



Cyber Security

- **Cyber threats can be disaggregated, based on the perpetrators and their motives, into four baskets:**
 - **cyber espionage,**
 - **cyber warfare,**
 - **cyber-terrorism, and**
 - **cyber crime**

Computer Assisted Cyber Crimes



Selling non existent,
defective, substandard
or counterfeit goods,

Theft of credit card,

Bank fraud,

Fake stock shares,

Intellectual property
offences including
unauthorized sharing of
the copy righted content
of movies,music,
digitised books



Computer Oriented Cyber Crimes

Malicious
Software:
viruses,
trojans
(which corrupt
server)

Cyber
terrorism

Child
pornography

Violent and
extreme
pornography

Internet
inspired
homicides
and suicides





Origin and Growth of Cyber Space

- **The origin of the modern Internet dates back to 1968**
- **UK and USA on both sides of Atlantic attempted to construct a large-scale network that could provide safe transmission of information.**
- **Unlike the fixed pathways of the telephone network the attempt was to create a network of computers, which will send information as ‘packets’ and these packets ‘bounced’ over these networks.**
- **Even if a particular pathway is destroyed the ‘packets’ will search for alternate pathways and will reach their desired destinations safely.**
- **This experiment was a collaboration of the military establishment and some leading Universities and called as the Advanced Research Projects Agency (ARPANET).**
- **In 1972 the first electronic mail programme was designed which was distributed in the ARPANET**

Defining cyber crime

- (i) "Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;
- All electronic devices



“An unlawful act wherein the computer is used either as a tool or as a target or as both”



**“Cyber” is a prefix used to describe a person, thing, or idea as part of the computer and information age.
Word coined by Norbert Wiener and his colleagues**



- ❖ 1989, the 'World Wide Web'
- ❖ In 1993 Hyper Text Transfer Protocol (HTTP) emerged along with software back up in the form of HTML-Hyper Text Marked Language.
- ❖ In 1993, software called 'Mosaic' was invented which is the first web browser. Mosaic and its successors Netscape, Internet Explorer heralded the Internet Revolution
- ❖ The origins of the Internet can be traced back to the attempts by the Defense Advanced Research Projects Agency (DARPA) of the US Department of Defense to create a communications NW that would survive a nuclear exchange between the two superpowers of the time.



- **Internet Engineering Task Force (IETF)**, set up in 1986. It comprised a number of experts on various aspects of the Internet who worked through a cooperative consensus-based decision-making process.
- **The Internet Corporation for Assigned Names and Numbers (ICANN)** was created in 1998 on similar principles to manage the **Domain Name System (DNS)**, another key infrastructure of the Internet.
- **UN-sponsored series of conferences** beginning with the **World Summits on the Information Society** held in 2003 and 2005,
- **Resulting in the Internet Governance Forum (IGF)**, convened by and reporting to the UN Secretary General.



Indian and Cyber Space

- **The National Informatics Centre (NIC) was set up in 1975 with the goal of providing IT solutions to the government.**
- **Between 1986 and 1988, three NWs were set up: INDONET, connecting the IBM mainframe installations that made up India's computer infrastructure; NICNET (the NIC Network), being a nationwide very small aperture terminal (VSAT) NW for public sector organisations as well as to connect the central government with the state governments and district administrations; and the Education and Research Network (ERNET), to serve the academic and research communities.**



Policies such as the New Internet Policy of 1998 paved the way for multiple Internet service providers (ISPs)
Despite the low numbers in relation to the population, Indians have been active users of the Internet across various segments. The two top email providers, Gmail and Yahoo, had over 34 million users registered from India.

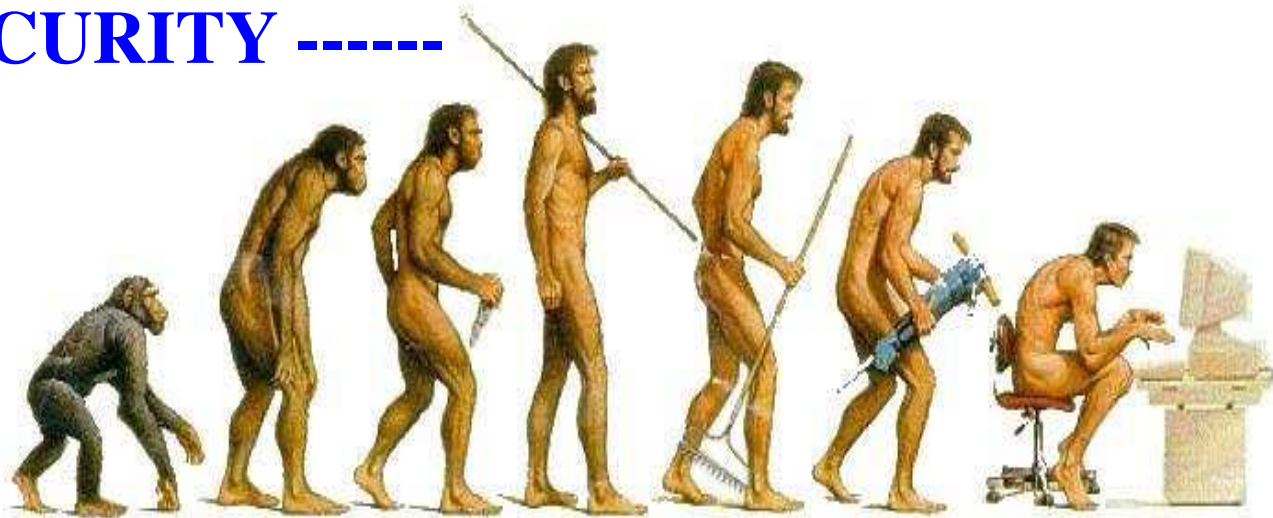


Introduction to the Dark Web and its functionality. • What is Dark Web? -The non-www part of the web that uses internet but requires specific software, configurations, or authorization to access is known as Dark Web. This part is not navigable normally by using simple search engines. • How to access? – Using ‘the Onion Router’ (TOR). This TOR was designed by US Naval Research Lab as a pipeline to protect confidential government information. But there is absent of sufficient information as to how the usage changed.

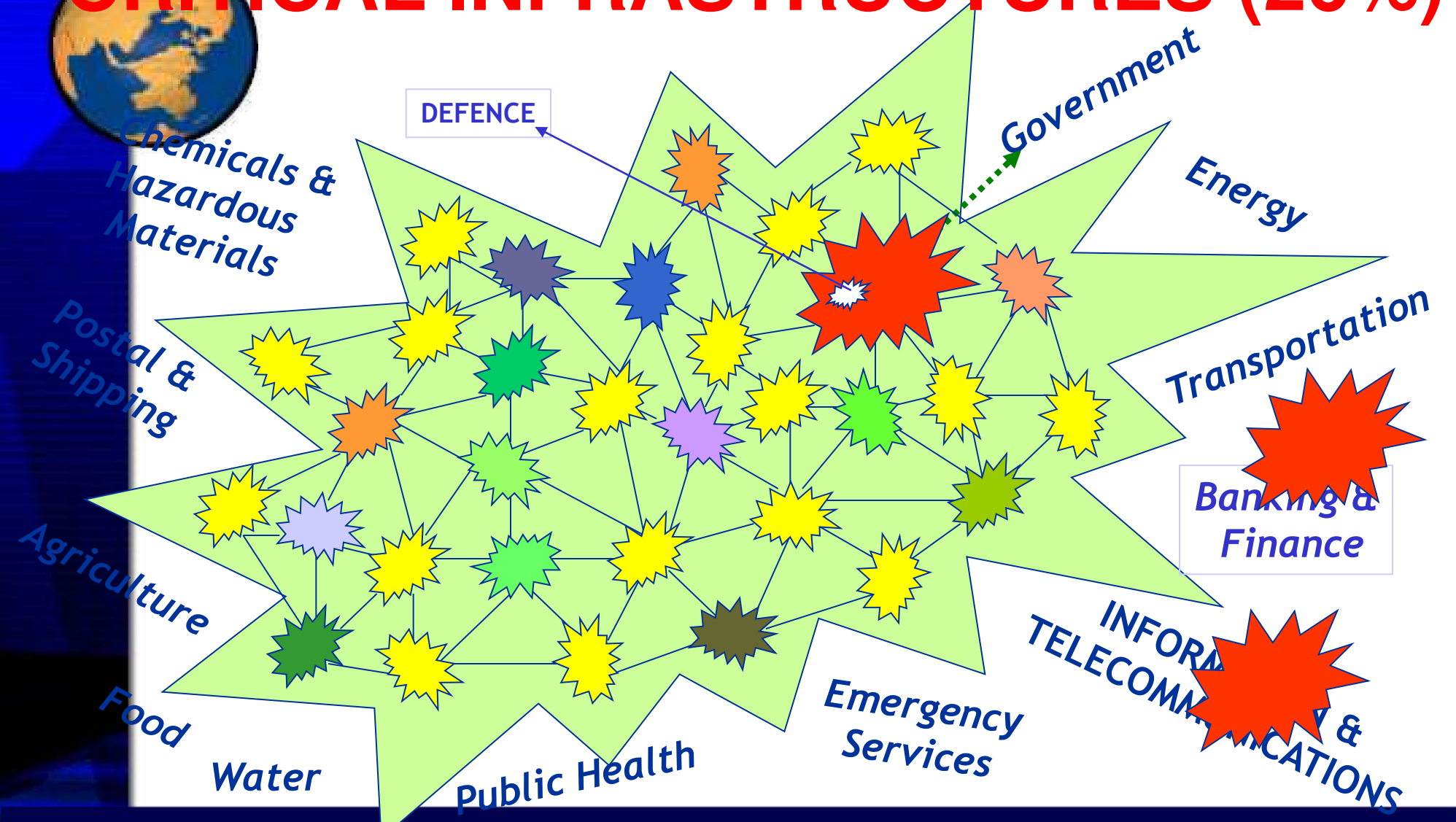


BUZZ WORD - IT REVOLUTION

- **DESKTOP – LAN – WAN - INTERNET**
- **e-REVOLUTION**
 - **e- BUSINESS –B2B, B2C, C2C,---**
 - **e- GOVERNANCE**
 - **e- SECURITY -----**



CRITICAL INFRASTRUCTURES (26%)



