

EMERGENCE OF CYBER CRIMES

KRISHNA SASTRY PENDYALA,
CYBER FORENSIC DIVISION,
DIRECTORATE OF FORENSIC SCIENCES,
MINISTRY OF HOMEAFFAIRS,
HYDERABAD.



CAN YOU-----

- * KILL A PATIENT IN CAREWELL HOSPITAL, NEWYORK FROM BENARAS?
- * MAKE A THRETANING CALL TO PRESIDENT FROM L.K ADVANI MOBILE PHONE.
- * MAKE YOUR NEIGHBOUR TELEVISION NON FUNCTIONAL BY SITTING IN YOUR HOUSE?
- * STEAL MONEY FROM NEWYORK BANK BY SITTING AT HYDERABAD?
- * PURCHASE A SHIRT ON SOME BODY CREDIT CARD WITHOUT HIS KNOWLEDGE?
- * WHAT IS GURANTEE THAT THE WASHING MACHINE YOU PURCHASED WILL WORK AFTER GURANTEE PERIOD?
- * MAKE YOUR SON/ DAUGHTER/BROTHER A TOPPER IN ENGINEERING EXAM.

LAST ONE MONTH---

- ★ “MATINEE MASALA”
 - KAPOOR + KAREENA
- ★ “ROOM WITH VIEW”
 - MOHAN KULKARNI OF PUNE
- ★ MISS “TAKE”
 - ANARI GUPTA
- ★ SHOWER SEEN
 - TRISHA HEROINE
- ★ BOY, WHAT A “FRIEND”
 - TANVIR ANSARI ALIAS CHAMPION



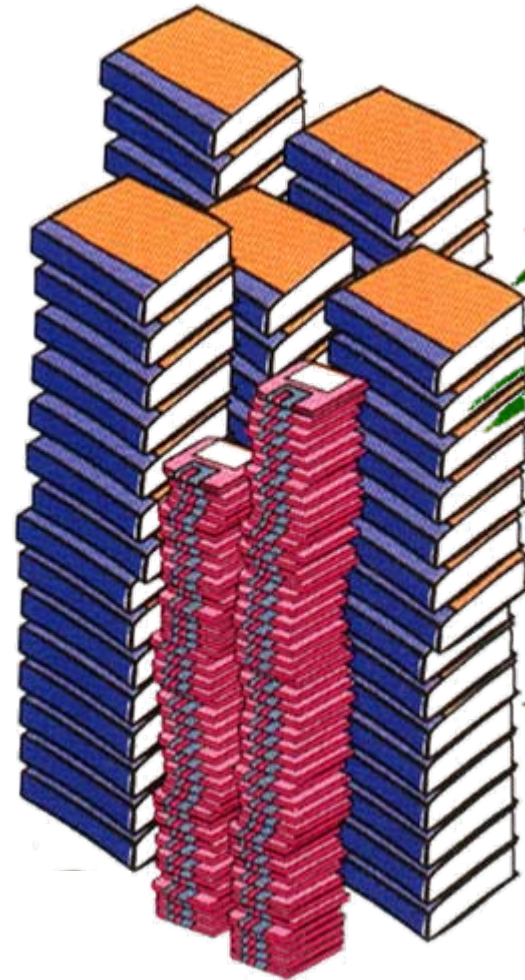
AGENDA

- ★ BACKGROUND
- ★ HOW SECURE WE ARE IN TODAY'S e-ENVIRONMENT?
- ★ WHAT IS CYBER CRIME ?
 - CHARACTERISTICS CYBER CRIMES
- ★ TYPES OF CYBER CRIMES
 - INDIAN SCENARIO
 - ★ CASE STUDIES
- ★ CLOSING THOUGHTS
- ★ QUESTIONS



LAST DECADE- IT REVOLUTION

- ★ CONVERGENCE OF COMMUNICATIONS, COMPUTERS, & NETWORKING
- ★ INTERNET-
GLOBALIZATION OF INFORMATION EXCHANGE



WE ARE IN e- REVOLUTION

- ★ e- BUSINESS
- ★ e- COMMERCE
- ★ e- GOVERNANCE
- ★ e- SECURITY



WAYS TO PROTECT THE ORGANIZATION

- ★ INTRUSION DETECTION SYSTEMS
 - ★ FIREWALLS
 - ★ VPN'S
 - ★ ACCESS CONTROL (BIOMETRICS, PASSWORD)
 - ★ ENCRYPTION (CRYPTOGRAPHY)
 - ★ ANTI- VIRUS
-
- NETWORK SECURITY - NEVER ENDING PROCESS
 - 100% SECURE SYSTEM IS A MYTH



2001 CSI/FBI Computer Crime and Security Survey

Of the organizations suffering security compromises in the last year – 95% had Firewalls and 61% had IDSs !

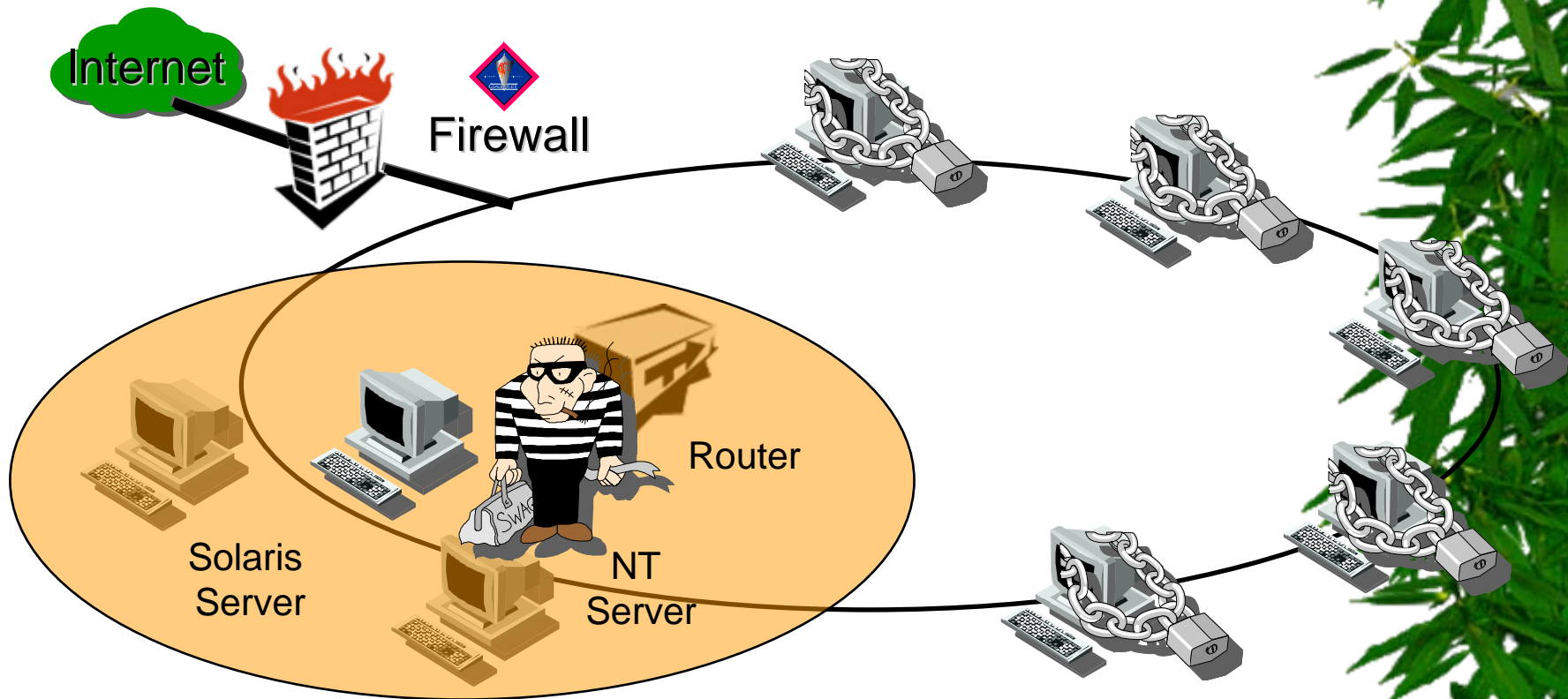
	1998	1999	2000	2001
SECURITY TECHNOLOGIES USED	%	%	%	%
Intrusion Detection Systems	35	42	50	61
Firewalls	81	91	78	95
Encrypted Files	50	61	62	64
Anti-virus software	96	98	100	98
Access Control	89	93	92	90

• False sense of security - *"We already have a Firewall"*

Question: Do the risks outweigh the benefits?



