

Rohas Nagpal
Asian School of Cyber Laws

Cyber Crime Investigation Manual





Rohas Nagpal is a lawyer by qualification, a cyber crime investigator by profession, a hacker at heart and a programmer by passion.

He advises corporates, law firms, Governments and law enforcement agencies on issues relating to technology law, cyber crime investigation, information warfare and cyber terrorism. He has assisted the Government of India in drafting rules and regulations under the Information Technology Act.

He is an active public speaker on technology issues and has addressed thousands of students, law enforcement personnel, lawyers and other professionals around the world.

Rohas conducts training programs in technology law and cyber crime investigation and has authored several books, papers and articles on these topics.

He has authored several books in digital forensic investigation, technology law and financial law. One of his publications, the Cyber Crime Investigation Manual, has been referred to as a "bible for cyber crime investigators" by Times of India – the world's largest selling English newspaper. He is also the author of the first ever Commentary on the Information Technology Act.

Papers authored by him include Internet Time Theft & the Indian Law (Bangalore, 2001), Legislative Approach to Digital Signatures (Ecuador, 2001), Indian Legal position on Cyber Terrorism, Encryption and preventive measures (on behalf of the Karnataka Police for Otto Schily, Interior Minister, Federal Republic of Germany), Defining Cyber Terrorism (Nagpur, 2002), The mathematics of terror (Nagpur, 2002) and Cyber Terrorism – A Global Perspective (Spain, 2002).

He has also co-authored an Internet Draft titled Biometric based Digital Signature scheme, which proposes a method of using biometrics to generate keys for use in digital signature creation and verification.

He was part of the team that developed the world's smallest cyber crime investigation device, pCHIP a Portable Mega Investigation & Forensic Solution. This device is capable of capturing volatile evidence from a live computer, has an easy to use interface, and provides detailed reports.

He is the founder of CyberAttack, an open community working for cyber security. He also maintains www.bugs.ms, a specialized search engine that tracks bugs and vulnerabilities in Microsoft® products. He is also the founder of the proudIndian.me project and the Woman 2.0 Foundation.

He is a member of Information Systems Audit and Control Association (ISACA), International Association for Cryptologic Research (IACR), and a Sustaining Member of the Internet Society (ISOC), which is the organizational home of the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the Internet Engineering Steering Group (IESG), and the Internet Research Task Force (IRT) - the standards setting and research arms of the Internet community.

In 1999, Rohas Nagpal co-founded Cyber Tribe which today is comprised of 10 organizations - Asian School of Cyber Laws, TechJuris Law Consultants, ASCL Law School, Data64 Techno Solutions Pvt. Ltd., Republic of Cyberia, Association of Digital Forensic Investigators, Security Standards and Controls Development Organization, Corporate Crime Control Organization, Data64 Cyber Solutions and Data64 Technologies Pvt. Ltd.

SUN PUBLICATIONS
#1 Piyush Residency, 236 Kasba Peth, Pune-411011



ISBN 978-81-910597-2-4
Rs. 3000

TABLE OF CONTENTS

1. TYPES OF CYBER CRIMES.....	11
1. FINANCIAL CRIMES	12
2. CYBER PORNOGRAPHY	13
3. SALE OF ILLEGAL ARTICLES	14
4. ONLINE GAMBLING	14
5. INTELLECTUAL PROPERTY CRIMES	15
6. EMAIL SPOOFING	15
7. FORGERY	16
8. CYBER DEFAMATION.....	16
9. CYBER STALKING	17
10. WEB DEFACEMENT	18
11. EMAIL BOMBING.....	19
12. DATA DIDDLING.....	20
13. SALAMI ATTACKS	20
14. DENIAL OF SERVICE ATTACKS.....	21
15. VIRUS / WORM ATTACKS	22
16. TROJANS AND KEYLOGGERS.....	24
17. INTERNET TIME THEFT	25
18. WEB JACKING.....	25
19. EMAIL FRAUDS	27
20. CYBER TERRORISM	29
21. USE OF ENCRYPTION BY TERRORISTS.....	32
2. HACKER METHODOLOGY	36
1. FOOTPRINTING	36
2. ANALYZING THE ROBOTS.TXT FILE	39
3. WEB CRAWLING.....	40
4. PORT SCANNING	40
5. COOKIE MANIPULATION	41
6. ESHOPLIFTING	44
7. WEB DEFACEMENT	45
8. USING GOOGLE AS A HACKING TOOL.....	46
9. PACKET SNIFFING	50

3. TROJANS	51
1. INTRODUCTION TO TROJANS.....	51
2. TYPES OF TROJANS	52
3. MANIPULATING WINDOWS SUFFIXES.....	54
4. MIMICKING FILE NAMES	57
5. WRAPPER TOOLS	60
6. TROJANING SOFTWARE DISTRIBUTION SITES.....	63
7. POISONING THE SOURCE.....	65
8. EASTER EGGS	67
9. TROJAN RELATED CASES.....	68
4. COMPUTER WORMS.....	72
1. INTRODUCTION.....	72
2. A BRIEF HISTORY OF WORMS.....	74
5. COMPUTER VIRUSES.....	79
6. CYBER CRIMES HIT LIST	81
7. INTRODUCTION TO CYBER CRIME INVESTIGATION	88
1. EXTERNAL EXAMINATION.....	89
2. CONFISCATION AND SEIZURE.....	90
2.1 <i>When to confiscate</i>	90
2.2 <i>What to confiscate</i>	91
2.3 <i>Transporting confiscated material</i>	93
2.4 <i>Chain of custody form</i>	95
3. WHOIS SEARCH	98
4. DNS LOOKUP	107
5. TRACEROUTE	108
6. IP TRACING	109
7. INVESTIGATING SERVER LOGS	109
8. EMAIL TRACKING AND TRACING	111
9. RECOVERING DELETED EVIDENCE	111
10. PASSWORD BREAKING.....	111
11. HANDLING ENCRYPTED FILES.....	112

