1. INTRODUCTION ........................................................................................................ 3

2. INCOME TAX RAID CASE ...................................................................................... 6
   Request for Service ................................................................................................. 7
   Chain of Custody Form ......................................................................................... 8
   Investigation Report .............................................................................................. 9

3. SOURCE CODE THEFT CASE ............................................................................ 12
   Request for Service .............................................................................................. 14
   Chain of Custody Form ....................................................................................... 15
   Investigation Report ............................................................................................ 16

4. CYBER SABOTAGE CASE .................................................................................. 18
   Request for Service ............................................................................................. 21
   Investigation Report ............................................................................................ 22

5. LOTTERY FRAUD CASE ...................................................................................... 27
   Request for Service ............................................................................................. 29
   Investigation Report ............................................................................................ 30

6. ACCOUNTING FRAUD CASE ............................................................................ 31
   Request for Service ............................................................................................. 32
   Investigation Report ............................................................................................ 33

7. DIGITAL SIGNATURE FRAUD CASE................................................................. 38
   Request for Service ............................................................................................. 39
   Investigation Report ............................................................................................ 40

ANNEX 1: EVIDENCE IN COMPUTER DEVICES ......................................................... 47

ANNEX 2: INVESTIGATION GUIDELINES ................................................................. 49

   1. ORKUT FAKE PROFILE CASES ........................................................................ 50
   2. EMAIL ACCOUNT HACKING ........................................................................... 52
   3. CREDIT CARD FRAUD .................................................................................... 54
   4. ONLINE SHARE TRADING FRAUD ................................................................. 56
   5. TAX EVASION AND MONEY LAUNDERING .................................................. 58
   6. SOURCE CODE THEFT ................................................................................... 60
   7. THEFT OF CONFIDENTIAL INFORMATION .................................................. 62
   8. SOFTWARE PIRACY ......................................................................................... 65
   9. MUSIC PIRACY ............................................................................................... 67
  10. EMAIL SCAMS .................................................................................................. 69
  11. PHISHING ......................................................................................................... 71
  12. CYBER PORNOGRAPHY ................................................................................... 73
  13. ONLINE SALE OF ILLEGAL ARTICLES ......................................................... 75
  14. USE OF INTERNET AND COMPUTERS BY TERRORISTS ............................. 77
  15. VIRUS ATTACKS ............................................................................................... 79
  16. WEB DEFAECMENT ......................................................................................... 81

© 2008 Rohas Nagpal. All rights reserved.
ANNEX 3: INTRODUCTION TO DIGITAL SIGNATURES ............................................. 83

ANNEX 4: LIST OF USEFUL SOFTWARE .......................................................... 100
1. Introduction

While investigating cyber crime cases, Asian School of Cyber Laws (ASCL) investigators follow the process outlined below:

1. The filled in Request for Service (RFS) is obtained from the client.

   The RFS helps ASCL to understand what the client expects from the investigation. In the RFS, the client describes the crime and requests ASCL to investigate it.

2. Then ASCL appoints a lead investigator for the case. The lead investigator meets the client to discuss the investigative avenues and potential evidence being sought in the investigation.

   The lead investigator and the investigation team for each case are appointed with great care and caution. The technical requirements of the investigation are the primary basis for the selection of the team and the lead investigator.

3. The relevant computer(s), media, documents etc are then received from the client. The chain of custody form in respect of each of these items is duly filled in by ASCL investigators.

   The chain of custody form in respect of each device is meticulously updated throughout the investigation. One copy of the chain of custody form in respect of each device is handed over to the client at the end of the investigation.

4. Where possible, the media (hard disk, floppy etc) is imaged. The original media is returned to the client and the image is retained for investigation.

   The images are authenticated using MD5 and / or SHA1 hash function.

5. Detailed cyber forensic analysis and investigation is carried out as per the requirements of the client.

   All analysis and investigations are carried out in a secure and confidential manner by skilled ASCL professionals.

6. The findings of the analysis and investigation are properly documented and relevant reports are submitted to the client.
# Request for Service

<table>
<thead>
<tr>
<th>RFS No.</th>
<th>Date</th>
</tr>
</thead>
</table>

## Client name and address

## Client's authorised representative

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
<th>Fax</th>
</tr>
</thead>
</table>

## Background of the case

## Details of computer(s), media etc

Have the computer(s), media etc mentioned above been accessed / examined prior to being handed over to ASCL? If yes, give details.

## Services requested from ASCL

## For internal ASCL use only

(Pl leave blank)

<table>
<thead>
<tr>
<th>Case recd on</th>
<th>Case recd by</th>
<th>Referred by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tax</td>
<td>Porn</td>
<td>Financial</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Chain of Custody Form

**Lead Investigator:**

---

1. **Case Number:** 

2. **Evidence number:**

3. **Date and time of confiscation / recovery:**

4. **Person from whom confiscated / recovered:**

5. **Place of Confiscation / recovery:**

6. **Details of prior access / investigation:**

7. **Description of hard disk:**
   - **Model no:**
   - **Manufacturer:**
   - **Serial no:**
   - **Dimensions:**
   - **Capacity:**
   - **Jumper:**
   - **Interface:**
   - **LBA Add. Sec.:**

8. **Unusual marks, if any:**

---

### Chain of Custody

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>Released by</th>
<th>Released to</th>
<th>Purpose of change of custody</th>
</tr>
</thead>
</table>

---

---

---
2. Income Tax Raid case

Gurubhai Batiwala is a rich middle-aged businessman settled in Zimblia. He owns a huge bungalow in a posh locality in Zimblia. A lover of costly luxury cars, Gurubhai recently imported a Bentley Brooklands.

On 19th March 2008 the Income Tax officials raided Gurubhai’s house on grounds of suspected tax evasion. As soon as Gurubhai saw the officials, he formatted the hard disk of his laptop computer.

The Income Tax officials suspect that Gurubhai has undisclosed bank accounts in tax haven countries and information relating to his “black” money is contained in the formatted hard disk.

The formatted hard disk has been recovered from Gurubhai. It has been handed over to ASCL investigators.

The primary objective of the investigation is to ascertain whether the formatted hard disk contains relevant evidence proving details of undisclosed bank accounts.

**Note:** The relevant evidence file for this case study is provided in the folder titled “Case 1” in the DVD accompanying this book.
Request for Service

RFS No.
IN-PNQ/03-08/084

Date
19th March, 2008

Client name and address
Income Tax Department
Zimblia

Client’s authorised representative
Name
Manoj Kumar
Email
mk@it.zimblia.gov
Phone
34221341
Fax
3423412

Background of the case
On 19th March the Income Tax officials raided the suspect’s (Gurubhai Batliwala) house on grounds of suspected tax evasion. As soon as Gurubhai saw the Income Tax officials, he formatted the hard disk of his laptop computer. The formatted hard disk has been recovered from Gurubhai.

It is suspected that the suspect has undisclosed bank accounts in tax haven countries and information relating to his “black” money is contained in the formatted hard disk.

Details of computer(s), media etc
Samsung SV4002H hard disk bearing serial number 0439J1BT731517

Have the computer(s), media etc mentioned above been accessed / examined prior to being handed over to ASCL? If yes, give details.
The hard disk has been seized from the suspect. Thereafter there has been no access / examination of the said hard disk.

Services requested from ASCL
Analyze the seized hard disk to recover evidence relating to undisclosed income, money laundering, foreign bank accounts etc.

For internal ASCL use only (Pl leave blank)
Case recd on
19th March 2008
Case recd by
Rohas Nagpal
Referred by
Manoj Kumar
Tax  Porn  Financial  Cyber
Priority 1 2 3 4 5 6 7 8 9 10
## Chain of Custody Form

<table>
<thead>
<tr>
<th>1. Case Number:</th>
<th>IN-PNQ/03-08/084</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Evidence number:</td>
<td>HDD-01</td>
</tr>
<tr>
<td>3. Date and time of confiscation / recovery:</td>
<td>19th March 2008 [1425 hours]</td>
</tr>
<tr>
<td>4. Person from whom confiscated / recovered:</td>
<td>Gurubhai Batliwala</td>
</tr>
<tr>
<td>5. Place of Confiscation / recovery:</td>
<td>128, Crescent Avenue, Zimblia</td>
</tr>
<tr>
<td>6. Details of prior access / investigation:</td>
<td>NIL</td>
</tr>
<tr>
<td>7. Description of hard disk:</td>
<td></td>
</tr>
<tr>
<td>Model no:</td>
<td>SV4002H</td>
</tr>
<tr>
<td>Manufacturer:</td>
<td>Samsung</td>
</tr>
<tr>
<td>Serial no:</td>
<td>0439J1BT731517</td>
</tr>
<tr>
<td>Dimensions:</td>
<td>10cm<em>14.5 cm</em>2.5 cm</td>
</tr>
<tr>
<td>Capacity:</td>
<td>40GB</td>
</tr>
<tr>
<td>Jumper:</td>
<td>Master</td>
</tr>
<tr>
<td>Interface:</td>
<td>IDE</td>
</tr>
<tr>
<td>LBA Add. Sec.:</td>
<td>78,242,976</td>
</tr>
<tr>
<td>8. Unusual marks, if any:</td>
<td>None</td>
</tr>
</tbody>
</table>

### Chain of Custody

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>Released by</th>
<th>Released to</th>
<th>Purpose of change of custody</th>
</tr>
</thead>
</table>
| 20th Mar 2008 1005 hours | Rohas Nagpal | Parag Singh | Creation of image  
Computation of hash value |
| 20th Mar 2008 1245 hours | Parag Singh | Rohas Nagpal | For returning to client |
| 20th Mar 2008 1430 hours | Rohas Nagpal | Manoj Kumar | Returned to client |
Investigation Report

The MD5 hash value of HDD-01 [Case: IN-PNQ/03-08/084] as computed by me using Winhex 14.4 SR2 software (hereafter referred to as Winhex) licenced to Asian School of Cyber Laws is:
DFF0AC234C03F75E9EC13DFF77C48911

The image of evidence number HDD-01 was created by Parag Singh using Winhex. The image was named as HDD-01. The MD5 hash value of the image as computed using Winhex is:
DFF0AC234C03F75E9EC13DFF77C48911

I then began analysis of the said image file named HDD-01.

1. I opened the image file using WinHex using the “Specialist → Interpret Image File as Disk” option (illustrated below).

2. I then viewed the contents of the image file in the Directory Browser of Winhex (illustrated below).
3. On previewing the data of the image I found that there are many deleted files and folders. These files and folders were recovered by me using Winhex.

5. The files and folders in the `.Trash-root` folder contain information relating to tax haven countries and information for tax evasion methods.

6. Two files appear to be particularly relevant - `details1.txt` and `details2.txt`.

7. The file `details1.txt` contains a list of banks and account numbers with the account balances as under:

<table>
<thead>
<tr>
<th>No.</th>
<th>Country</th>
<th>Bank</th>
<th>Account</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Antigua</td>
<td>Caribbean Offshore Bank</td>
<td>1212199</td>
<td>505000</td>
</tr>
<tr>
<td>2</td>
<td>Cayman Island</td>
<td>Cayman Island Bank</td>
<td>831232</td>
<td>1200000</td>
</tr>
<tr>
<td>3</td>
<td>Cyprus</td>
<td>Central Bank of Cyprus</td>
<td>128403299</td>
<td>450000</td>
</tr>
<tr>
<td>4</td>
<td>Liberia</td>
<td>Global Bank Liberia</td>
<td>2199171</td>
<td>90000</td>
</tr>
<tr>
<td>5</td>
<td>Liechtenstein</td>
<td>Leichtenstein Global Trust</td>
<td>332183</td>
<td>100000</td>
</tr>
<tr>
<td>6</td>
<td>Monaco</td>
<td>Bank Von Ernst</td>
<td>1010122</td>
<td>40000</td>
</tr>
<tr>
<td>7</td>
<td>Switzerland</td>
<td>Swiss Bank</td>
<td>9927310121</td>
<td>1250000</td>
</tr>
<tr>
<td>8</td>
<td>St. Vincent</td>
<td>Loyal Bank</td>
<td>9121988321</td>
<td>900000</td>
</tr>
<tr>
<td>9</td>
<td>Latvia</td>
<td>Rietumu bank</td>
<td>812810000</td>
<td>495000</td>
</tr>
</tbody>
</table>

8. The file `details2.txt` contains details of transactions as under:

<table>
<thead>
<tr>
<th>No.</th>
<th>Month</th>
<th>Paid To</th>
<th>Place</th>
<th>Method</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jan</td>
<td>Seema</td>
<td>Dubai</td>
<td>Hawala</td>
<td>200000</td>
</tr>
<tr>
<td>2</td>
<td>Jan</td>
<td>Rahul</td>
<td>Singapore</td>
<td>E-banking</td>
<td>150000</td>
</tr>
<tr>
<td>3</td>
<td>Jan</td>
<td>Car</td>
<td>Surat</td>
<td>Cash</td>
<td>60000</td>
</tr>
<tr>
<td>4</td>
<td>Jan</td>
<td>Air</td>
<td>Switzerland</td>
<td>Cash</td>
<td>45000</td>
</tr>
<tr>
<td>5</td>
<td>Jan</td>
<td>Vijay</td>
<td>Monaco</td>
<td>Agent</td>
<td>45000</td>
</tr>
<tr>
<td>6</td>
<td>Jan</td>
<td>Andre</td>
<td>Latvia</td>
<td>Agent</td>
<td>40000</td>
</tr>
<tr>
<td>7</td>
<td>Jan</td>
<td>New Flat</td>
<td>India</td>
<td>Cash/cheque</td>
<td>900000 /550000</td>
</tr>
<tr>
<td>8</td>
<td>Feb</td>
<td>Bank Deposit</td>
<td>Liechenstein</td>
<td>E-banking</td>
<td>200000</td>
</tr>
<tr>
<td>9</td>
<td>Feb</td>
<td>Bank Deposit</td>
<td>Liberia</td>
<td>Agent</td>
<td>100000</td>
</tr>
<tr>
<td>10</td>
<td>Feb</td>
<td>Bank Deposit</td>
<td>Cyprus</td>
<td>Agent</td>
<td>100000</td>
</tr>
<tr>
<td>11</td>
<td>Feb</td>
<td>Bank Deposit</td>
<td>Latvia</td>
<td>Cash</td>
<td>50000</td>
</tr>
<tr>
<td>12</td>
<td>Mar</td>
<td>Diamond Set</td>
<td>India</td>
<td>Cash</td>
<td>100000</td>
</tr>
<tr>
<td>13</td>
<td>Mar</td>
<td>Air Tickets</td>
<td>Antigua</td>
<td></td>
<td>25000</td>
</tr>
<tr>
<td>14</td>
<td>Mar</td>
<td>Bussiness Deal</td>
<td>India</td>
<td></td>
<td>120000</td>
</tr>
</tbody>
</table>
3. Source code theft case

SystNetSoft is a leading software development company. It is currently working on a revolutionary buddy system for Unix. A Buddy System is basically a memory allocation strategy which recursively divides allocatable blocks of memory into pairs of adjacent equal-sized blocks called buddies.

