and had introduced new features to let users identify forwarded messages. — PTI

Human Trafficking

Social networking sites such as Facebook, MySpace and many websites are used for human trafficking. The techniques used by the offenders to gain trust vary widely, including expressing love and admiration of the victim, promising to make the victim a star, and providing online employment search and results in an unsuspecting victim relocating from her home on the promise of an unbelievably good job. After the victim has joined the offender, various techniques are used to restrict the victim’s access to communication with home, such as imposing physical punishment unless the victim complies with the trafficker’s demands and making threats of harm and even death to the victim and her family.