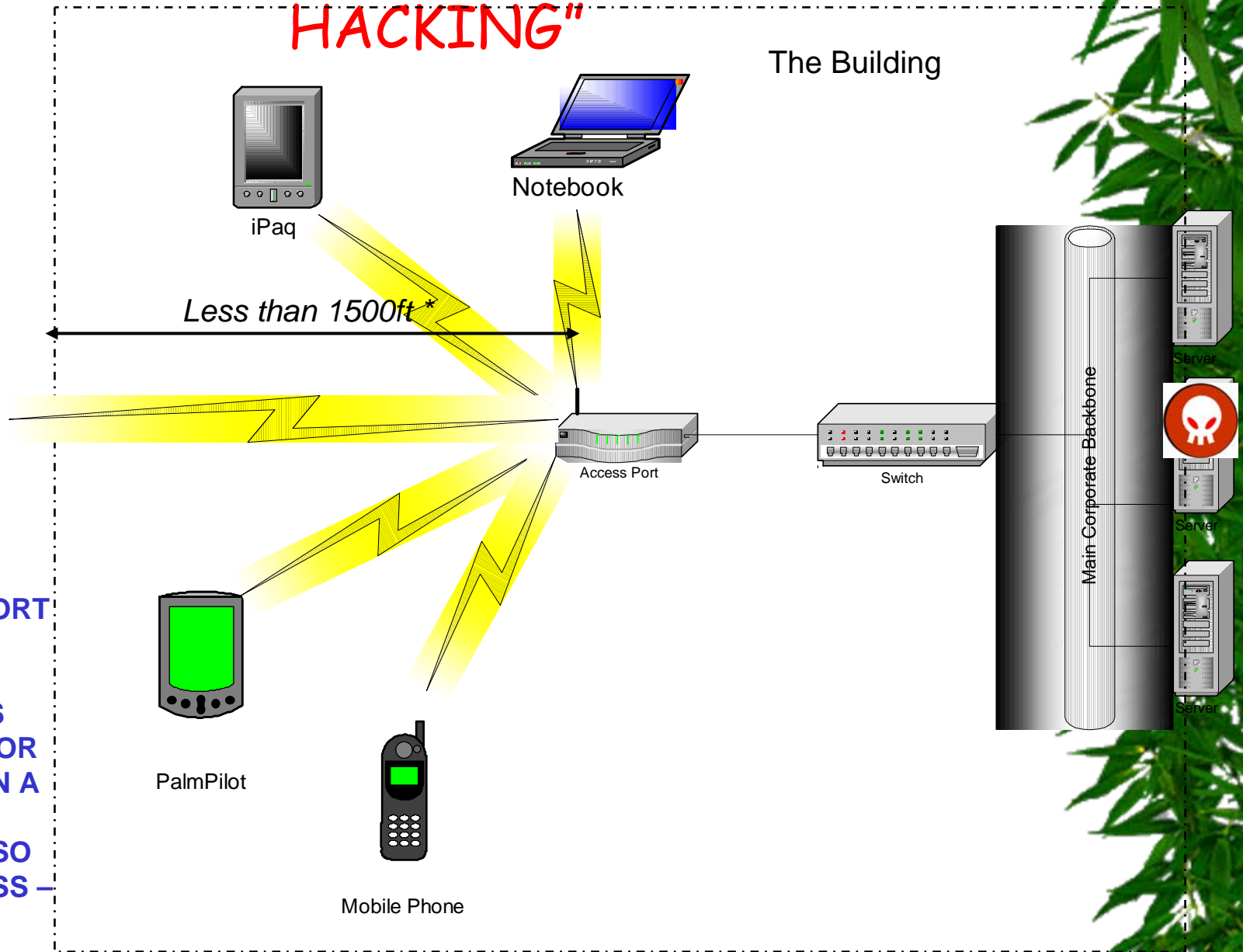
HACKING



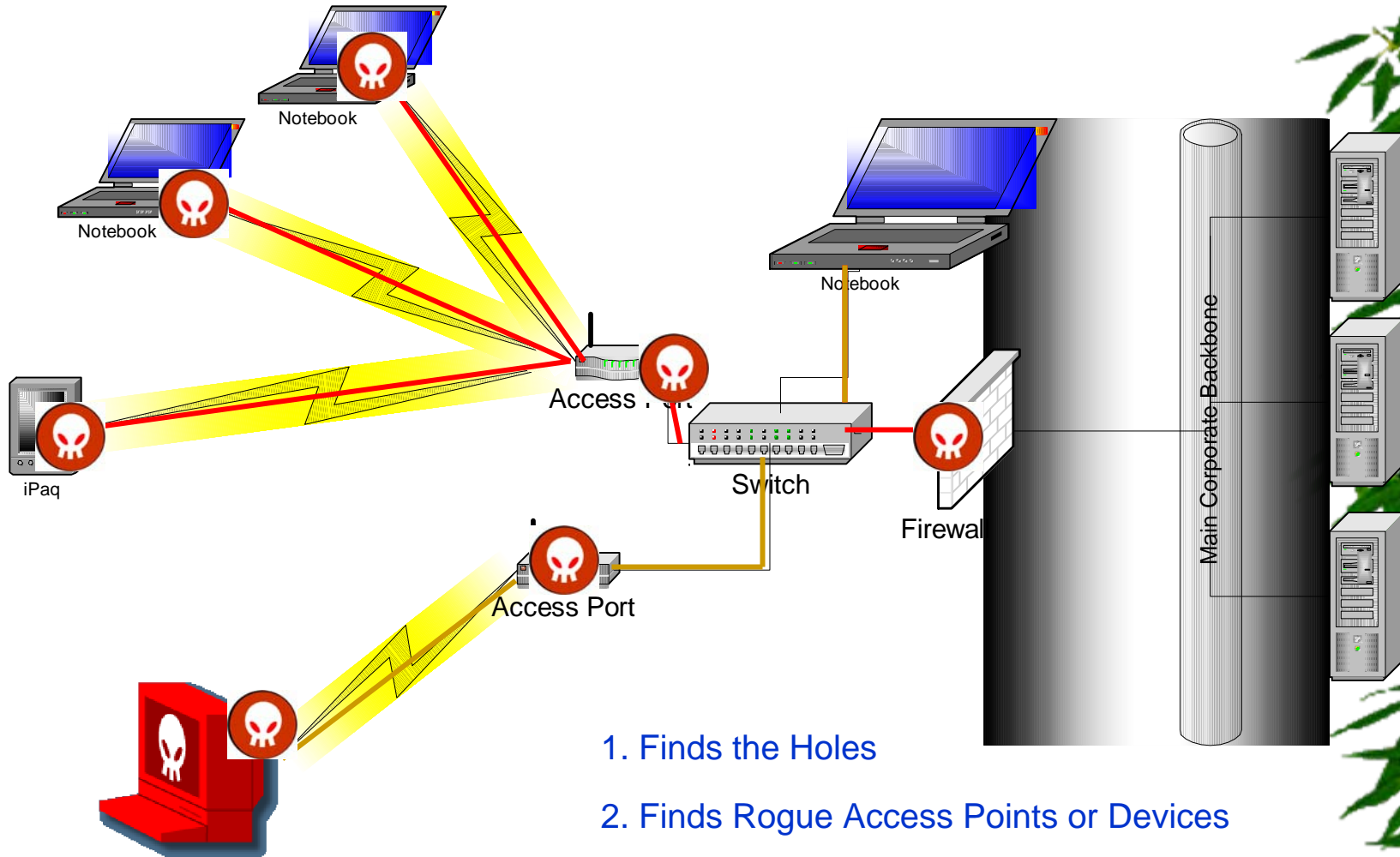
THE PROBLEM ... "DRIVE BY HACKING"



IF THE DISTANCE FROM THE ACCESS PORT TO THE STREET OUTSIDE IS 1500 FEET OR LESS, THEN A HACKER COULD ALSO GET ACCESS – WHILE SAT OUTSIDE



PLANTING A VIRUS?



COMPUTER CRIME STATISTICS

- AVERAGE COMPUTER CRIME -
\$5,00,000
AVERAGE BANK ROBBERY - \$1300
- 80% OF COMPUTER CRIME INVOLVES
INTERNET
- - INTERNET IS IN 100 COUNTRIES
 - OVER 50 MILLION USERS
 - 15%/MONTH GROWTH RATE



WHAT IS CYBER CRIME ?

- NO DEFINITION
- DEFINITION OF CRIME CHANGED
- CRIME IN ONE COUNTRY NEEDNOT BE A CRIME IN OTHER COUNTRY?



DEFINITION OF CRIME CHANGED THEFT

- ★ **REAL-WORLD THEFT:**
POSSESSION OF PROPERTY
SHIFTS COMPLETELY FROM
A TO B, I.e., A **HAD** IT,
NOW B **HAS** IT
- ★ **CYBER-THEFT:** PROPERTY
IS COPIED, SO A "**HAS**" IT
AND B ALSO.



COPYING AS THEFT?

- ★ RANDALL SCHWARTZ WORKED FOR INTEL
- ★ CHARGED WITH COMPUTER THEFT FOR COPYING A PASSWORD FILE
- ★ CLAIMED IT WASN'T THEFT BECAUSE INTEL DID NOT "LOSE" ANYTHING - INTEL STILL HAD THE PASSWORDS, AND SO DID SCHWARTZ



CRIME IN USA NOT A CRIME IN PHILIPPINES

MR. ONEL DE GUZMAN, ACCUSED
I LOVE YOU VIRUS



★ *Cost \$10 billion
Computer
Economics*



CHARACTERISTICS OF CYBER CRIME

- ANNONIMITY
- SILENT IN NATURE
- LARGE OPERATIONAL CANVAS
- ALMOST NO PHYSICAL EVIDENCE/CLUES
- HIGH IMPACT & INTENSITY
- MANY TIMES FAR AWAY FROM THE SCENE OF CRIME



E-MAIL CHEATING (MUMBAI)

★ 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 COULDN'T MEET X AS PROMISED
- X COMMITTED SUICIDE.



E-MAIL CHEATING (MUMBAI)

- ★ 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)



E-MAIL CHEATING (MUMBAI)

- ★ TWO DESK TOP COMPUTERS, TWO LAPTOPS WERE SENT FOR FORENSIC ANALYSIS
- ★ ANALYSIS PROVED
 - ALL WAS DONE BY A SINGLE MAN NAMED MR.PRANAB MITRA, GENERAL MANAGER, AMBUJA CEMENTS



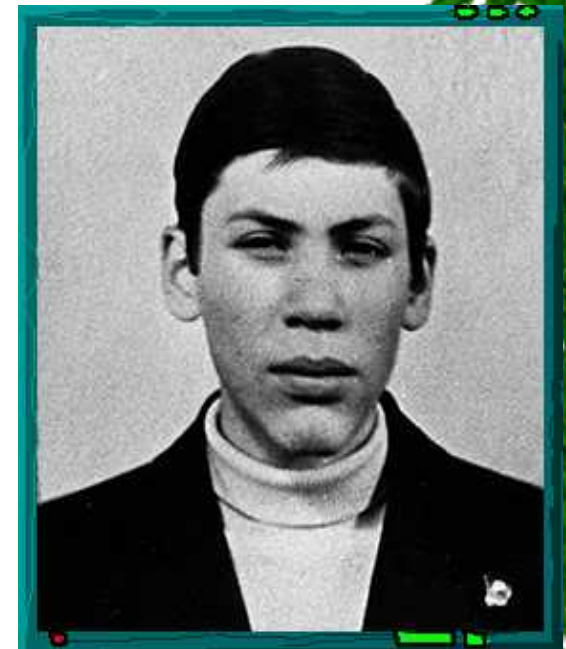
CHARACTERISTICS OF CYBER CRIME

- ANNONIMITY
- SILENT IN NATURE
- LARGE OPERATIONAL CANVAS
- ALMOST NO PHYSICAL EVIDENCE/ CLUES
- HIGH IMPACT & INTENSITY
- MANY TIMES FAR AWAY FROM THE SCENE OF CRIME