The Company has a lot of expectations from the project and is hoping to make huge profits once the system is ready for sale. The entire development for the project is done by a select team of programmers at SystNetSoft Lab no. 210. This lab has 25 networked computers. These computers are highly secure and are not connected to the Internet. They are also not connected to the main SystNetSoft network.

A strict security policy is enforced wherein no one other than the CEO of SystNetSoft and the programmers working on the Buddy System project are allowed access to Lab no 210. Even these people are prohibited from carrying any data storage device into or out of Lab no 210.

Pooja is an attractive young engineer recently recruited by the company especially for the Buddy System project. She has a luxurious lifestyle for which her salary is never enough.

On 17th December 2006, Pooja comes to Lab 210 listening to music on her iPod. The security guard objects to her entering the Lab with the iPod. After a long argument Pooja manages to convince the guard that the iPod is simply a music player and not a data storage device.

The next day the security guard reads a newspaper article on misuse of iPods for data theft. Alarmed by the concept, he calls up the SystNetSoft Security Head and informs him about the argument he had with Pooja the previous day.

The Security Head informs the CEO and an urgent system log audit is conducted on the computers in Lab 210. It is discovered that the following files had been unauthorizedly copied onto an external data storage device:

<table>
<thead>
<tr>
<th>File name</th>
<th>MD-5 hash value</th>
</tr>
</thead>
<tbody>
<tr>
<td>automated-sheet.c</td>
<td>BFDF2A39169C6701C9AB28479BB1C256</td>
</tr>
<tr>
<td>buddy.c</td>
<td>4CA95ECEF433D29C69566E6AAD9635494</td>
</tr>
<tr>
<td>calendar.c</td>
<td>38FB0A9F8D5C2942B942FCA237FBB33C</td>
</tr>
<tr>
<td>e-m-automation.c</td>
<td>680F17E9314F77715A431653E65F9020</td>
</tr>
<tr>
<td>tic-tac- toe.c</td>
<td>F32543DC2B10DA617A18B2C1884720B4</td>
</tr>
</tbody>
</table>

With the help of the local police, Pooja is arrested on suspicion of having stolen some of the Buddy System source code files. Her iPod is imaged by the police. This image file is handed over to the Computer Investigation department of Asian School of Cyber Laws (ASCL) for analysis.
The **primary objective of the investigation** is to ascertain whether Pooja gained unauthorized access to the Buddy System source code files and copied them to her iPod.

**Note:** The relevant evidence file for this case study is provided in the folder titled “Case 2” in the DVD accompanying this book.
Request for Service

RFS No. (Pl leave blank)  IN-PNQ/03-08/085
Date  19th March, 2008

Client name and address
SystNetSoft
Zimblia

Client's authorised representative
Name  Manoj Kumar
Email  mk@SystNetSoft.com
Phone  34221341
Fax  3423412

Background of the case
Some files were unauthorizedly copied onto an external data storage device from the computers in Lab 210 of SystNetSoft. The suspect (Pooja) has been arrested on suspicion of having unauthorizedly copied these files onto her iPod. Her iPod is imaged by the police.

Details of computer(s), media etc
Image of the iPod seized from the suspect.

Have the computer(s), media etc mentioned above been accessed / examined prior to being handed over to ASCL? If yes, give details.
The iPod seized from the suspect has been cloned by the police. Only the image of the said iPod has been handed over to ASCL.

Services requested from ASCL
Analyze the image of the iPod and determine if the following files had been copied onto the said iPod.

<table>
<thead>
<tr>
<th>File name</th>
<th>MD-5 hash value</th>
</tr>
</thead>
<tbody>
<tr>
<td>automated-sheet.c</td>
<td>BFDF2A39169C6701C9AB28479BB1C256</td>
</tr>
<tr>
<td>buddy.c</td>
<td>4CA95ECF433D29C69566E6AAD9635494</td>
</tr>
<tr>
<td>calendar.c</td>
<td>38FB0AA8D5C2942B942FCA237FBB33C</td>
</tr>
<tr>
<td>e-m-automation.c</td>
<td>680F17E9314F77715A431653E65F9020</td>
</tr>
<tr>
<td>tic-tac-toe.c</td>
<td>F32543DC2B10DA617A18B2C1884720B4</td>
</tr>
</tbody>
</table>

For internal ASCL use only
(Pl leave blank)

Case recd on  19th March 2008
Case recd by  Rohas Nagpal
Referred by  Manoj Kumar

Tax  Porn  Financial  Cyber  Source Code  Priority  1 2 3 4 5 6 7 8 9 10
### Chain of Custody Form

<table>
<thead>
<tr>
<th>1. Case Number:</th>
<th>IN-PNQ/03-08/085</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Evidence number:</td>
<td>IMG-01</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. Date and time of confiscation / recovery:</th>
<th>19th March 2008 [1425 hours]</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>4. Person from whom confiscated / recovered:</th>
<th>Pooja</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>5. Place of Confiscation / recovery:</th>
<th>128, Crescent Avenue, Zimblia</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>6. Details of prior access / investigation:</th>
<th>NIL</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>7. Description of image file:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size: 507,490 KB</td>
</tr>
<tr>
<td>MD-5 hash: 2D1D9725845E93FE1211C659D51108C6</td>
</tr>
<tr>
<td>SHA-1 hash: DCBF669CB5667558593146AD3FD43B8B40FE6B38</td>
</tr>
<tr>
<td>Original media: iPod Shuffle 512 MB [Serial No. 5C644ZJCRS9]</td>
</tr>
</tbody>
</table>

### Chain of Custody

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>Released by</th>
<th>Released to</th>
<th>Purpose of change of custody</th>
</tr>
</thead>
<tbody>
<tr>
<td>20th Mar 2008 1430 hours</td>
<td>Rohas Nagpal</td>
<td>Manoj Kumar</td>
<td>Returned to client</td>
</tr>
</tbody>
</table>
Real World CCI Case Studies

Investigation Report

1. I first opened the image file using X-Ways Forensics 13.0 SR17 software (hereafter referred to as X-Ways Forensics) licenced to Asian School of Cyber Laws. I used the "Specialist → Interpret Image File as Disk" option as illustrated below.

2. On careful examination I found that ?title9.mp3 was actually a ZIP archive and not an mp3 file.


4. I then renamed the ?title9.mp3 file to ?title9.zip and tried to extract the contents of the file using WinZip 9.0 SR1. The file was found to be password protected.

5. I recovered the password [tRee1] using Elcomsoft Advanced Zip Password Recovery software version 3.54.

6. Using this password I recovered the following files from the ?title9.zip file:
<table>
<thead>
<tr>
<th>File name</th>
<th>MD-5 hash value</th>
</tr>
</thead>
<tbody>
<tr>
<td>automated-sheet.c</td>
<td>BFDF2A39169C6701C9AB28479BB1C256</td>
</tr>
<tr>
<td>buddy.c</td>
<td>4CA95ECF433D29C695666E6AAD9635494</td>
</tr>
<tr>
<td>calendar.c</td>
<td>38FB0AAF8D5C2942B942FCA237FBB33C</td>
</tr>
<tr>
<td>e-m-automation.c</td>
<td>680F17E9314F77715A431653E65F9020</td>
</tr>
<tr>
<td>tic-tac-toe.c</td>
<td>F32543DC2B10DA617A18B2C1884720B4</td>
</tr>
</tbody>
</table>

7. The hash values of these files are identical to the hash values of the files that have allegedly been unauthorizedly copied from the computers in Lab 210 of SystNetSoft.
4. Cyber Sabotage case

MegaOil Corporation is one of the world’s largest oil companies. It has been using Distributed Control Systems (DCS) since the mid 1970s as the means for monitoring, and automatically controlling its industrial processes.

In the early years, the architecture of its DCS consisted of a set of distributed computer units that were interfaced with the field-based process equipment and which communicated with plant operators, at computer workstations, via a high-speed local area network.

The only "external" connections were the local-area network circuits that were run around the plant and used to communicate between and among the process controllers and the operator workstations. The communications technologies used for this local area networking were vendor proprietary. Communications over these circuits was managed using specialized, proprietary, vendor-specific, communication protocols.

These protocols included basic error detection and correction capabilities, but nothing that guaranteed “secure” communications. Over time, the need for higher performance, plus the cost of supporting proprietary hardware and software, forced MegaOil Corporation to procure a DCS that adopted vendor neutral technologies.

Since the DCS systems collected a lot of data and generated a lot of reports, MegaOil decided that the DCS systems would be connected to the business systems for an automatic exchange of this data using the TCP/IP networking and standardized IP applications like “FTP”.

The Directors were apprehensive that cyber terrorists would launch a cyber attack on their systems and this could cripple the company.

To periodically ascertain the security of the systems, they approved a regular penetration test on the DCS. Data64 Technologies Pvt Ltd, a subsidiary of Asian School of Cyber Laws was contracted to launch ethical hacking attacks on the DCS.

The reports submitted by Data64 subsequent to the attacks were used to bolster the security systems. The most recent penetration test proved that someone with a laptop computer running IP packet capture/generation software and a compatible Ethernet NIC could connect to the plant LAN and send out control commands that would be accepted by the process control computers as coming from the operator workstations.

This attack totally bypassed the operator access mechanisms and went directly to the computer equipment where control and monitoring is actually being performed.
The report prepared by Data64 also said that:

“A similar attack could be made by connecting directly to the “console/diagnostic” port of the process control computer. This would require physical access to the controller unit and knowledge of the vendors diagnostic tools. DCS systems, by their nature, support the downloading of control logic into the process control computers via the LAN. This opens up the possibility of a terrorist “reprogramming” a process controller via this same mechanism. But, in reality, to accomplish any of these attacks this would require exact and detailed knowledge of the DCS system software, data structures and the site-specific configuration information”.

Alarmed by the findings of this report, the Board of Directors ordered a complete revamp of the DCS systems. A competent team of MegaOil employees worked for 6 months to complete the system revamp. The system revamp was concluded on 10th October, 2006.

On 13th November, 2006 at around 11:07 am, a major explosion took place at MegaOil. 18 people were seriously injured and the company lost crores of rupees worth of machinery and stock. A full scale investigation was launched into the issue. The report of the internal investigation carried out by MegaOil was as under:

The explosion took place because the temperature in chamber 1104 had risen to 128 degrees Celsius.

The **DCS Control Manager** is the software application that controls several parts of the MegaOil plant including chamber 1104. The DCS Control Manager was programmed to read the following files to ascertain the levels at which warnings need to be sent to the Plant Managers:

**File Name: temp.megaoil**
This is a file containing two numbers (default value is 70:110). The system treats the numbers as the temperature values in degrees Celsius.
If the temperature in any chamber exceeds the first number (70 degrees Celsius) the system generates a warning to the operators to take definitive action.

If the temperature in any chamber exceeds the second number (110 degrees Celsius) the system automatically shuts down all processes in that chamber so as to bring the temperature down to an acceptable level.

**File Name: press.megaoil**
This is a file containing two numbers (default value is 0.75:0.92). The system treats the numbers as the pressure values in mega pascal.

If the pressure in any chamber exceeds the first number (0.75 mega pascal) the system generates a warning to the operators to take definitive action.

If the pressure in any chamber exceeds the second number (0.92 mega pascal) the system automatically shuts down all processes in that chamber so as to bring the pressure down to an acceptable level.

Subsequent to the explosions, these files were examined and found to be unchanged. Despite this the system had not generated any warnings or initiated any automatic shutdown.

The **primary objective** of the investigation is to determine if the temp.megaoil and press.megaoil have been tampered and, if so, to identify who tampered the files.

**Note:** The MegaOil systems can be accessed at:
http://www.asianlaws.org/students/current/cea/14/index.htm
Request for Service

**RFS No.** (Pl leave blank)  
IN-PNQ/11-06/086  
**Date**  
20th November, 2006

**Client name and address**  
MegaOil Corporation  
Zimbia

**Client’s authorised representative**

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manoj Kumar</td>
<td><a href="mailto:mk@megaoil.com">mk@megaoil.com</a></td>
<td>34221341</td>
<td>3423412</td>
</tr>
</tbody>
</table>

**Background of the case**

On 13th November, 2006 at around 11:07 am, a major explosion took place at MegaOil. 18 people were seriously injured and the company lost crores of rupees worth of machinery and stock. It is suspected that the explosion was a result of unauthorised tampering with the MegaOil systems.