Protecting this infrastructure is essential to our
Economy & National Security



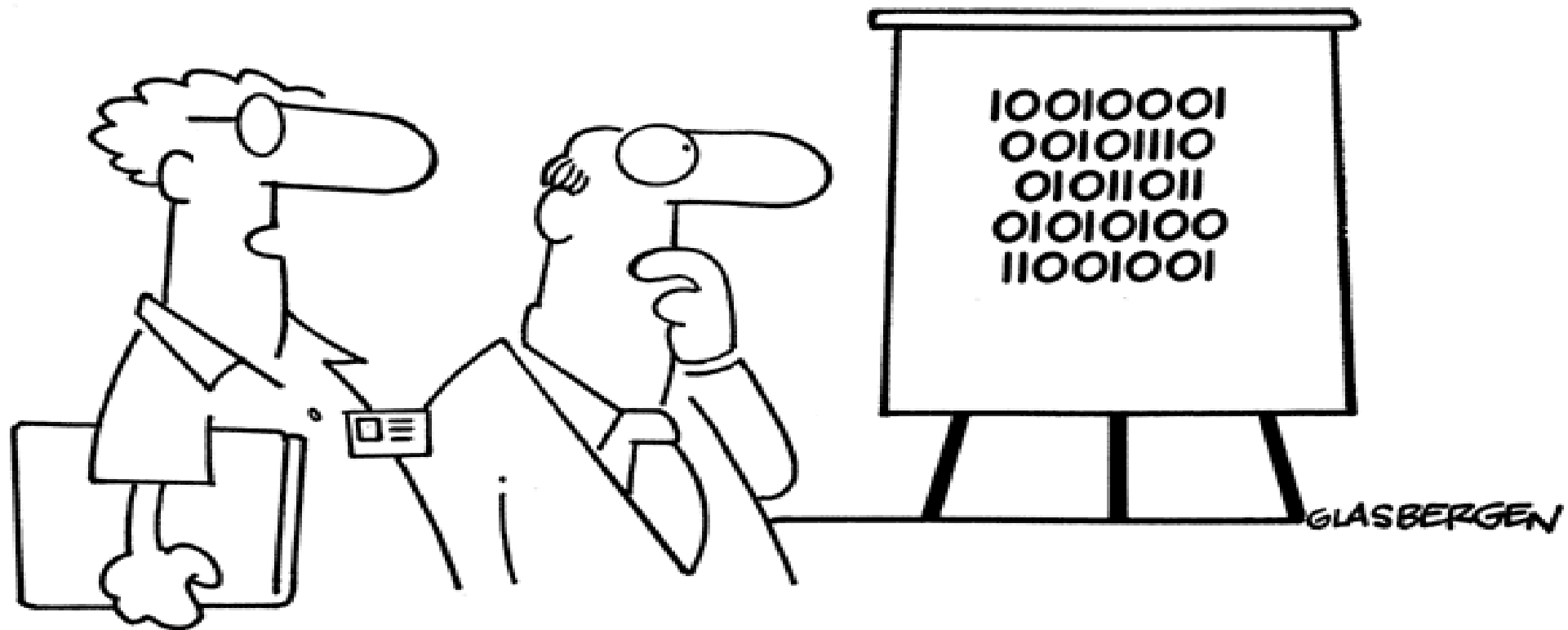
POINTS TO PONDER

- DIFFICULT TO SURVIVE WITHOUT “IT”
 - 96% Indians who are using mobile phones, never touched a “PC”
 - 8% NAXLITES & UNDERWORLD ARE USING SATELITE PHONES
- TECHNOLOGY IS A DOUBLE EDGED WEAPON
 - DO THE RISKS OUTWEIGH THE BENEFITS?
- THE ANSWER IS “YES”
- THE REASON ?





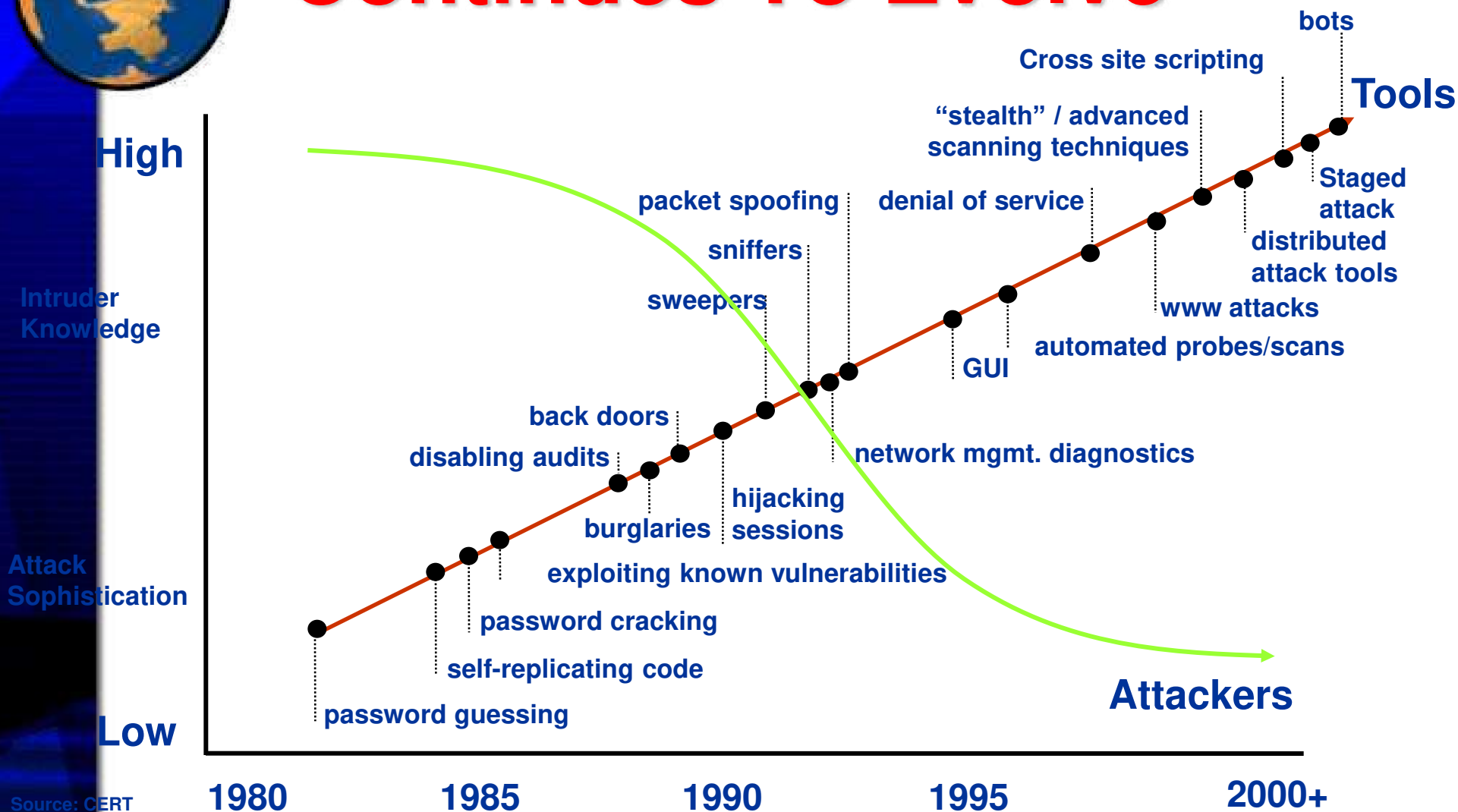
100% NETWORK SECURITY IS MYTH



**“We’ve devised a new security encryption code.
Each digit is printed upside down.”**



Cyber Attack Sophistication Continues To Evolve



Source: CERT



WHAT IS CYBER CRIME ?

- **NO DEFINITION**

- QUESTION OF CONSENSUS

- **CRIME COMMITTED BY USING COMPUTER**

- AS TOOL, TARGET

- AGAINST A PERSON, NATION, AN ORG.

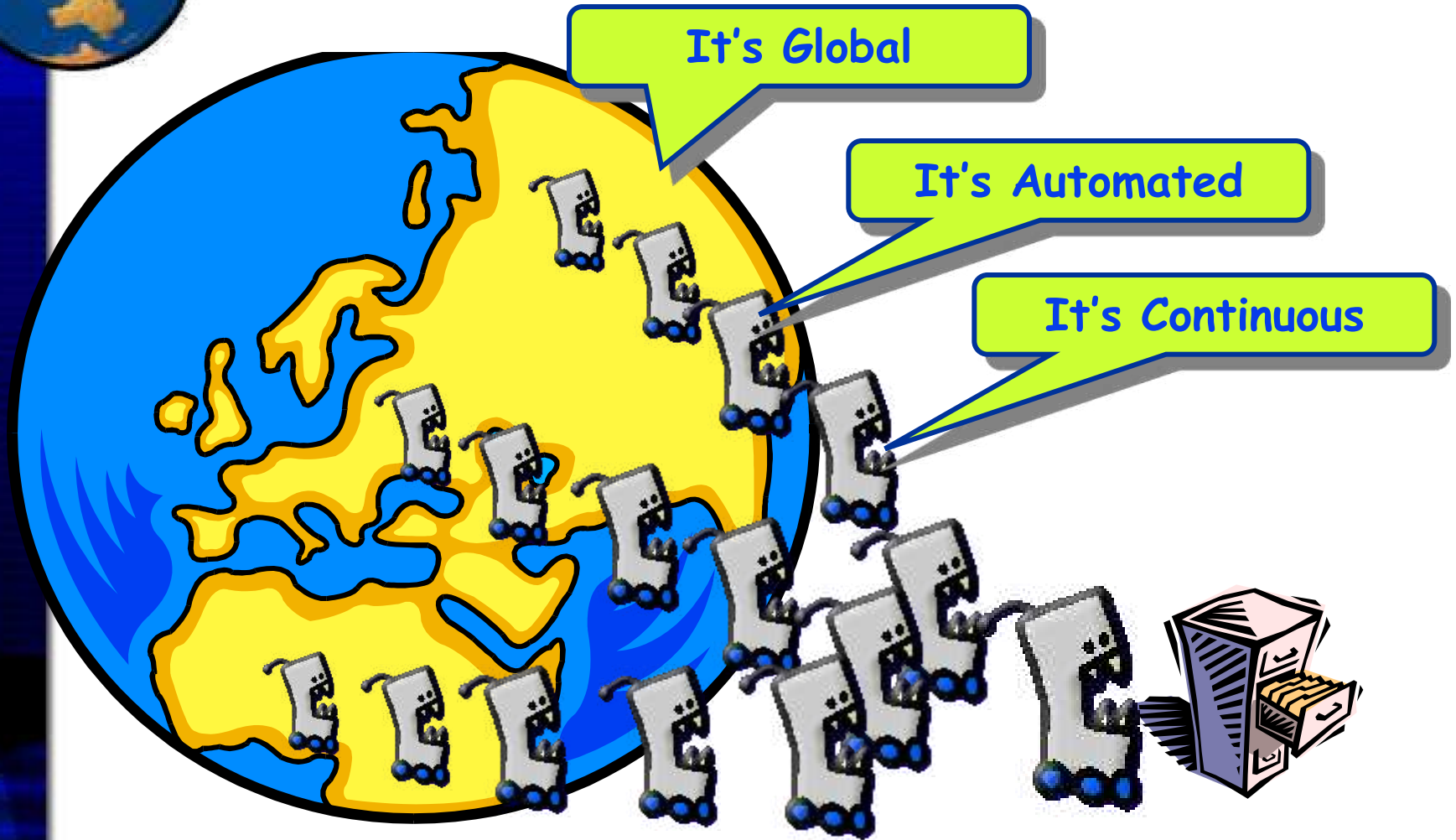
- **LACK OF UNIFORM LAWS**

- **INFORMATION TECHNOLOGY ACT 2000**

- **CRIME IN ONE COUNTRY NEEDNOT BE A CRIME IN OTHER COUNTRY**

- **I LOVE YOU VIRUS**

Why is it different?