12. HANDLING STEGANOGRAPHY.....	112
13. HANDLING HIDDEN DATA	114
14. USING KEYLOGGERS FOR INVESTIGATION	116
15. SEARCHING FOR KEYWORDS	117
8. INVESTIGATING EMAILS.....	118
1. ANALYSIS OF THE GMAIL HEADER	118
2. ANALYSIS OF THE REDIFFMAIL HEADER	124
3. ANALYSIS OF THE YAHOO HEADER.....	130
4. ANALYSIS OF EMAIL SENT FROM THUNDERBIRD CLIENT	135
5. ONLINE EMAIL HEADER ANALYSIS TOOLS	143
6. TRACKING EMAIL ACCOUNTS.....	148
STEP BY STEP GUIDE TO USING READNOTIFY	153
7. CASE STUDY.....	169
9. INVESTIGATING SERVER LOGS.....	174
1. FTP SERVER LOGS	174
1.1 Connecting to a closed FTP server.....	174
1.2 FTP server is started up	176
1.3 Password cracking attempt.....	176
1.4 Logging onto an FTP Server.....	180
1.5 Attempting to connect from a banned IP	184
1.6 Attempting to upload a banned file	187
1.7 Uploading a file	189
1.8 Renaming a file	193
1.9 Deleting a file	196
1.10 Downloading a file	198
1.11 Creating a directory.....	201
1.12 Deleting a directory.....	203
1.13 Making a directory writable by public.....	205
1.14 List of raw FTP commands.....	207
1.15 FTP Status and Error Codes	212
2. WEB SERVER LOGS	216

10. CYBER FORENSICS	219
1. INTRODUCTION	219
2. KEY TERMS	221
3. ASCL BEST PRACTICES FOR CYBER FORENSICS	224
3.1 <i>Guidelines for Evidence collection</i>	224
3.2 <i>Guidelines for Evidence archival</i>	226
3.3 <i>Guidelines for Hard disk examination</i>	227
3.4 <i>Guidelines for USB drive / floppy disk examination</i>	228
3.5 <i>Using Forensic software</i>	228
11. PASSWORD BREAKING.....	229
1. BREAKING FILE PASSWORDS.....	229
1.1 <i>Using Advanced Office Password Recovery software</i>	229
1.2 <i>Using Encryption Analyzer</i>	236
1.3 <i>Using Passware Kit Enterprise</i>	239
1.4 <i>Using EDPR</i>	240
1.5 <i>Using Decryptum</i>	242
2. BREAKING OPERATING SYSTEM PASSWORDS.....	246
3. HANDLING ENCRYPTED FILES.....	250
3.1 <i>How cryptography works</i>	251
3.2 <i>Keys</i>	252
3.3 <i>Symmetric Cryptography</i>	254
3.4 <i>Asymmetric Cryptography</i>	255
3.5 <i>Hash function</i>	256
3.6 <i>Digital Signatures</i>	257
3.7 <i>Using PGP</i>	259
3.8 <i>Using EDPR to crack PGP passwords</i>	263
3.9 <i>Using MD5 hashes to protect passwords</i>	264
3.10 <i>Using EDPR to crack MD5 hashes</i>	266
3.11 <i>Using Cain & Abel to crack MD5 hashes</i>	268
3.12 <i>Using gdata to crack MD5 hashes</i>	271
4. HANDLING STEGANOGRAPHY.....	272
4.1 <i>What is Steganography?</i>	272
4.2 <i>What is Steganography used for?</i>	273
4.3 <i>Using Camouflage</i>	273
4.4 <i>Using SNOW</i>	280
4.5 <i>Using Steganos Security Suite</i>	282

12. INVESTIGATING INTELLECTUAL PROPERTY CRIMES.....	291
1. UNDERSTANDING COMPUTER SOFTWARE	291
2. COMPUTER SOFTWARE & COPYRIGHT LAW	298
2.1 <i>Meaning of Copyright</i>	298
2.2 <i>First owner of copyright</i>	299
2.3 <i>Term of copyright</i>	300
2.4 <i>Licences</i>	300
2.5 <i>Infringement of Copyright</i>	301
<i>Microsoft Corporation v Mr. Kiran & Another.</i>	302
3. SOFTWARE LICENSES.....	306
3.1 <i>Freeware Licenses</i>	307
3.2 <i>Windows License</i>	309
3.3 <i>Open Source Licenses</i>	312
3.4 <i>GNU General Public License</i>	315
4. COMPUTER DATABASES & THE LAW	319
<i>Diljeet Titus case</i>	320
5. DOMAIN NAME DISPUTES	324
5.1 <i>What is a domain name?</i>	324
5.2 <i>Domain Name Disputes</i>	326
5.3 <i>Domain Name Disputes in India</i>	327
5.4 <i>The .in Domain Name Dispute Resolution Policy</i>	327
5.5 <i>The INDRP Rules</i>	329
6. WEB RELATED ISSUES	332
6.1 <i>Meta tags</i>	332
6.2 <i>Framing</i>	333
6.3 <i>Deep Hyperlinking</i>	335
7. INVESTIGATING IPR CRIMES	337
<i>Source code theft case</i>	337
<i>Request for Service</i>	339
<i>Chain of Custody Form</i>	340
<i>Investigation Report</i>	341
13. INVESTIGATING FINANCIAL CRIMES	343
1. BASIC TERMS	345
2. SHARES	351
2.1 <i>Types of shares</i>	351
2.2 <i>Indian Capital & Stock Markets</i>	353
2.3 <i>Initial Public Offering (IPO)</i>	355
2.4 <i>Rights issue</i>	356
2.5 <i>Bonus issue</i>	357

