

Scrutiny and Evaluation of (Digital) Evidence



Nature of Computer Crimes

- Illegal Act
- Computer is used as tool or target or both
- Electronic Evidence
 - Computer crimes
 - Physical crimes

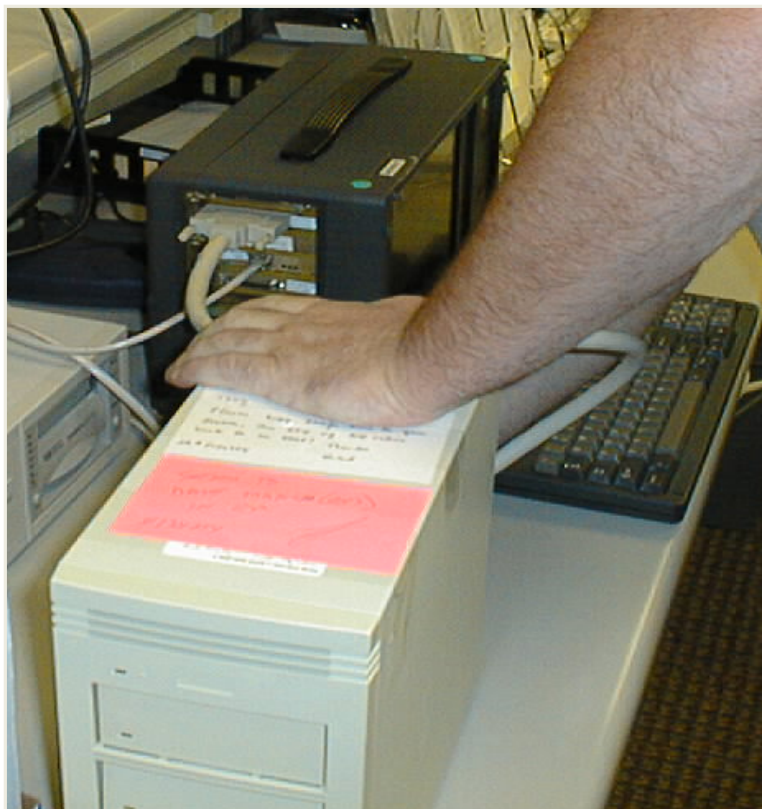
Collection of digital evidence

- Any action during investigation should not compromise evidence
- If accessing original media is necessary, the IO responsible must be competent to do so
- All procedures should be documented and preserved in a manner verifiable by an independent third party

Compromising Evidence

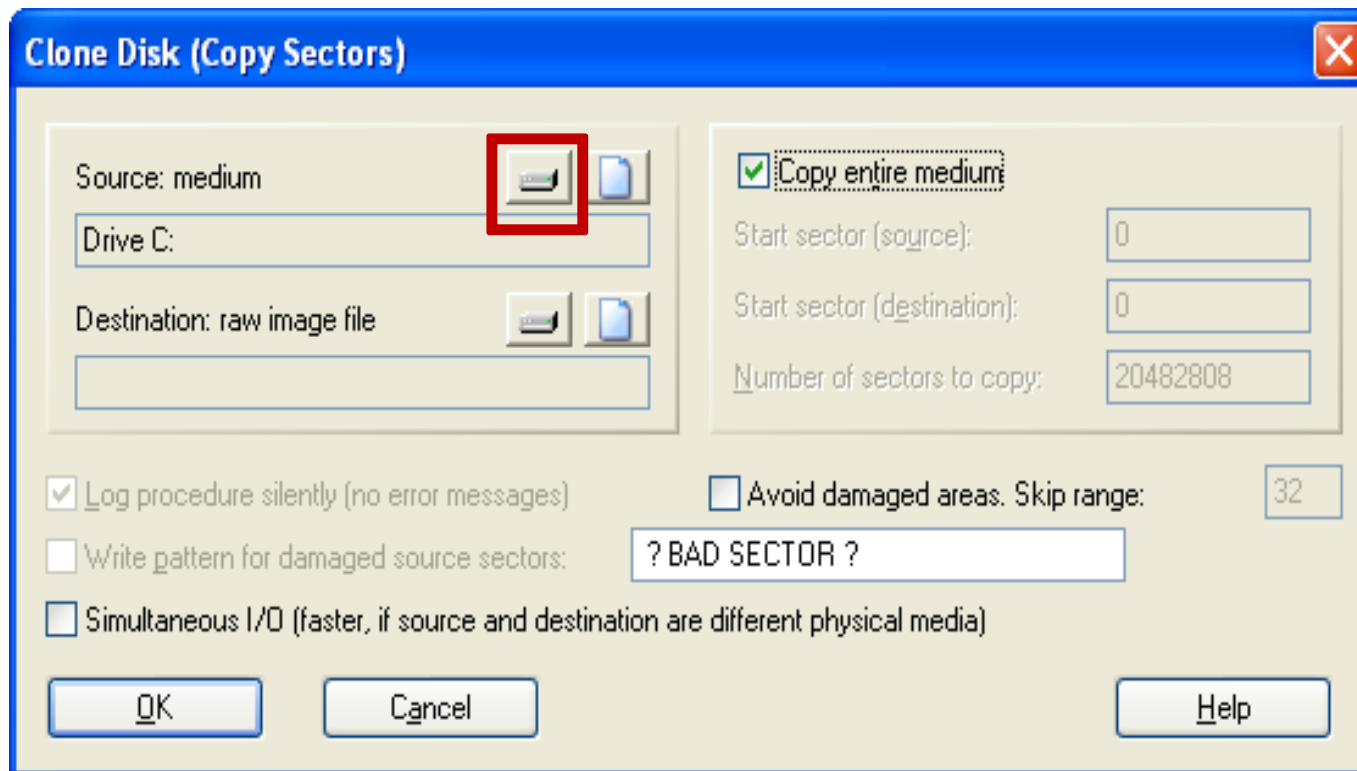
- U.S. Doorframe Case
- Logic Bombs
 - Not switching a suspect computer on or off
- Admissibility