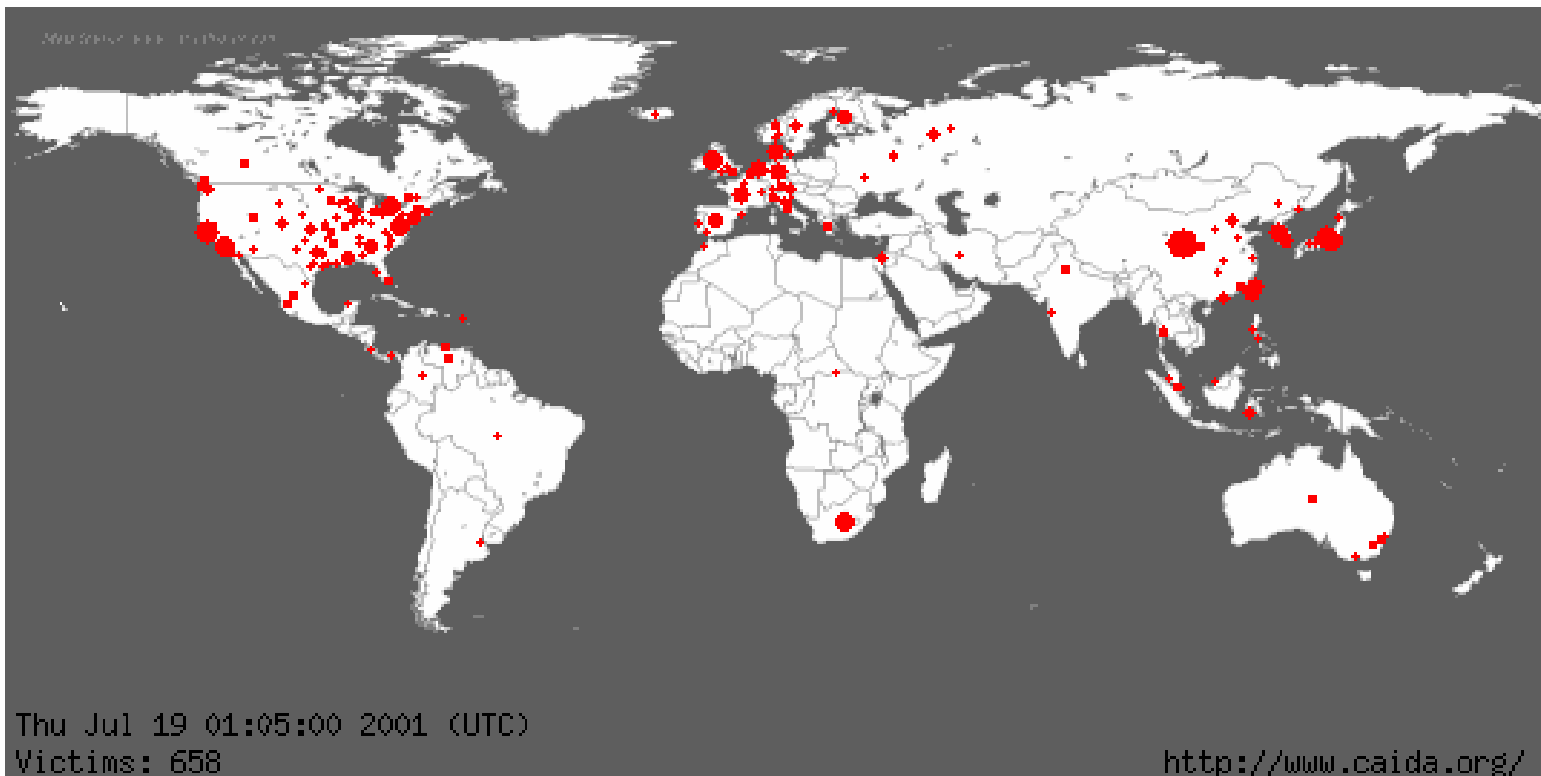


CITI-BANK

- ★ Vladimir Levin:
 - System Administrator St. Petersburg, Russia
- ★ ATTACKED CITI-BANK SYSTEM AND OBTAINED USERIDS AND PASSWORDS
- ★ SETUP ACCOUNTS IN BANKS THROUGHOUT THE WORLD
 - BANK OF AMERICA, BANCO DEL SUD ARGENTINA, BANK ARTHA GRAHA INDONESIA
- ★ TRANSFERRED \$12 MILLION TO THE VARIOUS ACCOUNTS