<i>2.6 Sweat Equity</i>	358
<i>2.7 Employee Stock Options (ESOP)</i>	358
<i>2.8 Buy-back of shares</i>	359
<i>2.9 Investing in shares</i>	359
3. DEBT INSTRUMENTS	363
<i>3.1 Types of Debentures</i>	363
<i>3.2 Types of Bonds</i>	365
<i>3.3 Credit Rating</i>	370
4. COMMODITIES	373
5. DERIVATIVES	375
6. FUTURES	377
<i>6.1 Index Futures</i>	379
<i>6.2 Cost of carry model</i>	380
<i>6.3 Important Terms</i>	380
7. HEDGING	383
8. OPTIONS	385
<i>8.1 Call Option</i>	385
<i>8.2 Put Option</i>	385
9. SWAPS	388
10. ARBITRAGE	389
11. HEDGING	390
12. RELATED CONCEPTS	392
<i>12.1 Equity Linked Note</i>	392
<i>12.2 Catastrophic Bonds</i>	392
<i>12.3 Weather derivatives</i>	394
<i>12.4 The Nicholas Leeson Derivatives Fraud</i>	396
13. CARBON CREDITS	399
<i>ICE ECX Carbon Financial Instruments Futures</i>	400
14. DEPOSITORY RECEIPTS	403
<i>14.1 American Depository Receipts</i>	403
<i>14.2 ADRs v/s GDRs</i>	404
15. INVESTIGATING FINANCIAL CRIMES	405
<i>15.1 Income Tax Raid case</i>	405
<i>Request for Service</i>	406
<i>Chain of Custody Form</i>	407
<i>Investigation Report</i>	408
<i>15.2 Lottery Fraud case</i>	411
<i>Investigation Report</i>	414
<i>15.3 Accounting Fraud case</i>	415
<i>Request for Service</i>	416
<i>Investigation Report</i>	417

14. INVESTIGATING DIGITAL SIGNATURE CRIMES.....	423
1. INTRODUCTION.....	423
2. CASE STUDY	428
15. LEGAL ISSUES.....	438
SECTION 65. TAMPERING WITH COMPUTER SOURCE DOCUMENTS	439
SECTION 66. COMPUTER RELATED OFFENCES	441
SECTION 66A. PUNISHMENT FOR SENDING OFFENSIVE MESSAGES THROUGH COMMUNICATION SERVICE, ETC	445
SECTION 66B. PUNISHMENT FOR DISHONESTLY RECEIVING STOLEN COMPUTER RESOURCE OR COMMUNICATION DEVICE	448
SECTION 66C. PUNISHMENT FOR IDENTITY THEFT	450
SECTION 66D. PUNISHMENT FOR CHEATING BY PERSONATION BY USING COMPUTER RESOURCE	452
SECTION 66E. PUNISHMENT FOR VIOLATION OF PRIVACY.....	455
SECTION 66F. PUNISHMENT FOR CYBER TERRORISM	457
SECTION 67. PUNISHMENT FOR PUBLISHING OR TRANSMITTING OBSCENE MATERIAL IN ELECTRONIC FORM	460
SECTION 67A. PUNISHMENT FOR PUBLISHING OR TRANSMITTING OF MATERIAL CONTAINING SEXUALLY EXPLICIT ACT, ETC., IN ELECTRONIC FORM	462
SECTION 67B. PUNISHMENT FOR PUBLISHING OR TRANSMITTING OF MATERIAL DEPICTING CHILDREN IN SEXUALLY EXPLICIT ACT, ETC., IN ELECTRONIC FORM	464
SECTION 67C. PRESERVATION AND RETENTION OF INFORMATION BY INTERMEDIARIES....	467
SECTION 68. POWER OF THE CONTROLLER TO GIVE DIRECTIONS	469
SECTION 69. POWER TO ISSUE DIRECTIONS FOR INTERCEPTION OR MONITORING OR DECRIPTION OF ANY INFORMATION THROUGH ANY COMPUTER RESOURCE.....	471
SECTION 69A. POWER TO ISSUE DIRECTIONS FOR BLOCKING PUBLIC ACCESS OF ANY INFORMATION THROUGH ANY COMPUTER RESOURCE	473
SECTION 69B. POWER TO AUTHORISE TO MONITOR AND COLLECT TRAFFIC DATA OR INFORMATION THROUGH ANY COMPUTER RESOURCE FOR CYBER SECURITY	475
SECTION 70. PROTECTED SYSTEM	477
SECTION 70B. INDIAN COMPUTER EMERGENCY RESPONSE TEAM TO SERVE AS NATIONAL AGENCY FOR INCIDENT RESPONSE	479
SECTION 71. PENALTY FOR MISREPRESENTATION	481
SECTION 72. PENALTY FOR BREACH OF CONFIDENTIALITY AND PRIVACY.....	483
SECTION 72A. PUNISHMENT FOR DISCLOSURE OF INFORMATION IN BREACH OF LAWFUL CONTRACT	485

SECTION 73. PENALTY FOR PUBLISHING ELECTRONIC SIGNATURE CERTIFICATE FALSE IN CERTAIN PARTICULARS.....	487
SECTION 74. PUBLICATION FOR FRAUDULENT PURPOSE	489
SECTION 77A. COMPOUNDING OF OFFENCES	491
SECTION 77B. OFFENCES WITH THREE YEARS IMPRISONMENT TO BE BAILABLE	496
SECTION 78. POWER TO INVESTIGATE OFFENCE	506
SECTION 80. POWER OF POLICE OFFICER AND OTHER OFFICERS TO ENTER, SEARCH, ETC ..	511
16. SAMPLE DOCUMENTATION.....	518
1. INTRODUCTION.....	518
<i>Request for Service.....</i>	519
<i>Chain of Custody Form</i>	520
<i>Computer Evidence Assessment Checklist.....</i>	521
<i>Computer Evidence Analysis Checklist.....</i>	522
<i>Computer Evidence Analysis Report.....</i>	523
<i>Cyber Forensic Analysis Report</i>	525
2. FIR	528
<i>2.1 Sample FIR.....</i>	529
<i>2.2 Sample criminal complaint.....</i>	533
3. PROPERTY SEARCH & SEIZURE FORM	535
<i>Sample Property Search & Seizure Form</i>	536
4. FINAL FORM / REPORT	540
<i>Sample Property Final Form / Report.....</i>	541
5. ADJUDICATION PROCEEDINGS.....	548
<i>Sample Complaint to the Adjudicating Officer.....</i>	550
17. GUIDELINES FOR REAL WORLD INVESTIGATIONS.....	553
1. SOCIAL NETWORKING SITES RELATED CASES	553
2. EMAIL ACCOUNT HACKING	555
3. CREDIT CARD FRAUD	557
4. ONLINE SHARE TRADING FRAUD	559
5. TAX EVASION AND MONEY LAUNDERING	561
6. SOURCE CODE THEFT	563
7. THEFT OF CONFIDENTIAL INFORMATION	565
8. SOFTWARE PIRACY	567
9. MUSIC PIRACY.....	569
10. EMAIL SCAMS.....	571
11. PHISHING	572