The computer forensics process

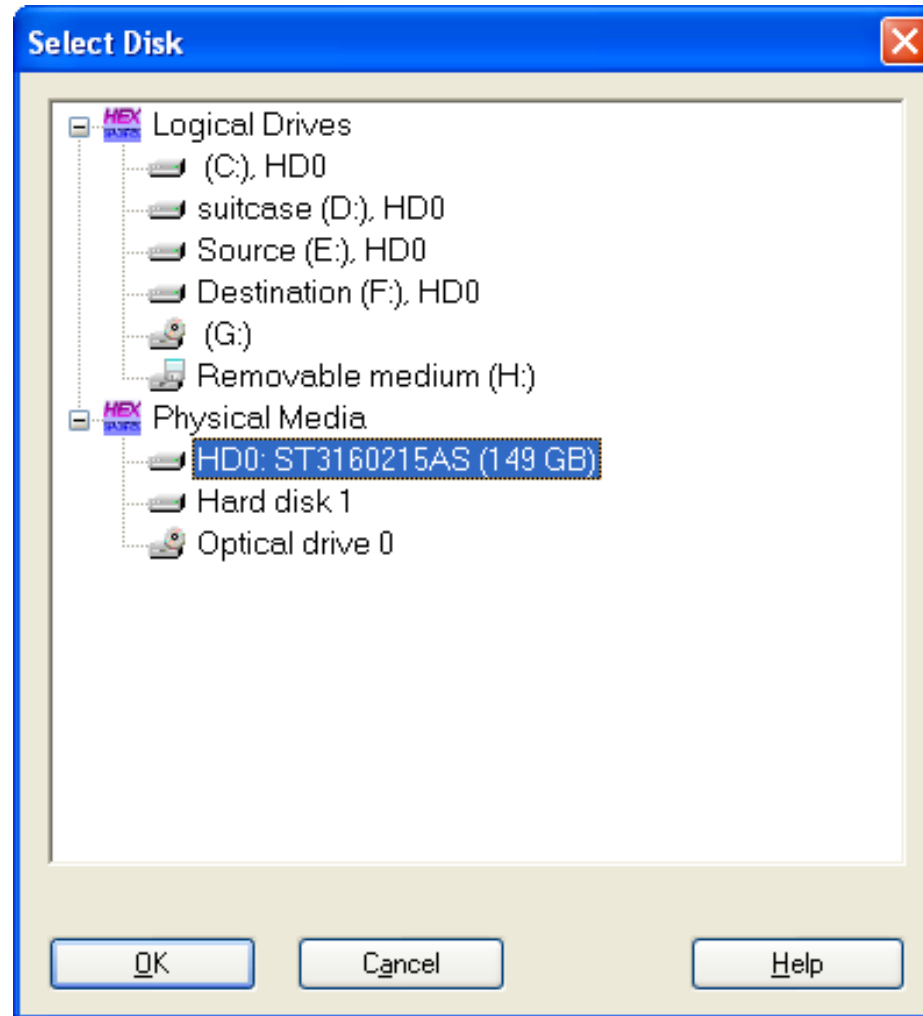


- Acquire
- Authenticate
- Analyze
- Document

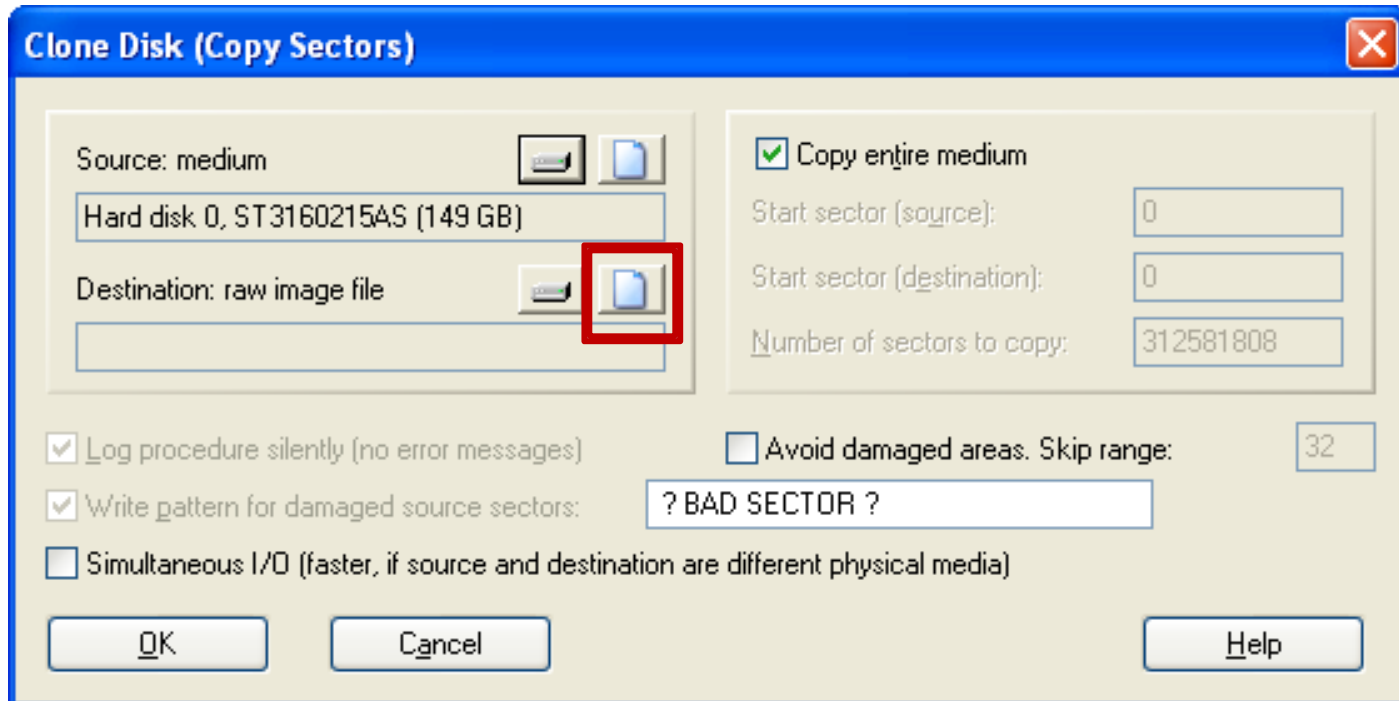
Select source medium



Select source medium



Select destination for the image file



Authenticate

- **Using hash functions to ensure authenticity of image**
- **If acquisition hash equals verification hash, image is authentic**

WinHex - [Drive E:] 14.4 SR-1

File Edit Search Position View Tools Specialist Options Window Help

Case Data

| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|
| 00000000 | B | 58 | 90 | 4D | 53 | 44 | 4F | 53 | 35 | 2E | 30 | 00 | 02 | 04 | 26 | 00 | EX\MSDOS5.0 & |
| 00000010 | 02 | 00 | 00 | 00 | 00 | F8 | 00 | 00 | 3F | 00 | FF | 00 | 00 | 00 | 00 | 00 | ø ? ý |
| 00000020 | FE | CF | 07 | 00 | E5 | 03 | 00 | 00 | 00 | 00 | 00 | 00 | 02 | 00 | 00 | 00 | pİ á |
| 00000030 | 01 | 00 | 06 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |)'¡@INO NAME |
| 00000040 | 00 | 01 | 29 | 91 | 8D | D8 | CC | 4E | 4F | 20 | 4E | 41 | 4D | 45 | 20 | 20 | FAT32 3É Ñ%ø |
| 00000050 | 20 | 20 | 46 | 41 | 54 | 33 | 32 | 20 | 20 | 20 | 33 | C9 | 8E | D1 | BC | F4 | { Á Ü% IN V@' |
| 00000060 | 7B | 8E | C1 | 8E | D9 | BD | 00 | 7C | 88 | 4E | 02 | 8A | 56 | 40 | B4 | 08 | Í s 'ýý ñf @øf |
| 00000070 | CD | 13 | 73 | 05 | B9 | FF | FF | 8A | F1 | 66 | 0F | B6 | C6 | 40 | 66 | 0F | Ñ á?-á Áí Af · |
| 00000080 | B6 | | | | | | | | | | | | | | | | Éf-áf Fø ~ u8 ~ |
| 00000090 | C9 | | | | | | | | | | | | | | | | * w2f F f Á » ' |
| 000000A0 | 2A | | | | | | | | | | | | | | | | è+ éH ú}')} ð~ |
| 000000B0 | 01 | | | | | | | | | | | | | | | | Át <ýt ' » Í ë |
| 000000C0 | 84 | | | | | | | | | | | | | | | | i ú}èá ú}èà Í Í |
| 000000D0 | EE | | | | | | | | | | | | | | | | f`f;Fø J fj fP |
| 000000E0 | 66 | | | | | | | | | | | | | | | | Sfh ~ ' |
| 000000F0 | 53 | | | | | | | | | | | | | | | | A»³U V@Í úU |
| 00000100 | 41 | | | | | | | | | | | | | | | | ³ öÁ þF ' |
| 00000110 | AA | 0F | 85 | 14 | 00 | F6 | C1 | 01 | 0F | 84 | 0D | 00 | FE | 46 | 02 | B4 | B V@ óí `úfXfXfX |
| 00000120 | 42 | 8A | 56 | 40 | 8B | F4 | CD | 13 | B0 | F9 | 66 | 58 | 66 | 58 | 66 | 58 | fXe*f3øf ·N f-ñþ |
| 00000130 | 66 | 58 | EB | 2A | 66 | 33 | D2 | 66 | 0F | B7 | 4E | 18 | 66 | F7 | F1 | FE | Á Éf DfÁé ÷v Ö |
| 00000140 | C2 | 8A | CA | 66 | 8B | D0 | 66 | C1 | EA | 10 | F7 | 76 | 1A | 86 | D6 | 8A | V@ èÁá Í, Í fa |
| 00000150 | 56 | 40 | 8A | E8 | C0 | E4 | 06 | 0A | CC | B8 | 01 | 02 | CD | 13 | 66 | 61 | Ty Á f@I qyÁ |
| 00000160 | 0F | 82 | 54 | FF | 81 | C3 | 00 | 02 | 66 | 40 | 49 | 0F | 85 | 71 | FF | C3 | NTLDR |
| 00000170 | 4E | 54 | 4C | 44 | 52 | 20 | 20 | 20 | 20 | 20 | 20 | 00 | 00 | 00 | 00 | 00 | |
| 00000180 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000190 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000001A0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0D | 0A | 52 | 65 |
| 000001B0 | 6D | 6F | 76 | 65 | 20 | 64 | 69 | 73 | 6B | 73 | 20 | 6F | 72 | 20 | 6F | 74 | Re |
| 000001C0 | 68 | 65 | 72 | 20 | 6D | 65 | 64 | 69 | 61 | 2E | FF | 0D | 0A | 44 | 69 | 73 | move disks or ot |
| 000001D0 | 6B | 20 | 65 | 72 | 72 | 6F | 72 | FF | 0D | 0A | 50 | 72 | 65 | 73 | 73 | 20 | her media.ý Dis |
| | | | | | | | | | | | | | | | | | k errorý Press |