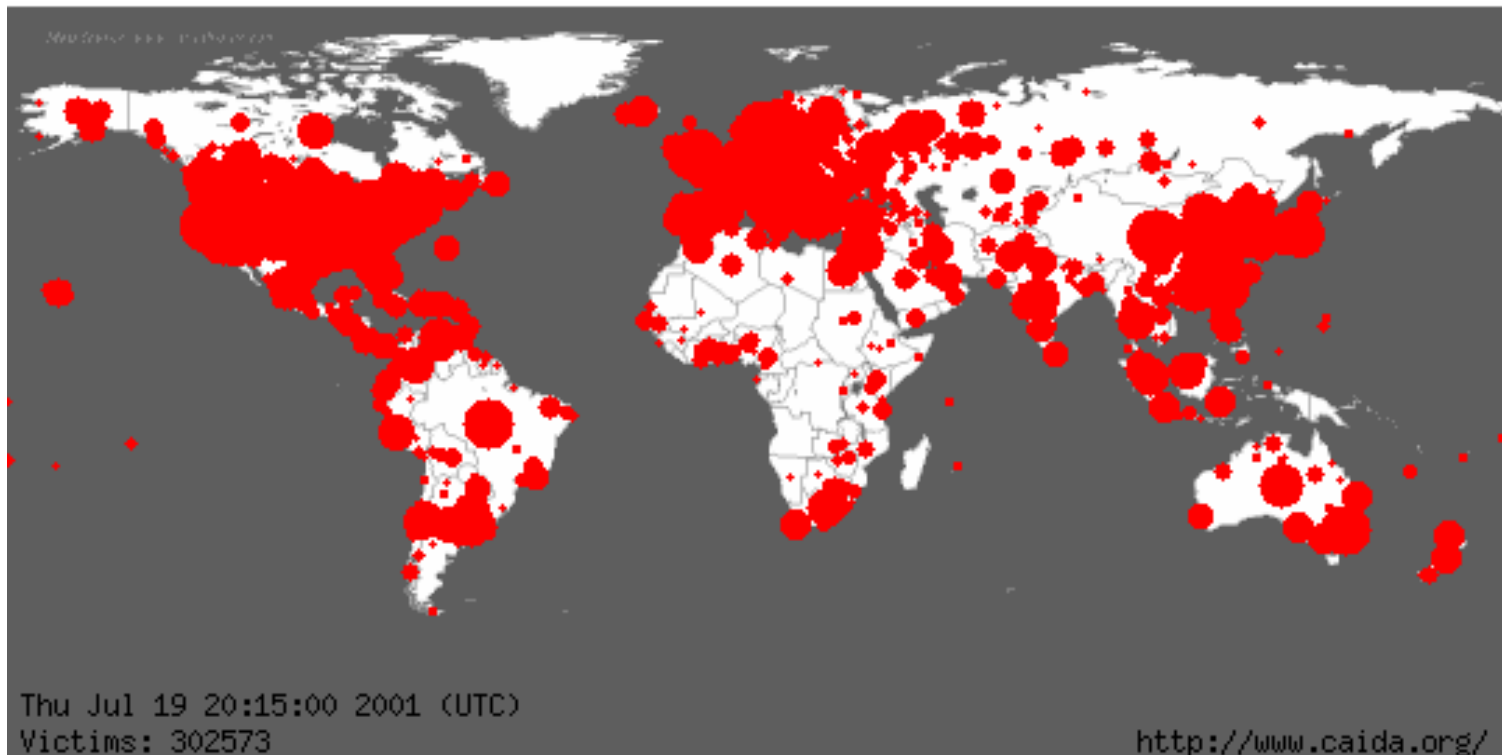


SPREAD OF WORM

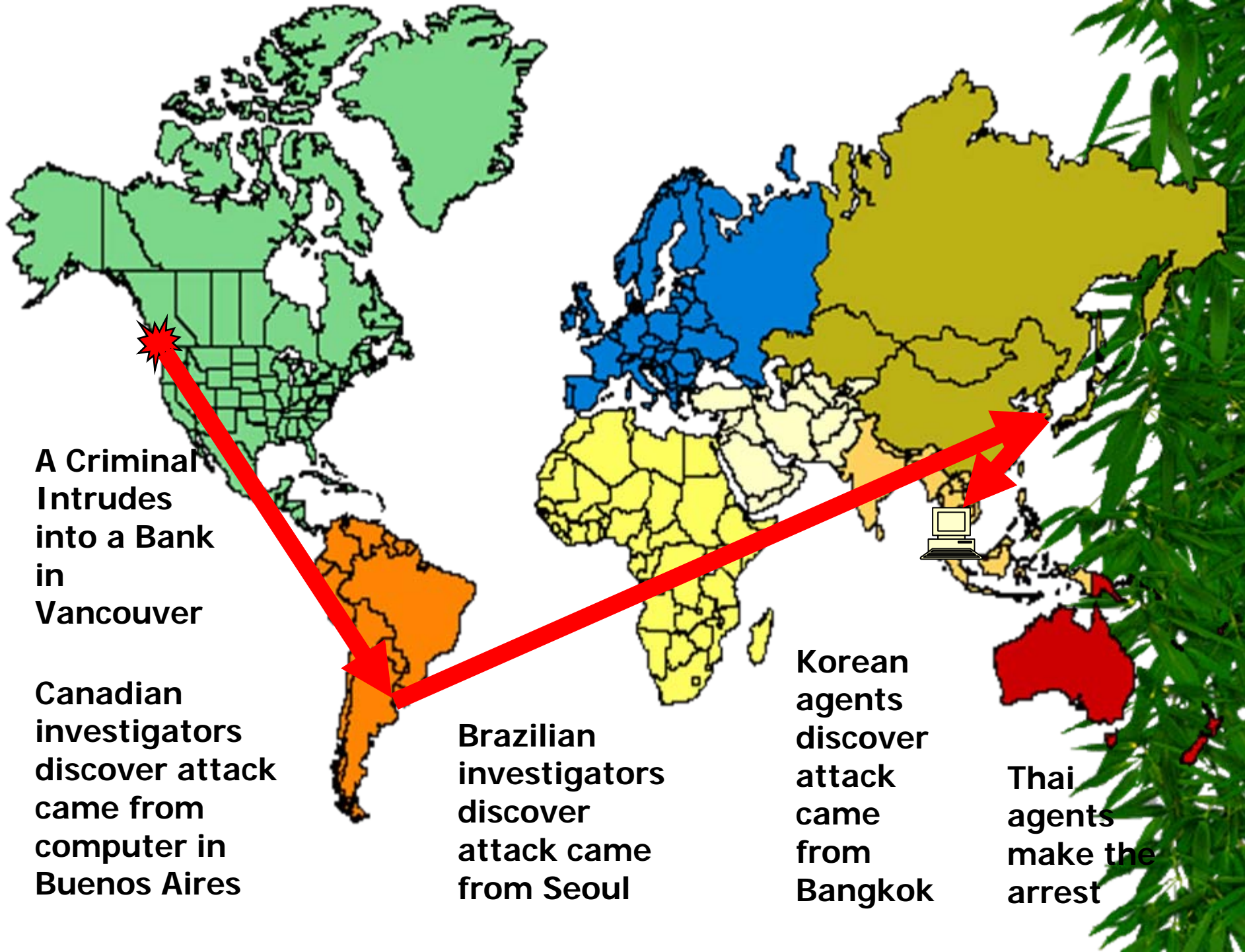


July 19 01:05:00 2001

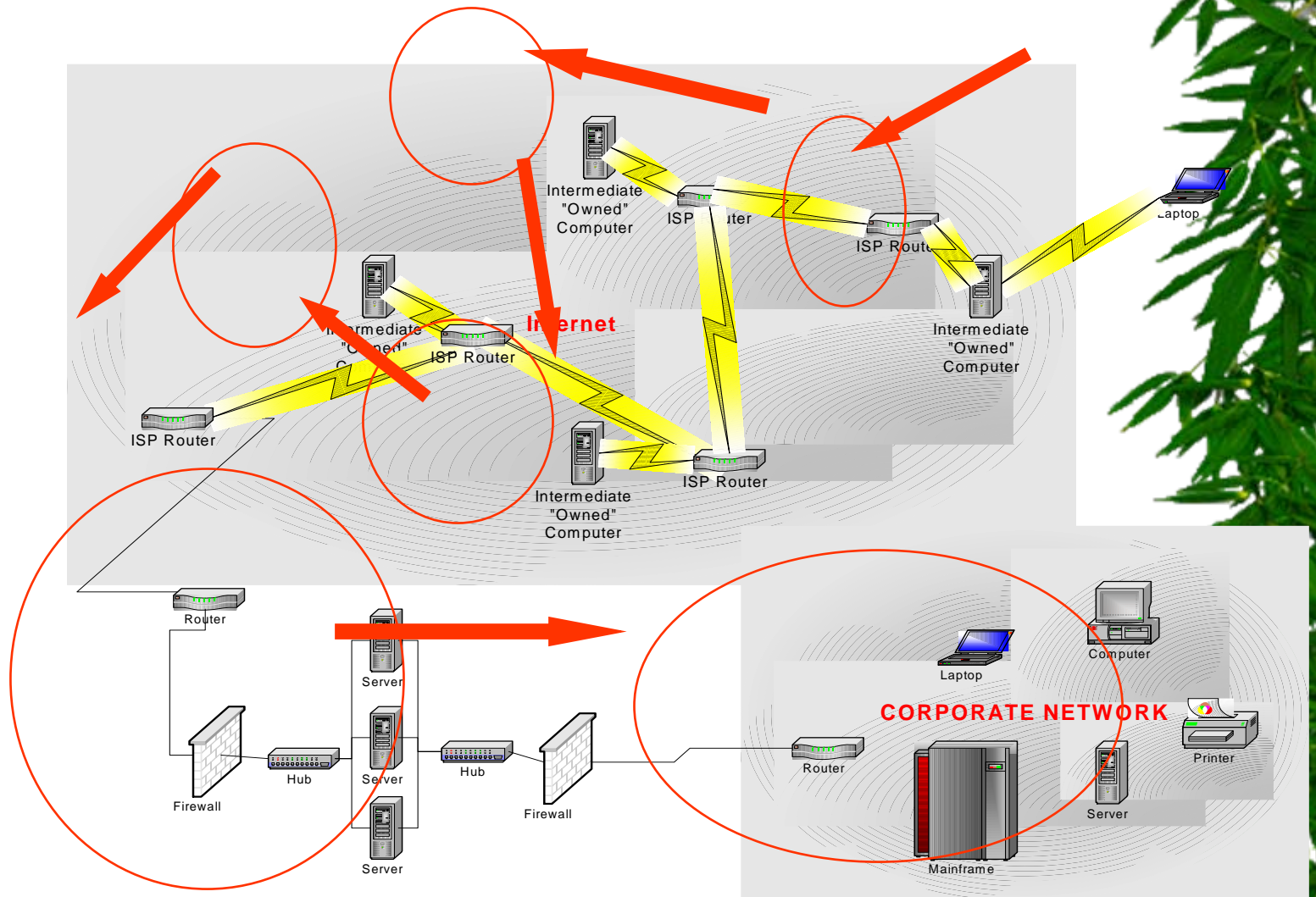
SPREAD OF WORM



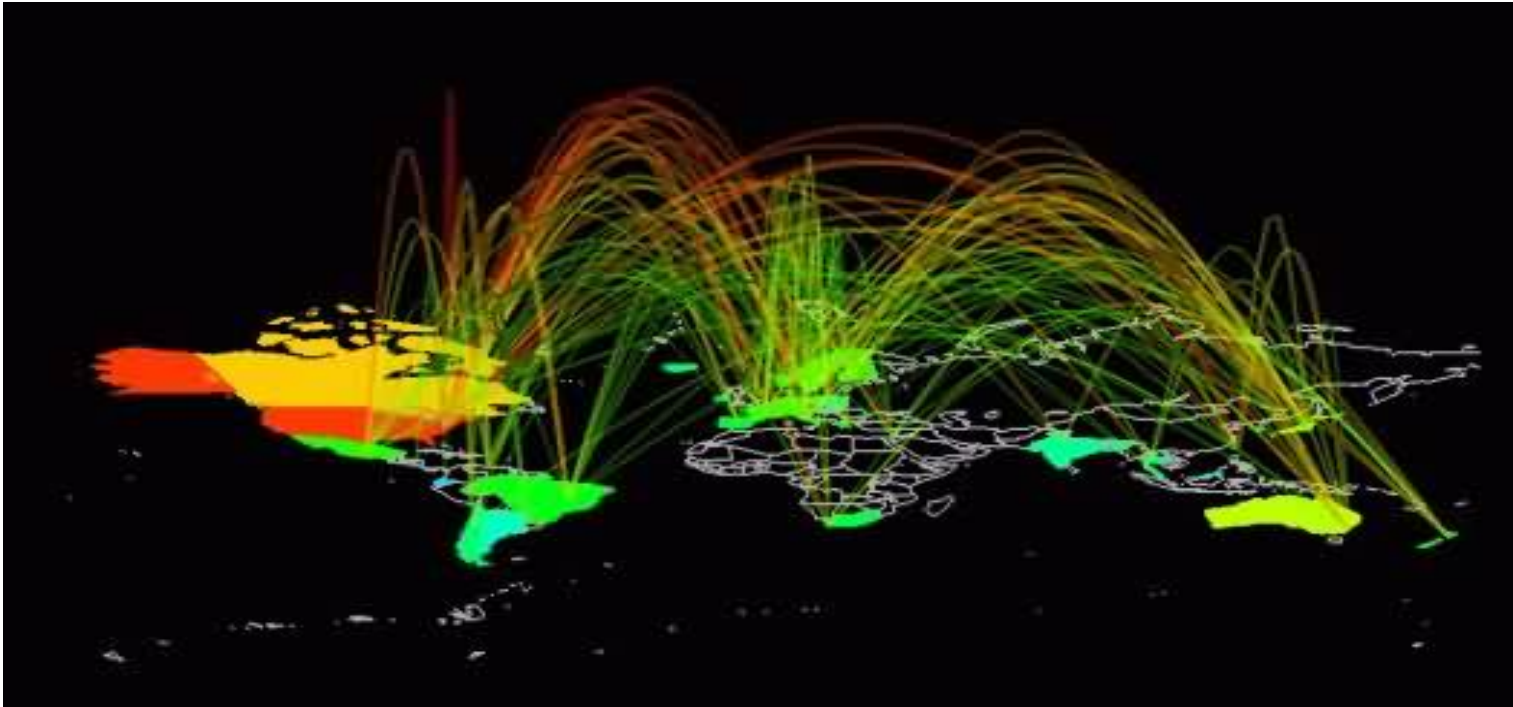
July 19 20:15:00 2001



HACKING



Cybercrime: proximity



"In the networked world, no island is an island."

CRITICAL ISSUES

- ★ IS OUR POLICE ARE CAPABLE ENOUGH TO INVESTIGATE?
- ★ IS OUR FORENSIC LABS HAVE FACILITIES TO ANALYSE THE DIGITAL EVIDENCE?
- ★ IS OUR PRESENT LAWS ARE SUFFICIENT?
- ★ IS OTHER COUNTRIES HELP?



TRADITIONAL VS CYBER CRIMES



PAPER BASED VS CYBER BASED THREATS

CRIME

PAPER BASED

CYBER

UNAUTHORIZED
ACCESS

BREAKING AND
ENTERING

PASSWORD
SNOOPING

VANDALISM

PHYSICAL
GRAFFITI;

SABOTAGE, WEB
SITE

THEFT (MONEY)

THEFT OF CASH

ELECTRONIC
FUNDS
TRANSFER

THEFT (ASSETS)

THEFT OF
PHYSICAL
PROPERTY

THEFT OF IP,
SOFTWARE
PIRACY



DEFINITION OF COMPUTER CRIME

- ★ NO CONSENSUS REGARDING THE DEFINITION
- ★ AGAINST
 - INDIVIDUAL
 - COMPUTER ENVIRONMENT
- ★ AGAINST
 - PEOPLE,
 - PROPERTY,
 - THE GOVERNMENT



COMPUTER CRIME IS AN INDIVIDUAL'S ATTEMPT, FRAUDULENTLY OR OTHERWISE

- TO PREVENT THE COMPUTER TO PERFORM ITS DUTIES AS DESIGNED, OR
- TO SLOWDOWN ITS OPERATIONS, OR
- TO CORRUPT THE DATA OR SOFTWARE, OR
- TO COPY THE DATA OR SOFTWARE WITHOUT AUTHORITY



COMPUTER ENVIRONMENT

- UNAUTHORIZED ATTEMPT TO ACCESS, ALTER, ADD, DELETE OR HIDE DATE.
- UNAUTHORIZED ATTEMPT TO ACCESS, ALTER, ADD, DELETE OR HIDE PROGRAM OR SYSTEM
- STEALING OF DATA OR PROGRAMS IN ANY MANNER
- UNAUTHORIZED (PHYSICAL AND/OR LOGICAL) ENTRY INTO COMPUTER WORK ENVIRONMENT.
- CHANGE OR ALTER THE DEFINED SYSTEMS.



GENERIC CLASSIFICATION OF COMPUTER CRIME

- * DATA RELATED CRIMES

- * SOFTWARE RELATED CRIMES

- * PHYSICAL CRIMES.



DATA RELATED CRIMES

- ★ DATA DIDDLING
- ★ DATA LEAKAGE
- ★ DATA SPYING
- ★ SCAVENGING



SOFTWARE RELATED CRIMES

- # TROJAN HORSE
- # TRAP DOOR
- # WIRE-TRAPPING
- # TIME BOMBS
- # LOGIC BOMBS
- # SALAMI LOGIC
- # WORMS
- # VIRUSES.



Physical Crimes

THEFT

BREAKAGE

DESTROYING DATA, OUTPUT
OR MEDIA

INTER-PROCESSING
MANIPULATIONS



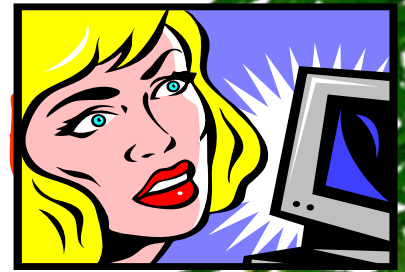
VARIOUS TYPES OF CRIMES

* NO STATISTICS IN INDIA

- CYBER STALKING/HARASSMENT
- ON LINE BETTING/ GAMBLING,
- MONEYLAUNDERING
- ATM & CREDITCARD FRAUDS
- DATA MANIPULATION
- HACKING & CRACKING
- DATA THEFT -IDENTITY THEFT
- IP OFFENCES: ILLEGAL SOFTWARE;
COPYRIGHT BREACHES ETC
- COMPUTER FORGERY
- PORNOGRAPHY



CYBERSTALKING/ONLINE HARASSMENT



- * SENDING HARASSING OR
THREATENING E-MAILS, POSTING
ATTACKING OR LIBELOUS MATERIAL
IN WEB SITES OR IN CHAT ROOMS,
POSTING THEIR NAME, PHONE
NUMBER, OR ADDRESS IN CHAT
ROOMS OR ON WEB PAGES, SENDING
MAIL BOMBS, UNWANTED MESSAGES
OR FILES, AND MAKING
INAPPROPRIATE REQUESTS IN CHAT
ROOMS.

CYBER HARASSMENT

- ★ MRS. SANGEETA RANE MADE A COMPLAINT -TELEPHONE CALLS.
- ★ INDIATIMES ROMANCE COLUMN
 - semi-nude photograph, phone number etc.
- ★ MANAGER OF INT. BANK
- ★ NOT ADVISABLE TO GIVE VISITING CARD TO A UNKNOWN PERSON.