**Details of computer(s), media etc**

The MegaOil systems that can be accessed at:

http://www.asianlaws.org/students/current/cea/14/index.htm

Have the computer(s), media etc mentioned above been accessed / examined prior to being handed over to ASCL? If yes, give details.

N.A

**Services requested from ASCL**

1. To determine if the MegaOil systems have been unauthorizedly accessed.
2. To determine if the temp.megaoil and press.megaoil have been tampered with and, if so, to identify who tampered the files.

**For internal ASCL use only** (Pl leave blank)

<table>
<thead>
<tr>
<th>Case recd on</th>
<th>Case recd by</th>
<th>Referred by</th>
</tr>
</thead>
<tbody>
<tr>
<td>20th November 2006</td>
<td>Rohas Nagpal</td>
<td>Manoj Kumar</td>
</tr>
</tbody>
</table>

**Priority**

1  2  3  4  5  6  7  8  9  10
Investigation Report

1. The first step was to investigate the DCS Control Manager console. On opening up the console, the "Submit Query" link in the lower right corner of the screen was clicked. The following error message showed up:

   Unknown Command, " " - please type 'help' for a list of commands.

2. Typing 'help' in the console and pressing enter or clicking on the "Submit Query" link leads to the following message:

   logs - Shows the system logs
   contact - Shows the contact information
   ls - Lists available files and directories
   exit - Exit console
   wget - Gets specified available file in directory

3. On using the "ls" command, the following message appears:

   [C:] ls
   Sorry. You are not authorised to use this command.

4. Upon using the 'Logs' command, the following details appear:

   Files Uploaded to System in last 12 months:
   
<table>
<thead>
<tr>
<th>File Name</th>
<th>IP Address</th>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>update.js</td>
<td>14.12.10.10</td>
<td>12Jan06</td>
<td>0714</td>
</tr>
<tr>
<td>update.js</td>
<td>14.11.10.10</td>
<td>12Feb06</td>
<td>0714</td>
</tr>
<tr>
<td>update.js</td>
<td>14.12.11.10</td>
<td>12Mar06</td>
<td>0714</td>
</tr>
<tr>
<td>update.js</td>
<td>14.12.11.12</td>
<td>12Apr06</td>
<td>0714</td>
</tr>
<tr>
<td>update.js</td>
<td>14.14.10.19</td>
<td>12May06</td>
<td>0714</td>
</tr>
<tr>
<td>update.js</td>
<td>14.12.19.89</td>
<td>12Jun06</td>
<td>0714</td>
</tr>
<tr>
<td>update.js</td>
<td>13.11.11.94</td>
<td>12Jul06</td>
<td>0714</td>
</tr>
<tr>
<td>update.js</td>
<td>14.10.10.15</td>
<td>12Aug06</td>
<td>0714</td>
</tr>
<tr>
<td>update.js</td>
<td>14.19.10.10</td>
<td>12Sep06</td>
<td>0714</td>
</tr>
<tr>
<td>update.js</td>
<td>14.12.10.16</td>
<td>12Oct06</td>
<td>0714</td>
</tr>
<tr>
<td>update.js</td>
<td>14.12.10.24</td>
<td>12Nov06</td>
<td>0714</td>
</tr>
</tbody>
</table>

   All uploaded files are permanently archived.
   To download files use the wget command.
   To access the server logs use the srvlogs command.

5. On using the "wget upload.js" command, various log files can be obtained, but they do not contain any relevant information.
6. On using the "SrvLogs" command, the following log is displayed:

Srvlogs
Currently only the Log Files for 13 Nov 2006 are available.
#Version: 1.0
#Date: 2006-11-13
10:48:15
#Fields: time c-ip cs-method cs-uri-stem sc-status sc-win32-status
10:48:15 10.1.39.47 [85]closed - 426 64
10:48:15 10.1.39.47 [87]USER administrator 331 0
10:48:15 10.1.39.47 [88]USER administrator 331 0
10:48:15 10.1.39.47 [90]USER administrator 331 0
10:48:15 10.1.39.47 [91]USER administrator 331 0
10:48:15 10.1.39.47 [90]PASS - 530 1326
10:48:15 10.1.39.47 [89]USER administrator 331 0
10:48:15 10.1.39.47 [92]USER administrator 331 0
10:48:15 10.1.39.47 [93]USER administrator 331 0
10:48:15 10.1.39.47 [94]USER administrator 331 0
10:48:15 10.1.39.47 [87]USER administrator 331 0
10:48:15 10.1.39.47 [90]USER administrator 331 0
10:48:15 10.1.39.47 [92]USER administrator 331 0
10:48:15 10.1.39.47 [90]PASS - 530 1326
10:48:15 10.1.39.47 [88]USER administrator 331 0
10:48:15 10.1.39.47 [91]USER administrator 331 0
10:48:15 10.1.39.47 [88]USER administrator 331 0
10:48:15 10.1.39.47 [88]USER administrator 331 0
10:48:15 10.1.39.47 [90]USER administrator 331 0
10:48:15 10.1.39.47 [92]USER administrator 331 0
10:48:15 10.1.39.47 [93]USER administrator 331 0
10:48:15 10.1.39.47 [88]USER administrator 331 0
10:48:15 10.1.39.47 [91]USER administrator 331 0
10:48:15 10.1.39.47 [88]USER administrator 331 0
10:48:15 10.1.39.47 [90]USER administrator 331 0
10:48:15 10.1.39.47 [87]USER administrator 331 0
10:48:15 10.1.39.47 [88]USER administrator 331 0
10:48:15 10.1.39.47 [90]USER administrator 331 0
7. Careful perusal of the above log provides the following useful information.

a. The Log File is for 13 Nov 2006, which is the day when the mishap happened at MegaOil.

b. The Log file displays activities taking place from a single IP 10.1.39.47
c. Close perusal of the activities taking place from the IP 10.1.39.47 shows that someone from this IP is trying to log in to the system by trying random usernames and passwords.

d. A close examination of the timing shown in the logs and the rate at which usernames and passwords are been tried on the system indicates that some brute force password cracking software (e.g. Brutus) may have been tried to crack the password.

8. The last few entries are very interesting and important from the investigation point of view. These are:

```plaintext
10:49:12 10.1.39.47 [96]USER administrator 331 0
11:06:22 10.1.39.47 [97]USER administrator 331 0
11:06:26 10.1.39.47 [97]PASS - 230 0
11:06:34 10.1.39.47 [97]created /press.megaoil 226 0
11:06:37 10.1.39.47 [97]created /temp.megaoil 226 0
11:06:40 10.1.39.47 [97]QUIT - 226 0
11:08:01 10.1.39.47 [98]USER administrator 331 0
11:08:01 10.1.39.47 [98]PASS - 230 0
11:08:05 10.1.39.47 [98]created /press.megaoil 226 0
11:08:07 10.1.39.47 [98]created /temp.megaoil 226 0
11:08:08 10.1.39.47 [98]QUIT - 226 0
```

9. It can be concluded by examining these entries that whoever was brute forcing the system obtained the password and used it to log onto the system.

10. It is known that the files "temp.megaoil" and "press.megaoil" are very critical for the system and any alteration in these files could lead to a big accident.

11. It can also be concluded that the suspect replaced these original files named "temp.megaoil" & "press.megaoil" with altered files of the same name. The altered files probably contained incorrect values and thus the warnings were not generated by the system even when the temperature and pressure exceeded the safe values.

12. In all probability, the original files were later restored, to eliminate proof of the sabotage. The log files show the duration of the suspicious activity to be from 10:49:12 hours to 11:08:08 hours.

13. Next, the Business Systems console of Mega Oil was investigated. On examining the Attendance Logs, the details of
the attendance on the said day for all the personnel of MegaOil were displayed. These are as follows:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Time In</th>
<th>Time Out</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.39.75</td>
<td>09:30:14</td>
<td>10:15:05</td>
<td>G. Alok (Emp ID-3297843)</td>
</tr>
<tr>
<td>10.1.39.21</td>
<td>09:35:40</td>
<td>10:29:17</td>
<td>V. Singh (Emp ID-3297844)</td>
</tr>
<tr>
<td>10.1.39.69</td>
<td>09:55:00</td>
<td>10:35:19</td>
<td>S. Sarnath (Emp ID-3297846)</td>
</tr>
<tr>
<td>10.1.39.92</td>
<td>10:03:12</td>
<td>10:08:04</td>
<td>N. Golaknathan (Emp ID-3297847)</td>
</tr>
<tr>
<td>10.1.39.64</td>
<td>10:10:31</td>
<td>10:26:22</td>
<td>V. Narayan (Emp ID-3297849)</td>
</tr>
<tr>
<td>10.1.39.47</td>
<td>10:30:22</td>
<td>11:10:50</td>
<td>A. Mallick (Emp ID-3297864)</td>
</tr>
<tr>
<td>10.1.39.64</td>
<td>10:45:09</td>
<td>11:26:22</td>
<td>R. Nagpal (Emp ID-3297881)</td>
</tr>
<tr>
<td>10.1.39.35</td>
<td>11:15:17</td>
<td>11:41:50</td>
<td>N. Balik (Emp ID-3297899)</td>
</tr>
</tbody>
</table>

14. While the Attendance Logs were used to record the names of the people who used the system along with their Employee IDs (and IPs), the Server Logs recorded the FTP activity that occurred on the System i.e. the DCS.

15. According to the Attendance Logs, on the 13th of November (the day the explosion occurred) the system was used from 10:30:22 to 11:10:50 by A. Mallick (Emp ID-3297864).

16. According to the Server Logs within the same time span a lot of FTP activity took place. Someone (in all probability A. Mallick) logged in from the computer with the IP 10.1.39.47 and began to brute force the DCS system. The suspect then obtained unauthorised access to the system and replaced the two critical files. After the explosion the suspect probably replaced the critical files with the original versions.
5. Lottery Fraud case

LottoOnline is a reputed on-line national lottery that has deployed state-of-the-art lottery terminals to more than 13,000 retail outlets in the country.

Online lottery is based on the communication between a client which is a lottery terminal maintained by the retailer and the hub, which is the lottery gaming system at LottoOnline.

When a customer approaches a retailer to buy a ticket, he is required to choose an alphabet (from A through Z) and a two digit number (between 10 and 99). His transaction is fed into the retailer terminal and undergoes extensive encryption and travels from the terminal, across the network to LottoOnline.

When it gets to LottoOnline, it is decrypted, captured, validated for authenticity, processed and a unique 26-character ticket number is allocated.

The first character of this 26 digit number is identical to the alphabet chosen by him and the last two characters are identical to the two digit number chosen by the customer.

**Example:** If a customer chooses "B" and "77" then his 26 character ticket number would be in the format Bxxxxxxxxxxxxxxxxxxxxxxxxxx77.

This information is re-encrypted and returned to the terminal from which it originated and there a unique ticket (bearing the unique 26 character ticket number) is produced. This whole process takes between three to four seconds. The player then takes the ticket with him to await the announcement of results (which is every Saturday evening).

Each ticket is priced at Rs 10. LottoOnline computers randomly pick seven winning numbers for the week. All those tickets whose alphabet and last two digits are identical to the winning numbers for the week are the winning tickets. The holder of each winning ticket wins Rs 100,000. The winners can encash the prize from any of the retailers.

The retailers are required to update their terminals by downloading an executable file from the LottoOnline website at 5 pm every Saturday evening. A ticket holder can present his ticket to any of the retailers. The retailer inserts the ticket into the terminal. The authenticity of the ticket is verified. Subsequently the terminal checks whether the ticket is a winning ticket. In case of winning tickets, the terminal dispenses a cheque for the prize money and cancels the ticket and updates the LottoOnline systems.

A group of LottoOnline customers suspect that some fraudulent activities are taking place at NR Lotto, one of the biggest LottoOnline retailers. The executable file published by LottoOnline on February 18, 2006 is available at the company website.
The primary objective of this case is to determine if NR Lotto, a Lotto Online retailer or any other party was involved in fraudulent activity.

Note: The LottoOnline website can be accessed at:
http://asianlaws.org/students/current/ccci/case_8/18022006.htm
## Request for Service

<table>
<thead>
<tr>
<th>RFS No. (Pl leave blank)</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>IN-PNQ/02-06/086</td>
<td>18th Feb, 2006</td>
</tr>
</tbody>
</table>

**Client name and address**

Manoj Kumar  
24/2 Zimbla Drive

**Client’s authorised representative**

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manoj Kumar</td>
<td><a href="mailto:mk@gmail.com">mk@gmail.com</a></td>
<td>34221341</td>
<td>3423412</td>
</tr>
</tbody>
</table>

**Background of the case**

As per details provided in the pages before this.

**Details of computer(s), media etc**

The LottoOnline website that can be accessed at:  
http://asianlaws.org/students/current/cea/19/18022006.htm

Have the computer(s), media etc mentioned above been accessed / examined prior to being handed over to ASCL? If yes, give details.

N.A

**Services requested from ASCL**

To investigate and ascertain whether some fraudulent activities are taking place at NR Lotto, one of the biggest LottoOnline retailers.