12. CYBER PORNOGRAPHY	574
13. ONLINE SALE OF ILLEGAL ARTICLES	576
14. USE OF INTERNET AND COMPUTERS BY TERRORISTS	578
15. VIRUS ATTACKS	580
16. WEB DEFACEMENT.....	582
18. ANNEXURES.....	584
1. CASE STUDY ON FOOTPRINTING	584
2. SOLUTION TO CASE STUDY ON FOOTPRINTING	585
3. INTERNATIONAL CASE STUDIES	595
<i>3.1 Man charged for targeting fiancé’s bank account</i>	<i>595</i>
<i>3.2 Trojans used for infecting thousands of computers for fraud</i>	<i>596</i>
<i>3.3 Russian computer hackers sentenced to 3 years in prison</i>	<i>597</i>
<i>3.4 Indian hackers indicted for online brokerage intrusion scheme</i>	<i>599</i>
<i>3.5 E-Gold indicted for Money Laundering and Illegal Money Transmitting.....</i>	<i>600</i>
<i>3.6 One man convicted for counterfeiting Citibank ATM cards.....</i>	<i>602</i>
<i>3.7 Elaborate phishing scam mastermind jailed for 7 years.....</i>	<i>602</i>
<i>3.8 Romanian admits role in international phishing scheme</i>	<i>603</i>
<i>3.9 Teacher charged for hacking protected system</i>	<i>604</i>
<i>3.10 Hacker controlling 7000 botnets convicted.....</i>	<i>605</i>
<i>3.11 Brazilian charged with conspiracy to infect 100,000 computers.....</i>	<i>606</i>
<i>3.12 “Botmaster” sentenced to 5 years in prison.....</i>	<i>607</i>
4. HARDWARE DEVICES	609
<i>4.1 Computer Hardware components.....</i>	<i>611</i>
<i>4.2 Central Processing Unit (CPU)</i>	<i>611</i>
<i>4.3 RAM</i>	<i>611</i>
<i>4.4 ROM BIOS Chip.....</i>	<i>614</i>
<i>4.5 Motherboard or Mainboard.....</i>	<i>614</i>
<i>4.6 Ports, Buses, Interfaces</i>	<i>615</i>
<i>4.7 Data Storage Devices</i>	<i>618</i>
<i>4.8 Peripheral devices</i>	<i>620</i>
<i>4.9 Other electronic devices</i>	<i>620</i>
<i>4.10 Evidence in computer devices.....</i>	<i>621</i>
5. SETTING UP A CYBER CRIME INVESTIGATION CELL.....	624
<i>5.1 Need for a Cyber Crime Investigation Cell</i>	<i>624</i>
<i>5.2 Setting up a Cyber Crime Investigation Cell.....</i>	<i>625</i>

1. Types of Cyber Crimes

The first recorded cyber crime took place in the year 1820!

That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime!

Today, computers have come a long way with neural networks and nano-computing promising to turn every atom in a glass of water into a computer capable of performing a billion operations per second. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants are being run on computers, cyber crime has assumed rather sinister implications.

Cyber crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief. The abuse of computers has also given birth to a gamut of new age crimes such as hacking, web defacement, cyber stalking, web jacking etc.

A simple yet sturdy definition of cyber crime would be “unlawful acts wherein the computer is either a tool or a target or both”.

The term computer used in this definition does not only mean the conventional desktop or laptop computer. It includes Personal Digital Assistants (PDA), cell phones, sophisticated watches, cars and a host of gadgets.

Recent global cyber crime incidents like the targeted denial of service attacks on Estonia have heightened fears. Intelligence agencies are preparing against coordinated cyber attacks that could disrupt rail and air traffic controls, electricity distribution networks, stock markets, banking and insurance systems etc.

Unfortunately, it is not possible to calculate the true social and financial impact of cyber crime. This is because most crimes go unreported.

This chapter discusses various prominent types of cyber crimes such as financial crimes, cyber pornography, online sale of illegal articles, online

gambling, intellectual property crimes, email spoofing, forgery, cyber defamation, cyber stalking, web defacement, email bombing, data diddling, salami attacks, denial of service attacks, virus, worm and Trojan attacks, internet time theft, web jacking and email frauds.

It also deals with cyber terrorism and the use of encryption by terrorists.

1. Financial Crimes

Money is the most common motive behind all crime. The same is also true for cyber crime. Globally it is being observed that more and more cyber crimes are being committed for financial motives rather than for “revenge” or for “fun”.

With the tremendous increase in the use of internet and mobile banking, online share trading, dematerialization of shares and securities, this trend is likely to increase unabated. Financial crimes include cyber cheating, credit card frauds, money laundering, hacking into bank servers, computer manipulation, accounting scams etc.

Illustration 1: Punjab National Bank in India was cheated to the tune of Rs. 13.9 million through false debits and credits in computerized accounts.

Illustration 2: Rs. 2,50,000 were misappropriated from Bank of Baroda in India through falsification of computerized bank accounts.

Illustration 3: The Hyderabad police in India arrested an unemployed computer operator and his friend, a steward in a prominent five-star hotel, for stealing and misusing credit card numbers belonging to hotel customers.

The steward noted down the various details of the credit cards, which were handed by clients of the hotel for paying their bills. Then, he passed all the details to his computer operator friend who used the details to make online purchases on various websites.

Illustration 4: In 2004, the US Secret Service investigated and shut down an online organization that trafficked in around 1.7 million stolen credit cards and stolen identity information and documents.

This high-profile case, known as “Operation Firewall,” focused on a criminal organization of some 4,000 members whose Web site functioned as a hub for identity theft activity.

Illustration 5: In 2003, a hacker was convicted in the USA for causing losses of almost \$25 million. The defendant pleaded guilty to numerous charges of conspiracy, computer intrusion, computer fraud, credit card fraud, wire fraud, and extortion.

The hacker and his accomplices from Russia had stolen usernames, passwords, credit card information, and other financial data by hacking into computers of US citizens. They would then extort money from those victims with the threat of deleting their data and destroying their computer systems.