HARASSMENT AT WORK PLACE----- & BLACK MAILING



HARASSEMENT OF WOMEN AT WORK PLACE & BLACK MAILING



THE CASE OF MS TRISHA, HEROINE



CHILD PORNOGRAPHY

- ★ POSSESSION OR DISTRIBUTION OF COMPUTER-BASED CHILD PORNOGRAPHY IMAGES
- ★ PEDOPHILES USE THE INTERNET TO LURE CHILDREN, OFTEN BY ACTING AS CHILDREN



CYBER PORNOGRAPHY

- * ABOUT 60 PER CENT OF ALL WEB SITES HAVE SEXUAL CONTENT
- * AN ESTIMATED REVENUE OF \$ 2.5 BILLION IS GENERATED ANNUALLY,
- * 4.2 MILLION PORNOGRAPHIC WEB SITES
- * 12% OF TOTAL WEB SITES
- * 372 MILLION PORNOGRAPHIC PAGES
- * 4.5% INTERNET USERS EVERY DAILY VISIT THE SITES
- * 21% MEN ADMITTED ACCESSING PORNOGRAPHY AT WORK PLACE



CYBER PORNOGRAPHY

- ★ IMAGE PROCESSING TECHNIQUES
- ★ MULTI MEDIA DEVELOPMENTS
- ★ MOBILE PHONES WITH IN BUILT CAMERA



**What We REALLY wish to see
on Extraa Innings!**



Examples

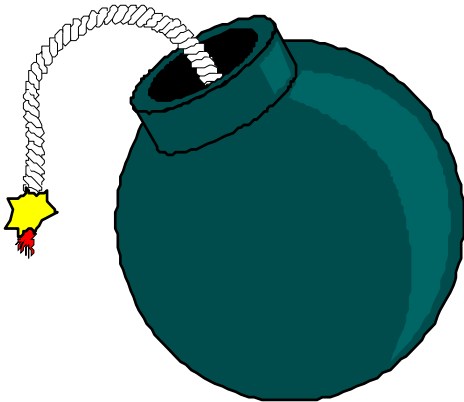
- ★ State of Tamilnadu versus Dr. L Prakash
 - December 2001
 - Running of porn websites www.realindiaporn.com and www.tamilsex.com and circulation of obscene pictures through emails
- ★ Air Force Bal Bharati School Case
 - Delhi Police
 - 15 year old boy created a URL www.amazing-gents.8m.net on free web space featuring 'sexy' girls and teachers of the school



Trojan Horse



- Vehicle for viruses and logic bombs



TROJAN HORSE

- ★ A PROGRAM THAT APPEARS TO DO SOMETHING USEFUL OR ENTERTAINING, BUT CONCEALS A DESTRUCTIVE PURPOSE
- ★ TROJAN HORSES CAN ALSO DELETE FILES, TRANSMIT FILES, INSTALL OTHER PROGRAMS, OR EXECUTE PRIVILEGE ELEVATION ATTACKS



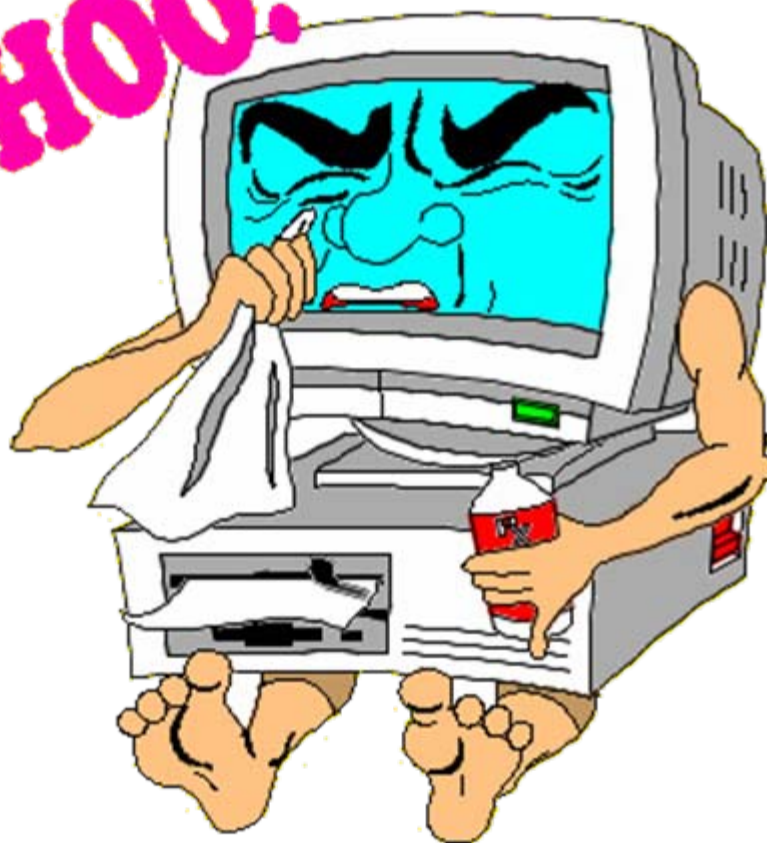
LOGIC BOMB

- ★ CODE SURREPTITIOUSLY INSERTED INTO AN APPLICATION OR OPERATING SYSTEM THAT CAUSES IT TO PERFORM SOME DESTRUCTIVE OR SECURITY-COMPROMISING ACTIVITY WHENEVER SPECIFIED CONDITIONS ARE MET
- ★ MANY COMPANIES ARE KEEPING LOGIC BOMBS
- ★ SAMSUNG Vs KOREAN GOVT



Viruses

AH -
CHOO!



Viruses & WORMS

- ★ VIRUS: A SELF-REPLICATING PROGRAM THAT ATTACHES TO OTHER PIECES OF CODE (THE HOST) AND INFECTS OTHER PROGRAMS
- ★ WORM: A SELF-REPLICATING, SELF-CONTAINED PROGRAM THAT PROPAGATES ITSELF OVER A NETWORK; DOES NOT REQUIRE A HOST



VIRUS STATISTICS

- * GLOBALLY, ABOUT 64% OF COMPANIES WERE HIT BY AT LEAST ONE VIRUS IN THE PAST 12 MONTHS, UP FROM 53% THE YEAR BEFORE.
- * TO DATE, THERE ARE AN ESTIMATED MORE THAN 53,000 COMPUTER VIRUSES IN EXISTENCE.
- * IT IS ESTIMATED THAT PC VIRUSES COST BUSINESSES APPROXIMATELY \$55 BILLION IN DAMAGES IN 2003.

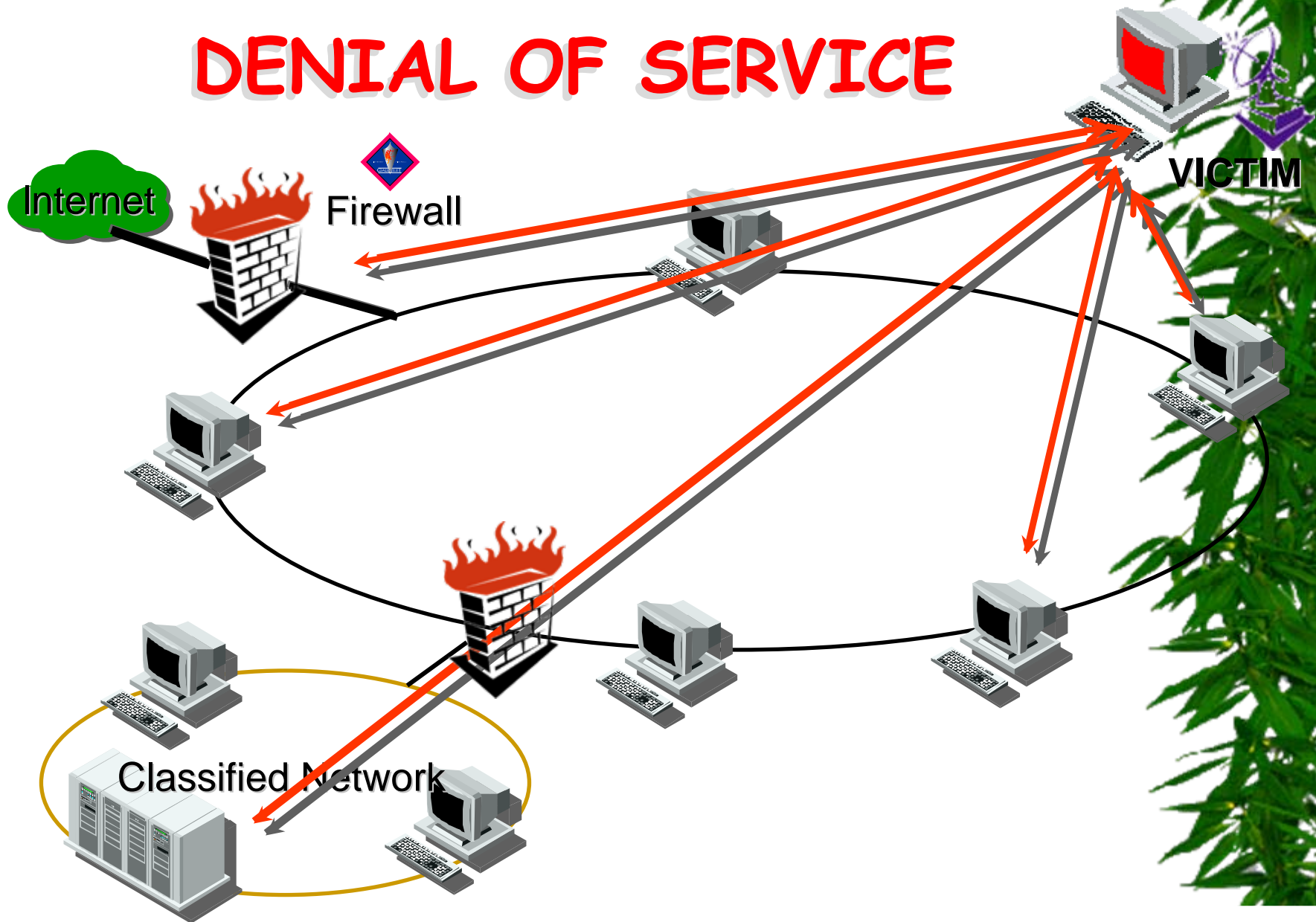


Denial of Service Attacks

- ★ PROGRAMS THAT REPEATEDLY REQUEST INFORMATION FROM THE VICTIM'S COMPUTER UNTIL THE COMPUTER IS OVERLOADED.
- ★ DISTRIBUTED DENIAL OF SERVICE ATTACKS (DDOS) ARE AUTOMATED ATTACKS THAT RUN SIMULTANEOUSLY FROM MULTIPLE COMPUTERS.
- ★ AT A GIVEN HOUR, ALL INVOLVED COMPUTERS COORDINATE REQUESTS FOR INFORMATION FROM THE OVERLOADED VICTIM COMPUTER.
- ★ **EFFECT:** LOCKS OUT LEGITIMATE USERS FROM WEBSITES OR NETWORKS.