Sector 0 of 511998 Offset: 0 = 235 Block: n/a Size: n/a

MD5 (128 bit)

...for Drive E::

B44AE398F81383E43E30A2D5B371400D

Close

Document



- A forensic examination report must
 - List softwares used & their versions
 - be in simple language
 - list the hash results
 - list all storage media numbers, model, make

Document

- Chain-of-custody log
 - ACL of people having access to collected evidence
 - Tracks evidence from source to courtroom
 - Unbroken chain-of-custody authenticates electronic evidence

Document

- The five “Ws” of chain-of-custody log
 - Who – took possession of the evidence
 - What – description of evidence
 - Where – did they take it to
 - When – time and date
 - Why – purpose for taking evidence

The Omega Case

- July 31, 1996
- The Servers of CNC department in Omega Corporation are booted
- Message flash saying file server is being fixed
- Subsequent system crash
- All programs deleted, manufacturing halts

The Omega Case

- No backup tapes found
- All programs and code generators destroyed
- 25, 000 products to customize 500, 000 designs affected
- 34 years of growth lost in 1 year
- Disgruntled network administrator
- Fired because of non – cooperation

The Omega Case

- Network Administrator's house searched
 - Computers, CDs, motherboards, 500 disks, 12 hard drives, 2 formatted backup tapes
 - Backup tapes were labeled 14/5/96 and 1/7/96
- The cause of deletion, a six line program

The Omega Case

- 30/7/96 (Trigger Date)
- F: (Accessing the server)
- F:\LOGIN\LOGIN 12345 (first user logs in with supervisory rights and no password)
- CD\PUBLIC (gives access to the PUBLIC directory, a file system area)
- FIX.EXE /Y F:*.* (Run code, A=Yes, All files)
- PURGE F:\ /ALL

Evidence

- All items seized from the suspect's house: CDs, HDD, formatted Back up tapes, etc.
- But what is needed to establish guilt beyond reasonable doubt?
 - Correct procedure having been followed by IO
 - The function of the 6 line program (Expert Opinion)
 - The fact that it could only have been installed by the suspect

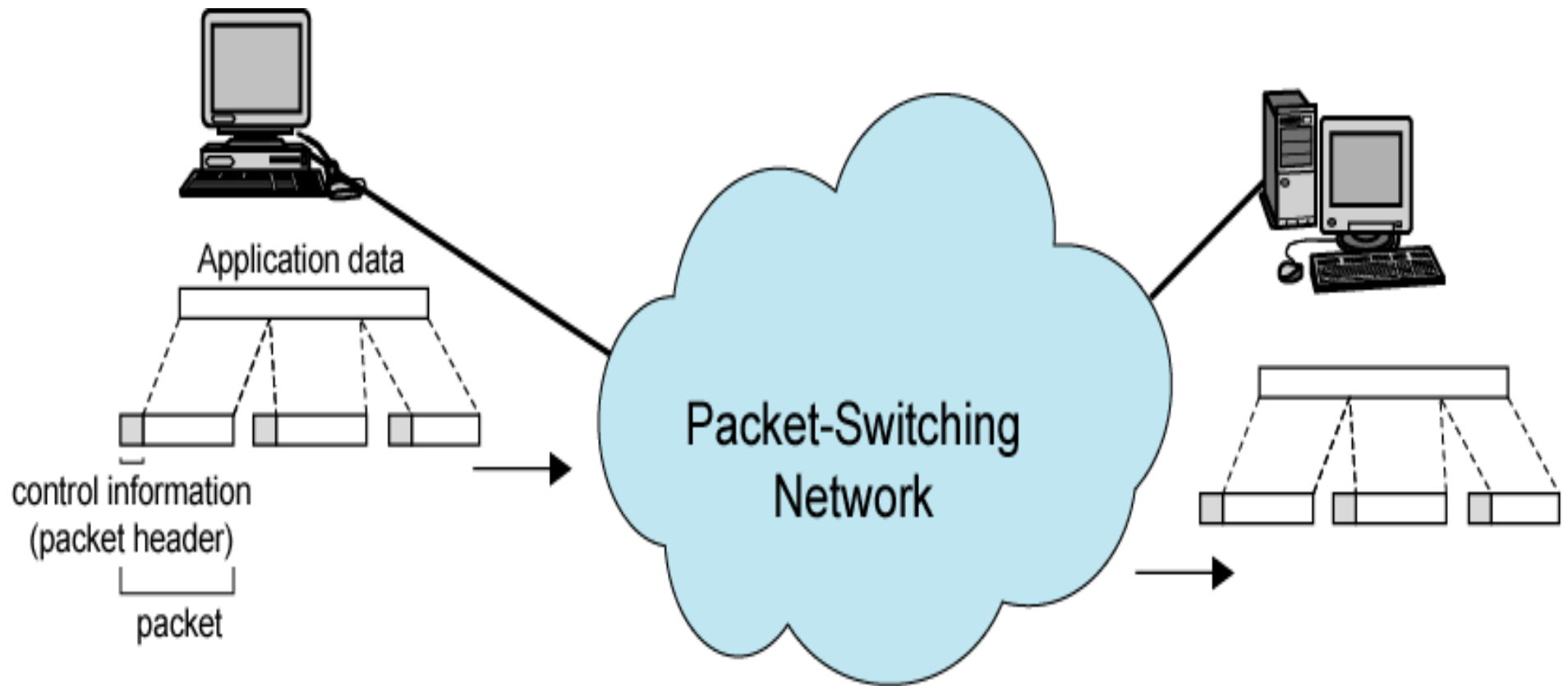
Internet based crimes

- DNS spoofing
- Web defacement
- FTP attacks
- Bogus Websites
- Web spoofing
- Website based launch of malicious code, cheating and fraud