2. Cyber Pornography

Cyber pornography is believed to be 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 covers 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).

Illustration 1: A school student from Delhi (India), who was regularly teased for having a pockmarked face, used a free hosting provider to create www.amazing-gents.8m.net. He regularly uploaded “morphed” photographs of teachers and girls from his school onto the website. He was arrested when the father of one of the victims reported the case to the police.

Illustration 2: The CEO of online auction website bazee.com (a part of the ebay group) was arrested by the Delhi police for violating India’s strict laws on cyber pornography. An engineering student was using the bazee website to sell a video depicting two school students having sexual intercourse. Bazee.com was held liable for distributing porn and hence the CEO was arrested.

Illustration 3: The CEO of a software company in Pune (India) was arrested for sending highly obscene emails to a former employee.

3. Sale of Illegal Articles

It is becoming increasingly common to find cases where sale of illegal articles such as narcotic 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.

It is practically impossible to control or prevent a criminal from setting up a website to transact in illegal articles. Additionally, there are several online payment gateways that can transfer money around the world at the click of a button. The Internet has also created a marketplace for the sale of unapproved drugs, prescription drugs dispensed without a valid prescription, or products marketed with fraudulent health claims.

Many sites focus on selling prescription drugs and are referred to by some as “Internet pharmacies.” These sites offer for sale either approved prescription drug products, or in some cases, unapproved, illegal versions of prescription drugs. This poses a serious potential threat to the health and safety of patients.

The broad reach, relative anonymity, and ease of creating new or removing old websites, poses great challenges for law enforcement officials.

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 modes of communication for gathering people for the illegal “drug” party.

4. Online Gambling

There are thousands of websites that offer online gambling. The special issue with online gambling is that it is legalised in several countries. So legally the owners of these websites are safe in their home countries.

The legal issues arise when a person residing in a foreign country like India (where such websites are illegal) gambles on such a website.

Illustration: The website ladbrokes.com permits users to gamble on a variety of sports such as cricket, football, tennis, golf, motor racing, ice hockey, basketball, baseball, darts, snooker, boxing, athletics, rugby, volleyball, motor cycling etc.

Additionally it also features an online casino. The website has no technical measures in place to prohibit residents of certain countries (where online gambling is illegal) from betting at their website.

5. Intellectual Property Crimes

These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc.

Illustration 1: A software professional from Bangalore (India) was booked for stealing the source code of a product being developed by his employers. He started his own company and allegedly used the stolen source code to launch a new software product.

Illustration 2: In 2003, a computer user in China obtained the source code of a popular game - LineageII from an unprotected website. This proprietary code was then sold to several people in 2004. One of those people set up a website, www.l2extreme.com, to offer the “Lineage” game at a discount.

Despite legal warnings from the South Korean company that owned the Lineage source code, the suspect did not shut down the site. He rented powerful servers - enough to accommodate 4,000 simultaneous gamers - and solicited donations from users to help defray the costs.

The loss in potential revenues for the South Korean company was estimated at \$750,000 a month. The US FBI arrested the suspect and the website was shut down.

6. Email Spoofing

A spoofed email is one that appears to originate from one source but actually has been sent from another source e.g Pooja has an e-mail address pooja@asianlaws.org. Her ex-boyfriend, Sameer spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Pooja, her friends may take offence and relationships may be spoiled for life.

Illustration 1: In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold.

This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly.

Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.

Illustration 2: A branch of the erstwhile Global Trust Bank in India experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts.

An investigation revealed that someone had sent out spoofed emails to many of the bank's customers stating that the bank was in very bad shape financially and could close operations at any time. The spoofed email appeared to have originated from the bank itself.

7. Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets, academic certificates etc are made by criminals using sophisticated computers, printers and scanners.

Illustration 1: In October 1995, Economic Offences Wing of Crime Branch, Mumbai (India), seized over 22,000 counterfeit share certificates of eight reputed companies worth Rs. 34.47 crores. These were allegedly prepared using desktop publishing systems.

Illustration 2: Abdul Kareem Telgi, along with several others, was convicted in India on several counts of counterfeiting stamp papers and postage stamps totalling several billion rupees.

8. Cyber Defamation

This occurs when defamation takes place with the help of computers and / or the Internet. e.g. Sameer publishes defamatory matter about Pooja on a website or sends e-mails containing defamatory information to Pooja's friends.

Illustration 1: Abhishek, a teenaged student was arrested by the Thane police in India following a girl's complaint about tarnishing her image in the social networking site Orkut.

Abhishek had allegedly created a fake account in the name of the girl with her mobile number posted on the profile.

The profile had been sketched in such a way that it drew lewd comments from many who visited her profile. The Thane Cyber Cell tracked down Abhishek from the false e-mail id that he had created to open up the account.

Illustration 2: The Aurangabad bench of the Bombay high court issued a notice to Google.com following a public interest litigation initiated by a young lawyer.

The lawyer took exception to a community called ‘We hate India’, owned by someone who identified himself as Miroslav Stankovic. The community featured a picture of the Indian flag being burnt.

Illustration 3: Unidentified persons posted obscene photographs and contact details of a Delhi school girl. Suggestive names like ’sex teacher’ were posted on the profile.

The matter came to light after the girl’s family started receiving vulgar calls referring to Orkut. Two strangers even came knocking at their door, telling them that the girl had invited them for sex through the Internet.

9. Cyber Stalking

Cyber stalking refers to the use of the Internet, e-mail, or other electronic communications devices to stalk another person.

Stalking generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person’s home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person’s property.

Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim’s immediate family.

Illustration 1: In the first successful prosecution under the California (USA) cyber stalking law, prosecutors obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances.

He terrorized the 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized about being raped.

On at least six occasions, sometimes in the middle of the night, men knocked on the woman’s door saying they wanted to rape her.

Illustration 2: An honours graduate from the University of San Diego in USA terrorized five female university students over the Internet for more than a year. The victims received hundreds of violent and threatening e-mails, sometimes receiving four or five messages a day.

The student, who pleaded guilty, told the police that he had committed the crimes because he thought the women were laughing at him and causing others to ridicule him. In reality, the victims had never met him.