DENIAL OF SERVICE



Denial of Service - 02/2000

- ★ YAHOO, AMAZON, EBAY, CNN & BUY.COM WERE ALL ATTACKED
- ★ 15-YEAR-OLD PLED GUILTY TO THE ATTACKS, WHICH DID AN ESTIMATED \$1.7 BILLION IN DAMAGE



PIRACY



- ★ AS MUCH AS \$12 BILLION OF AMERICAN SOFTWARE IS ILLEGALLY COPIED AND DISTRIBUTED WORLDWIDE ANNUALLY. (SOFTWARE AND INFORMATION INDUSTRY ASSOCIATION)
- ★ 90% OF THE SOFTWARE USED IN INDIA IS PIRATED

A CASE OF CBI/FBI

- ★ Mr. SHEKAR VERMA WORKING FOR M/S SOLID WORKS AS TEAM LEADER SOFTWARE DEV. GROUP IN USA.
- ★ LEFT THE COMPANY
- ★ OPENED THE WEBSITE
- ★ CONTACTED THE CUSTOMERS FOR SELLING THE SOURCE CODE
- ★ FBI TEAM VISITED INDIA
- ★ ARRESTED AT ASHOKA HOTEL, NEW DELHI.
- ★ SEVERAL CASES FROM PUNE, MUMBAI



CYBERTERRORISM

- ★ THE USE OF INFORMATION TECHNOLOGY AND MEANS BY TERRORIST GROUPS AND AGENTS TO INFLUENCE OR DISRUPT A COUNTRY'S POLICY;
 - OCCURS WHEN AN INDIVIDUAL CRACKS INTO A GOVERNMENT OR MILITARY WEB SITE



ISI AGENT

- ★ POSING AS A PRESS REPORTER
- ★ SENDING CRUCIAL
INFORMATION THROUGH
DIGITAL WATCH



[CASIO Wrist Camera](#)

Wrist-type wearable digital camera WQV-1 Wrist Camera



Infrared Communication

Wrist Camera



Wrist Camera



Windows® PC



News

Business

Sports

Local

Health

Technology

Living • Travel

TV News

Opinions

Weather

Shop@MSNBC

MSN.com

QwestDex
online yellow pages
Find a Local Business

**AMERICA AT WAR
THE WAR**

Complete coverage

Al-Qaida's secret weapon: computers

**Communication
by terrorists
relies on laptops
and broadband**



A tape aired by Middle East Broadcasting Corp. shows Osama bin Laden, date unknown, sitting with several of his deputies.

Middle East Broadcasting Corp. / via APTN

By Robert Windrem

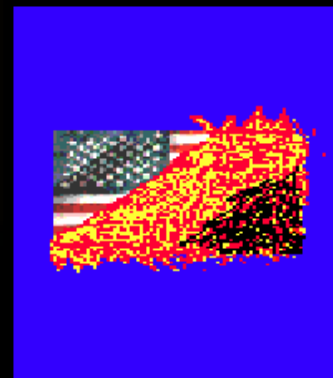
NBC NEWS

NEW YORK, April 18 — Al-Qaida's apparent use of computers and inexpensive editing software to put together videotapes that emerged this week came as no surprise to U.S. intelligence officials, who told NBC News that laptops and high-speed Internet access had become terrorists' primary tools for communicating over the past several



jihad

Islamic unity



I see at last I am no longer on my own in the cyber war against the jews.
(notice how i didn't say israel ? well I don't recognise Israel as a country)
I am pleased to see my Muslim brothers in Gforce and PHC contributing to the
destruction of jewish internet sites.

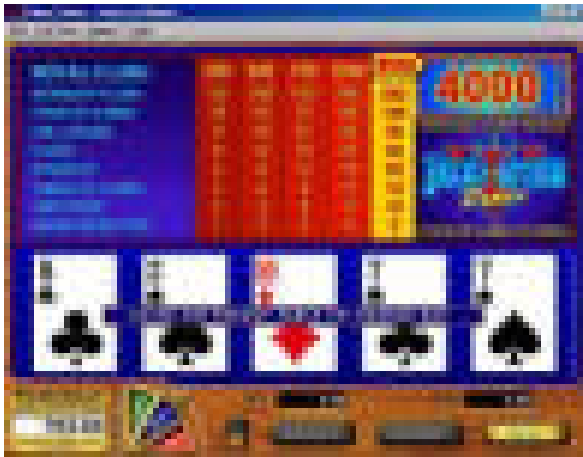
Today is Friday 3rd Novemeber:

Netvision.net.il's backbone was held down for another hour leaving many .gov.
web sites inacessible. Expect more in the coming weeks.
This time even the unnet peering router was badly lagged.

As for www.idf.il I don't care where you move your propaganda machine I will
to take it out

ON-LINE GAMBLING/BETTING

- ★ MR. MEHTA WAS CAUGHT ON BETTING CHARGES
- ★ TWO LAPTOPS SEIZED.
- ★ AN EXCELLENT SOFTWARE
- ★ AMOUNT INVOLVED IS Rs 220 CRORES
- ★ BETTING ON WORLD CUP CRICKET/HOCKEY MATCHES

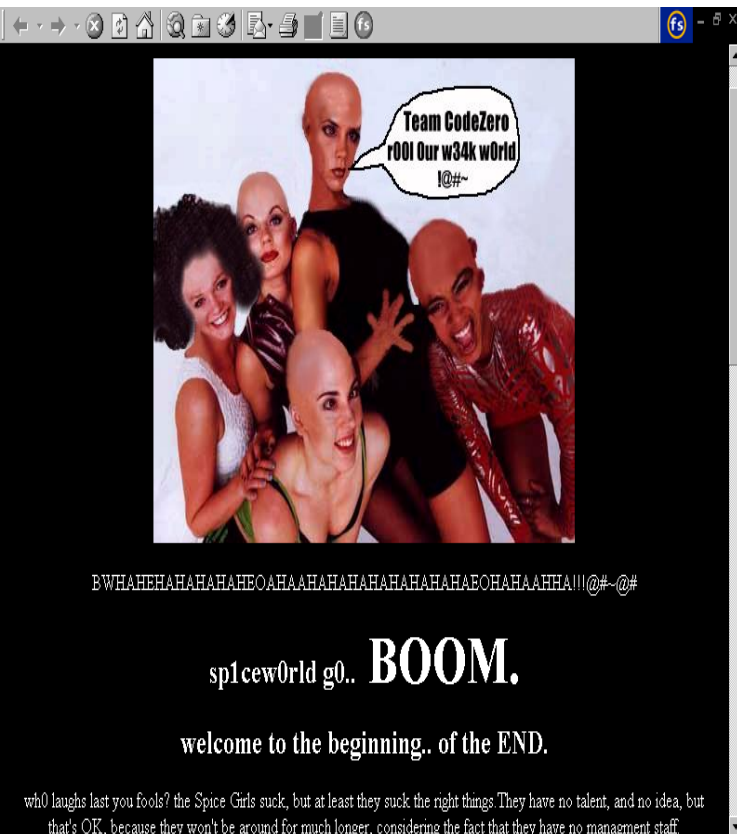


WEB PAGE DEFAACEMENT

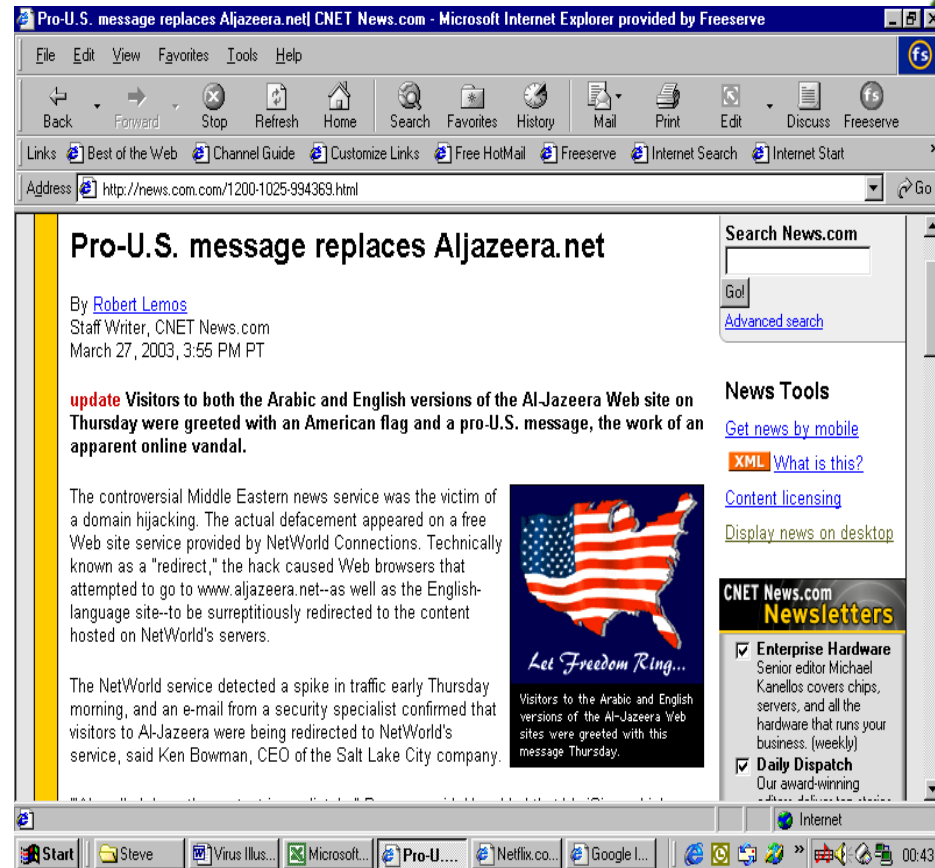
- ★ WEB PAGES ARE COMPUTER FILES STORED IN DIRECTORIES ON A SERVER COMPUTER.
- ★ IF A HACKER GAINS ACCESS TO THESE FILES, HE OR SHE CAN REPLACE OR ALTER THEM IN ANY WAY.
- ★ THE CIA AND THE NEW YORK TIMES WEB PAGES HAVE BEEN ATTACKED IN THE PAST.



WEB DEFACEMENT



Spice Girls Website Hacked
and Defaced 1999



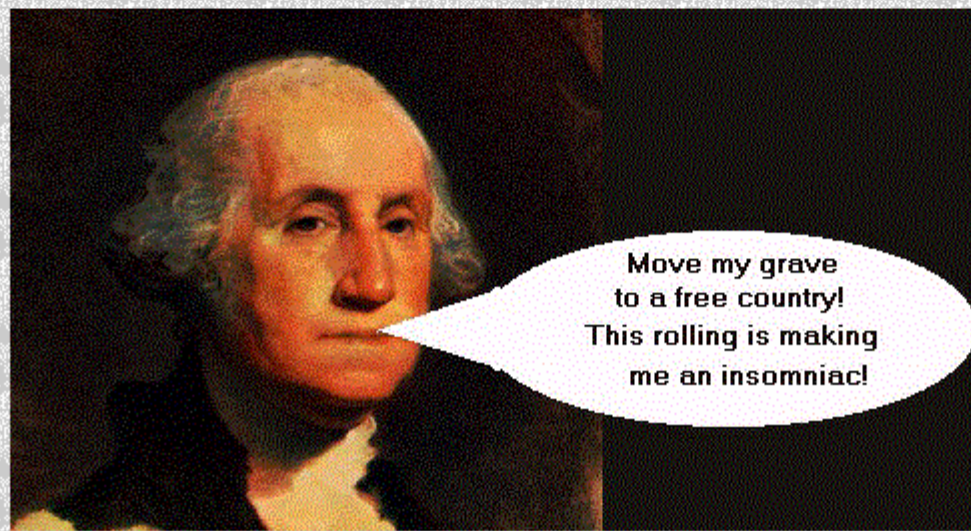
Aljazeera TV Website Hacked
and Defaced 2003



United States Department of Injustice

This page is in violation of the Communications Decency Act!