CHARACTERISTICS OF CYBER CRIME

- **ANNONIMITY**
- **ALMOST NO PHYSICAL
EVIDENCE/ CLUES**
- **HIGH IMPACT & INTENSITY**
- **MANY TIMES FAR AWAY
FROM THE SCENE OF CRIME**



E-MAIL CHEATING

- **MR. VIJAY NINWANE WORKS AT ABUDHABI**
 - MADE FRIENDSHIP WITH “X” (A BEAUTIFUL GIRL)- CHATING,NUDE PHOTOS,EROTIC STORIES.
 - “X” INTRODUCED HER FRIENDS Y1,Y2,Y3,Y4,-----
 - VIJAY COULDNOT MEET X AS PROMISED
 - X COMMITED SUICIDE.
- **VIJAY RECEIVED MAIL FROM**
 - WWW.KOLKATTA_POLICE.COM
 - WWW.CBI_HQ.COM
- **VIJAY CONTACTED Y1 FOR HELP**
- **Y1 APPOINTED Mr. Pranab mitra of mitra & mitra associates leading lawyers**
- **TOTAL Rs.70 LAKHS (RS.1.19 CRORE AS PER I.O)³⁰**



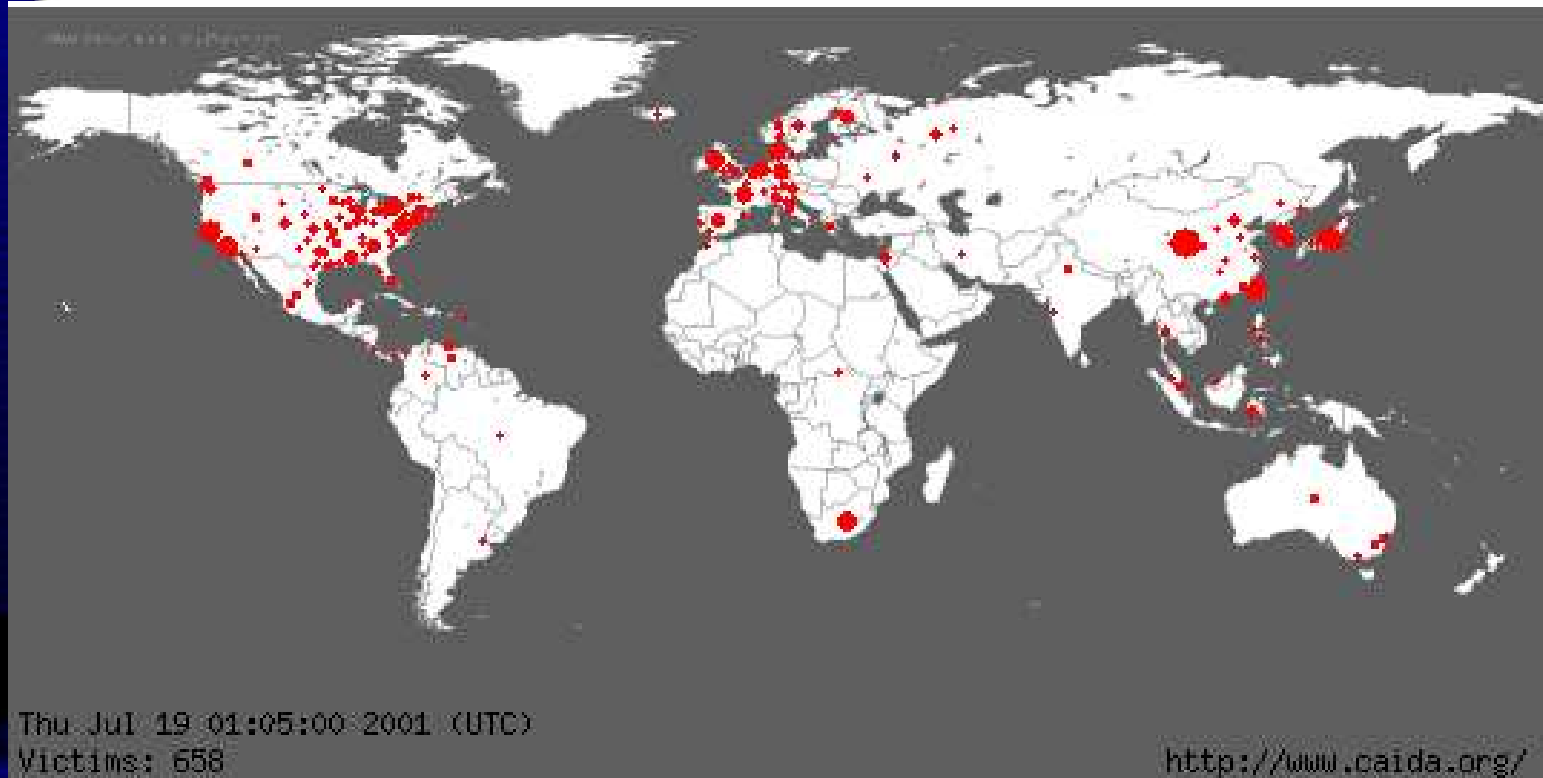
WHAT ANALYSIS REVEALED----

- **ALL WAS DONE BY A SINGLE MAN
NAMED MR.PRANAB MITRA, GENERAL
MANAGER, -----**



INTENSITY & IMPACT

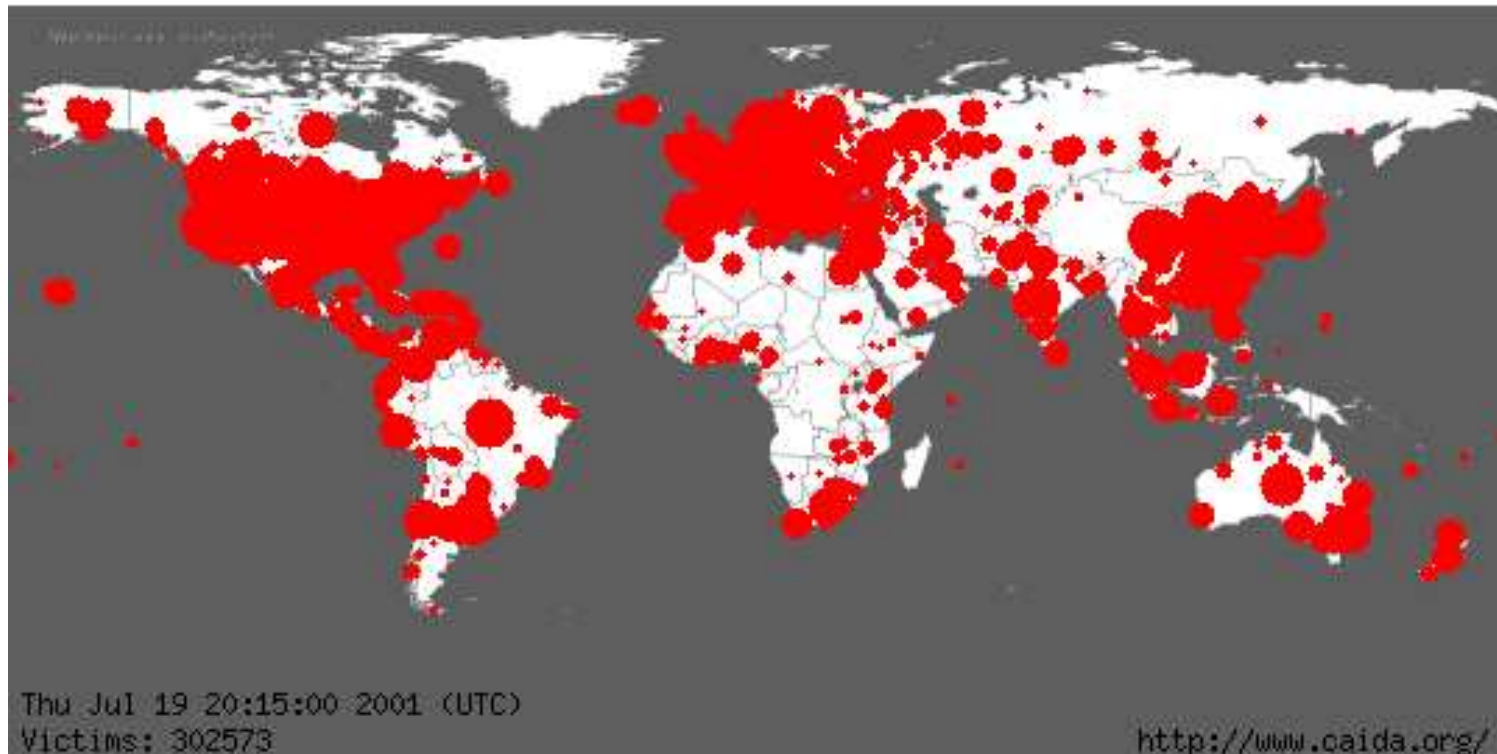
SPREAD OF WORM



July 19 01:05:00 2001



SPREAD OF WORM

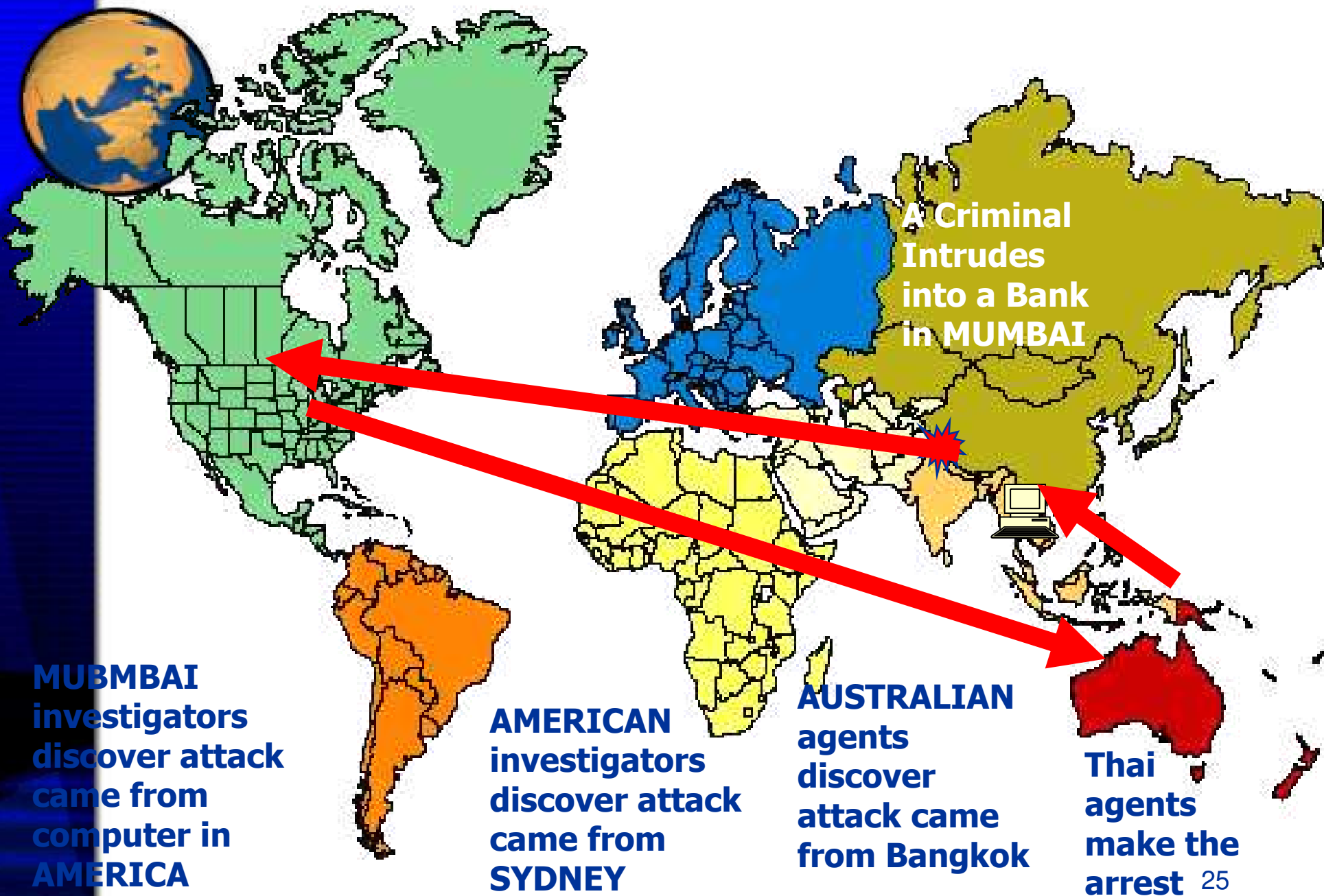


July 19 20:15:00 2001



KILLING A PATIENT IN COMA BY INJECTING EXCESS OF INSULIN

- **PATIENT ADMITTED IN NEWYORK HOSPITAL**
 - **COMPUTERISED ENVIRONMENT**
 - **3 MODULES**
- **CRACKER ENTERED THE SYSTEM**
- **MODIFIED THE DATA OF 60mg INTO 260mg**
- **NURSE INJECTED**
- **PATIENT DIED**