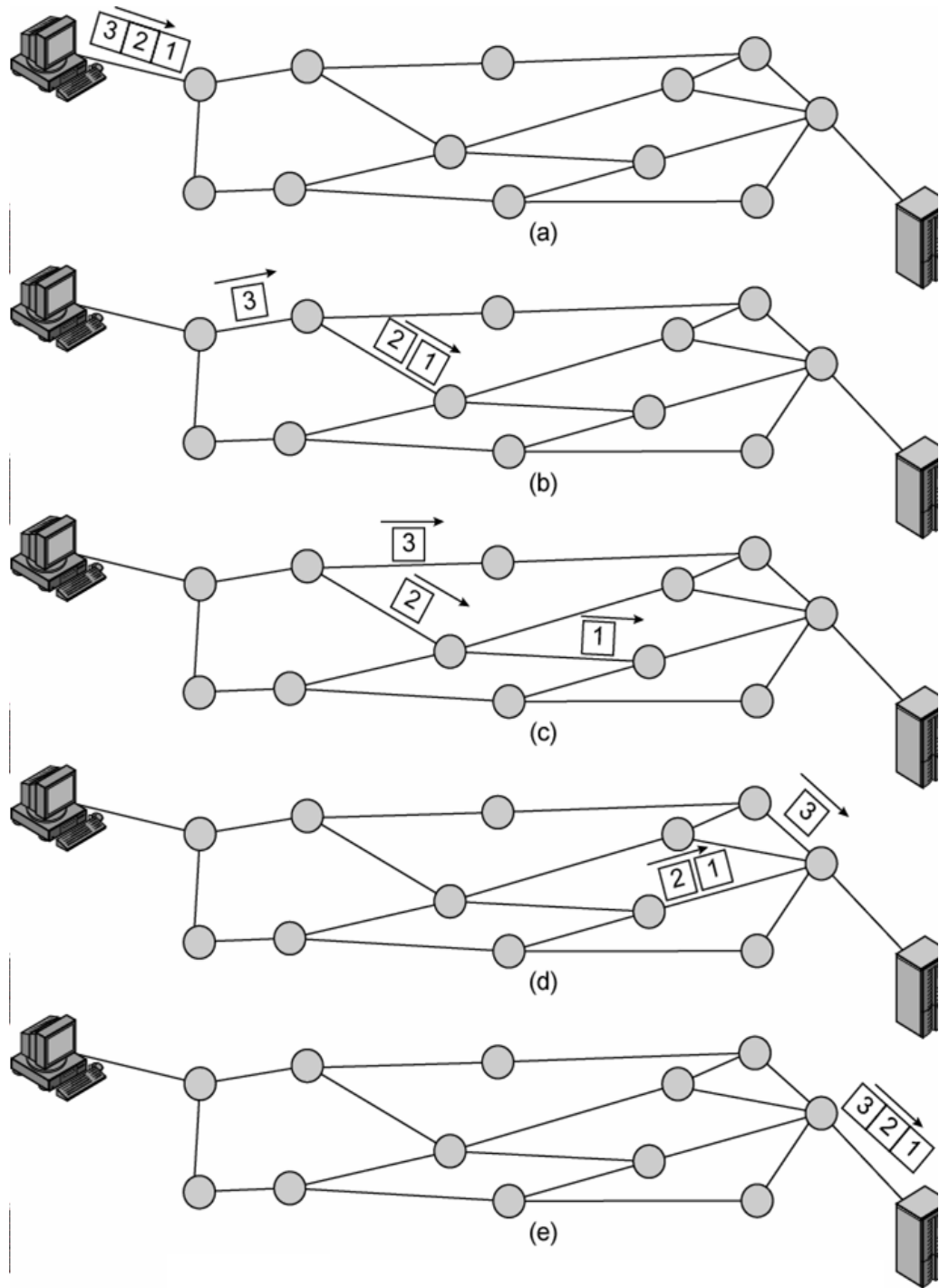
Internet Concepts

- Information travels in data packets
- Files get broken at their source
- Files are reassembled and “joined” at the destination

Packet Switching



Packet Switching



Packet Header

| | |
|---------------------|-------------------|
| No: | 47 |
| MAC source address: | 00-80-C8-05-D3-21 |
| Protocol: | HTTP |
| Source IP address: | 202.123.45.231 |
| Dest IP address: | 197.168.100.31 |
| Source port: | 202.123.45.231:80 |
| SEQ: | 1312 |
| ACK: | 9918611 |
| Packet size: | 69507 |
| TTL | 30 ms |

Packet Data

0010: 46 6F 72 20 65 78 61 6D 70 6C 65 20 70 6F 72 74
0020: 20 6E 75 6D 62 65 72 20 32 31 20 69 73 20 74 68
0030: 65 20 46 54 50 20 70 6F 72 74 2E 20 50 6F 72 74
0040: 20 6E 75 6D 62 65 72 20 32 33 20 69 73 20 74 68
0050: 65 20 74 65 6C 6E 65 74 20 70 6F 72 74 20 61 6E
0060: 64 20 61 6C 6C 20 77 65 62 20 70 61 67 65 73 20
0070: 61 72 65 20 76 69 65 77 65 64 20 75 73 69 6E 67
0080: 20 74 68 65 20 48 79 70 65 72 20 54 65 78 74 20

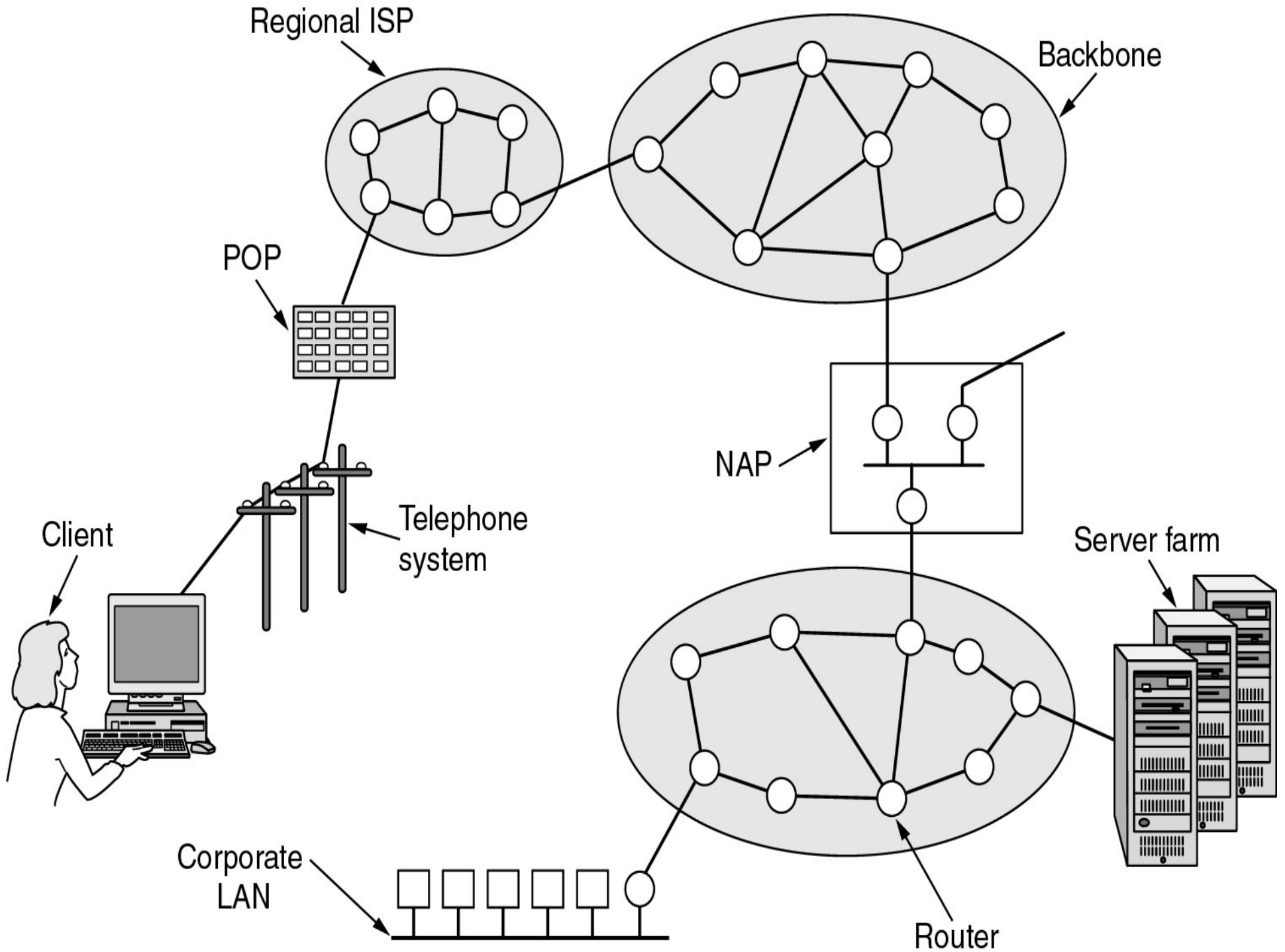
For example port number 21 is the FTP port. Port number 23 is the telnet port and all web pages are viewed using the Hyper Text