Words from our Forefather George Washington



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

FINANCIAL FRAUD

- ★ PURCHASE, STEAL, OR FIND FREE IN ON-LINE DATABASES (MASTERCARD)
- ★ CRACK INTO COMMERCIAL WEB SITES
- ★ COLLECT FROM "CLONED" CHAT ROOMS THAT INCLUDE LINKS TO OUTSIDE FAKE WEB SITES THAT OFFER SERVICES OR PRODUCTS
- ★ SKIMMING - ICICI, HDFC CREDIT CARDS



WEB SPOOFING

- ★ SET UP A SPOOF WEB SITE WHICH RECREATES A LEGITIMATE WEB SITE TO CAPTURE PERSONAL AND CREDIT CARD INFORMATION



WEB SPOOFING

- ★ MR. DUTTA SENT RS 85,000 TO AN WWW.AUTOMOBILE-MUMBAI.COM TO BUY A BMW (USED) CAR.

- ★ FAKE SITE
MR.DUTTA NEVER
GOT HIS BMW
NOR HIS MONEY



- ★ ICICI WEB SPOOFING

Hacking



- ★ HACKER: A PERSON WHO BREAKS INTO COMPUTER SYSTEMS, USING THEM WITHOUT AUTHORIZATION JUST TO SHOW OFF
- ★ CRACKER: MALICIOUSLY

DATA DIDDLING

- ★ CBI Vs CORPORATE HOSPITALS - 300 CRORE
- ★ KARNATAKA MEDICAL EXAM(K-CET) SCAM
 - OCR BASED ANSWERED SHEET.
 - MODIFIED THE ANSWERED PROGRAM AS PER THE STUDENT ANSWERED SHEET.
 - MADE FAILED CANDIDATES SUCCESSFUL.
- ★ BIHAR BOARD SCAM
- ★ DELHI ELECTRICITY BOARD SCAM



COMPUTER FORGERY

- ★ PRODUCTION OF FAKE CURRENCY, POSTAL STAMPS, JUDICIARY STAMPS, UNIVERSITY CERTIFICATES, DTC BUS PASSES,
- ★ PAN CARDS - PASSPORT ISSUED
- ★ UP TRANSPORT CORPORATION IS LOOSING 10-15 CRORES PER YEAR.

CHANDIGARH ADMINISTRATION



Certificate of registration of Motor Vehicle

Registration No.

Name

Address

Prev. Reg. No.

Prev. Owner

Chassis No.

Engine No.

Make

Year of manufacturing

Seating Capacity

Road Tax Paid Up to

Counterfeited Certificates



Haryana Police	
	<p>Code: _____ Unit: _____</p> <p>Name: _____ Rank: _____</p> <p>Emg. Tel #: _____ Bd. Gp: _____</p> <p>I.D. Mark: _____</p> <p>Valid Till: 31/06/2005</p> <p>M.S. MALIK (D.G.P.) ISSUING AUTHORITY</p>

Haryana Police	
	<p>Code: 790000231 Unit: KKR</p> <p>Name: DEEM SINGH Rank: Constable</p> <p>Emg. Tel #: 01744-22100 Bd. Gp: AB-46</p> <p>I.D. Mark: Scar on eye.</p> <p>Valid Till: 31/08/2006</p> <p>M.S. MALIK (D.G.P.) ISSUING AUTHORITY</p>

DRIVING LICENCE FATEHGARH SAHIB	
	<p>No. 9832 Dt. 07/05/02</p> <p>Name : Jagdeep Singh</p> <p>S/D/W of : Gurbinder Singh</p> <p>D.O.B. : 04.04.94</p> <p>Address : 16 Mall Road, Gobindgarh Fatehgarh Sahib</p> <p>Valid upto 06/05/2022</p> <p>Holder Sig. _____</p> <p>Endorsements: 3 A 5</p> <p>Holder is licensed to drive throughout India vehicles of the above description.</p>



Haryana Police



Code: 90RTK1548

Unit: RTK

Name: Surjit Singh

Rank: Constable

Emq. Tel #: 01262-251672

Bd.Gp: 0+ve

I.D Mark: Scar on right eye.

Surjit Singh
101/10

M.S. Malik

M.S. MALIK (D.G.P.)
ISSUING AUTHORITY

Valid Till: 31 08 2006



Haryana Police



Code: 75KKR0231

Unit: KKR

Name: BHIM SINGH

Rank: Constable

Emq. Tel #: 01744-22100

Bd.Gp: AB+ve

I.D Mark: Scar on eye.

Bhim Singh
101/10

M.S. Malik

M.S. MALIK (D.G.P.)
ISSUING AUTHORITY

Valid Till: 31 08 2006

MINISTRY OF HOME AFFAIRS

This is to certify that this car belongs to the minisry of home affairs. and this is the property of india.No body alows to stop this car.India is very bad country and we hate india we want to destroy india and with hte 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 there brother bush he is also a very bad person he will be next target he is also the killer of innocent people he have to die and we will do it.Ministry of home affairs Goverment of India.





Name :
Desig :

Cyber Tech Computer Training Centre

(Identity Card)



IDENTITY THEFT



- ★ THEFT OF ONE'S IDENTITY FOR ILLEGAL USE.
- ★ TYPES:
 - FRAUDULENTLY OBTAINING CREDIT OR IDENTITY INFORMATION, AND THEN SELLING IT TO OTHERS
 - STEALING MONEY FROM VICTIM'S BANK ACCOUNTS

CREDIT CARD FRUDS

Vast online credit card theft revealed - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

Bookmarks Location: <http://stacks.msnbc.com/news/382561.asp> What's Related

Trade commission-free for 1 month.

MSNBC HEALTH
Interactive **CHECKUP**

MSNBC HOME
News
Business
Sports
Local
Health
Technology
Living + Travel
TV News
Opinions
Weather
Shop@MSNBC
MSN.com

Technology
HACKS, ATTACKS & SCAMS


Vast online credit card theft revealed

Hacker hid data on 485,000 cards on U.S. agency's Web site

'Over 485,000 Visa, MasterCard, AMEX and Discover Card numbers were discovered, along with expiration date, cardholder name and address.'

MSNBC

Advertisement
Shopping on MSN

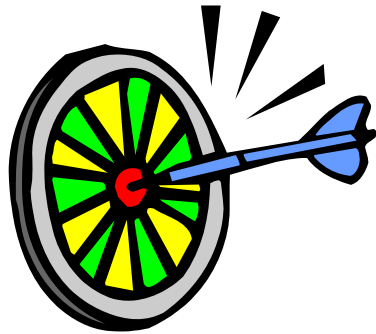

RCA® Water-Resistant LCD TV
\$249.99 **Sale**
\$179.99
RadioShack.com
[more Televisions](#)

RadioShack
BestBuy BestBuy.com
800.com electronics

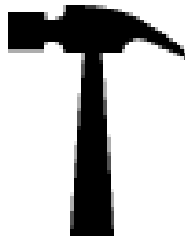
Document: Done

COMPUTERS CAN PLAY THREE ROLES IN A CRIME

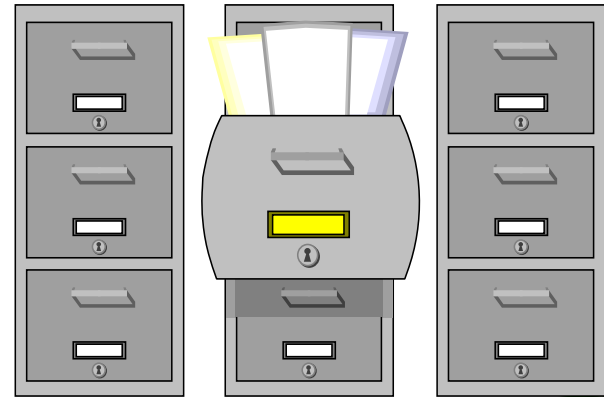
Weapon/Target



- Tool



- Storage Facility

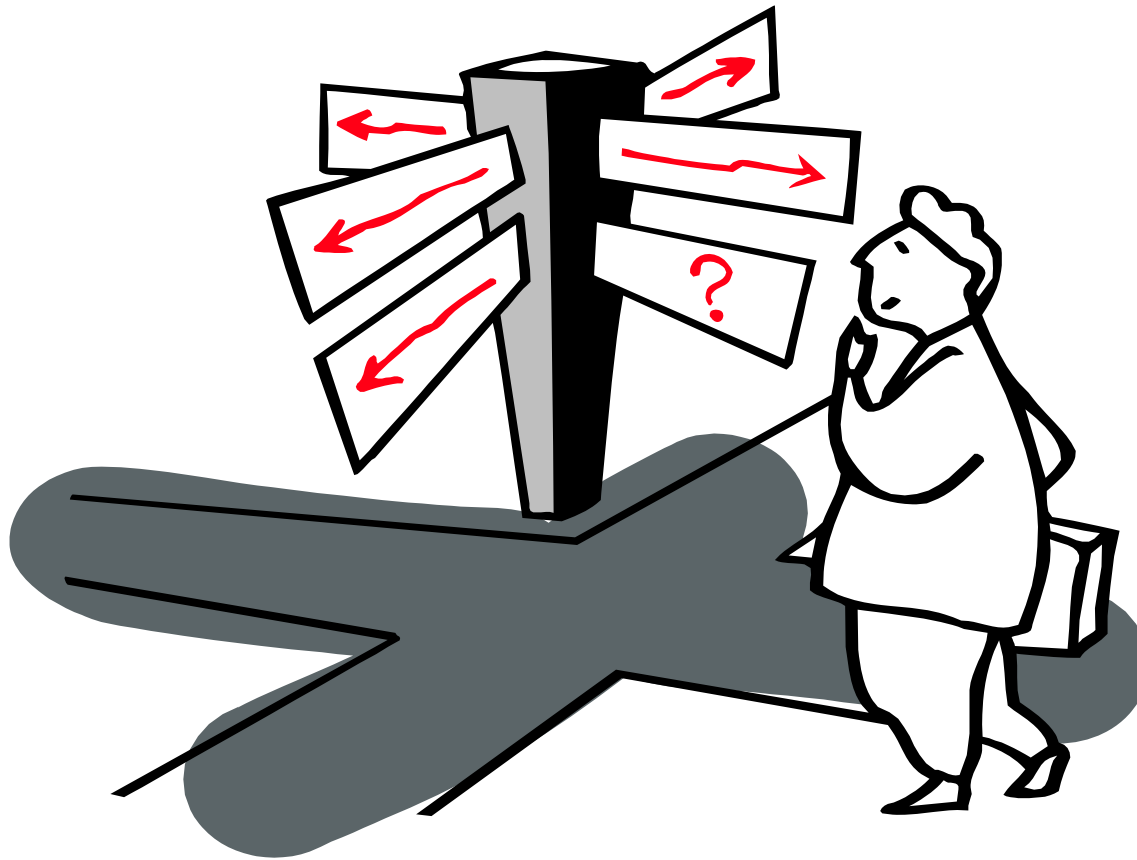


EMBEDDED SYSTEMS CRIMES

- ★ WASHING MACHINES & TV
MEMORY CHIP CRIMES
- ★ GOA SKY BUS CASE



PAUSE FOR QUESTIONS



WHAT IS DIGITAL EVIDENCE?

- * DIGITAL EVIDENCE IS ANY INFORMATION OF PROBATIVE VALUE THAT IS EITHER STORED OR TRANSMITTED IN A **BINARY FORM**" (SWG)
- * DIGITAL EVIDENCE **INCLUDES** COMPUTER EVIDENCE, DIGITAL AUDIO, DIGITAL VIDEO, CELL PHONES, FAX MACHINES, ETC.....ALL DIGITAL, BUT WITH DIFFERENT OUTPUTS.