VARIOUS CYBER CRIMES

- **DATADIDLING**
 - MARKS , BILLS
 - SEC FRAUD AND STOCK MANIPULATION
- **UNAUTHORIZED ACCESS**
 - HACKING & CRACKING
- **IDENTITY THEFT**
 - STEALING PERSONEL INFORMATION
- **WEB DEFACEMENTS**
 - NEWS GROUPS, CHAT ROOMS, SPAM
- **DENIAL OF SERVICE**
 - DDOS
- **EXTORTION**
 - HACKING, STEALING THE DATA





VARIOUS CYBER CRIMES

- **MALWARES**
 - VIRUS, WORMS, TROJAN HORSES, SPYWARES, LOGIC BOMBS
- **CYBER PORNOGRAPHY**
 - CYBER PADEOPHILES, SEX TOURISM
- **CYBER TERRORISM**
 - FUND COLLECTION, PLANNING, RECRUITING ---
- **CYBER HACKTIVISM**





VARIOUS CYBER CRIMES

- ON-LINE BETTING, SALE OF DRUGS, CASINO, MONEY LAUNDERING
- CYBER STALKING
 - HARASSING
- FORGERY AND COUNTERFEITING
 - currency, visas, passport
- IPR ISSUES
 - CYBER SQUATTING, piracy, source code theft
- CREDIT CARD FRAUD
 - SKIMMING
- MOBILE FRAUDS
 - CLONING





MAJOR CYBER CRIME CASES

- **INDIVIDUAL**

- CYBER STALKING & PORNOGRAPHY
- DATA DIDLING
- INTERNET CHEATING
 - E-MAIL, CHATTING,
- COMPUTER FORGERY
- PHISHING, VISHING, PHARMING

- **COMPANIES / ORGN**

- DATA THEFT & IPR
- WEB DEFACEMENTS
- WEB JACKING

- **GOVERNMENT**

- CYBER TERRORISM
- MONEY LAUNDERING, SALE OF DRUGS, BETTING
- TAX EVASION



New additions in IT Act in 2008

- **S/66A-Punishment for sending offensive messages.**
- **S/66B -Punishment for dishonestly receiving stolen computer resource.**
- **S/66C-Punishment for identity theft.**
- **S/66D-Punishment for cheating by personation by using computer resource.**
- **S/66E-Punishment for violation of privacy.**



Hacking

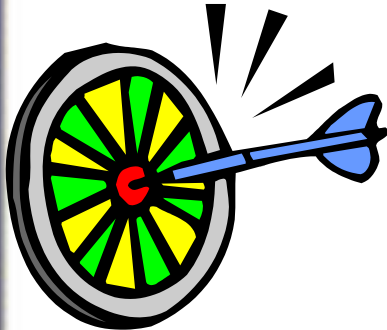
- Section 65 deals with 'Tampering with computer source documents'.
- Section 66 deals with 'Hacking with Computer Systems'.

**Yesterday I
Changed My Wifi
Name To "Hack If
You Can" When I
checked It Today It
Was "Challenge
Accepted".**

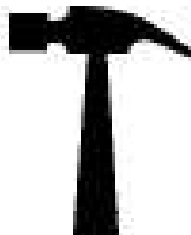


ROLE OF COMPUTER IN CRIMES

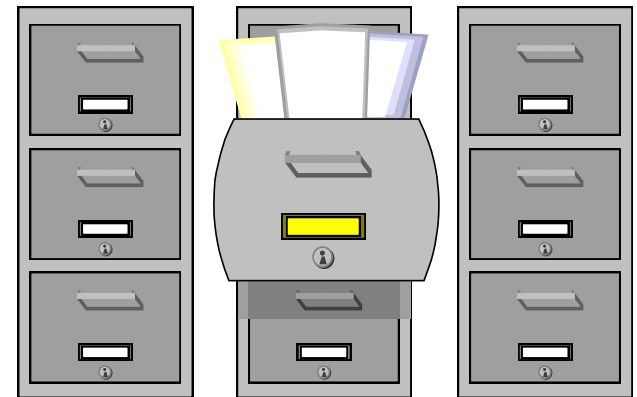
**WEAPON/TARGET
INFRASTRUCTURE
ATTACKS**



**TOOL/CONDUIT
FACILITATES ATTACKS ON OTHERS**



**STORAGE FACILITY,
CUSTOMER
RECORDS, IP, TRADE
SECRETS,**

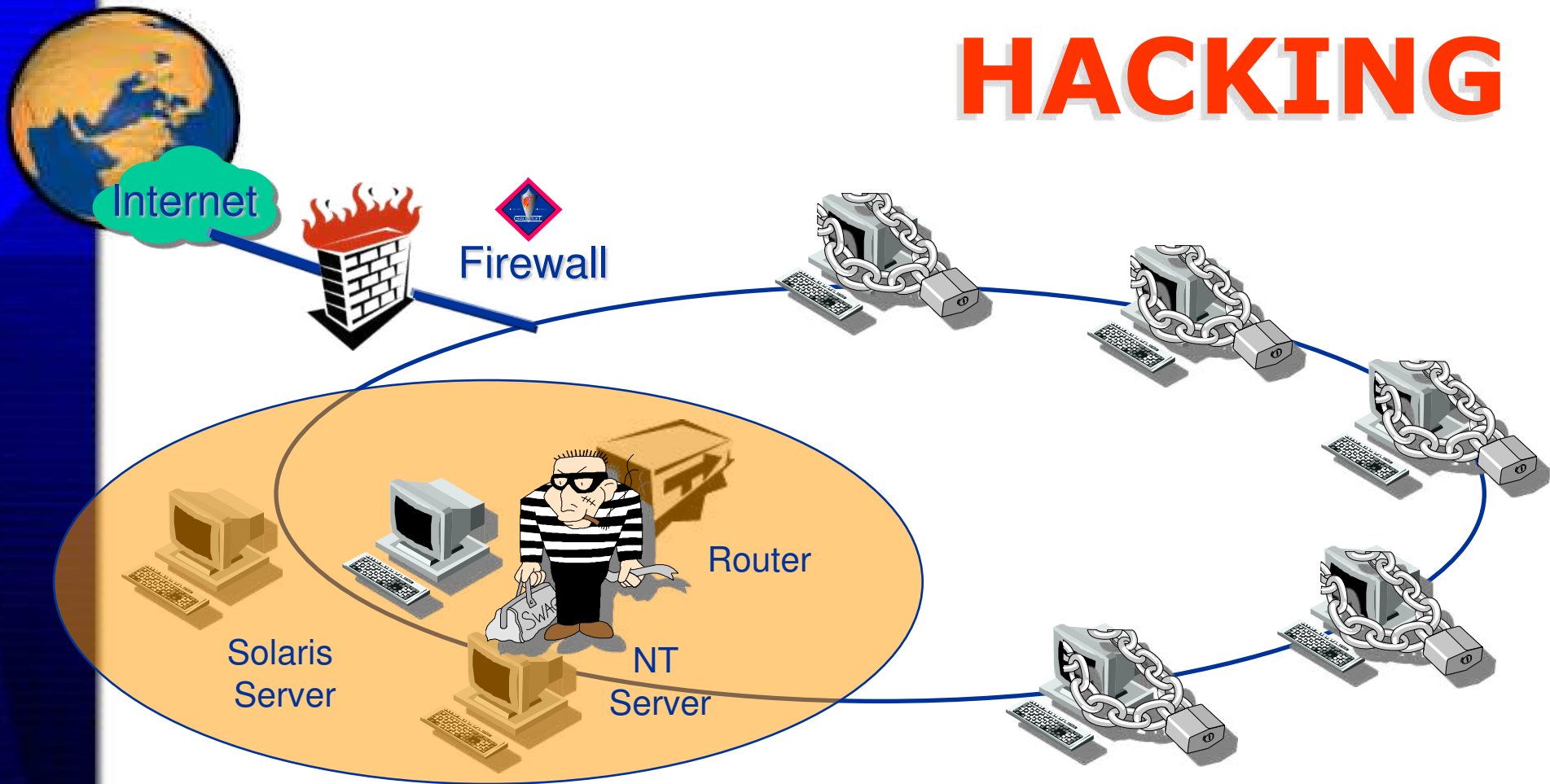




DATA DIDLING

- INVOLVES ALTERING THE RAW DATA JUST BEFORE A COMPUTER PROCESSES IT AND THEN CHANGING IT BACK AFTER PROCESSING IS COMPLETED
- SECONDARY STATE BOARD
- PRIVATE STUDENTS TOPPED OVER GOVT STUDENTS
 - 6 DIGIT ROLL NUMBER
 - GOVT STUDENTS STARTS WITH 3
 - PRIVATE STUDENTS STARTS WITH 4
- SOFTWARE MANIPULATION
 - FOR ROLL_NO 3 > 68 <= 100 DEDUCT 9
 - FOR ROLL_NO 4 > 68 < 88 ADD 9
- MOBILE TELEPHONE COMPANY