**For internal ASCL use only (Pl leave blank)**

<table>
<thead>
<tr>
<th>Case recd on</th>
<th>Case recd by</th>
<th>Referred by</th>
</tr>
</thead>
<tbody>
<tr>
<td>18th February 2006</td>
<td>Rohas Nagpal</td>
<td>Manoj Kumar</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tax</th>
<th>Porn</th>
<th>Financial</th>
<th>Cyber</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1 2 3 4 5 6 7 8 9 10</td>
</tr>
</tbody>
</table>
Investigation Report

1. The website provides the following:
   a. The result for February 18, 2006
   b. The updated executable file for February 18, 2006
   c. The MD5 hash value for the above said file:
      52848E32D7EF152214899505F400E07E

2. Double clicking the executable shows that the lottery result is

3. The next step of the investigation is to examine the executable file
   by opening it in a text / hex editor. The actual result stored in the
   file now appears to be: contents are now found to be
   A:12-B:34-C:56-D:98-E:40-F:61-G:78

4. The conclusion that can be drawn is that LottoOnline is
   manipulating the lottery results. The values that the executable
   "appears" to update on the systems of the resellers are the
   correct results. But in reality incorrect results are being updated.
   This results in genuine winners being deprived of the prize
   money.
6. Accounting Fraud case

The Fly-in Florist (FF) is a leading flower retailer that has been in business for more than 8 years. Customers have to call up the FF call center to place their orders. The FF executive enters client, payment and order information into the “FF Order System” [which has been developed by SysSoft Technologies].

After the payment has been authenticated the flowers are delivered to the provided address within 12 hours.

FF uses a sophisticated computerized system for calculating how many flowers it should keep in stock. This system uses sales information collected over the past 3 years to predict the likely sales on a particular day. The company then procures the predicted number of flowers and stores them in its air-conditioned storage facilities.

The system has been running successfully for more than 4 years. The average difference between the actual orders received by the company and the number of flowers stocked is not more than 1%. These excess 1% flowers are destroyed on a daily basis as the flowers lose their freshness in 24 hours.

In 2007, however, the company has noticed a disturbing trend. The average difference between the actual orders received by the company and the number of flowers stocked has shot up to more than 10%. This trend has been noticed since the day the “FF Order System” was upgraded from version 1 to version 2.

The management suspects that there is a flaw in the “FF Order System”. Pooja Singh, the CEO of SysSoft Technologies claims that the system is flawless. She claims that the sales of flowers have dipped due to customers preferring other flower retail outlets.

The primary objective of the investigation is to ascertain if there is some flaw in the FF order system and if there is then what is the problem.

Fly-in Florist website can be accessed at:
http://www.asianlaws.org/students/current/cea/22/flyinflorist/index.htm

The dummy credit card number **ASDF132207ZB1** can be used for testing the FF Order System
Request for Service

RFS No. (Pl leave blank)  
IN-PNQ/03-08/086  

Date  
19th March, 2008

Client name and address

Client's authorised representative

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manoj Kumar</td>
<td><a href="mailto:mk@flyinflorist.in">mk@flyinflorist.in</a></td>
<td>34221341</td>
<td>3423412</td>
</tr>
</tbody>
</table>

Background of the case

As per details provided in the pages before this.

Details of computer(s), media etc

Fly-in Florist systems can be accessed at:
http://www.asianlaws.org/students/current/cea/22/flyinflorist/index.htm

The dummy credit card number ASDF132207ZB1 can be used for testing the FF Order System

Have the computer(s), media etc mentioned above been accessed / examined prior to being handed over to ASCL? If yes, give details.

N.A

Services requested from ASCL

To ascertain if there is a fraud taking place by manipulating the Fly-in Florist online accounting and distribution systems.

For internal ASCL use only (Pl leave blank)

<table>
<thead>
<tr>
<th>Case recd on</th>
<th>Case recd by</th>
<th>Referred by</th>
</tr>
</thead>
<tbody>
<tr>
<td>19th March 2008</td>
<td>Rohas Nagpal</td>
<td>Manoj Kumar</td>
</tr>
</tbody>
</table>

Tax  Porn  Financial  Cyber  
Priority 1 2 3 4 5 6 7 8 9 10
Investigation Report

1. I was informed by the management of Fly-in-Florist that:
   
   a. The Fly-in Florist (FF) is a leading flower retailer. Customers have to call up the FF call center to place their orders. The FF executive enters client, payment and order information into the “FF Order System” [which has been developed by SysSoft Technologies].

   b. FF’s order system uses sales information collected over the past 3 years to predict the likely sales on a particular day. The company then procures the predicted number of flowers and stores them in its air-conditioned storage facilities.

   c. The average difference between the actual orders received by the company and the number of flowers stocked is not more than 1%.

   d. The average difference between the actual orders received by the company and the number of flowers stocked has shot up to more than 10%. This trend has been noticed since the day the “FF Order System” was upgraded from version 1 to version 2.

   e. The management suspects that there is a flaw in the “FF Order System”.

2. A dummy credit card number [ASDF132207ZB1] has been provided to me by the management to investigate the case.

3. I accessed the FF Order System on 2nd March 2008. The screenshot of the web interface is as illustrated below:
4. I then used the “Take Order” page to create 20 dummy entries as illustrated below:

5. Each dummy entry was for 10 units of the product having product code TU-01. The delivery date entered for each dummy order was 3rd March 2008.

6. After entering the details of each dummy entry I pressed on the “Process Order” button.

7. For each dummy entry I received the following confirmation message - “The order has been processed”.

8. On 4th March 2008 I queried the FF Order System using the “View Delivery Reports” option. I found that all 20 dummy entries were reflected in the delivery report indicating that all deliveries had been made. The bills numbers allotted to the entries were from TFF-TU-977-2007 to TFF-TU-996-2007.
9. The extract of the delivery report is as under:

<table>
<thead>
<tr>
<th>Name</th>
<th>Bill No.</th>
<th>Phone no.</th>
<th>Delivery Address</th>
<th>Delivery date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-977-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-978-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-979-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-980-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-981-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-982-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-983-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-984-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-985-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-986-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-987-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-988-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-989-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-990-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-991-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-992-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-993-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-994-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-995-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-996-2007</td>
<td>91-20-65206029</td>
<td>6th Floor, Pride Senate</td>
<td>3-March-2008</td>
</tr>
</tbody>
</table>

10. I then queried the FF Order System using the “View Sales Reports” option. I found that only 16 dummy entries were reflected in the sales report.

11. The extract of the sales report is as under:

<table>
<thead>
<tr>
<th>Name</th>
<th>Bill No.</th>
<th>Product ID</th>
<th>Quantity</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-977-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-978-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-979-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-981-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-982-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-983-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-984-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-986-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-987-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-988-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-989-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-991-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-992-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-993-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-994-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-995-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TFF-TU-996-2007</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
</tr>
</tbody>
</table>

© 2008 Rohas Nagpal. All rights reserved.
- 35 -
12. The following bill numbers were not reflected in the sales report:
   a. TFF-TU-980-2007
   b. TFF-TU-985-2007
   c. TFF-TU-990-2007
   d. TFF-TU-995-2007

13. I then queried the FF Order System using the “View Customer Details” option. I found that the customer “Rohas Nagpal” was shown only 16 times in the customer details report.

14. I then viewed the report (using the View Report option) for the usage of the dummy card using the NFS Bank web interface at: http://www.asianlaws.org/students/current/cea/22/dc/index.htm

15. The extract of the usage report for the dummy credit card is as under:

<table>
<thead>
<tr>
<th>Name</th>
<th>Product ID</th>
<th>Quantity</th>
<th>Amount</th>
<th>Bill No.</th>
<th>Merchant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-977-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-978-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-979-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-980-2007</td>
<td>FLYINGFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-981-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-982-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-983-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-984-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-985-2007</td>
<td>FLYINGFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-986-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-987-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-988-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-989-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-990-2007</td>
<td>FLYINGFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-991-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-992-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-993-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-994-2007</td>
<td>FLYINFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-995-2007</td>
<td>FLYINGFLORIST</td>
</tr>
<tr>
<td>Rohas Nagpal</td>
<td>TU-01</td>
<td>10</td>
<td>1000</td>
<td>TFF-TU-996-2007</td>
<td>FLYINFLORIST</td>
</tr>
</tbody>
</table>
16. On analyzing the above report, it can be found that the Merchant for the 4 bill numbers missing from the sales report is FLYINGFLORIST.

17. On analyzing the above report, it can be found that the Merchant for the other 16 bill numbers (present in the sales report) is FLYINFLORIST.

18. It may be concluded that the FF Order System has a programming bug or flaw. This bug causes every 5th entry to be hidden from the Sales Report. This results in the management not getting to know about the sales from every 5th entry.

19. The bug does not hide every 5th entry from the delivery report.

20. The bug also ensures that the payment for every 5th entry goes to another merchant (FLYINGFLORIST) and not to the genuine merchant namely FLYINFLORIST.

21. The stock delivered for every 5th entry is put in as a part of the wasted or thrown away flowers.

22. I can safely conclude that the programming flaw / bug is not accidental but rather it has been deliberately put into the systems to carry out the fraud.
7. Digital Signature Fraud case

Pradeep Kumar is a senior programmer with Data64 LLC, an American software company that has offices in several countries. Pradeep is heading the team of programmers working on Project Medusa – a software development project that has been awarded to Data64 LLC by the Government of Zimblia.

On 2nd January, 2008 a scheduled internal penetration test was conducted on the computer systems being used for Project Medusa. The test revealed that most of the computers were infected with a Trojan program. Further investigation revealed that the Trojan spread through an infected Microsoft Word document (titled taxdetails.doc) that Pradeep had sent to all his team members. It was also discovered that the Trojan had stolen credit card information, bank account passwords and confidential source code from the infected computers. This stolen information had been uploaded to some FTP servers, all of which were now non-existent.

When questioned by the management, Pradeep admitted to having sent that document to all his team members. He stated that he had received an official email from the finance department asking him to download the document from https://finance.data64.com and to distribute the document to all his team members. The email had been deleted by Pradeep. Pradeep said that he trusted the document because the website that he downloaded it from was SSL protected and was part of the data64.com network.

The finance department claims that it had never sent such an email to Pradeep. They also clarified that https://finance.data64.com was never used by them. The IT department of Data64 also stated that https://finance.data64.com never existed.

The **primary objective of the investigation** is to ascertain who is responsible for infecting the systems and stealing the information and source code.

**Note:** The relevant evidence file for this case study is provided in the folder titled “Case 7” in the DVD accompanying this book.
Request for Service

RFS No. (Pl leave blank)  
IN-PNQ/01-08/086

Date  
5th January, 2008

Client name and address  
Manoj Kumar,  
Data64 LLC

Client’s authorised representative  
Name  Email  Phone  Fax  
Manoj Kumar  mk@data64.com  34221341  3423412

Background of the case  
As per details provided in the pages before this.

Details of computer(s), media etc  
SONY Laptop bearing serial number 12345678 that had been officially allotted to Pradeep Kumar.

Have the computer(s), media etc mentioned above been accessed / examined prior to being handed over to ASCL? If yes, give details.  
No

Services requested from ASCL  
To ascertain who is responsible for infecting the Data64 systems and stealing the information and source code.

For internal ASCL use only (Pl leave blank)  
Case recd on  
19th March 2008

Case recd by  
Rohas Nagpal

Referred by  
Manoj Kumar

Tax  Porn  Financial  Cyber  Priority  1  2  3  4  5  6  7  8  9  10

© 2008 Rohas Nagpal. All rights reserved. - 39 -
Investigation Report

1. I checked the Microsoft Word document titled “taxdetails.doc” for infections using VirusTotal.com

VirusTotal.com is a service that analyzes suspicious files and facilitates the quick detection of viruses, worms, Trojans, and all kinds of malware detected by antivirus engines.

VirusTotal.com is a free, independent service that uses multiple antivirus engines and features real-time automatic updates of virus signatures.

2. The results of the VirusTotal.com scan showed that the taxdetails.doc file was in reality a Trojan infected file named “taxdetails.doc.exe”. This file was infected with the CIA Trojan.

The CIA Trojan is a program that enables an attacker to get nearly complete control over an infected PC.
3. The file taxdetails.doc.exe described as under is stored in the CD ROM accompanying this investigation report.

File size: 125692 bytes
MD5: 9f0247316edd0d885efe1116fde5f56f
SHA1: 3466bee9e491e718a080264ac07386c958655aa4

4. I then checked for the https://finance.data64.com but the site did not exist. The IT department of Data64 also stated that https://finance.data64.com never existed.

5. On examining Pradeep’s computer using X-Ways Trace, it appeared that Pradeep had in fact visited https://finance.data64.com
6. I then examined the digital signature certificates stored on Pradeep's computer. I compared the certificates present on computers allotted to other Data64 employees with the certificates present on Pradeep's computer.

7. This examination showed three certificates that were not present on other Data64 computers. The first was a certificate issued by Data64 to Pooja Sharma. This certificate was stored in the "Other People" tab of the certificate store on Pradeep's computer.

<table>
<thead>
<tr>
<th>Issued To</th>
<th>Issued By</th>
<th>Expiration</th>
<th>Friendly Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pooja Sen</td>
<td>Data64 LLC</td>
<td>12/1/2008</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>Sameer Sen</td>
<td>Baltimore E2 by DST</td>
<td>7/7/2000</td>
<td>&lt;None&gt;</td>
</tr>
</tbody>
</table>

8. On being asked how he had obtained Pooja Sen's certificate, Mr. Pradeep said that he had been sent some documents from Pooja Sen of the Data64 LLC Human Resources Department. These documents had been digitally signed and hence he had obtained Pooja Sen’s certificate from her.