Basic concepts

- IP Address
- Domain names
- Domain name servers
- Web Servers
- Web Browsers

Internet Service Providers

- Provide access to the Internet
- Also provide direct connection from a company's networks to the Internet
- Connect users through POP (points of presence)
- Each user is given a unique IP address when he logs on to the Internet



Internet backbone

- Referred to the central network that linked all parts of the Internet
- Mainly consists of optic fiber cables
- Now consists entirely of ISPs and private networks.

Internet Protocol (IP) Address

- 32 – bit address separated by periods.

202.11.34.56

11001010. 00001011. 00100010. 00111000

- Each field can contain a value between 0-255, known as octets

0-255.0-255.0-255.0-255 = 2^8 . 2^8 . 2^8 . 2^8

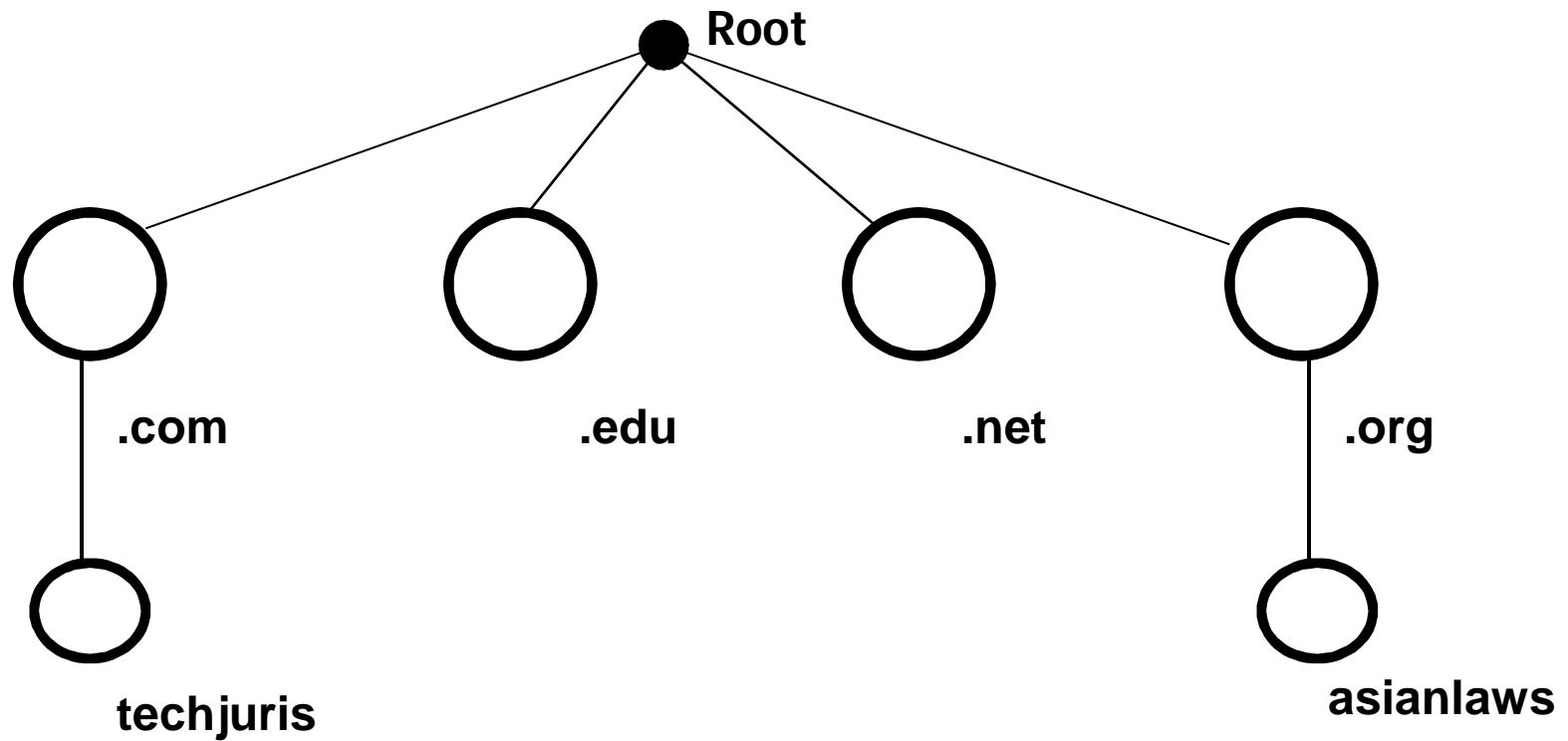
Domain Name System

- Maps host names to IP addresses
- Allows independence from knowledge of physical location of host
- A resolver grants access to the system

Organization

- Uses a hierarchical naming scheme known as domain names
- The root of the DNS tree is a special node with a null label (.)
- The name of each node (except root) may consist up to 63 characters.

Organization



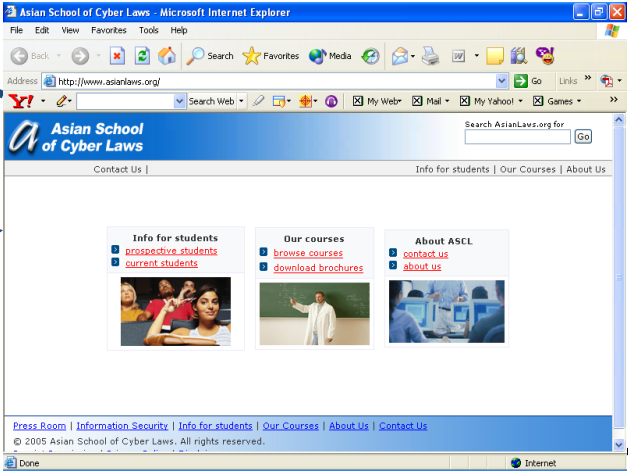
DNS caching

- A DNS caches information received about a mapping
- A later query for the same mapping uses the cached result
- DNS caches are updated periodically