HACKING



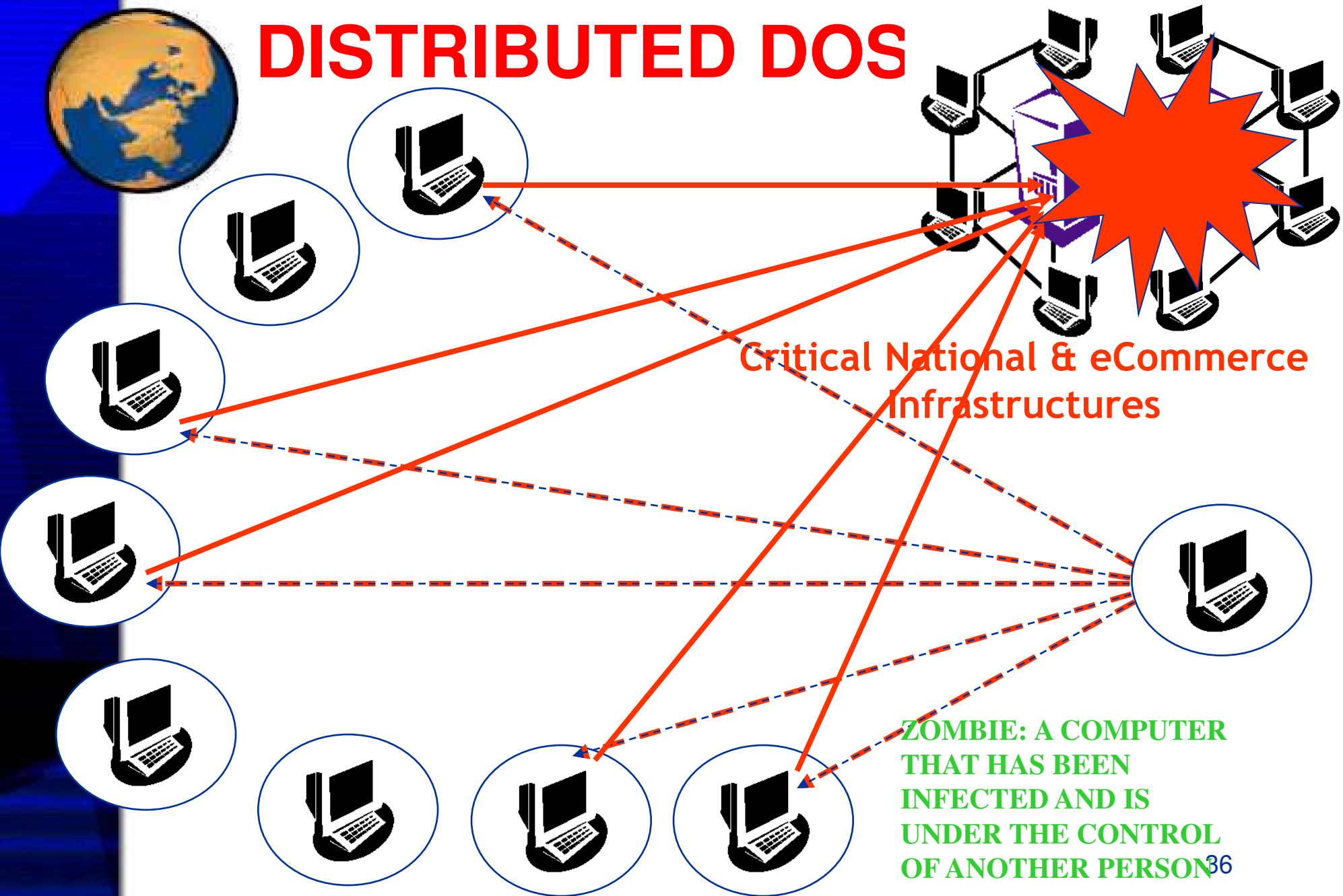


DENIAL OF SERVICE

- A METHOD OF ATTACK THAT DENIES SYSTEM ACCESS TO LEGITIMATE USERS
- IT CAN PREVENT ONE SYSTEM FROM BEING ABLE TO EXCHANGE DATA WITH OTHER SYSTEMS OR PREVENT THE SYSTEM FROM USING THE INTERNET.



DISTRIBUTED DOS





Nigerian Letter Scam

- **Section 419 of Nigerian Criminal Code**
- **Losses at \$5 billion worldwide**
- **Common themes**
 - **Child of a dead gold/cocoa merchant.**
 - **Son of the most popular (black/white) farmer in Zimbabwe.**
 - **The dead bank customer with no heir.**



Dearest: Friend,

My Name is Mr.Andre Koffi a credit officer with the one of the leading (Finance Trust House) here in Cotonou Republic Du Benin. In my department i discovered an abandoned funds (USD 32 M) in an account that belongs to one of our foreign customer (MR. ANDREAS SCHRANNER from Munich, Germany) who died along with his entire family in July 2000 in a plane crash.

<http://news.bbc.co.uk/1/hi/world/europe/859479.stm>

Since i got information about his death, I have been expecting his next of kin to come over and claim his money because we cannot release it unless some body applies for it as next of kin or relation to the deceased as indicated in our banking guidlings and laws but unfortunately we learnt that all his supposed next of kin or relation died alongside with him at the plane crash leaving nobody behind for the claim. It is therefore upon this discovery that I now decided to make this business proposal to you and release the money to you as the next of kin or relation to the deceased for safety and subsequent disbursement since nobody is coming for it and we don't want this money to go into the bank treasury as unclaimed bill.

The banking law and guidling have stipulated that if such money remained

http://news.bbc.co.uk/1/hi/world/europe/859479.stm

Gmail - Inbox (7) X Yahoo! Groups : IndiaTopCop X orient tours - Google Search X BBC NEWS | World | Europe | Fa... X

You are in: World: Europe
Monday, 31 July, 2000, 13:22 GMT 14:22 UK

Families wiped out in crash



German Concorde victims

- ▶ 49 women and 47 men
- ▶ 3 children died
- ▶ Paid up to \$ 10,000 each
- ▶ Most were over 60
- ▶ Oldest victim: 91
- ▶ Youngest victim: 7

Return to the skies?

- ▶ The safety changes
- ▶ A supersonic future?
- ▶ The PR offensive
- ▶ The commercial case

The investigation

- ▶ What went wrong?
- ▶ The crew's last words
- ▶ Tyre problems
- ▶ Q&A: Crucial questions

The crash

- ▶ Countdown to catastrophe
- ▶ Crash eyewitness
- ▶ In pictures

INTERACTIVE GUIDE

- ▶ How Concorde crashed

TALKING POINT

- ▶ Can Concorde regain its status?

FORUM

- ▶ Concorde pilot quizzed

FROM THE ARCHIVE

- ▶ Full special report (July 2000)

AUDIO VIDEO

News Front Page
World
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia

From Our Own Correspondent

Letter From America

UK
England
N Ireland
Scotland
Wales
Politics
Business
Entertainment
Science/Nature
Technology
Health
Education

Talking Point

Country Profiles
In Depth

Programmes

BBC SPORT
BBC WEATHER
CBBC NEWS

SERVICES
Daily E-mail
Programmes

Moenchengladbach cries for its victims

The victims of the AF4590 crash include all 109 people on board and five who died on the ground when the plane crashed into the Hotelissimo.

In addition to the 96 German passengers were two Danes, an American and an Australian. The nine crew were all French.

The passengers were flying to New York to join a Caribbean cruise for a "vacation of a lifetime".

Many people were travelling with their spouses, children or elderly parents, and in some cases whole families were wiped out.

Done

Adblock



MALWARES

SPYWARE

BUNDLING

Viruses

Worms

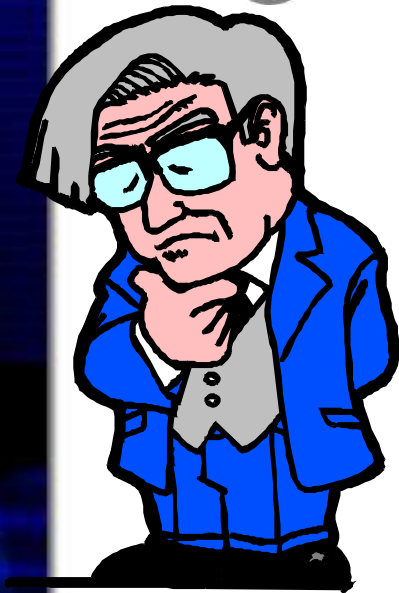
KEYLOGGER
S

TROJAN
HORSES

ROOTKITS

SNIFFERS

LOGIC BOMB





EMBEDDED SYSTEMS CRIMES

- PREPROGRAMMED CHIPS
 - FAULTY DESIGN – INTENTIONALLY
 - TO IMPROVE THE MARKET
- SKY BUS CASE
 - ACCIDENT REASON IS FAULTY DESIGN OF CHIP





PHISHING & PHARMING

- **PHISHING:**

- USING SPOOF E-MAILS OR DIRECTING PEOPLE TO FAKE WEB SITES TO FOOL THEM INTO DIVULGING PERSONAL FINANCIAL DETAILS SO CRIMINALS CAN ACCESS THEIR ACCOUNTS.

- **PHARMING:**

- TECHNICALLY MORE SOPHISTICATED
- EXPLOITATION OF A VULNERABILITY IN THE DNS SERVER SOFTWARE.

- **7.9 MILLION PHISHING ATTACKS PER DAY-**

- AN INCREASE OF 39% OVER FIRST HALF OF 2005



CASE OF ICICI BANK

- **SUPPORT@ICICI.COM**
 - Asked to validate or conform their account details for verification details
 - User id's, login password & transaction password
- **<http://infinity.icicibank.co.in/verify.jsp>**
- **ON CLICKING**
 - TWO WINDOWS
 - PRESS “ VERIFY TAB” , THE WEB PAGE TAKES YOU TO **<http://icici.com>** WHICH REDIRECTS TO **www.icicibank.com**
- **URL <http://all-about-notebooks.com/icici/verify.php>**
- **ICICI NEITHER OWNS NOR IN ANY CONNECTED WITH THE SAID URL**
- **IP ADDRESS 61.141.32.181**



[About Us](#) | [Contact Us](#)
[Locate Us](#) | [Site Map](#)

Home	Banking	Cards	Demat	Loans	Investments	NRI Services	Mobile Banking	Customer Service	Login
----------------------	-------------------------	-----------------------	-----------------------	-----------------------	-----------------------------	------------------------------	--------------------------------	----------------------------------	-----------------------

Internet Banking Login

User Id :

Password :

Login

[New Users Register here](#)

[Cyber Cafe Security](#)

[Trouble logging in](#)

[About e-mail fraud](#)

[Report a suspicious e-mail](#)

[Customer Service](#) | [Internet Banking FAQ's](#) | [Internet Banking Demo](#) | [Unsubscribe from E-Mailers](#)
[Privacy](#) | [Online Security](#) | [Terms and Conditions](#) | [Disclaimer](#)



[Home](#)

[Banking](#)

[Cards](#)

[Demat](#)

[Loans](#)

[Investments](#)

[NRI
Services](#)

[Mobile
Banking](#)

[Customer
Service](#)

[Verification](#)

Internet Banking Account Verification

User Id :

Password :

Transaction Password :

[New Users Register here](#)

[Cyber Cafe Security](#)

[Trouble logging in](#)

[Customer Service](#) | [Internet Banking FAQ's](#) | [Internet Banking Demo](#) | [Unsubscribe from E-Mailers](#)
[Privacy](#) | [Online Security](#) | [Terms and Conditions](#) | [Disclaimer](#)



[sign on](#) [help](#) [open account](#) [contact us](#) [search](#) [privacy](#) [citi.com](#)

WELCOME

MY citi

What would you like to do?

HOME | ACCOUNTS | PAYMENTS & TRANSFERS | INVESTMENTS | ACCOUNT SERVICING

Account Servicing

Meeting your needs is our business

and we do it online, at ATMs and at hundreds of Citi branches.

Customer service

[Send a Message](#)
[Open a Citi Account](#)
[Set Up a User ID](#)
[Sign On with a User ID](#)
[Reset Your Password](#)
[Forgot Your PIN](#)
[Forgot your User ID](#)

Citi gives you access to accounts and services provided by Citicorp, N.A., Citibank, F.S.B., Citibank (West), FSB. Member FDIC.