Illustration 3: In 2005, a minor from Massachusetts (USA) was convicted in connection with approximately \$1 million in victim damages.

Over a 15-month period, he had hacked into Internet and telephone service providers, stolen an individual's personal information and posted it on the Internet, and made bomb threats to many high schools.

10. 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. For example, there are online contests in which hackers are awarded points for defacing the largest number of web sites in a specified amount of time. Corporations are also targeted more often than other sites on the Internet and they often seek to take measures to protect themselves from defacement or hacking in general.

Web sites represent the image of a company or organisation and these are therefore especially vulnerable to defacement. Visitors may lose faith in sites that cannot promise security and will become wary of performing online transactions. After defacement, sites have to be shut down for repairs, sometimes for an extended period of time, causing expenses and loss of profit.

Illustration 1: Mahesh Mhatre and Anand Khare (alias Dr Neukar) were arrested in 2002 for allegedly defacing the website of the Mumbai Cyber Crime Cell.

They had allegedly used password cracking software to crack the FTP password for the police website. They then replaced the homepage of the website with pornographic content. The duo was also charged with credit card fraud for using 225 credit card numbers, mostly belonging to American citizens.

Illustration 2: In 2001, over 200 Indian websites were hacked into and defaced. The hackers put in words like bugz, death symbol, Paki-king and allahuakbar.

In the case of 123medicinindia.com, a message was left behind which said – “Catch me if uuu can my deraz lazy adminzzz” – challenging the system administrators to trace the miscreants.

The offenders were allegedly a group of hackers who go by the name of ‘Pakistani Cyber Warriors’.

Illustration 3: In 2006, a Turkish hacker using the handle iSKORPiTX was able to breach the security of a group of web servers, containing more than 38,500 web sites in less than a day!

Illustration 4: The first Defacers Challenge took place on Sunday, July 6, 2003. There was a special prize for the first contestant to deface 6,000 web sites.

The contest was conducted over a six-hour period. Points were awarded based on the server’s operating system. [Windows: 1 point, Linux: 2 points, BSD: 2 points, AIX: 3 points, HP-UX: 5 points, Macintosh: 5 points]

11. Email Bombing

Email bombing refers to sending a large number of emails to the victim resulting in the victim’s email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

Email bombing is a type of denial-of-service attack. A denial-of-service attack is one in which a flood of information requests is sent to a server, bringing the system to its knees and making the server difficult to access.

Illustration 1: A British teenager was cleared of launching a denial-of-service attack against his former employer, in a ruling under the UK Computer Misuse Act.

The teenager was accused of sending 5 million e-mail messages to his ex-employer that caused the company's e-mail server to crash. The judge held that the UK Computer Misuse Act does not specifically include a denial-of-service attack as a criminal offence.

Illustration 2: In one case, a foreigner who had been residing in Simla, India for almost 30 years wanted to avail of a scheme introduced by the Simla Housing Board to buy land at lower

rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India.

He decided to take his revenge. Consequently, he sent thousands of mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed.

12. Data Diddling

One of the most common forms of computer crime is data diddling - illegal or unauthorized data alteration. These changes can occur before and during data input or before output. Data diddling cases have affected banks, payrolls, inventory records, credit records, school transcripts and virtually all other forms of data processing known.

Illustration 1: The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the New Delhi Municipal Council.

Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional.

He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

Illustration 2: A keyboard operator processing orders at an Oakland USA department store changed some delivery addresses and diverted several thousand dollars worth of store goods into the hands of accomplices.

Illustration 3: A ticket clerk at the Arizona Veterans' Memorial Coliseum in USA issued full-price basketball tickets, sold them and then, tapping out codes on her computer keyboard, recorded the transactions as half-price sales.

13. Salami Attacks

These attacks are used for committing financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed.

For instance, a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 2 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month.

Why is the attack called a “salami attack”? Some security specialists claim that it refers to slicing the data thinly, like a salami. Others argue that it means building up a significant object or amount from tiny scraps, like a salami.

Illustration 1: In January 1993, four executives of a rental-car franchise in Florida USA were charged with defrauding at least 47,000 customers using a salami technique.

They modified a computer billing program to add five extra gallons to the actual gas tank capacity of their vehicles. From 1988 through 1991, every customer who returned a car without topping it off ended up paying inflated rates for an inflated total of gasoline. The thefts ranged from \$2 to \$15 per customer - difficult for the victims to detect.

Illustration 2: In January 1997, Willis Robinson of Maryland USA, was sentenced to 10 years in prison (six of which were suspended) for having reprogrammed his Taco Bell drive-up-window cash register - causing it to ring up each \$2.99 item internally as a 1-cent item, so that he could pocket \$2.98 each time.

He made \$3,600 before he was caught. Another correspondent adds that management assumed the error was hardware or software and only caught the perpetrator when he bragged about his crime to co-workers.

Illustration 3: In Los Angeles USA in October 1998, four men were charged with fraud for allegedly installing computer chips in gasoline pumps that cheated consumers by overstating the amounts pumped.

The problem came to light when an increasing number of consumers claimed that they had been sold more gasoline than the capacity of their gas tanks.

However, the fraud was difficult to prove initially because the perpetrators programmed the chips to deliver exactly the right amount of gasoline when asked for five- and 10-gallon amounts - precisely the amounts typically used by inspectors.

14. Denial of Service Attacks

This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource.

One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable.

DoS attacks are generally implemented by: (1) forcing the targeted computer(s) to reset, or consume its resources such that it can no longer provide its intended service; and/or, (2) obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread.

It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support thereby making the servers crash.

Illustration 1: A series of distributed denial of service attacks in February 2000 crippled many popular websites including yahoo.com, amazon.com and cnn.com

Illustration 2: A series of more than 125 separate but coordinated denial of service attacks hit the cyber infrastructure of Estonia in early 2007.

The attacks were apparently connected with protests against the Estonian government's decision to remove a Soviet-era war memorial from the capital city. It is suspected that the attacks were carried out by Russian hackers. The attack lasted several days.

15. Virus / Worm Attacks

Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation. A virus might corrupt or delete data on the victim's computer, use the victim's e-mail program to spread itself to other computers, or even erase everything on the victim's hard disk.