9. Enquiries with the Data64 LLC Human Resources Department showed that there was no employee named Pooja Sen.

10. I then examined the certificate in detail.
11. The subject of the certificate was

E = ps@data64.com
CN = Pooja Sen
OU = Finance
O = Data64 LLC
L = Pune
S = Maharashtra
C = IN

12. The certification path of this certificate is illustrated below:

13. From the above it is apparent that a root certifying authority named Global Root CA issued a certificate to an intermediary certifying authority named Data64, which in turn issued a certificate to Pooja Sen.

14. Further examination of the “certificate store” on Pradeep’s computer showed that a certificate issued by Global Root CA to Data64 was stored in the Intermediate Certification Authorities section. Additionally the certificate of Global Root CA was stored in the Trusted Root Certification Authorities section. This is illustrated below:
15. The IT department of Data64 stated that they had never applied
to Global Root CA for a digital signature certificate.

16. I then visited the Global Root CA (www.globalroot-ca.com)
website to ascertain its contact information. The email ID was
listed as info@globalroot-ca.com

17. I then used the ReadNotify.com email tracking service to send
tracking emails to info@globalroot-ca.com and ps@data64.com

18. The email sent to info@globalroot-ca.com was accessed but no
reply was received. The IP address from where the email was
accessed was ascertained from the ReadNotify report which is
illustrated below:

![ReadNotify Report]

19. With the help of the relevant Internet Service Provider it was
ascertained that the above IP address had been allotted to the
computer at the residence of Mr. Siddharth Kumar, who
incidentally was the System Administrator at Data64 LLC.

20. I then conducted a detailed examination of the computer at the
residence of Mr. Siddharth Kumar. The computer was running
Windows 2003 Server operating system and had certificate
services installed.

21. Examination of the certificate services showed that “Global Root
CA” had been installed as a standalone root certifying authority
and “Data64 LLC” had been installed as a standalone subordinate
certifying authority.
22. Examination of the certificate services also showed that the “Pooja Sen” certificate had been generated on the said computer. An SSL certificate in the name of finance.data64.com was also recovered from the computer.

23. From the above investigation it may be concluded that:

a. Siddharth Kumar used Windows 2003 Certificate Services on his personal computer to create “Global Root CA” as a standalone root certifying authority and “Data64 LLC” as standalone subordinate certifying authority under Global Root CA.

b. Siddharth Kumar then generated a digital signature certificate in the name of Pooja Sen.

c. Using social engineering (and maybe email spoofing), Siddharth Kumar convinced Pradeep to install the Pooja Sen certificate on his computer. When Pradeep did this, automatically the following happened:

   i. Global Root CA certificate got installed in the Trusted Root Certification Authorities section of his certificate store.

   ii. Fake Data64 LLC certificate got installed in the Intermediate Certification Authorities section of his certificate store.

d. Siddharth Kumar then set up the fake https://finance.data64.com website on the Data64 LLC internal network. This website used the fake Data64 SSL certificate generated by Siddharth Kumar.

e. Siddharth Kumar then sent a spoofed email to Pradeep, asking him to download the taxdetails.doc file from https://finance.data64.com

f. When Pradeep visited the fake https://finance.data64.com site, he did not receive any Certificate warning for the fake Data64 LLC SSL certificate. This is because the fake certificate had been issued by “Global Root CA” and the certificate of “Global Root CA” was already installed in the Trusted Root Certification Authorities section of Pradeep’s certificate store.
Annex 1: Evidence in computer devices

This section provides a read reference guide to the important computer files and devices and the evidence that they can contain.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description &amp; uses</th>
<th>Potential Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard disk</td>
<td>This is the primary data storage device of the suspect computer.</td>
<td><strong>Computer-Created Files</strong>&lt;br&gt;System files&lt;br&gt;Swap files&lt;br&gt;Temporary files&lt;br&gt;Backup files&lt;br&gt;Log files&lt;br&gt;Configuration files&lt;br&gt;Printer spool files&lt;br&gt;Cookies&lt;br&gt;Hidden files&lt;br&gt;History files&lt;br&gt;<strong>Other evidence</strong>&lt;br&gt;Computer date &amp; time&lt;br&gt;BIOS and OS password&lt;br&gt;Deleted files&lt;br&gt;Unallocated space&lt;br&gt;Slack space&lt;br&gt;Free space&lt;br&gt;Metadata</td>
</tr>
<tr>
<td>Storage devices</td>
<td>This includes the hard disk(s) of the suspect computer and&lt;br&gt;1. external disks,&lt;br&gt;2. floppies,&lt;br&gt;3. CDs,&lt;br&gt;4. DVDs,&lt;br&gt;5. USB disks etc.</td>
<td><strong>User-Created Files</strong>&lt;br&gt;E-mails &amp; email archives&lt;br&gt;Audio / video files&lt;br&gt;Image files.&lt;br&gt;Address books&lt;br&gt;Calendar entries&lt;br&gt;Internet bookmarks&lt;br&gt;Favourite sites&lt;br&gt;Database files&lt;br&gt;Spreadsheet files.&lt;br&gt;Document / text files.&lt;br&gt;Compressed files&lt;br&gt;<strong>User-Protected Files</strong>&lt;br&gt;Encrypted files&lt;br&gt;Password-protected files&lt;br&gt;Steganographic files&lt;br&gt;Misnamed files&lt;br&gt;Hidden &amp; system files</td>
</tr>
<tr>
<td>Central Processing</td>
<td>This is the brain of the computer and processes</td>
<td>The CPU is evidence in case of theft or</td>
</tr>
<tr>
<td>Unit</td>
<td>data.</td>
<td>counterfeiting</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RAM</td>
<td>Stores user’s programs and data while the computer is powered on.</td>
<td>Information such as passwords and encryption keys can be obtained while the computer is powered on. Otherwise the RAM itself may be evidence in case of theft or counterfeiting.</td>
</tr>
<tr>
<td></td>
<td>The information is lost when the computer is powered off / shutdown.</td>
<td></td>
</tr>
<tr>
<td>Smart card</td>
<td>This contains a microprocessor capable of storing</td>
<td>Since it is primarily used for access control, it contains important identification and / or authentication information.</td>
</tr>
<tr>
<td></td>
<td>1. encryption keys</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. passwords,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. monetary value,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. digital certificate etc.</td>
<td></td>
</tr>
<tr>
<td>Dongle</td>
<td>It is a small device that plugs into a computer port.</td>
<td>Since it is primarily used for access control, it contains important identification and / or authentication information.</td>
</tr>
<tr>
<td></td>
<td>It is capable of storing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. encryption keys</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. passwords,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. monetary value,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. digital certificate etc.</td>
<td></td>
</tr>
<tr>
<td>Biometric scanner</td>
<td>It is a device, connected to a computer, that recognizes physical characteristics of a person such as fingerprint, retina, voice, face etc.</td>
<td>Since it is primarily used for access control, it contains important identification and / or authentication information.</td>
</tr>
<tr>
<td>Digital Cameras</td>
<td>They capture images (and sometimes videos) in a digital format that can easily be transferred to computer.</td>
<td>- Photos</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Video</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Sound</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Time stamps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Removable memory card</td>
</tr>
<tr>
<td>Personal Digital</td>
<td>PDAs are small devices that have computing as well as telecommunication features.</td>
<td>User-Created Files</td>
</tr>
<tr>
<td>Assistants</td>
<td></td>
<td>E-mails &amp; email archives</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Audio / video / image files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Address books</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Calendar entries</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internet bookmarks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Favourite sites</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spreadsheet files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Document / text files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Compressed files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User-Protected Files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encrypted files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password-protected files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Steganographic files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Misnamed files</td>
</tr>
</tbody>
</table>
Annex 2: Investigation Guidelines

This section serves as a ready reference guide for cyber crime investigators.

First the various scenarios are covered.

For a detailed discussion on the various cyber crimes, please refer to the ASCL publication titled “Understanding Hackers and Cyber Criminals”.

Then the applicable law and legal liabilities are covered.

For a detailed discussion on the legal provisions, please refer to the ASCL publication titled “Cyber Crime & Digital Evidence – Indian Perspective”.

Then the modus operandi usually followed by the criminals is discussed.

Finally the investigation guidelines for cyber crime investigators are discussed.

For real world case studies on investigation of cyber crimes, please refer to the ASCL publication titled “Case Studies on Cyber Crime Investigation”.
1. Orkut Fake Profile cases

Orkut.com is a very popular online community and social networking website. Orkut users can search for and interact with people who share the same hobbies and interests. They can create and join a wide variety of online communities. The profiles of Orkut members are publicly viewable.

The scenarios

Misuse of Orkut is a very common case nowadays. The likely scenarios are:

1. A fake profile of a woman is created on Orkut. The profile displays her correct name and contact information (such as address, residential phone number, cell phone number etc). Sometimes it even has her photograph.

   The problem is that the profile describes her as a prostitute or a woman of “easy virtue” who wants to have sex with anyone. Other Orkut members see this profile and start calling her at all hours of the day asking for sexual favours. This leads to a lot of harassment for the victim and also defames her in the society.

2. An online hate community is created. This community displays objectionable information against a particular country, religious or ethnic group or even against national leaders and historical figures.

3. A fake profile of a man is created on Orkut. The profile contains defamatory information about the victim (such as his alleged sexual weakness, alleged immoral character etc)

The law

Scenario 1: Section 67 of Information Technology Act and section 509 of the Indian Penal Code

Scenario 2: Section 153A and 153B of Indian Penal Code

Scenario 3: Section 500 of Indian Penal Code

Who is liable?

Scenario 1: Directors of Orkut as well as all those who create and update the fake profile.

Scenario 2: Same as Scenario 1.
Scenario 3: Same as Scenario 1.

The motive

Scenario 1: Jealousy or revenge (e.g. the victim may have rejected the advances made by the suspect)

Scenario 2: Desire to cause racial hatred (e.g. Pakistani citizens creating an anti-India online community)

Scenario 3: Hatred (e.g. a school student who has been failed may victimize his teachers).

Modus Operandi

1. The suspect would create a free Gmail account using a fictitious name.

2. The email ID chosen by him would be unrelated to his real identity.

3. The suspect would then login to Orkut.com and create the offensive profile.

Investigation Guidelines

If the victim has a reasonable suspicion about the identity of the suspect, then the police should question the suspect. Conventional investigation techniques can be very effective as the suspects are usually not hardened or shrewd criminals.

The cooperation of Orkut officials is required to obtain the IP addresses used to:
1. create and update the offensive profile,
2. create and access the relevant Google account.

Once these IP addresses are obtained, a WHOIS search will reveal the Internet Service Provider (ISP). The ISP can provide the customer contact information. The suspect’s computer can be examined using X-Ways Trace and Winhex and all relevant evidence can be extracted.

Sometimes the investigation may lead to a cyber café or other public computer. In this situation conventional investigation can be used (e.g.
photographs of the suspects can be shown to the cyber café manager).

2. Email account hacking

Emails are increasingly being used for social interaction, business communication and online transactions. Most email account holders do not take basic precautions to protect their email account passwords.

Cases of theft of email passwords and subsequent misuse of email accounts are becoming very common.

The scenarios

The likely scenarios are:

1. The victim’s email account password is stolen and the account is then misused for sending out malicious code (virus, worm, Trojan etc) to people in the victim’s address book. The recipients of these viruses believe that the email is coming from a known person and run the attachments. This infects their computers with the malicious code.

2. The victim’s email account password is stolen and the hacker tries to extort money from the victim. The victim is threatened that if he does not pay the money, the information contained in the emails will be misused.

3. The victim’s email account password is stolen and obscene emails are sent to people in the victim's address book.

The law

Scenario 1: Sections 43 and 66 of Information Technology Act

Scenario 2: Sections 43 and 66 of Information Technology Act and section 384 of Indian Penal Code

Scenario 3: Sections 43, 66 and 67 of Information Technology Act and section 509 of the Indian Penal Code

Who is liable?

Scenario 1: Persons who have stolen the email account password and who are misusing the email account.
Scenario 2: Persons who have stolen the email account password and who are threatening to misuse it.

Scenario 3: Persons who have stolen the email account password and who are misusing the email account.

The motive

Scenario 1: Corporate Espionage, perverse pleasure in being able to destroy valuable information belonging to strangers etc

Scenario 2: Illegal financial gain

Scenario 3: Revenge, jealousy, hatred

Modus Operandi

1. The suspect would install keyloggers in public computers (such as cyber cafes, airport lounges etc) or the computers of the victim.

2. Unsuspecting victims would login to their email accounts using these infected computers.

3. The passwords of the victim’s email accounts would be emailed to the suspect.

Investigation Guidelines

If the victim has a reasonable suspicion about the identity of the suspect, then the police should question the suspect. Conventional investigation techniques can be very effective as the suspects are usually not hardened or shrewd criminals.

The cooperation of the email service provider is required to obtain the IP addresses used to access the account after the date of hacking. Once these IP addresses are obtained, a WHOIS search will reveal the Internet Service Provider (ISP). The ISP can provide the customer contact information. The suspect’s computer can be examined using X-Ways Trace and Winhex and all relevant evidence can be extracted.

Sometimes the investigation may lead to a cyber café or other public computer. In this situation conventional investigation can be used (e.g.
photographs of the suspects can be shown to the cyber café manager).

3. Credit card fraud
Credit cards are commonly being used for online booking of airline and railway tickets and for other ecommerce transactions.

Although most of the ecommerce websites have implemented strong security measures (such as SSL, secure web servers etc), the instances of credit card frauds are increasing.