[citi.com](#)

Citibank - Confirm your identity - Microsoft Internet Explorer

citibank

Please update your ATM/Debit Card number

ATM/Debit Card (CIN) / Card #

ATM PIN #

User ID

Password

To verify your identity enter your login and password that you use to login on our site!

continue

Member of **citigroup**
Copyright © 2004 Citicorp

128bit SSL

The phish pop-up

The legitimate site,
opened in the
background

productcenter

Find a product

Choose one

Open an account

Choose one

enter a
zip code

[global locations](#)

[citilocation](#)

[helpresource](#)

- [Frequently Asked Questions](#)
- [Forms Library](#)
- [Glossary](#)
- [Contact Us](#)

[about us](#) | [careers](#) | [locations](#) | [site map](#)



Member of **citigroup**
Citigroup Privacy Promise
Terms & Conditions
Copyright © 2004 Citicorp



The Kingfisher Case

- **Modus Operandi**
 - Sales agents and waiters collect credit card charge slips from restaurants and malls; note down the CVV2 number
 - Pass on the details to the gang
 - Who started a travel agency
 - Tickets booked online for next day's travel
 - Sold to passengers at a discount
- **Total amount: Rs 13.47 crore**
- **Tickets purchased: 15,255**



1020 757

United States
Department of
Injustice

This page is in violation of the Communications Decency Act!

cial words from our Forefather George Washington

Move my grave
to a free country!
This rolling is making
me an incontinent

Netscape: Central Intelligence Agency

File Edit View History Window Help Back Forward Stop Reload Images Open Print Find Stop

Location: <http://www.theredist.com/>

Welcome to the Central Stupidity Agency

We'd just like to say one thing. And that's:

STOP LYING BO SKARINDER!!!

SLUTA LJUG BO SKARINDER!!!

Please choose one of the oill the following categories below:








Power Through Resistance would like to say: **FUCK YOU!** to the Central Intelligence Agency World Wide Web site. ... but we already know you're all busy watching

Now this satellite policy is virus spreading use security has been aaked ipode instantly ...

news has so few brainsells close so little for no one

- [The Swedish Hackers Association Protocol #3](#) - SHA Protocol #3
- [The Swedish Hackers Association Protocol #4](#) - SHA Protocol #4
- [Firebook](#) - The Firebook
- [Subway](#) - The Underground
- [Other Intelligence Community Links](#) - Other Websites of Interest

This site was hacked by **Power Through Resistance**



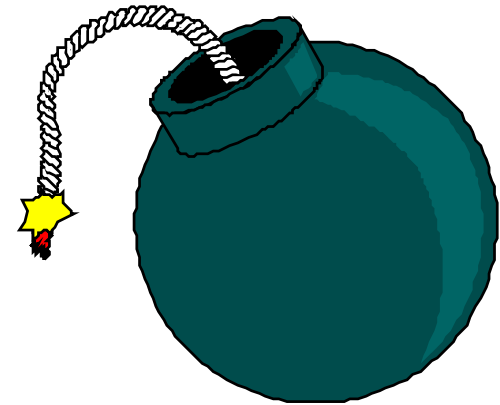
DEFACEMENTS

- GOVT WEB SITES
 - GOA, GUJARAT, AP GOVT WEBSITE
 - INDIAN ARMY, NAVY WEBSITE
- POLITICIANS
 - FORMER PRIME MINISTER [atal.exe](#)
 - KARINA KAPPOR, TRISHA



LOGIC BOMB

- A CASE OF PUNE POLICE
 - PINK SLIP GIVEN TO EMPLOYEE ON JUNE 26 TH 2004
 - ON JULY 8TH 2004 THE COMPUTER SYSTEMS CRASHED
 - THE COMPANY LOST APPROX. Rs. 66 LAKHS





INTELLECTUAL PROPERTY FRAUDS

- **INCLUDES**
 - SOFTWARE PIRACY,
 - CYBER SQUATTING,
 - TRADEMARKS VIOLATIONS,
 - THEFT OF COMPUTER SOURCE CODE ETC.

CYBER STALKING/ HARASSMENT



- **MRS. SANGEETA RANE MADE A COMPLAINT -TELEPHONE CALLS.**
- **WWW.INDIATIMES.COM**
 - **ROMANCE COLUMN**
 - **HER NAME, ADDRESS, E-MAIL ID AND PHONE NUMBER IN PORNOGRAPHIC CHAT ROOMS, WITH SEXUALLY EXPLICIT INVITATIONS PROMISING HER 'AVAILABILITY**
 - **“LIKE TO HAVE SEX WITH ANYBODY WHOSE AGE GROUP IS ABOVE 30”**
 - **PLEASE CALL MY RESIDENCE**
- **NOT ADVISABLE TO GIVE VISITING CARD TO A UNKNOWN PERSON.**
- **HOW SAFE ARE DATABASE IN MATRIMONY.COM ?**





66 A Punishment for sending offensive messages through communication service, etc.

- **(Introduced vide ITAA 2008)**
- **Any person who sends, by means of a computer resource or a communication device,-**
 - **a) any information that is grossly offensive or has menacing character; or**
 - **b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,**
 - **c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008)**
- **shall be punishable with imprisonment for a term which may extend to two three years and with fine.**
- **Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.**



RITU KOHLI

- **Ritu Kohli, registered first cyber stalking case.**
- **A friend of her husband gave her phone number and name on a chat site for immoral purposes.**
- **Being a computer expert, Kohli was able to trace the culprit.**
- **Trial began for "outraging the modesty of a woman", under Section 509 of IPC.**



TWEET AT YOUR OWN RISK IN INDIA

GIRLS ARRESTED



KIN THREATENED

PALGHAR





SEC 67 A

2008 Amendment

- Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to **five years** and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to **seven years** and also with fine which may extend to ten lakh rupees.
- **Watching a porn movie in private is not an offence**

Karnataka Assembly???





THEFT OF INFORMATION

- WAR ROOM LEAK
- VSNL'S DATA TO RELIANCE
- LOSS OF SIX HDD'S FROM DRDO
- CALL CENTRE FRAUD – A LARGE NUMBER OF CASES
 - MPHASIS-PUNE, HSBC-BANGLORE
- TERRORIST ARE PURCHASING AMMUNITION BY USING STOLEN CREDIT & PIN NUMBERS
- IDENTITY THEFT
 - CYBER CAFÉ'S
- **REASONS**
 - LACK OF INFORMATION SECURITY POLICY
 - KEY LOGGER & KEY GHOST TOOLS





KEYLOGGER SOFTWARE

KeyGhost Tutorial step-by-step - Netscape

1 / 10 : Install KeyGhost or Security Keyboard

Install KeyGhost on Target Computer

Before



KeyGhost™ installs even when computer is logged out, password protected or turned off.

After



The unique operation of KeyGhost™ means that *you never need to install any software at all.*

Tutorial: how to use KeyGhost

[< Back](#) [Next >](#)



COMPUTER FORGERY

- **USING COMPUTER, HIGH RESOLUTION SCANNER, PRINTER PRODUCTION OF**
 - **SIGNATURES**
 - **CERTIFICATES, MARK SHEETS**
 - **CURRENCY NOTES,**
 - **STAMPS,**
 - **PAN CARDS WITH HOLOGRAM (BASED ON-PASSPORTS ISSUED)**
 - **BUS PASSES etc.,**



PARLIAMENT ATTACK CASE

- **DELHI POLICE SEIZED A LAPTOP WHERE THEY STORED THE INCRIMINATING MATERIAL.**
- **ON FORENSIC ANALYSIS:**
 - **HOW THE COMPUTER WAS USED TO PRODUCE THE MHA STICKER**
 - **IP ADDRESSES OF PAKISTAN**
 - **TELEPHONE NUMBERS**
 - **CODED MESSAGES**



Cyber terrorism and cyber warfare

66 F: Cyber Terrorism



- [illegible]



Cyber Defamation

66 A:



Defamation – cyber defamation

- The term defamation is used to define the injury that is caused to the **reputation** of a person in the eyes of a third person. The injury can be done by words oral or written, or by signs or by visible representations. The intention of the person making the defamatory statement must be **to lower the reputation** of the person against whom the statement has been made in the eyes of the general public.
- Cyber defamation **is publishing of defamatory** material against another person **with the help of computers or internet**. If someone publishes some defamatory statement about some other person on a website or send emails containing defamatory material to other persons with the intention to defame the other person about whom the statement has been made would amount to cyber defamation



Law on cyber defamation

- The Section 66A of the Information Act, 2000 does not specifically deal with the offence of cyber defamation but it makes punishable the act of sending grossly offensive material for causing insult, injury or criminal intimidation.
- Section 66A of the IT Act says that any person who sends, by means of a computer resource or a communication device:-
 - any information that is **grossly offensive** or has menacing character; or
 - any content information which he **knows to be false**, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,
 - any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.
-



Judicial Response to cyber defamation

- ❖ In the first case of cyber defamation in India, SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra (CS(OS) No. 1279/2001, Delhi High Court), the reputation of a corporate was being defamed by an employee of the plaintiff company by sending derogatory, defamatory, obscene, emails obscene, vulgar, filthy and abusive emails to its employers and also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director. The Hon'ble Judge of the Delhi High Court passed an ex-prate ad interim injunction observing that a prima facie case had been made out by the plaintiff.

The Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs.



MINISTRY OF HOME AFFAIRS

This is to certify that this car belongs to the ministry of home affairs, and this is the property of India. No body allows to stop this car. India is a very bad country and we hate India. We want to destroy India and with the grace of God we will do it. God is with us and we will try our best. This ediet wajpiee and Advani we will kill them. They have killed many innocent people and they are very bad persons and their brother Bush he is also a very bad person. He will be the next target. He is also the killer of innocent people. He has to die and we will do it. Ministry of home affairs Government of India.



QUESTIONS DEFENCE RAISED (IN P-ATTACK CASE)

- **CAN THE HARD DISK OF A COMPUTER CAN BE CHANGED ?**
- **CAN THE CLOCK OF A COMPUTER CAN BE CHANGED ?**
- **WHY A BACK-UP OF HARD DISK WAS NOT TAKEN?**
- **TIME STAMPS ?**



TYPICAL SCENARIO

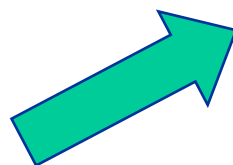
WHAT IS THE EVIDENCE ?



IS EVIDENCE
VISIBLE ?



HOW TO
COLLECT ?



WHERE IS THE EVIDENCE



FEW QUESTIONS--

- **ANY DIFFICULTY IN GATHERING THE EVIDENCE**
 - IDENTIFICATION OF THE EVIDENCE
 - CAN YOU SWITCH ON THE COMPUTER TO SEE WHERE IS THE EVIDENCE ?
 - **BY KEEPING QUICK LEADS TO INVESTIGATION IN MIND**
 - DATE & TIME STAMPS
 - » EVIDENTIAL INTEGRITY
 - **IS IT IN A READABLE FORMAT ?**
 - MAY BE
 - » ENCRYPTED
 - » PASSWORD PROTECTED
 - CAN YOU SWITCH OFF THE COMPUTER IF THE SYSTEM IS ON MODE
 - **FATE OF VOLATILE DATA (EVIDENCE)**
- **LEGAL ADMISSIBILITY OF EVIDENCE ?**



QUESTIONS BEFORE INVESTIGATING OFFICER

- **IS THERE ANY SOLUTION**
 - TO SEE THE ENTIRE CONTENTS OF THE SUSPECTED STORAGE DEVICE
 - TO COPY/ TAKE THE PRINT OUT OF IMPORTANT FILES/FOLDERS
 - TO SEE PASSWORD PROTECTED/ ENCRYPTED/ HIDDEN/ DELETED FILES
 - TO COLLECT STORED, TRANSMITTED & VOLATILE EVIDENCE.
 - TO IDENTIFY THE EVIDENCE etc.,
 - TO LINK PHYSICAL WORLD TO VIRTUAL WORLD
- **ALL THESE ACTIONS WITHOUT LOOSING INTEGRITY OF EVIDENCE**



DIGITAL EVIDENCE?