Viruses are most easily spread by attachments in e-mail messages or instant messaging messages. Viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. Viruses can also spread through downloads on the Internet. They can be hidden in illicit software or other files or programs.

Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

Brain (in its first incarnation written in January 1986) is considered to be the first computer virus for the PC. The virus is also known as Lahore, Pakistani, Pakistani Brain, Brain-A and UIUC. The virus was written by two brothers, Basit and Amjad Farooq Alvi, who lived in Lahore, Pakistan. The brothers told TIME magazine they had written it to protect their medical software from piracy and was supposed to target copyright infringers only.

The virus came complete with the brothers' address and three phone numbers, and a message that told the user that their machine was infected and for inoculation the user should call them.

When the brothers began to receive a large number of phone calls from people in USA, Britain, and elsewhere, demanding them to disinfect their machines, the brothers were stunned and tried to explain to the outraged callers that their motivation had not been malicious.

They ended up having to get their phone lines cut off and regretted that they had revealed their contact details in the first place. The brothers are still in business in Pakistan as internet service providers in their company called Brain Limited.

Illustration 1: The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate. In May 2000, this deadly virus became the world's most prevalent virus. Losses incurred during this virus attack were pegged at US \$ 10 billion. VBS_LOVELETTER utilized the addresses in Microsoft Outlook and e-mailed itself to those addresses.

The e-mail, which was sent out, had "ILOVEYOU" in its subject line. The attachment file was named "LOVE-LETTER-FOR-YOU.TXT.vbs". People wary of opening e-mail attachments were conquered by the subject line and those who had some knowledge of viruses, did not notice the tiny .vbs extension and believed the file to be a text file. The message in the e-mail was "kindly check the attached LOVELETTER coming from me".

Illustration 2: Probably the world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. The Internet was, then, still in its developing years and this worm, which affected thousands of computers, almost brought its development to a complete halt. It took a team

of experts almost three days to get rid of the worm and in the meantime many of the computers had to be disconnected from the network.

Illustration 3: In 2002, the creator of the Melissa computer virus was convicted. The virus had spread in 1999 and caused more than \$80 million in damage by disrupting personal computers, business and government computer networks.

Illustration 4: In 2006, a US citizen was convicted for conspiracy to intentionally cause damage to protected computers and commit computer fraud.

Between 2004 and 2005, he created and operated a malicious software to constantly scan for and infect new computers.

It damaged hundreds of US Department of Defence computers in USA, Germany and Italy. The software compromised computer systems at a Seattle hospital, including patient systems, and damaged more than 1,000 computers in a California school district.

Illustration 5: Logic bombs are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. e.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

16. Trojans and Keyloggers

A Trojan, as this program is aptly called, is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

Keyloggers are regularly used to log all the strokes a victim makes on the keyboard.

This assumes sinister proportions, if a keylogger is installed on a computer which is regularly used for online banking and other financial transactions. Key-loggers are most commonly found in public computers such as those in cyber cafes, hotels etc.

Unsuspecting victims also end up downloading spyware when they click on “friendly” offers for free software.

Illustration 1: A young lady reporter was working on an article about online relationships. The article focused on how people can easily find friendship and even love on the Internet.

During the course of her research she made a lot of online friends. One of these ‘friends’ managed to infect her computer with a Trojan.

This young lady stayed in a small one bedroom apartment and her computer was located in one corner of her bedroom. Unknown to her, the Trojan would activate her web camera and microphone even when the Internet was switched off.

A year later she realized that hundreds of her pictures were posted on pornographic sites around the world!

Illustration 2: The network administrator in a global bank received a beautifully packed CD ROM containing “security updates” from the company that developed the operating system that ran his bank’s servers.

He installed the “updates” which in reality was Trojanized software. Three years later, the effects were still being felt in the bank’s system!

17. Internet Time Theft

This connotes the usage by an unauthorized person of the Internet hours paid for by another person.

Illustration: In May 2000, the Delhi police arrested an engineer who had misused the login name and password of a customer whose Internet connection he had set up. The case was filed under the Indian Penal Code and the Indian Telegraph Act as the Information Technology Act was not in force at that time.

18. Web Jacking

Just as conventional hijacking of an airplane is done by using force, similarly web jacking means forcefully taking over control of a website. The motive is usually the same as hijacking – ransom. The perpetrators have either a monetary or political purpose which they try to satiate by holding the owners of the website to ransom.

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.

How does web jacking take place? The administrator of any website has a password and a username that only he (or someone authorized by him)

may use to upload files from his computer on the web server (simply put, a server is a powerful computer) where his website is hosted.

Ideally, this password remains secret with the administrator. If a hacker gets hold of this username and password, then he can pretend to be the administrator.

Computers don't recognize people – only usernames and passwords. The web server will grant control of the website to whoever enters the correct password and username combination.

There are many ways in which a hacker may get to know a password, the most common being password cracking wherein a “cracking software” is used to guess a password. Password cracking attacks are most commonly of two types.

The first one is known as the dictionary attack. In this type of attack the software will attempt all the words contained in a predefined dictionary of words.

For example, it may try Rahim, Rahul, Rakesh, Ram, Reema, Reena ... in a predefined dictionary of Indian names. These types of dictionaries are readily available on the Internet.

The other form of password cracking is by using ‘brute force’. In this kind of attack the software tries to guess the password by trying out all possible combinations of numbers, symbols, letters till the correct password is found. For example, it may try out password combinations like abc123, acbd5679, sdj#%^, weuf*(-)*.

Some software, available for password cracking using the brute force technique, can check a huge number of password combinations per second. When compared with a dictionary attack, a brute force attack takes more time, but it is definitely more successful.

Illustration: In an incident reported in the USA, the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website. They demanded a ransom of 1 million dollars from her.

The owner, a schoolteacher, did not take the threat seriously. She felt that it was just a scare tactic and ignored the e-mail. It was three days later that she came to know, following many telephone calls from all over the country, that the hackers had web jacked her website. Subsequently, they had altered a portion of the website which was entitled ‘How to have fun with goldfish’.

In all the places where it had been mentioned, they had replaced the word ‘goldfish’ with the word ‘piranhas’.