The scenario
The victim’s credit card information is stolen and misused for making online purchases (e.g. airline tickets, software, subscription to pornographic websites, online gambling transactions etc).

The law
Sections 43 and 66 of Information Technology Act and section 420 of Indian Penal Code

Who is liable?
All persons who have stolen the credit card information as well as those who have misused it.

The motive
Illegal financial gain

Modus Operandi

Scenario 1: The suspect would install keyloggers in public computers (such as cyber cafes, airport lounges etc) or the computers of the victim. Unsuspecting victims would use these infected computers to make online transactions. The credit card information of the victim would be emailed to the suspect.

Scenario 2: Petrol pump attendants, workers at retail outlets, hotel waiters etc note down information of the credit cards used for making payment at these establishments. This information is sold to criminal gangs that misuse it for online frauds.

Investigation Guidelines

The websites, where the credit cards are misused, should be examined carefully. Sometimes criminals set up bogus ecommerce websites to misuse the credit card information.
The cooperation of the website operators is required to obtain the IP addresses used to make the fraudulent transactions. Once these IP addresses are obtained, a WHOIS search will reveal the Internet Service Provider.

The ISP can provide the customer contact information. The suspect's computer can be examined using X-Ways Trace and Winhex and all relevant evidence can be extracted.

Sometimes the investigation may lead to a cyber café or other public computer. In this situation conventional investigation can be used (e.g. photographs of the suspects can be shown to the cyber café manager). In case physical goods are delivered pursuant to the fraud, the address should be investigated.
4. Online share trading fraud

With the advent of dematerialization of shares in India, it has become mandatory for investors to have demat accounts. In most cases an online banking account is linked with the share trading account. Although most of the online share trading and online banking websites have implemented strong security measures (such as SSL, secure web servers etc), the instances of online share trading frauds are increasing.

The scenario

Scenario 1: The victim’s account passwords are stolen and his accounts are misused for making fraudulent bank transfers.

Scenario 2: The victim’s account passwords are stolen and his share trading accounts are misused for making unauthorised transactions that result in the victim making losses.

The law

Scenario 1: Sections 43 and 66 of Information Technology Act and section 420 of Indian Penal Code

Scenario 2: Sections 43 and 66 of Information Technology Act and section 426 of Indian Penal Code

Who is liable?

Scenario 1: All persons who have stolen the account information as well as those who have misused it.

Scenario 2: All persons who have stolen the account information as well as those who have misused it.

The motive

Scenario 1: Illegal financial gain

Scenario 2: Revenge, jealousy, hatred

Modus Operandi

Scenario 1: The suspect would install keyloggers in public computers (such as cyber cafes, airport lounges etc) or the computers of the victim. Unsuspecting victims would use these infected computers to login to their online banking and share trading accounts. The passwords and other information of the victim would be emailed to the suspect.
Scenario 2: Same as scenario 1.

Investigation Guidelines

The cooperation of the online service providers is required to obtain the IP addresses used to make the fraudulent transactions. Once these IP addresses are obtained, a WHOIS search will reveal the Internet Service Provider (ISP).

The ISP can provide the customer contact information. The suspect's computer can be examined using X-Ways Trace and Winhex and all relevant evidence can be extracted.

Sometimes the investigation may lead to a cyber café or other public computer. In this situation conventional investigation can be used (e.g. photographs of the suspects can be shown to the cyber café manager).

In case of fraudulent bank transfers, the bank officials can provide information provided to open the suspect bank account. This information can lead to the arrest of the suspect.
5. Tax evasion and money laundering

Many unscrupulous businessmen and money launderers (havala operators) are using virtual as well as physical storage media for hiding information and records of their illicit business.

The scenario

Scenario 1: The suspect uses physical storage media for hiding the information e.g. hard drives, floppies, USB drives, mobile phone memory cards, digital camera memory cards, CD ROMs, DVD ROMs, iPods etc.

Scenario 2: The suspect uses virtual storage media for hiding the information e.g. email accounts, online briefcases, FTP sites, Gspace etc.

The law

Scenario 1: Depending upon the case, provisions of the Income Tax Act and Prevention of Money Laundering Act will apply.

Scenario 2: Depending upon the case, provisions of the Income Tax Act and Prevention of Money Laundering Act will apply.

Who is liable?

Scenario 1: The person who hides the information.

Scenario 2: The person who hides the information. If the operators of the virtual storage facility do not cooperate in the investigation, then they also become liable.

The motive

Scenario 1: Illegal financial gain

Scenario 2: Illegal financial gain

Modus Operandi

Scenario 1: The suspect would purchase small storage devices with large data storage capacities.

Scenario 2: The suspect would open free or paid accounts with online storage providers.
Investigation Guidelines

**Scenario 1:** During the raid, the investigators must carefully identify and seize all storage devices. Sometimes it is very difficult to identify some storage devices e.g. USB data storage devices that look like calculators, pens, toys etc.

Investigators must remember that iPods, digital cameras and even mobile phones can be used to hide information.

The suspect’s data storage devices can be examined using Winhex and all relevant evidence can be extracted. Password cracking tools can be used in case the suspect has password protected the devices or his computer.

**Scenario 2:** Analysis of the suspect’s internet usage will reveal clues as to the online storage methods being used by him.

The suspect’s computer can be examined using X-Ways Trace and Winhex and all relevant evidence can be extracted.

The cooperation of the online storage providers may be required to access the hidden information as well as obtain conclusive evidence.
6. Source code theft

Computer source code is the most important asset of software companies. Simply put, source code is the programming instructions that are compiled into the executable files that are sold by the software development companies. As is expected, most source code thefts take place in software companies. Some cases are also reported in banks, manufacturing companies and other organisations who get original software developed for their use.

The scenario

**Scenario 1:** The suspect (usually an employee of the victim) steals the source code and sells it to a business rival of the victim.

**Scenario 2:** The suspect (usually an employee of the victim) steals the source code and uses it as a base to make and sell his own version of the software.

The law

**Scenario 1:** Sections 43, 65 and 66 of the Information Technology Act, section 63 of the Copyright Act.

**Scenario 2:** Sections 43, 65 and 66 of the Information Technology Act, section 63 of the Copyright Act.

Who is liable?

**Scenario 1:** The persons who steal the source code as well as the persons who purchase the stolen source code.

**Scenario 2:** The persons who steal the source code.

The motive

**Scenario 1:** Illegal financial gain

**Scenario 2:** Illegal financial gain

Modus Operandi

**Scenario 1:** If the suspect is an employee of the victim, he would usually have direct or indirect access to the source code. He would steal a copy of the source code and hide it using a virtual or physical storage device.
If the suspect is not an employee of the victim, he would hack into the victim’s servers to steal the source code. Or he would use social engineering to get unauthorised access to the code. He would then contact potential buyers to make the sale.

**Scenario 2:** If the suspect is an employee of the victim, he would usually have direct or indirect access to the source code. He would steal a copy of the source code and hide it using a virtual or physical storage device.

If the suspect is not an employee of the victim, he would hack into the victim’s servers to steal the source code. Or he would use social engineering to get unauthorised access to the code. He would then modify the source code (either himself or in association with other programmers) and launch his own software.

**Investigation Guidelines**

**Scenario 1:** The victim usually has a strong suspicion on the identity of the company who has purchased the stolen source code. The victim also may have a strong suspicion on who may have stolen the source code.

Cyber investigation such as analysis of the logs of the hacked computers, forensic examination of the computers and data storage devices of the suspects etc can reveal a lot of evidence. During the raid on the suspects, the investigators must carefully identify and seize all storage devices.

Sometimes it is very difficult to identify some storage devices e.g. USB data storage devices that look like calculators, pens, toys etc. Investigators must remember that iPods, digital cameras and even mobile phones can be used to hide information. The suspect’s data storage devices can be examined using Winhex and all relevant evidence can be extracted. Password cracking tools can be used in case the suspect has password protected the devices or his computer.

The bank statements of the suspects can also reveal clues as to the money received for the stolen source code.

**Scenario 2:** Same as scenario 1
7. Theft of confidential information

Most business organisations store their sensitive information in computer systems. This information is targeted by rivals, criminals and sometimes disgruntled employees.

The scenario

**Scenario 1:** A business rival obtains the information (e.g. tender quotations, business plans etc) using hacking or social engineering. He then uses the information for the benefit of his own business (e.g. quoting lower rates for the tender etc).

**Scenario 2:** A criminal obtains the information by hacking or social engineering and threatens to make the information public unless the victim pays him some money.

**Scenario 3:** A disgruntled employee steals the information and mass mails it to the victims rivals and also posts it to numerous websites and newsgroups.

The law

**Scenario 1:** Sections 43 and 66 of the Information Technology Act, section 426 of Indian Penal Code.

**Scenario 2:** Sections 43 and 66 of the Information Technology Act, section 384 of Indian Penal Code.

**Scenario 3:** Sections 43 and 66 of the Information Technology Act, section 426 of Indian Penal Code.

Who is liable?

**Scenario 1:** The persons who steal the information as well as the persons who misuse the stolen information.

**Scenario 2:** The persons who steal the information as well as the persons who threaten the victim and extort money.

**Scenario 3:** The disgruntled employee as well as the persons who help him in stealing and distributing the information.
The motive

**Scenario 1:** Illegal financial gain

**Scenario 2:** Illegal financial gain

**Scenario 3:** Revenge

**Modus Operandi**

**Scenario 1:** The suspect could hire a skilled hacker to break into the victim systems. The hacker could also use social engineering techniques

**Illustration:**
A very good looking woman went to meet the system administrator (sysadmin) of a large company. She interviewed the sysadmin for a “magazine article”.

During the interview she flirted a lot with the sysadmin and while leaving she “accidentally” left her pen drive at the sysadmin’s room.

The sysadmin accessed the pen drive and saw that it contained many photographs of the lady. He did not realise that the photographs were Trojanized!

Once the Trojan was in place, a lot of sensitive information was stolen very easily.

**Illustration:**
The sysadmin of a large manufacturing company received a beautifully packed CD ROM containing “security updates” from the company that developed the operating system that ran his company’s servers.

He installed the “updates” which in reality was Trojanized software. For 3 years after that a lot of confidential information was stolen from the company’s systems!
**Scenario 2:** Same as scenario 1.

**Scenario 3:** The disgruntled employee would usually have direct or indirect access to the information. He can use his personal computer or a cyber café to spread the information.

**Investigation Guidelines**

**Scenario 1:** The victim usually has a strong suspicion on the identity of the suspect who has stolen the information.

Cyber investigation such as analysis of the logs of the hacked computers, forensic examination of the computers and data storage devices of the suspects etc can reveal a lot of evidence. During the raid on the suspects, the investigators must carefully identify and seize all storage devices.

Sometimes it is very difficult to identify some storage devices e.g. USB data storage devices that look like calculators, pens, toys etc. Investigators must remember that iPods, digital cameras and even mobile phones can be used to hide information.

The suspect’s data storage devices can be examined using Winhex and all relevant evidence can be extracted. Password cracking tools can be used in case the suspect has password protected the devices or his computer.

**Scenario 2:** Same as scenario 1

**Scenario 3:** Same as scenario 1. Additionally, analysis of the suspect’s internet usage will reveal clues as to the online storage methods being used by him.

The suspect’s computer can be examined using X-Ways Trace and Winhex and all relevant evidence can be extracted.
8. Software Piracy

Many people do not consider software piracy to be theft. They would never steal a rupee from someone but would not think twice before using pirated software. There is a common perception amongst normal computer users to not consider software as “property”.

This has led to software piracy becoming a flourishing business.

The scenario

**Scenario 1:** The software pirate sells the pirated software in physical media (usually CD ROMs) through a close network of dealers.

**Scenario 2:** The software pirate sells the pirated software through electronic downloads through websites, bulletin boards, newsgroups, spam emails etc.

The law

**Scenario 1:** Sections 43 and 66 of the Information Technology Act, section 63 of Copyright Act.

**Scenario 2:** Sections 43 and 66 of the Information Technology Act, section 63 of Copyright Act.

Who is liable?

**Scenario 1:** The software pirate as well as the persons who buy the pirated software from him.

**Scenario 2:** The software pirate as well as the persons who buy the pirated software from him.

The motive

**Scenario 1:** Illegal financial gain

**Scenario 2:** Illegal financial gain

Modus Operandi

**Scenario 1:** The suspect uses high speed CD duplication equipment to create multiple copies of the pirated software. This software is sold through a network of computer hardware and software vendors.

**Scenario 2:** The suspect registers a domain name using a fictitious name and then hosts his website using a service provider that is based in a country that does not have cyber laws. Such service providers do not divulge client information to law enforcement officials of other countries.
Investigation Guidelines

**Scenario 1:** Conventional investigation methods can be used to identify the suspects and gather all relevant evidence.

**Scenario 2:** Tracing the website IP address is usually futile in such cases. One method of investigation is to email the contact persons operating the websites. These emails can be tracked to identify where they are being accessed from. If they are accessed from a country where cyber laws are enforced then the investigation can continue. Otherwise it can be discontinued.

In case the suspect is traced from his IP address, then forensic examination of his computers and data storage devices can reveal a lot of evidence.

During the raid on the suspects, the investigators must carefully identify and seize all storage devices. Sometimes it is very difficult to identify some storage devices e.g. USB data storage devices that look like calculators, pens, toys etc. Investigators must remember that iPods, digital cameras and even mobile phones can be used to hide information.

The suspect's data storage devices can be examined using Winhex and all relevant evidence can be extracted. Password cracking tools can be used in case the suspect has password protected the devices or his computer.