DIGITAL EVIDENCE IS ANY INFORMATION OF PROBATIVE VALUE THAT IS EITHER STORED OR TRANSMITTED IN A BINARY FORM” (SWG).

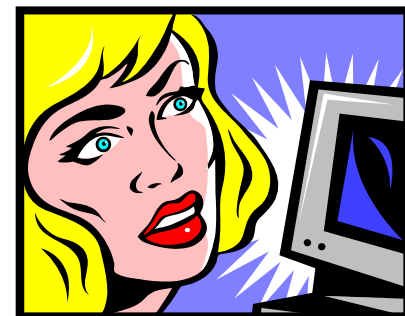
- **CHARACTERISTICS**

- IDENTIFICATION OF DIGITAL EVIDENCE
 - INVISIBLE
- COLLECTION OF EVIDENCE
 - VOLATILE EVIDENCE?
- TIME SENSITIVE
 - ACTION & REACTION SHOULD OVERLAP
- FRAGILE



TYPES OF DIGITAL EVIDENCE

- **HOW TO COLLECT**
 - **STORED DATA**
 - **TRANSMITTED DATA**
 - **VOLATILE DATA**





MAJOR PROBLEM ?



PHYSICAL
WORLD



VIRTUAL WORLD



THE SOLUTION

CYBER FORENSICS



WHAT IS CYBER FORENSICS?

- **YOUNGEST BRANCH OF FORENSIC SCIENCE**
 - Fastest growing, accepted by judiciary, well tested
- **THE PROCESS OF IDENTIFYING, PRESERVING, ANALYSING AND PRESENTING DIGITAL EVIDENCE IN A MANNER THAT IS LEGALLY ACCEPTABLE IN ANY JUDICIAL OR ADMINISTRATIVE HEARING**

THE LAW



CYBER FORENSICS



TECHNOLOGY



DIVERGENT FROM TRADITIONAL BRANCHES OF FORENSIC SCIENCE



- NEVER WORK ON DIGITAL EVIDENCE
- DONOT HAVE A LONG SPAN
- METHODOLOGY FOR ANALYSIS IS CASE DEPENDENT



CYBER FORENSICS - CLASSIFICATION

- **DISK FORENSICS**

- ACQUIRING AND ANALYZING THE DATA STORED ON SOME FORM OF PHYSICAL STORAGE MEDIA
 - **POST MORTEM ANALYSIS**
 - **COMPUTER FORGERY, TAX EVASION, PONOGRAPHY ETC.**

- **NETWORK FORENSICS**

- IS THE PROCESS OF EXAMINING NETWORK TRAFFIC
- ON-LINE & OFF-LINE ANALYSIS
 - **HACKING, E-MAIL CHEATING, ON-LINE FRAUDS ETC**



CYBER FORENSICS - CLASSIFICATION

- SOFTWARE FORENSICS
 - DETERMINE SOFTWARE OWNERSHIP OR SOFTWARE LIABILITY ISSUES
 - VIRUS, LOGIC BOMBS, IPR ISSUES
- EMBEDDED FORENSICS
 - FORENSIC ANALYSIS OF PRE PROGRAMMED CHIPS
 - SKY BUS, WASHING MACHINES, MOBILE PHONES

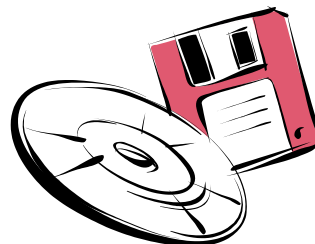


MORE COMPLEXITY

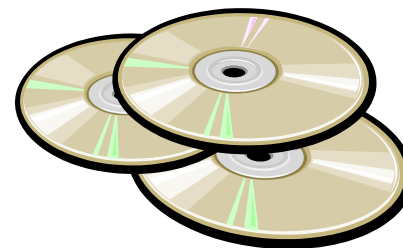
IS DIGITAL
EVIDENCE HERE?



HYDERABAD



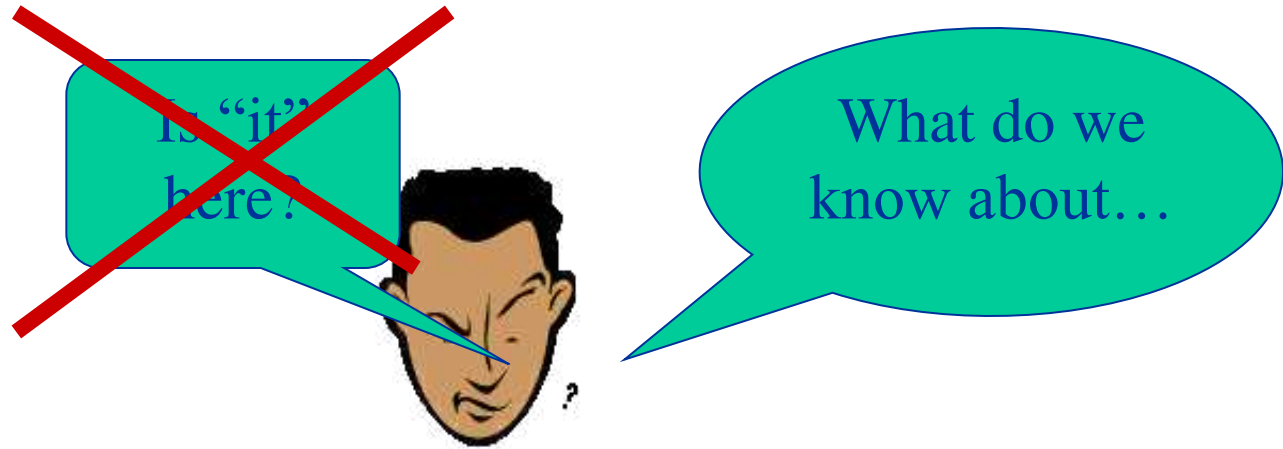
MUMBAI



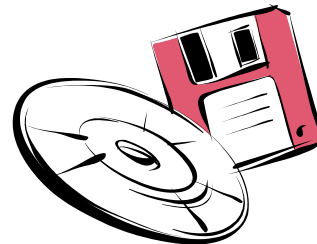
LAHORE



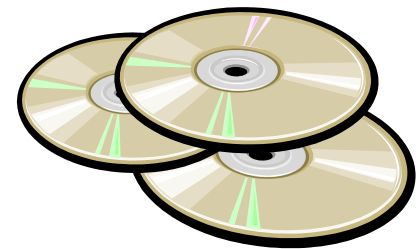
MORE COMPLEXITY



HYDERABAD



MUMBAI



NEWYORK



ACQUIRE

- **IDENTIFICATION OF EVIDENCE**
 - **FORENSIC PREVIEWING**
 - **TIME STAMPS WILL NOT CHANGE**
- **LOGICAL BACKUP**
 - **COPIES THE DIRECTORIES & FILES OF A LOGICAL VOLUME**
 - **DOESNOT CAPTURE DELETE FILES**
- **PHYSICAL BACKUP**
 - **ALSO CALLED DISK IMAGING/CLONING/MIRROR IMAGE**
- **ISSUES DURING IMAGING**
 - **DATA INTEGRITY**
 - **SPEED OF IMAGING**



Mobile Forensic Workstation





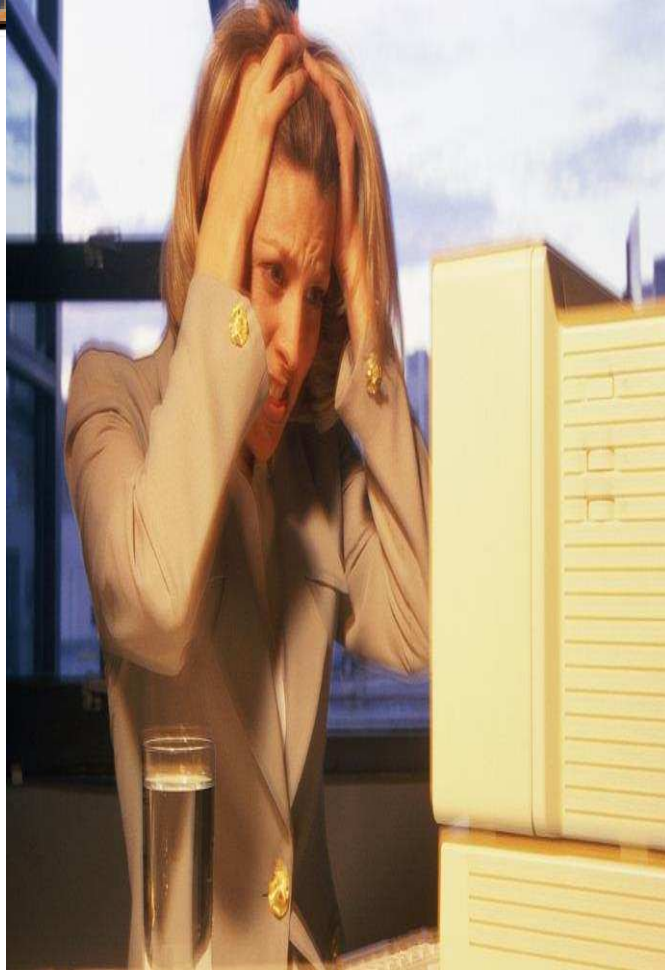
Why use Forensic Tools?