www.asianlaws.org

DNS

67.19.217.53



HTTP Request

www.asianlaws.org

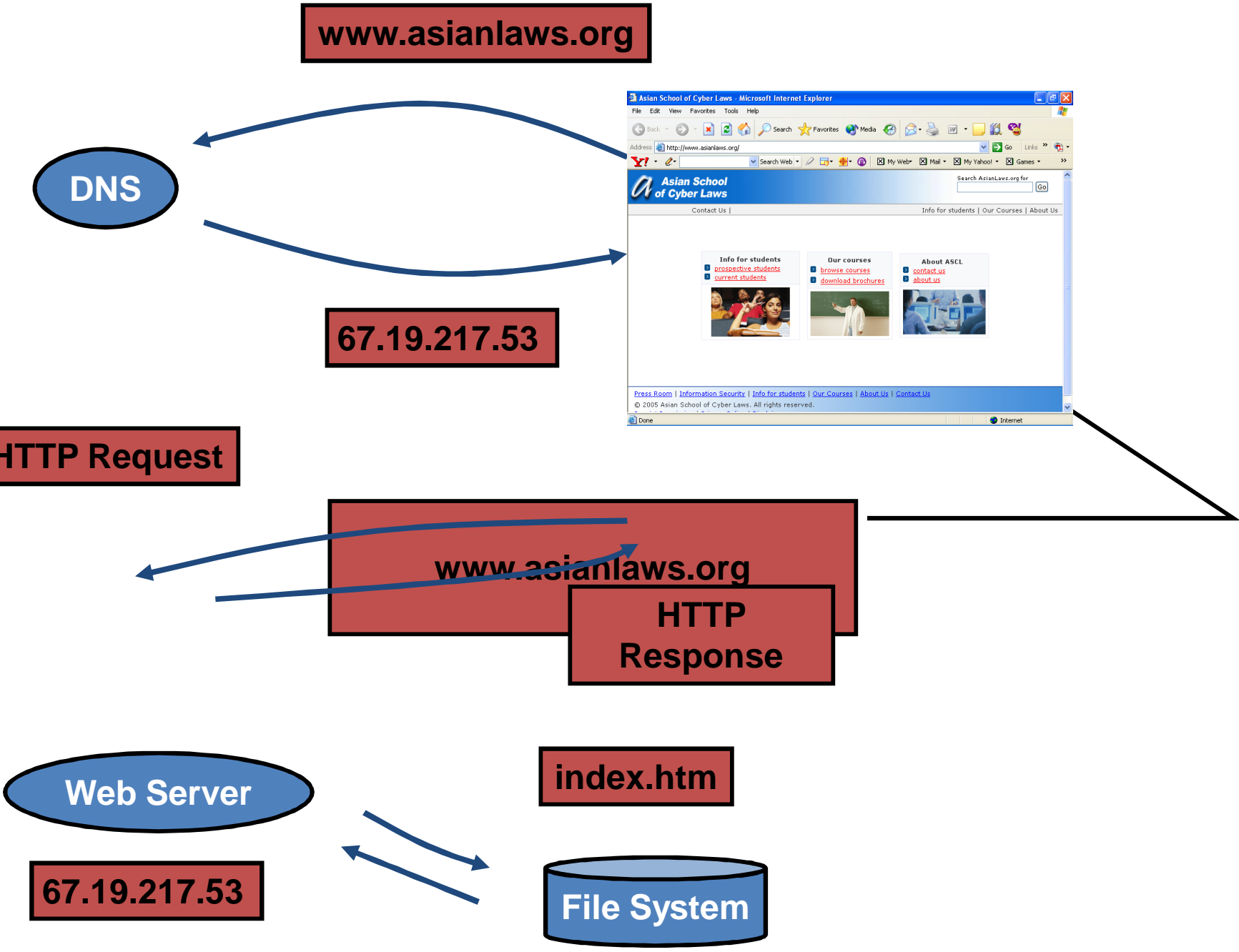
HTTP Response

Web Server

67.19.217.53

index.htm

File System



The spoofed email

The screenshot shows an email client interface. On the left is a sidebar with navigation links: **Inbox**, Starred (with a star icon), Chats (with a speech bubble icon), Sent Mail, **Drafts**, All Mail, **Spam**, Trash, and **Contacts**. The main area has a header with action buttons: « [Back to Inbox](#) », **Archive**, Report spam, Delete, and More Actions (with a dropdown arrow). Below the header, the email subject is **Urgent - Verification required** with a sub-label **Inbox | X**. The email header shows a star icon, the sender **info@noodlebank.com** to me, a [show details](#) link, the time **12:06 PM (9 minutes ago)**, and a **Reply** button with a dropdown arrow. The email body contains the following text:

Dear Mr. Debasis Nayak,

We suspect that your online banking account number 12345678 with Noodle Bank has been compromised.

An attempt to transfer Rs 250,000 out of your account has been made. We have blocked the transfer. To verify that the transfer must be blocked, please login to your account from:

<http://www.noodlebank.com>

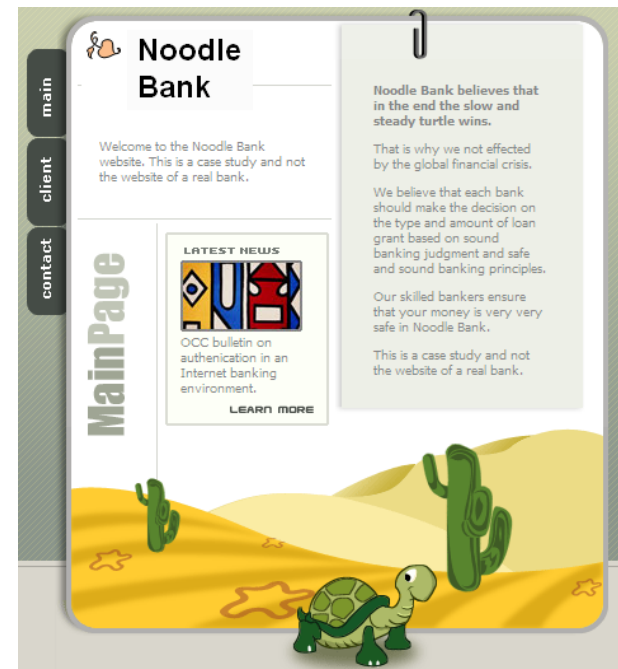
You need to login to your account by 12.30 pm on 27-January-2009 to cancel this transfer. If you do not do so, the transfer of Rs 250,000 out of your account will be permitted.

Regards,
Pooja Sharma,
Customer Care Executive,
Noodle Bank

The spoofing

- The link appears as www.noodlebank.com (i.e NOODLEBANK.com)
- But actually it links to www.nood1ebank.com (i.e NOOD1EBANK.com)

The fake site



Noodle Bank - Windows Internet Explorer

http://www.noodlebank.com/ Google

File Edit View Favorites Tools Help

Noodle Bank


main
client
contact

Noodle Bank

Welcome to the Noodle Bank website. This is a case study and not the website of a real bank.

MainPage

LATEST NEWS



OCC bulletin on authentication in an Internet banking environment.

[LEARN MORE](#)


Noodle Bank believes that in the end the slow and steady turtle wins.

That is why we not effected by the global financial crisis.

We believe that each bank should make the decision on the type and amount of loan grant based on sound banking judgment and safe and sound banking principles.

Our skilled bankers ensure that your money is very very safe in Noodle Bank.

This is a case study and not the website of a real bank.



Internet 100%

Noodle Bank - Windows Internet Explorer

http://www.noodlebank.com/client.html

File Edit View Favorites Tools Help

Noodle Bank

main
client
contact

MainPage

Noodle Bank

Welcome to the Noodle Bank Online Banking website.

LATEST NEWS



OCC bulletin on authentication in an Internet banking environment.

[LEARN MORE](#)

Noodle Bank believes that in the end the slow and steady turtle wins.