Additionally, analysis of the suspect’s internet usage will reveal clues as to the websites being hosted by him.
9. Music Piracy

Many people do not consider music piracy to be theft. They would never steal a rupee from someone but would not think twice before buying or using pirated music. There is a common perception amongst people users to not consider music as “property”. There is a huge business in music piracy. Thousands of unscrupulous businessmen sell pirated music at throw away prices.

**The scenario**

**Scenario 1:** The music pirate sells the pirated music in physical media (usually CD ROMs) through a close network of dealers.

**Scenario 2:** The music pirate sells the pirated music through electronic downloads through websites, bulletin boards, newsgroups, spam emails etc.

**The law**

**Scenario 1:** Sections 43 and 66 of the Information Technology Act, section 63 of Copyright Act.

**Scenario 2:** Sections 43 and 66 of the Information Technology Act, section 63 of Copyright Act.

**Who is liable?**

**Scenario 1:** The music pirate as well as the persons who buy the pirated software from him.

**Scenario 2:** The music pirate as well as the persons who buy the pirated software from him.

**The motive**

**Scenario 1:** Illegal financial gain

**Scenario 2:** Illegal financial gain

**Modus Operandi**

**Scenario 1:** The suspect uses high speed CD duplication equipment to create multiple copies of the pirated music. This music is sold through a network of dealers.

**Scenario 2:** The suspect registers a domain name using a fictitious name and then hosts his website using a service provider that is based in a country that does not have cyber laws. Such service providers do not divulge client information to law enforcement officials of other countries.
Investigation Guidelines

**Scenario 1:** Conventional investigation methods can be used to identify the suspects and gather all relevant evidence.

**Scenario 1:** Tracing the website IP address is usually futile in such cases. One method of investigation is to email the contact persons operating the websites.

These emails can be tracked to identify where they are being accessed from. If they are accessed from a country where cyber laws are enforced then the investigation can continue. Otherwise it can be discontinued.

In case the suspect is traced from his IP address, then forensic examination of his computers and data storage devices can reveal a lot of evidence.

During the raid on the suspects, the investigators must carefully identify and seize all storage devices. Sometimes it is very difficult to identify some storage devices e.g. USB data storage devices that look like calculators, pens, toys etc. Investigators must remember that iPods, digital cameras and even mobile phones can be used to hide information.

The suspect’s data storage devices can be examined using Winhex and all relevant evidence can be extracted. Password cracking tools can be used in case the suspect has password protected the devices or his computer.

Additionally, analysis of the suspect’s internet usage using Winhex and X-Ways Trace will reveal clues as to the websites being hosted by him.
10. Email scams

Emails are fast emerging as one of the most common methods of communication in the modern world. As can be expected, criminals are also using emails extensively for their illicit activities.

The scenario

In the first step, the suspect convinces the victim that the victim is going to get a lot of money (by way of winning a lottery or from a corrupt African bureaucrat who wants to transfer his ill gotten gains out of his home country). In order to convince the victim, the suspect sends emails (some having official looking documents as attachments).

Once the victim believes this story, the suspect asks for a small fee to cover legal expenses or courier charges. If the victim pays up the money, the suspect stops all contact.

The law

Sections 420 of Indian Penal Code

Who is liable?

The sender of the email.

The motive

Illegal financial gain

Modus Operandi

The suspect creates email accounts in fictitious names and sends out millions of fraudulent emails using powerful spam software.

Investigation Guidelines

First, analyse the email headers as well as track where the suspect email accounts are being accessed from.

In almost all these cases, the suspects are located in countries where cyber laws are not enforced (e.g. Nigeria). In such cases the investigations are futile.

If however the emails are accessed from India, or another country then the suspect can be tracked from his IP address. The suspect's computer can
be examined using X-Ways Trace and Winhex and all relevant evidence can be extracted.

Sometimes the investigation may lead to a cyber café or other public computer. In this situation conventional investigation can be used (e.g. photographs of the suspects can be shown to the cyber café manager).

In case the victim has transferred the money to a bank account in India, then the bank officials can provide information about the customer holding that account. Conventional investigation can be used to track and apprehend the suspect.
11. Phishing

With the tremendous increase in the use of online banking, online share trading and ecommerce, there has been a corresponding growth in the incidents of phishing being used to carry out financial frauds.

Phishing involves fraudulently acquiring sensitive information (e.g. passwords, credit card details etc) by masquerading as a trusted entity.

The scenario

**Scenario 1:** The victim receives an email that appears to have been sent from his bank. The email urges the victim to click on the link in the email. When the victim does so, he is taken to “a secure page on the bank’s website”.

The victim believes the web page to be authentic and he enters his username, password and other information. In reality, the website is a fake and the victim’s information is stolen and misused.

The law

Sections 43 and 66 of Information Technology Act and sections 419, 420 and 468 of Indian Penal Code

Who is liable?

All persons involved in creating and sending the fraudulent emails and creating and maintaining the fake website. The persons who misuse the stolen or “phished” information are also liable.

The motive

Illegal financial gain

Modus Operandi

The suspect registers a domain name using fictitious details. The domain name is usually such that can be misused for spoofing e.g. Noodle Bank has its website at [www.noodle.com](http://www.noodle.com) The suspects can target Noodle customers using a domain name like [www.noodle-bank-customerlogin.com](http://www.noodle-bank-customerlogin.com)

The suspect then sends spoofed emails to the victims. e.g. the emails may appear to come from info@noodle.com

The fake website is designed to look exactly like the original website.
Investigation Guidelines

Most phishing operations are carried out from countries where cyber laws are not enforced. In such cases, the investigation may not lead to the suspects.

In case the “phish” can be traced to India or some other country where cyber laws are enforced, then the suspects can be traced using the IP address.

The suspect's computer can be examined using X-Ways Trace and Winhex and all relevant evidence can be extracted.

Sometimes the investigation may lead to a cyber café or other public computer. In this situation conventional investigation can be used (e.g. photographs of the suspects can be shown to the cyber café manager).

In case of fraudulent bank transfers, the bank officials can provide information provided to open the suspect bank account. This information can lead to the arrest of the suspect.
12. Cyber Pornography

Cyber pornography is believed to one of the largest businesses on the Internet today. The millions of pornographic websites that flourish on the Internet are testimony to this. While pornography per se is not illegal in many countries, child pornography is strictly illegal in most nations today.

Cyber pornography includes pornographic websites, pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc).

The scenario

The suspect accepts online payments and allows paying customers to view / download pornographic pictures, videos etc from his website.

The law

Section 67 of Information Technology Act

Who is liable?

The persons who create and maintain the pornographic websites are liable. In some cases cyber café owners and managers may also be liable in case they knowingly allow their customers to access the pornographic websites.

The motive

Illegal financial gain

Modus Operandi

The suspect registers a domain name using fictitious details and hosts a website on a server located in a country where cyber pornography is not illegal.

The suspect accepts online payments and allows paying customers to view / download pornographic pictures, videos etc from his website.

Investigation Guidelines

Most pornographic websites are hosted in countries where cyber pornography is not illegal. In case the website (or its email IDs) can be traced to India or some other country where pornography is illegal, then the suspects can be traced using the IP address.
The suspect’s computer can be examined using X-Ways Trace and Winhex and all relevant evidence can be extracted.

Sometimes the investigation may lead to a cyber café or other public computer. In this situation conventional investigation can be used (e.g. photographs of the suspects can be shown to the cyber café manager).

In case of payments made by customers into a bank in India, the bank officials can provide information provided to open the suspect bank account. This information can lead to the arrest of the suspect.
13. Online sale of illegal articles

It is becoming increasingly common to find cases where illegal sale of narcotics drugs, weapons, wildlife etc. is being facilitated by the Internet. Information about the availability of the products for sale is being posted on auction websites, bulletin boards etc.

The scenario

The suspect posts information about the illegal sale that he seeks to make. Potential customers can contact the seller using the email IDs provided.

If the buyer and seller trust each other after their email and / or telephonic conversation, the actual transaction can be concluded. In most such cases the buyer and seller will meet face to face at the time of the final transaction.

Illustration:

In March 2007, the Pune rural police cracked down on an illegal rave party and arrested hundreds of illegal drug users. The social networking site Orkut.com is believed to be one of the mode of communication for gathering people for the illegal “drug” party.

The law

Depending upon the illegal items being transacted in, provisions of the Narcotic Drugs and Psychotropic Substances Act, Arms Act, Indian Penal Code, Wildlife related laws etc may apply.

Who is liable?

The persons who buy and sell these items are liable.

The motive

Illegal financial gain

Modus Operandi

The suspect creates an email ID using fictitious details. He then posts messages, about the illegal products, in various chat rooms, bulletin boards, newsgroups etc.

Potential customers can contact the seller using the email IDs provided.
If the buyer and seller trust each other after their email and/or telephonic conversation, the actual transaction can be concluded. In most such cases the buyer and seller will meet face to face at the time of the final transaction.

**Investigation Guidelines**

The first step is usually to track where the suspect email accounts are being accessed from. In case these accounts are being accessed from India, the suspect can be traced using the IP address.

The suspect's computer can be examined using X-Ways Trace and Winhex and all relevant evidence can be extracted.

Sometimes the investigation may lead to a cyber café or other public computer. In this situation conventional investigation can be used (e.g. photographs of the suspects can be shown to the cyber café manager).

Conventional investigation can lead to recovery of the illegal items.
14. Use of internet and computers by terrorists

Many terrorists are using virtual as well as physical storage media for hiding information and records of their illicit business. They also use emails and chat rooms to communicate with their counterparts around the globe.

**The scenario**

The suspects carry laptops wherein information relating to their activities are stored in encrypted and password protected form.

They also create email accounts using fictitious details. In many cases one email account is shared by many people. E.g. one terrorist composes an email and saves it in the draft folder.

Another terrorist logs into the same account from another city / country and reads the saved email. He then composes his reply and saves it in the draft folder.

The emails are not actually sent. This makes email tracking and tracing impossible.

The terrorist also use physical storage media for hiding the information e.g. hard drives, floppies, USB drives, mobile phone memory cards, digital camera memory cards, CD ROMs, DVD ROMs, iPods etc.

They also use virtual storage media for hiding the information e.g. email accounts, online briefcases, FTP sites, Gspace etc.

**The law**

Terrorist are covered by the conventional laws such as Indian Penal Code and special legislation relating to terrorism.

**Who is liable?**

Terrorist as well as those who help them to protect their information are liable. If email service providers do not assist the law enforcement personnel in the investigation then they are also legally liable.

**The motive**

Keeping terrorism related information confidential. Secure communication amongst terrorist group members.
Modus Operandi

The terrorists purchase small storage devices with large data storage capacities. They also purchase and use encryption software. The terrorists may also use free or paid accounts with online storage providers.

Investigation Guidelines

Scenario 1: During the raid, the investigators must carefully identify and seize all storage devices. Sometimes it is very difficult to identify some storage devices e.g. USB data storage devices that look like calculators, pens, toys etc.

Investigators must remember that iPods, digital cameras and even mobile phones can be used to hide information.

The suspect’s data storage devices can be examined using Winhex and all relevant evidence can be extracted. Password cracking tools can be used in case the suspect has password protected the devices or his computer.

Analysis of the suspect’s internet usage will reveal clues as to the online storage methods being used by him.

The suspect’s computer can be examined using X-Ways Trace and Winhex and all relevant evidence can be extracted.

The cooperation of the online storage providers may be required to access the hidden information as well as obtain conclusive evidence.
15. Virus attacks

Computer viruses are malicious programs that destroy electronic information. As the world is increasingly becoming networked, the threat and damage caused by viruses is growing by leaps and bounds.

The scenario

**Scenario 1:** The virus is a general “in the wild” virus. This means that it is spreading all over the world and is not targeted at any specific organisation.

**Scenario 2:** The virus targets a particular organisation. This type of a virus is not known to the anti-virus companies as it is a new virus created specifically to target a particular organisation.

The law

**Scenario 1:** Sections 43 and 66 of Information Technology Act and section 426 of Indian Penal Code

**Scenario 2:** Sections 43 and 66 of Information Technology Act and section 426 of Indian Penal Code

Who is liable?

**Scenario 1:** The creator of the virus

**Scenario 2:** The creator of the virus as well as the buyer who purchases the virus (usually to target his business rivals)

The motive

**Scenario 1:** Thrill and a perverse pleasure in destroying data belonging to strangers

**Scenario 2:** Illegal financial gain, revenge, business rivalry

Modus Operandi

**Scenario 1:** A highly skilled programmer creates a new type or strain of virus and releases it on the Internet so that it can spread all over the world.

Being a new virus, it goes undetected by many anti-virus software and hence is able to spread all over the world and cause a lot of damage. Anti-virus companies are usually able to find a solution within 8 to 48 hours.
Scenario 2: A highly skilled programmer creates a new type or strain of virus. He does not release it on the Internet. Instead he sells it for a huge amount of money.

The buyer uses the virus to target his rival company. Being a new virus, it may be undetected by the victim company’s anti-virus software and hence is able to cause a lot of damage.

Anti-virus companies may never get to know about the existence of the virus.

Investigation Guidelines

Scenario 1: This requires the cooperation of anti-virus companies and law enforcement officials in many countries. This investigation is outside the scope of this book.

Scenario 2: The first step is to identify how the virus entered the target systems. If it was through an email, then it may be possible to track the source.