SPECIAL PROBLEMS IN CYBERCRIMES

- ★ DIGITAL EVIDENCE IS HIGHLY FRAGILE.
- ★ BITS ARE EASY TO TAMPER THAN A PAPER



MAJOR PROBLEM ?



PHYSICAL WORLD



VIRTUAL WORLD

THE SOLUTION

CYBER FORENSICS

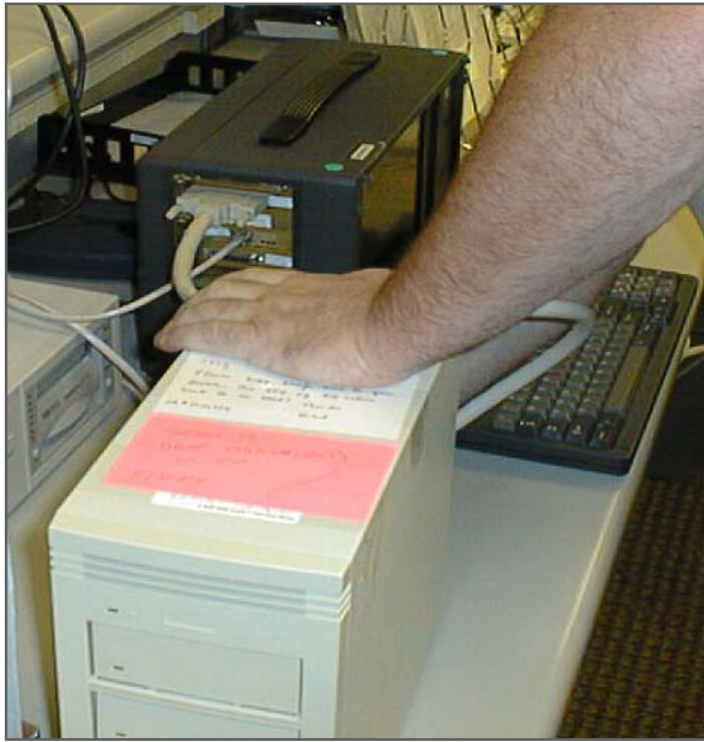


WHAT IS CYBER FORENSICS?

★ CYBER FORENSICS

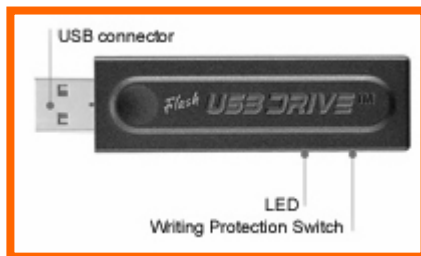
- DISCOVERY, ANALYSIS, AND RECONSTRUCTION OF EVIDENCE EXTRACTED FROM ANY ELEMENT OF COMPUTER SYSTEMS, COMPUTER NETWORKS, COMPUTER MEDIA, AND COMPUTER PERIPHERALS THAT ALLOW INVESTIGATORS TO SOLVE THE CRIME.

FORENSICS PROCESS

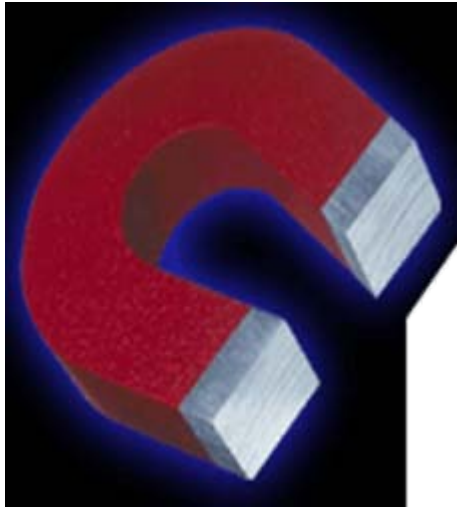


- FOUR STAGES
 - ACQUIRE
 - AUTHENTICATE
 - ANALYZE
 - DOCUMENT

DIFFERENT TYPE'S OF STORAGE MEDIA



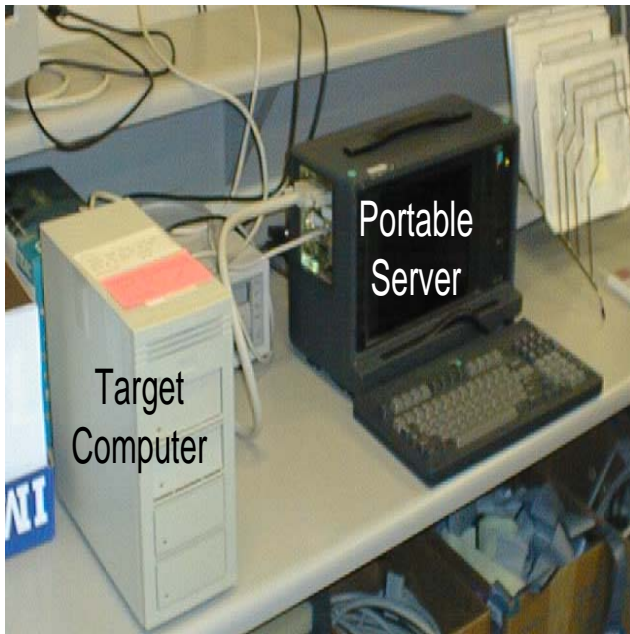
ELECTRONIC EVIDENCE PRECAUTIONS



- ★ Static Electricity
- ★ Magnetic Fields
- ★ Shock
- ★ Moisture



ACQUIRE



- ★ TRUE MIRROR
IMAGE IS A
SECTOR BY
SECTOR COPY OF
EVERY SECTOR
OF THE
ORIGINAL MEDIA

IMAGE HARD DISK

- ★ IMAGE TO WIPED AND FORMATTED HARD DISK



AUTHENTICATE

★ IS THE
DUPLICATE
AUTHENTIC ?



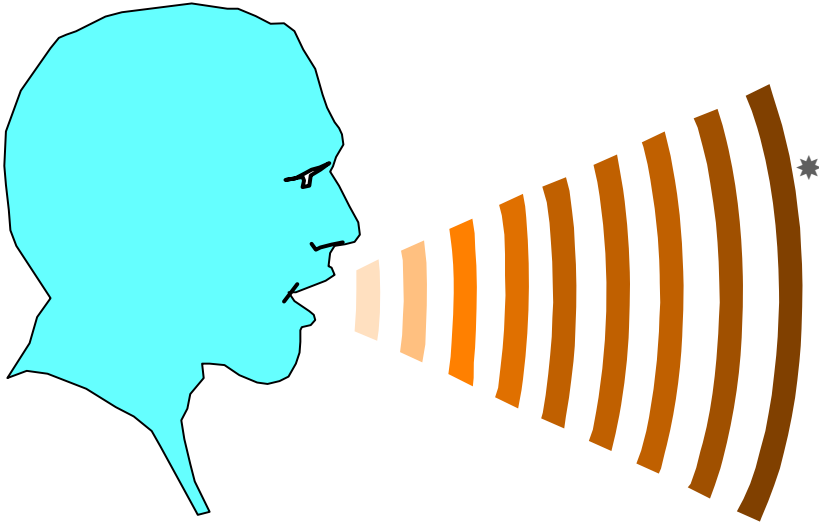
ANALYSIS



- ★ EXTRACT,
PROCESS,
INTERPRET
- ★ REMEMBER
ANALYSIS
SHOULD BE
REPEATABLE



GOOD DOCUMENTATION



EXERCISE TO MAKE THE JUDICIARY TO APPRECIATE

- REPORT SHOULD CLEARLY LIST
- SOFTWARES USED & VERSIONS
- REPORT SHOULD BE IN SIMPLE TERMS
- HASH RESULTS
- ALL STORAGE MEDIA NUMBERS, MODEL MAKE
- SUPPORTED BY PHOTOGRAPHS



CLOSING THOUGHTS

INVESTIGATORS, FORENSIC
SCIENTISTS, JUDICARY,
SUBJECT MATTER EXPERTS
MUST WORK AS A TEAM



CLOSING THOUGHTS

PREVENTING, DETECTING,
INVESTIGATING &
PROSECUTING CYBER
CRIMES MUST BECOME A
PRIORITY, IN ORDER TO
LESSEN THEIR IMPACT ON
THE ECONOMY



RICHARD POWER - "TANGLED WEB"

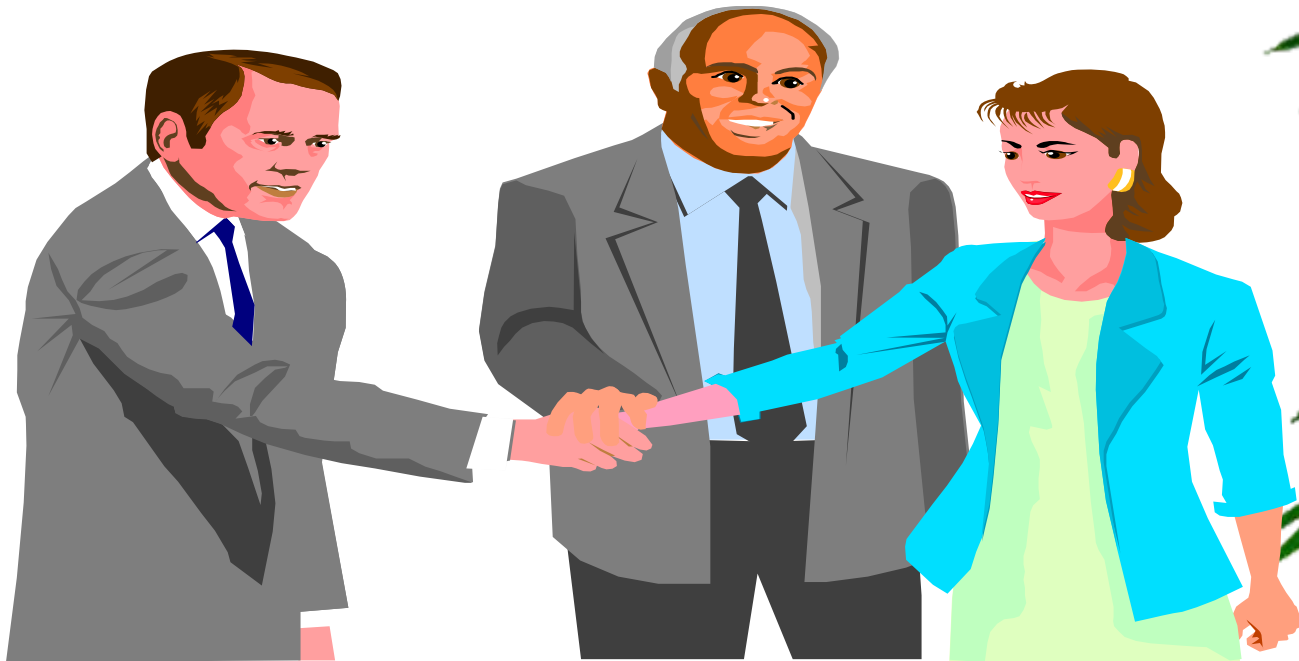
INFORMATION CRIME
DEMANDS
INFORMATION AGE
LAW ENFORCEMENT



QUESTIONS



THANK YOU



KRISHNA SASTRY PENDYALA
COMPUTER FORENSIC DIVISION
DIRECTORATE OF FORENSIC SCIENCE
MINISTRY OF HOME AFFAIRS,
GOVT. OF INDIA HYDERABAD