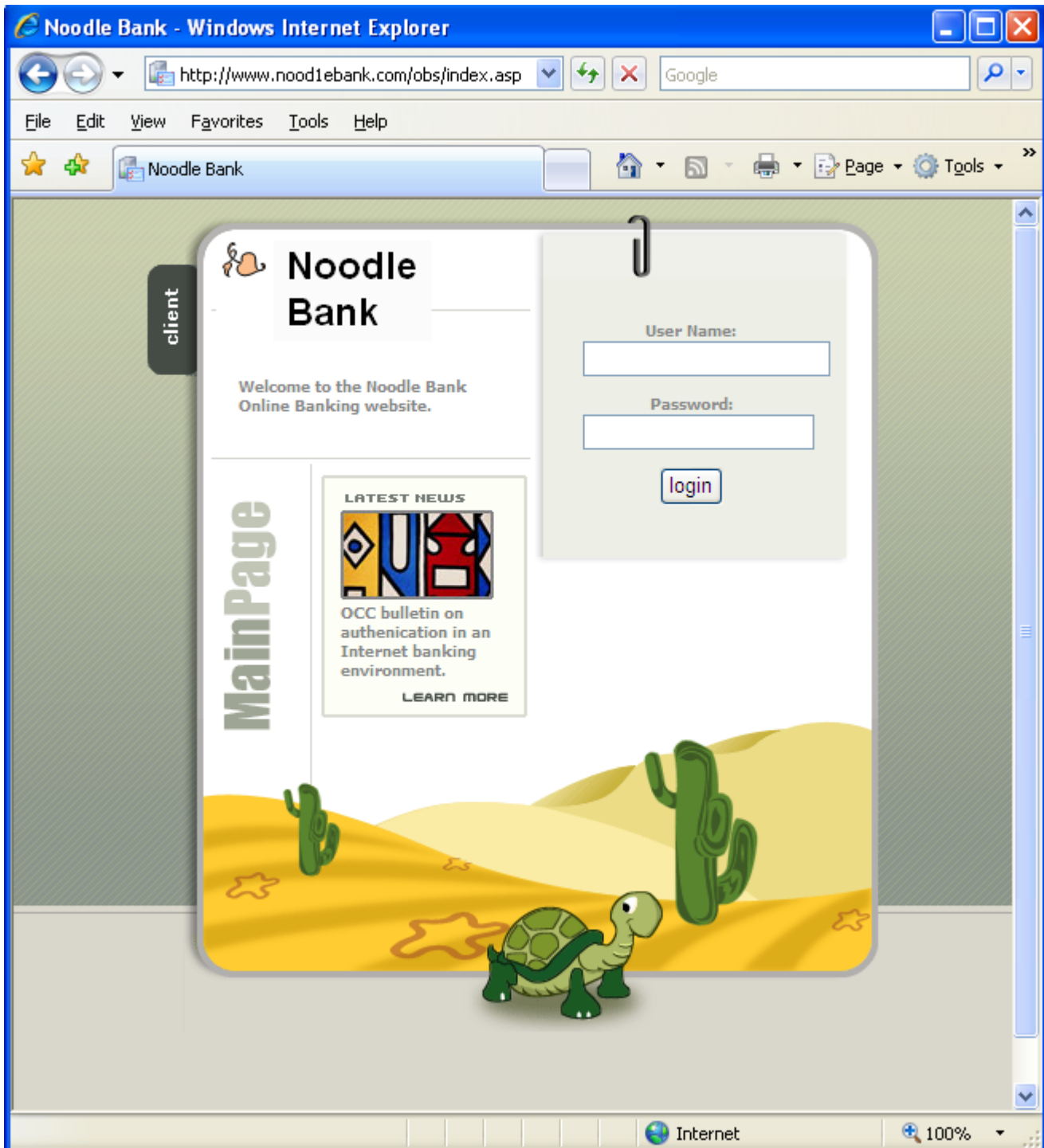
That is why we not effected by the global financial crisis.

We have shifted our online banking system to our new secure servers. In case you have any difficulty using the new systems, please **contact us** for assistance.

[Click here to use our new online banking systems.](#)



Internet 100%



Noodle Bank - Windows Internet Explorer

http://www.noodlebank.com/obs/index.asp

File Edit View Favorites Tools Help

Noodle Bank

client

Noodle Bank

Welcome to the Noodle Bank Online Banking website.


User Name:
debasis

Password:
.....

login

MainPage

LATEST NEWS



OCC bulletin on authentication in an Internet banking environment.

LEARN MORE



Internet 100%

Noodle Bank - Windows Internet Explorer

http://www.nood1ebank.com/obs/login.php

File Edit View Favorites Tools Help

Noodle Bank

Noodle Bank

Welcome to the Noodle Bank website. This is a case study and not the website of a real bank.

LATEST NEWS



OCC bulletin on authentication in an Internet banking environment.

[LEARN MORE](#)

Your account services have temporarily been blocked, as we suspect that your account has been compromised. An attempt to transfer Rs 250,000 to the account of Sid Kumar has been made. We have blocked the transfer.

To cancel this transfer, please click here.

To allow this transfer, please click here.



Internet 100%

Noodle Bank - Windows Internet Explorer

http://www.noodlebank.com/obs/cancel.asp

File Edit View Favorites Tools Help

Noodle Bank


main
contact

Noodle Bank

Welcome to the Noodle Bank website. This is a case study and not the website of a real bank.


The transfer has been cancelled. Your account services will resume after 24 hours. Thank you for your cooperation. We regret the inconvenience.

LATEST NEWS



OCC bulletin on authentication in an Internet banking environment.

[LEARN MORE](#)



Done Internet 100%


The “steal”

- When username-password at the spoofed website is entered, the username-password was sent across to the criminal carrying out the phishing attack.

Windows Internet Explorer window titled "Password obtained - spamavert.com". The address bar shows the URL <http://spamavert.com/mail.php?alias=noodleb>. The page content includes the SPAMAVERT.COM logo, an email header with the subject "Password obtained" from support@dimensionsnt.com, and a warning that the email contains more than plain text. The email body contains the text: "Username: debasis", "Password: nayak", and "NoodleBank.com website". The footer includes navigation links (FAQ, ABOUT SPAMAVERT, CONTACT, PRIVACY POLICY, PRESS ROOM) and a copyright notice for 2006 Digital Creations AS.

Subject: **Password obtained**
From: support@dimensionsnt.com
Date: **2009-01-27 07:39:00 GMT**
To: noodlebank_com@spamavert.com
CC:
Size: **0.3 KiB**

[Back to overview](#) [Subscribe](#) [Forward](#)

 This e-mail contains more than plain text. You should forward it to view it in its original form.

Username: debasis
Password: nayak
--
NoodleBank.com website

[FAQ](#) | [ABOUT SPAMAVERT](#) | [CONTACT](#) | [PRIVACY POLICY](#) | [PRESS ROOM](#)
Copyright © 2006 Digital Creations AS. All rights reserved.

Error on page. Internet 100%

Fundamentals of investigation

- The KEY to almost all web based crimes
 - **IP Address**
 - Figures in server logs
 - Figures in email headers
- Identify the correct IP address
 - Time zones
 - Shivaji Maharaj (Airtel case)

Fundamentals of investigation

- Track physical location of the IP Address
- Identify the suspect computer to which the IP address was allotted
- Collect corroborative evidence from suspect computer

Whois Search

Whois search for 208.113.199.97 using www.whois.net

```
OrgName:      New Dream Network, LLC
OrgID:        NDN
Address:      417 Associated Rd
Address:      PMB #257
City:         Brea
StateProv:    CA
PostalCode:   92821
Country:      US

NetRange:     208.113.128.0 - 208.113.255.255
CIDR:         208.113.128.0/17
NetName:      DREAMHOST-BLK6
NetHandle:    NET-208-113-128-0-1
Parent:       NET-208-0-0-0-0
NetType:      Direct Allocation
NameServer:   NS1.DREAMHOST.COM
NameServer:   NS2.DREAMHOST.COM
NameServer:   NS3.DREAMHOST.COM
Comment:
RegDate:      2006-04-12
Updated:      2007-11-01
```


Extended Info

IP Address: [208.113.199.97](#)

IP Location:  United States

Website Status: [active](#)

Server Type: Apache/2.0.61 (Unix) PHP/4.4.7

[mod_ssl/2.0.61](#) [OpenSSL/0.9.7e](#) [mod_fastcgi/2.4.2](#)

DAV/2 SVN/1.4.2

Cache Date: 2008-04-29 03:21:29 MST



Server Logs

#Software: Microsoft Internet Information
Services 6.0

#Version: 1.0

#Date: 2007-10-13 06:45:10

2007-10-13 00:45:26 172.224.24.114 -67.19.217.53 80
GET /index.htm - 200 7930 248 31
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+200
0+Server)

Evidence in phishing cases

- Who is the victim's ISP?
- Is there a copy of the email?
- Who is the purported sender?
- What is the domain name and IP address of the suspect site?
- When was the site visited by the complainant and from where?