**Your data
“iceberg”**



The data found by common tools

**The additional data found by
FORENSIC SOFTWARE TOOLS
(Deleted, renamed, hidden,
difficult to locate.)**



AUTHENTICATE

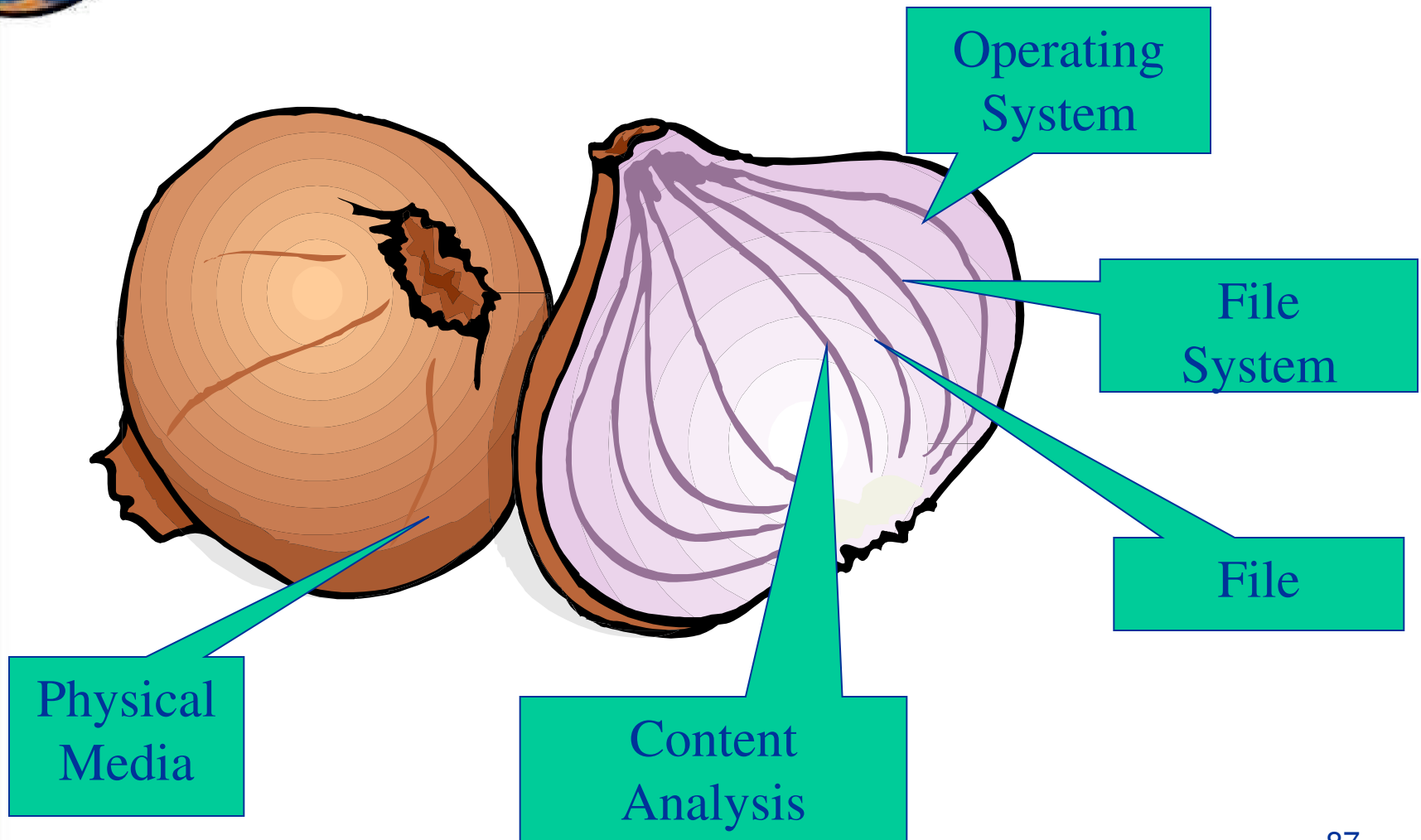
IS THE DUPLICATE AUTHENTIC ?

JUSTIFIED WITH HASH VALUE

**– ACQUISITION HASH VALUE =
VERIFICATION HASH**

MD5 HASH VALUE

ANALYSIS (ONION MODEL)

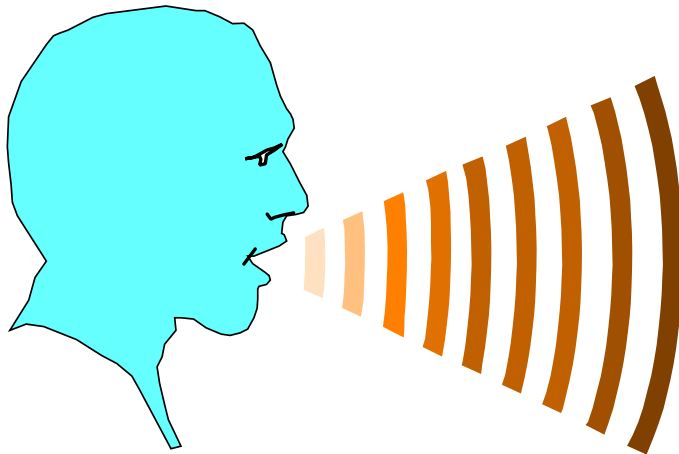




GOOD DOCUMENTATION



- **EXERCISE TO MAKE THE JUDICIARY TO APPRECIATE**
- **REPORT IN SIMPLE TERMS**





WHAT YOU CAN EXPECT FROM CYBER FORENSIC ANALYST ?

- **ACTIVE FILES**
- **DELETED FILES**
- **FILE META DATA —**
 - DATA ASSOCIATED WITH FILE LIKE DATE OF CREATION, MODIFIED ETC
- **SOFTWARE APPLICATIONS**
 - OPERATING SYSTEM RUNNING, ANY SPYWARE, TROJAN HORSE ----
- **HIDDEN FILES/FOLDERS/PARTITIONS**
 - CHANGING THE ATTRIBUTES, STEGANOGRAPHY
- **ENCRYPTED FILES**
 - PASSWORD PROTECTED, DECRYPTION
- **DATA IN UNALLOCATED SECTORS, SWAP FILES**



WHAT YOU CAN EXPECT FROM CYBER FORENSIC ANALYST ?

- ❖ DATA RETRIVEL FROM FORMATTED DISKS, DEFRAGMENTATION DISKS ----
- ❖ E- MAIL TRACING
- ❖ E-MAIL BOX RECOVERY
- ❖ RECYCLE BIN
- ❖ FORENSIC ANALYSIS OF MOBILE PHONES



LOGIC BEHIND CYBER FORENSICS



- **DELETE & QUICK FORMATTING – DOESNOT MEAN DATA HAS GONE**
 - ENTRY IN THE FAT IS REMOVED.
 - **LIMITATION: OVERWRITTEN DATA NOT POSSIBLE**



CYBER FORENSICS

Investigation

- **WHAT'S POSSIBLE?**
 - RECOVERY OF DELETED DATA
 - DISCOVERY OF WHEN FILES WERE MODIFIED, CREATED, DELETED, ORGANIZED
 - CAN DETERMINE WHICH STORAGE DEVICES WERE ATTACHED TO A SPECIFIC COMPUTER
 - WHICH APPLICATIONS WERE INSTALLED, EVEN IF THEY WERE UNINSTALLED BY THE USER
 - WHICH WEB SITES A USER VISITED...
- **WHAT'S NOT...**
 - IF DIGITAL MEDIA IS COMPLETELY (PHYSICALLY) DESTROYED, RECOVERY IS IMPOSSIBLE
 - IF DIGITAL MEDIA IS SECURELY OVERWRITTEN, RECOVERY IS VERY, VERY COMPLICATED, OR IMPOSSIBLE



“Deletion” Fallacies

- **“I DELETED, THE FILE, IT’S GONE.”**
 - DELETED FILES ARE RECOVERABLE USING DIGITAL FORENSICS TOOLS
- **“I CHANGED THE NAME OF THE FILE, NOW NO ONE WILL FIND IT”**
 - DIGITAL FORENSICS TOOLS IMMEDIATELY IDENTIFY FILES BASED ON CONTENT—NAMES DON’T MATTER AT ALL
- **“I FORMATTED THE DRIVE—WHEW!”**
 - THIS DESTROYS ALMOST NOTHING
- **“I USE ONLY WEB-BASED EMAIL”**
 - SOME EMAIL FRAGMENTS ARE STILL PRESENT LOCALLY
- **“I ENCRYPTED MY FILES”**
 - IT’S MORE DIFFICULT TO HIDE ALL YOUR DATA THAN ONE MIGHT THINK
- **“I PUT THE HARD DRIVE NEXT TO A HUGE MAGNET”**
 - THE MAGNET WOULD HAVE TO BE NOT ONLY HUGE, BUT TERRIFYING.
- **“I CUT THE FLOPPY INTO LITTLE PIECES”**
 - AT THIS POINT, IT’S A QUESTION OF HOW IMPORTANT IT IS TO RECOVER THE DATA, BECAUSE IT IS HARDER TO RECOVER THE DATA

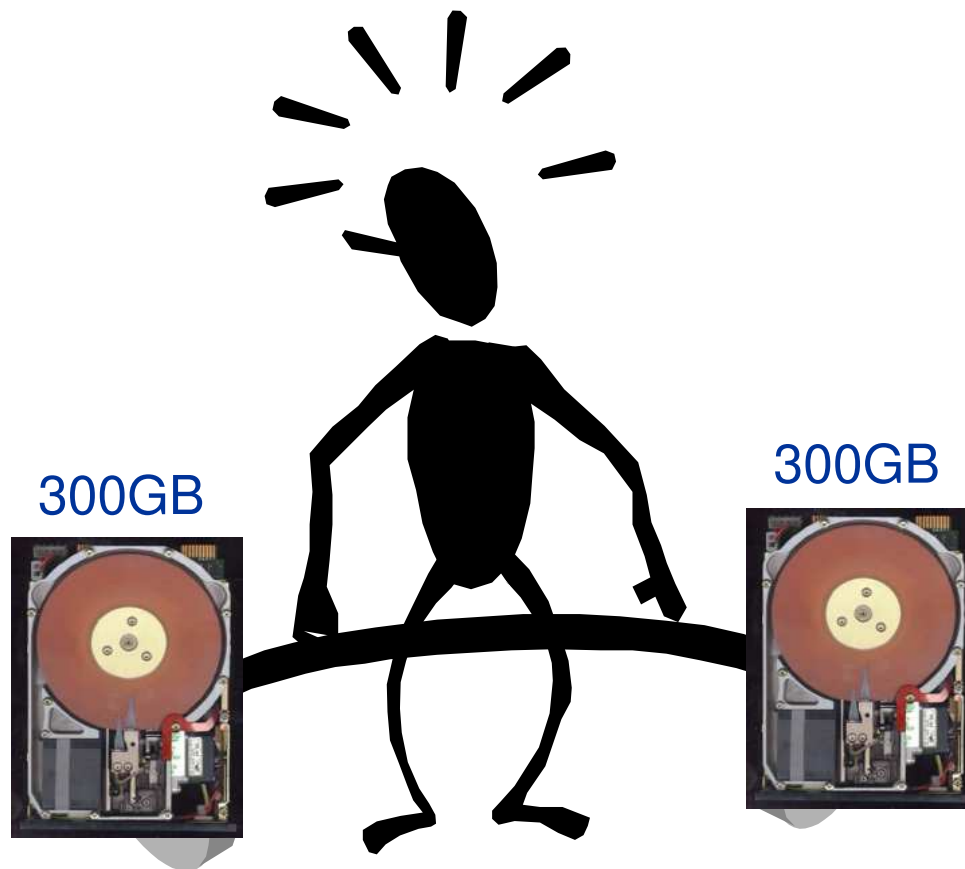


CHALLENGES

- **INCREASE IN ANTI-FORENSIC TRENDS**
 - Defilers toolkit
 - Evidence eliminator
 - Shredding
 - Encryption
 - Passwords
 - Steganography
- **ANALYSIS OF TERABYTES OF DATA**
 - Data mining & dataware housing
 - Need intelligent systems to classify data
- **MAINFRAME DIGITAL FORENSICS**
 - Current tools and methodologies mainly provide for Windows, Unix/ Linux and Mac.



Huge Datasets == The Biggest Challenge



Investigations can take days or weeks



SUMMING UP

- **TECHNOLOGY PERCOLATION CANNOT BE STOPPED.**
- **PROACTIVE APPROACH BETTER THAN REACTIVE**
 - **100% NETWORK SECURITY IS A MYTH**
- **CYBERCRIME IS A MAJOR PROBLEM & IT IS GROWING**
- **SUCCESSFUL PROSECUTION OF CYBERCRIME MUST BE A TEAM EFFORT**
 - **“IT” PERSONNEL MUST LEARN INVESTIGATION AND “LAW ENFORCEMENT” PERSONNEL MUST LEARN TECHNOLOGY**



RICHARD POWER FAMOUS BOOK “TANGLED WEB”



**INFORMATION CRIME
DEMANDS
INFORMATION AGE
LAW-ENFORCEMENT**