If it was through a physical source (e.g. beautifully packaged CDs sent by post to some employees), then conventional investigation may prove useful.
16. Web defacement

Website defacement is usually the substitution of the original home page of a website with another page (usually pornographic or defamatory in nature) by a hacker.

Religious and government sites are regularly targeted by hackers in order to display political or religious beliefs. Disturbing images and offensive phrases might be displayed in the process, as well as a signature of sorts, to show who was responsible for the defacement. Websites are not only defaced for political reasons, many defacers do it just for the thrill.

The scenario

The homepage of a website is replaced with a pornographic or defamatory page. In case of Government websites, this is most commonly done on symbolic days (e.g. Independence day of the country).

The law

Sections 43 and 66 of Information Technology Act [In some cases section 67 and 70 may also apply]

Who is liable?

The person who defaces the website.

The motive

Thrill or a perverse pleasure in inciting communal disharmony

Modus Operandi

The defacer may exploit the vulnerabilities of the operating system or applications used to host the website. This will allow him to hack into the web server and change the home page and other pages.

Alternatively he may launch a brute force or dictionary attack to obtain the administrator passwords for the website. He can then connect to the web server and change the webpages.

Investigation Guidelines

The first step is to analyse the log files of the victim server. This can provide the IP address of the suspect.

Once these IP addresses are obtained, a WHOIS search will reveal the Internet Service Provider (ISP). The ISP can provide the customer contact
information. The suspect’s computer can be examined using X-Ways Trace and Winhex and all relevant evidence can be extracted.

Sometimes the investigation may lead to a cyber café or other public computer. In this situation conventional investigation can be used (e.g. photographs of the suspects can be shown to the cyber café manager).
Annex 3: Introduction to Digital Signatures

Simply put, a person can authenticate a document by affixing his digital signature. Conceptually, a digital signature is similar to a hand written signature. Let us take a simple illustration to understand how digital signatures work.

**Illustration**

Sanya uses her computer to generate a public and private key pair. Simply put, these keys are very large numbers.

She then stores her private key very securely on her computer. She uploads her public key to the website of a licensed certifying authority (CA). She also couriers a filled in application form and photocopies of her passport and Income Tax PAN card to the CA.

After following some verification procedures, the CA sends Sanya a hardware device by post. This device contains Sanya’s digital signature certificate. The digital signature certificate contains Sanya’s public key along with some information about her and the CA.

Sanya then has to accept her digital signature certificate.

All digital signature certificates are stored in the online repository maintained by the Controller of Certifying Authorities.

Each Certifying Authority stores digital signature certificates issued by it in an online repository.

In order to digitally sign an electronic record, Sanya uses her private key.

In order to verify the digital signature, any person can use Sanya’s public key (which is contained in her digital signature certificate).

In case Sanya had originally generated her private key on a smart card or USB Crypto Token then the subsequent signatures...
created by her would be **secure digital signatures**.

**Note:** The smart card / crypto token have a chip built into it, which has crypto modules to enable the signing operation to happen in the device itself. The private key does not come out of the device in its original form.

In cases Sanya had generated and stored her private key on a hard disk, floppy, CD, pen drive etc then subsequent signatures are not secure digital signatures.

This annexure serves as a ready reference for the procedure of obtaining a digital signature certificate from a licenced Certifying Authority in India.

For the purposes of this annexure, the step by step procedure is outlined. The application for the certificate is made in the name of “Rohas Nagpal” to the Tata Consultancy Services Certifying Authority. A computer running Microsoft Windows XP operating system and Microsoft Internet Explorer 7 is used.

Where relevant, information obtained from the Tata Consultancy Services Certifying Authority website (www.tcs-ca.tcs.co.in) has been quoted.

The steps followed to obtain the digital signature certificate are as under:

1. **Downloading root certificate**

   Visit the website of the Controller of Certifying Authorities (CCA) at [www.cca.gov.in](http://www.cca.gov.in) to obtain the digital signature certificate of the CCA. This certificate must be installed on our computer before we begin the process to obtain our personal digital signature certificate. The detailed procedure for the same is outlined below:

   i. Click on “Download 2007 Root Certificate” image.

   ![Download 2007 Root Certificate](download.png)

   ii. The following screen will open up. Click on “Open”
iii. The following digital signature certificate will open up on your screen:

![Certificate Image]

iv. The certificate displays the message that:

“This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store”.

The reason for this is that this certificate is not installed in the Microsoft Internet Explorer browser by default. We will manually need to do so. Click on “Install Certificate”. The following screen opens up:
v. Click on "Next". The following screen will open up. Again click on "Next".

vi. The following screen will open up. Click on "Finish".
vii. This is the final stage for installing the CCA certificate on our computer. It must be clearly understood that once this root certificate is installed in our browser, it becomes a trusted root certificate. All Certifying Authorities who are issued certificates by the CCA will automatically be trusted by our computer.

viii. The following screen will open up. Click on “Yes”.

![Security Warning]

ix. The screen below will open up. Click “OK”.

![Certificate Import Wizard]

x. To view the installed CCA certificate, open up a window of Microsoft Internet Explorer and then click on Tools Æ Internet Options Æ Content
xi. When the above window opens up, click on "Certificates" and then click on the "Trusted Root Certification Authorities" tab. The following screen will open up. Click on "CCA India 2007" and then click on "View".
The certificate illustrated in the next page will now open up on your screen. Notice that when we had first seen this certificate while downloading it from the www.cca.gov.in website, it displayed the following notice:

“This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store”.

Now it does not display that notice. This is because we have installed it in the “Trusted Root Certification Authorities store” of our computer and thereby we have indicated to our computer that we trust this certificate.
2. Selecting a Certifying Authority

Visit the website of the Controller of Certifying Authorities at www.cca.gov.in to obtain a list of licenced Certifying Authorities in India. This website also provides the disclosure records of the various licenced Certifying Authorities. The links to the websites of these Certifying Authorities is also provided.

Based on this information and the study of the relevant websites, you can select a Certifying Authority. For this illustration we have selected the Tata Consultancy Services Certifying Authority (CA) which has the official website www.tcs-ca.tcs.co.in

3. Visit the website of the Certifying Authority

A visit to the www.tcs-ca.tcs.co.in website shows that the CA provides three types of digital signature certificates. The following information is provided in respect of these certificates:

Class-1 Certificates

Class-1 Certificates are personal email Certificates that allow you to secure your email messages. These Certificates can be used to:
Digitally sign email - You can digitally sign your email messages using TCS-CA Personal Digital Certificate so that the recipient is assured that the email has come from you.

Encrypt email - You can encrypt emails using TCS-CA Personal Digital Certificate to prevent unauthorized people from reading it.

Authenticate to Web Servers - You can authenticate yourself to a Web Server to engage in secure communication with Web Server using TCS-CA Personal Digital Certificate. This protects all information such as credit card details that you send to the Web Server.

Class-1 Certificates however, do not facilitate strong authentication of the identity of the Subscriber; hence are not intended for, and shall not be relied upon, for commercial use where proof of identity is required.

Class-2 Certificates
Class-2 Certificates are issued as Managed Digital Certificates to employees/ partners/ affiliates/ customers of business and government organizations that are ready to assume the responsibility of verifying the accuracy of the information submitted by their employees/ partners/ affiliates/ customers.

Class-2 Certificates are issued following a top down approach. The entire organization is treated as a Sub-CA/RA. The organization is given a Digital Certificate signed by TCS-CA to initiate the process of issuing Certificates to its employees/ partners/ affiliates/ customers. The Sub-CA/RA in turn requests the issue of Digital Certificates for employees/ partners/ affiliates/ customers of the organization from TCS-CA. In the case of a Class-2 Certificate, the verification of details supplied with the request for a Digital Certificate is done by the organization appointed as a Sub-CA/RA under the TCS-CA Trust Network.

Class-2 Certificates issued under the TCS-CA Trust Network are legally valid under the Indian IT Act 2000.

Class-3 Certificates
Class-3 Certificates are issued to individuals, companies and government organizations. They can be used both for personal and commercial purposes. They are typically used for electronic commerce applications such as electronic banking, electronic data interchange (EDI), and membership-based on-line services, where security is a major concern.

The level of trust created by the Digital Certificate is based on the authentication procedures used by the CA to verify your identity and the service guarantees offered by the CA to back up that authentication.

TCS-CA uses various procedures to obtain evidence of your identity before issuing you the Class-3 Certificate. During verification, you will also need to be physically present before a Registration Authority (RA), qualified by TCS-CA due to their neutrality and reliability. These validation procedures provide stronger assurances of an applicant's identity.

Class-3 Certificates issued by the TCS-CA are legally valid under the Indian IT Act 2000.
4. **Select the type of certificate needed**

We need a legally valid digital signature certificate for an individual. The relevant certificate is a **Class 3 certificate**.

5. **Submit an online request**

The next steps are to create a user account on the TCS CA website, complete an online enrollment form and generate a cryptographic key pair on our computer. The following issues have to borne in mind:

i. **Computer Requirements**

A computer running Microsoft Windows NT, 2000 or XP operating system is needed. Additionally the computer must have Internet Explorer 5.5 or higher.

ii. **Browser Settings**

Active-X controls need to be enabled in the Internet browser. To do this go to Tools >> Internet Options >> Security and click 'Default Settings' and set to 'Medium'.
iii. **Enrollment Instructions**

Cryptographic keys are generated and stored on our computer when we enroll for a digital certificate. Ownership of these keys forms the basis of our digital identity for digital signatures and encryption applications.

During enrollment we specify that we are enrolling for a **Signing Certificate (single key pair)**.

We also select “**Microsoft Enhanced Cryptographic Provider v1.0**” as the “Cryptographic Service Provider”.

After filling in the details, we click on “**Generate Request**”.

We then confirm our details at the next screen and click on “**OK**”. We are then asked whether we want to request a digital signature certificate. Click on “**Yes**”.

© 2008 Rohas Nagpal. All rights reserved.
The following screen will open up. Click on "OK".

The next screen will display the request number. Take a printout of this page and then click on “Go to Step 2”.

The next screen informs us that paper copies of the following need to be submitted to TCS CA:
1. filled Certificate Request Form and
2. supporting Validation documents.

The Certificate Request Form can be downloaded from this page in Word Format as well as PDF Format.

An email is also received from TCS CA regarding the application made by us.

Until the certificate is generated and downloaded by us successfully, we must:
1. not format the computer
2. not re-install or upgrade the Internet Explorer

A few days later we receive an email from TCS CA informing us that the digital signature certificate is ready for download. Using the Authentication PIN provided in the email, the digital signature certificate can be downloaded after logging into the TCS CA website. While downloading the certificate, the following screen may pop up. Click on “Yes”.

**Potential Scripting Violation**

This website is adding one or more certificates to this computer. Allowing an untrusted website to update your certificate is a security risk. The website could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.

Do you want this program to add the certificates now? Click “Yes” if you trust this website. Otherwise, click “No.”
To view your digital signature certificate, open up a window of Microsoft Internet Explorer and then click on **Tools → Internet Options → Content**

Now click on "**Certificates**".

Click on "**View**".
It is advisable to backup a copy of your digital signature certificate along with the private key to a secure location.

To do this, click on "Export" in the screen before this.

Click on "Next".
Select the “Yes, export the private key” option and then click on “Next”.

Select the options marked above and click on “Next”.

© 2008 Rohas Nagpal. All rights reserved.
You will now need to enter a password. Ensure that you enter a complex password that is not known to anyone else. Then click on “Next”.

After selecting a suitable location to save the digital signature certificate, click on “Next”.

Click on “OK” to complete the backup process. The following screen will then open up.
## Annex 4: List of useful software & websites

<table>
<thead>
<tr>
<th>Activity</th>
<th>Software / websites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whois search</td>
<td><a href="http://www.who.is">www.who.is</a></td>
<td>Covers 137 top level domain extensions.</td>
</tr>
<tr>
<td>Whois search</td>
<td><a href="http://www.whois.net">www.whois.net</a></td>
<td>Search by keyword option and search for deleted domains option available.</td>
</tr>
<tr>
<td>Tracking email accounts</td>
<td><a href="http://www.readnotify.com">www.readnotify.com</a></td>
<td>It tracks the IP address of the computer on which an email was read / re-opened / forwarded etc.</td>
</tr>
<tr>
<td>Recovering deleted evidence</td>
<td>Winhex</td>
<td>It can inspect and edit all kinds of files, recover deleted files or lost data from hard drives with corrupt file systems or from digital camera cards.</td>
</tr>
<tr>
<td>Recovering deleted evidence</td>
<td>X-Ways Trace</td>
<td>Allows tracking and examining web browsing activity and deletion of files through the Windows recycle bin.</td>
</tr>
<tr>
<td>Password Breaking</td>
<td>Passware Kit</td>
<td>Passware Kit combines over 25 password recovery modules in a convenient and cost-saving software pack.</td>
</tr>
<tr>
<td>Password Breaking</td>
<td>Encryption Analyzer</td>
<td>Finds all the password-protected or encrypted files on a computer / network. It lists recovery options and launches the appropriate password recovery modules if necessary.</td>
</tr>
<tr>
<td>Encryption Breaking</td>
<td>Elcomsoft Distributed</td>
<td>For recovery of passwords for PGP secret key rings (.SKR), PGP disks (.PGD), PGP self-decrypting archives, PGP whole disk encryption, Personal Information Exchange certificates - PKCS #12 (.PFX), and MD5 hashes.</td>
</tr>
<tr>
<td>Searching for keywords</td>
<td>dtSearch</td>
<td>Supports fuzzy searching, phonetic searching, stemming, synonym searching and numeric range search</td>
</tr>
</tbody>
</table>