Evidence in phishing cases

- Is a copy of the website saved or do screenshots exist?
- To which bank acc. were payments made?
- Is there any contact email address?
- Who are the relevant service providers?
- Have headers been examined?

Admissibility of Digital Evidence

Sec 65B (Indian Evidence Act)

- Computer output shall be deemed to be a document if the conditions mentioned in Sec 65B(2) section are satisfied
- It shall be admissible in any proceedings, without further proof of the original
 - As evidence of any contents of the original

Admissibility of Digital Evidence

Sec 65B(2)(a)(Evidence Act)

- That the computer output was produced during the period over which the computer was used regularly to store or process information..... by the person having lawful control over the use of the computer

Admissibility of Digital Evidence

Sec 65B(2)(b)(Evidence Act)

- During the said period, information of the kind contained in the electronic record..... was regularly fed into the computer in the ordinary course of the said activities;

Admissibility of Digital Evidence

Sec 65B(2)(c)(Evidence Act)

- Throughout the material part of the said period, the computer was operating properly or, if not,it was not such as to affect the electronic record or the accuracy of its contents;

Admissibility of Digital Evidence

Sec 65B(2)(d)(Evidence Act)

- The information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

Section 65B(4)

- “In any proceedings where it is desired to give a statement in evidence by virtue of this section, a *certificate*.....”
 - identifying the electronic record.. and describing the manner in which it was produced;
 - giving such particulars of any device involved ..
 - dealing with any of the matters to which the conditions mentioned in subsection (2) relate,

Section 65B(4) Contd.....

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

- the operation of the relevant device or the management of the relevant activities (whichever is appropriate) **shall be evidence** of any matter stated in the certificate

Who will give the Certificate under 65B(4)

- In criminal cases, where accused's computer is seized and his HDD is cloned
 - The cyber forensic analyst cloning the HDD and presenting evidence after analysis of the clone
- In civil cases
 - The Plaintiff or the Defendant who desires to furnish evidence from his computer

Amendment to Bankers' Books Evidence Act (Contd...)

- Printout/Copy of entry or the book shall be accompanied by
 - Cert. by Manager identifying the entry
 - Cert. by computer-in-charge giving details of data storage, safeguards and computer where such data is stored
 - Cert. by comp-in-charge (manner of affidavit) relating to integrity of printout and computer

State Vs. Navjot Sandhu

- Parliament attack case
- Laptop, storage devices recovered from a truck in Srinagar
- Laptop contained files relating to identity cards, stickers used by terrorists

State Vs. Navjot Sandhu

- Defense issues
 - Files created after the laptop was seized
 - Date setting can be edited
 - In the absence of verified time setting and concrete proof about the originality of the hard disk, evidence is inadmissible

State Vs. Navjot Sandhu

- Findings
 - If accuracy of computer evidence is to be challenged, burden lies on the side who makes such a challenge
 - User created files and system files, difference
 - Mere theoretical doubts cannot be cast on evidence

State Vs. Navjot Sandhu (Facts)

- The laptop was deposited in the malkhana on 16.1.2002
- Analysis revealed that two of the files were last written on 21.1.2001
 - one file was last accessed and last written on the same day
- Case diary noting - the laptop was accessed at the malkhana on 21.1.2002.

State Vs. Navjot Sandhu

- While cross examining PW73, a question was put as to how a file could be written without it being accessed.
- The witness answered that the file can be written without being accessed by copying it on a different storage media.

State Vs. Navjot Sandhu

- The learned counsel for the State is justified in his comment that the said answer was not a response pertaining to system files, which are self-generating and self-written.
- There was no suggestion to any witness that the date or time setting has been modified in the instant case so as to facilitate tampering.

State Vs. Navjot Sandhu

- A mountain out of mole hill is sought to be made out by reason of the observation of PW73 that some of the files were last written after the date of seizure and the answer given by PW73 with reference to a general, hypothetical question

State Vs. Navjot Sandhu

- Certificate under 65B(4) is an alternative method to prove electronic record
- Irrespective of the compliance of the requirements of Section 65B
 - there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, Ss. 63 & 65

State Vs. Navjot Sindhu

- Certificate containing details in S.Sec (4) of Section 65B may not have been filed
- That does not mean that secondary evidence cannot be given
 - *even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely Sections 63 & 65.*

State Vs. Navjot Sindhu

- Gist of findings
 - Accessing a suspect computer after date of seizure *ipso facto* does not render evidence inadmissible;
 - If accuracy of computer evidence is challenged, burden is on party making such challenge;
 - Certificate under 65(B)(4) is not mandatory for making electronic evidence admissible

Anwar Vs. PK Basheer, SC Sep '14

- Electronic record by way of secondary evidence is inadmissible unless accompanied by cert. at the time of taking the document
- Earlier proposition laid down regarding no mandatory requirement of Cert. in 65B is bad in law and is overruled

Position of law

- What happens to all those cases where 65B(4) certificates were not furnished because Navjot Sandhu held the field?

Examiner of Electronic Evidence

- Examiner of elec. Evidence
 - Central Govt. may notify in O.G.
 - Any agency/dept/body of C.G. or S.G.
 - For expert opinion on electronic evidence
- Opinion becomes relevant fact u/s 45A (new) of the Evidence Act

Admissibility of Text Messages

- Printouts of text message may be admitted following the usual method under Section 65B
- Court may summon the service provider to give details of text messages from a particular number
- Printouts must contain date, time, telephone number of each text message for verification

Admissibility of Whatsapp Messages

- The same procedure to be followed like in case of text messages
- However, Whatsapp messages are not stored on Whatsapp servers unlike TSPs in text messages
- Reliability must be established, if questioned

Audio/Video clippings in Mobile Phones

- Admissible
- Procedure under Section 65B to be followed
- If 65B cert. exists, oral evidence necessary only when authenticity is questioned
- If 65B conditions are met, phone itself is not necessary as an exhibit
- Only when trial court is not satisfied with evidence led, it may require original phone

Emails

- Procedure under Section 65B
- Contents of e-mails as evidence
 - If parties admit the contents
 - If email is digitally signed
 - By subsequent conduct of parties
- In the alternative, by an IP address trace
- Finally, by examination of witnesses

Emails

- If emails have been produced after
 - Following procedure in 65B
 - Genuineness has been proved by witnessesSubsequent deletion is inconsequential
- 65B(1) admitted as direct evidence
- 65(c) – When the original has been lost or destroyed

Tampering with evidence

- Hash value
- Expert report about file creation, access and modification
- In the absence of standard procedures being followed, by examination of witnesses

Magraj Patodia Vs. R.K.Birla, SC 1972

- Documents illegally produced as evidence in prosecution relating to election case
- Documents recovered illegally from person who was neither witness nor party to the case
- *“the fact that a document was procured by improper or even illegal means will not be a bar to its admissibility if it is relevant and its genuineness proved”*

Pooran Mal Vs. Director of Inspection, SC 1973

- Case relating to Income Tax
- Documents alleged to have been seized illegally during search and seizure
- *“...Neither by invoking the spirit of our Constitution nor by a strained construction of any of the fundamental rights can we spell out the exclusion of evidence obtained on an illegal search”*

State (N.C.T of Delhi) Vs. Navjot Sandhu, SC 2005

- CDR produced by illegal interception
- *“The non-compliance or inadequate compliance with the provisions of the Telegraph Act does not per se affect the admissibility.”*

IT Act 2000

- No Procedure for search and seizure specifically described
- 65B, Evidence Act talks only about admissibility on basis of Cert. under 65B(4)
- Conclusion?

Questions?