Piranhas are tiny but extremely dangerous flesh-eating fish. Many children had visited the popular website and had believed what the contents of the website suggested.

These unfortunate children followed the instructions, tried to play with piranhas, which they bought from pet shops, and were very seriously injured!

19. Email Frauds

Dear Mr. Justin Williams, I'm Vikas Manjit Singh from Punjab (India). I belong to a city named Ludhiana.

Mr. Williams, I am having a brother in Canada who is also named Justin Williams. He was adopted from my parents by some Mr. William Ram of Welland. Me and my mum came over to Canada to leave Justin to his new family (William Ram's Family). It happened in June 1985.

So Mr. Justin Williams, if you are the same person I'm talking about. Then please give me some time so that I can let you know the realities.

Imagine the thoughts going through Mr. Justin William's head after reading this email. Is he really adopted? Where are his birth parents? Is this email from his birth brother?

In reality, this is a scam email originating from a college in Sangroor (India)! Canadian citizens are targeted with these emails. If the targets start believing the sender to be their brother, they are asked to send money so that their "brother" can travel to Canada with the proof of the victim's adoption!

This is just one of the hundreds of email scams being perpetrated on the Internet. These scams are commonly referred to as Nigerian 419 scams. These scam emails are believed to originate from Nigeria and section 419 of the Nigerian Penal Code relates to cheating (like the famous section 420 of the Indian Penal Code).

The 419 letter scams originated in the early 1980s as the oil-based economy of Nigeria went downhill. In the 1990s, letter scams gave way to email scams.

In 2007, Asian School of Cyber Laws conducted a 3 month intensive investigation of hundreds of scam emails. The results were very surprising to say the least. Less than 10% of these emails had actually originated from Nigeria!

A majority of these emails (more than 60%) have originated from Israel, followed by the Netherlands, UK and other European countries. The “birth brother” email was the only one originating from India.

Most of these scam emails promise the receiver millions (or sometimes billions) of dollars. Most commonly the email says that some rich African bureaucrat or businessman or politician has died and left behind a lot of money.

The scamster states that the Government is going to confiscate the money. The only way out is to transfer the money to the bank account of the email recipient. All that the email recipient has to do is send his bank account details. For this a generous fee of a few million dollars will be paid!

If someone actually falls for this scam and provides the bank details, he is sent some official looking documents relating to the bank transfer of a huge sum of money. Once the victim is convinced of the “genuineness” of the transaction, something appears to go wrong.

The victim is informed that a small amount of money (ranging from US\$ 100 to 2500) is needed for bank charges or other paper work. This money is the motive behind the elaborate scam. Once the victim pays this money, the scamster disappears from the scene.

The lottery scam emails inform the recipient that he has won a million dollar lottery run by Microsoft, Yahoo or some other well known global company. The winner is asked to provide his bank details and pay a small sum for bank charges and other processing fees.

Another scam email begins with “This is to inform you that we are in possession of a consignment, deposited by British National Lottery which is to be couriered to you”. The email asks for 470 pounds to be sent to the courier company so that the cheque for the lottery prize can be sent.

Another scam email comes with the subject line “Blessed is the hand that giveth”. The sender claims to be a widow on her deathbed. She wants to donate her wealth to someone who will pray for her.

Another scam email comes from an “employee of the Euro Lottery”. The “employee” claims to be in a position to carry out a lottery fraud and is willing to share the money with the email recipient.

What is common in all these scams is that scanned versions of official documents are emailed to potential victims. Once the victim is convinced of the genuineness of the transaction, a small fee is requested for meeting bank charges / legal fees / courier charges etc. It is this small fee that is the motive behind the scam.

It is believed that thousands of people are defrauded of billions of dollars every year through these scams.

Illustration 1: In 2005, an Indian businessman received an email from the Vice President of a major African bank offering him a lucrative contract in return for a kickback of Rs 1 million.

The businessman had many telephonic conversations with the sender of the email. He also verified the email address of the ‘Vice President’ from the website of the bank and subsequently transferred the money to the bank account mentioned in the email.

It later turned out that the email was a spoofed one and was actually sent by an Indian based in Nigeria.

Illustration 2: A new type of scam e-mail threatens to kill recipients if they do not pay thousands of dollars to the sender, who purports to be a hired assassin.

Replying to the e-mails just sends a signal to senders that they’ve reached a live account. It also escalates the intimidation.

In one case, a recipient responded that he wanted to be left alone and threatened to call authorities. The scammer, who was demanding an advance payment of \$20,000, e-mailed back and reiterated the threat, this time with some personal details about the recipient—his work address, marital status, and daughter’s full name.

Then an ultimatum: “TELL ME NOW ARE YOU READY TO DO WHAT I SAID OR DO YOU WANT ME TO PROCEED WITH MY JOB? ANSWER YES/NO AND DON’T ASK ANY QUESTIONS!!!”

There is also a twist in the scam. E-mails are surfacing that claim to be from the FBI in London and inform recipients that an arrest was made in the case. The e-mail says the recipient’s information was found on the suspect and that they should reply to help further the investigation. This, too, is a scam!

20. Cyber Terrorism

Computer crime has hit mankind with unbelievable severity. Computer viruses, worms, Trojans, denial of service attacks, spoofing attacks and e-frauds have taken the real and virtual worlds by storm.

However, all these pale in the face of the most dreaded threat – that of cyber terrorism.

The author (see the paper titled “Defining Cyber terrorism” by Rohas Nagpal, Asian School of Cyber Laws) has defined cyber terrorism as:

Cyber terrorism is the premeditated¹ use of disruptive activities², or the threat³ thereof, in cyber space⁴, with the intention⁵ to further social, ideological, religious, political or similar objectives, or to intimidate⁶ any person⁷ in furtherance of such objectives.

Illustration 1: In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a US based Internet Service Provider (ISP) and damaged part of its record keeping system.

The ISP had attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "you have yet to see true electronic terrorism. This is a promise."

Illustration 2: In 1998, Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. E-mail was tied up and undeliverable to the ISP's users, and support lines were tied up with people who couldn't get their mail.

¹ Premeditated use implies use preceded by careful planning, thought and / or deliberation.

² Disruptive activities are those that prevent the normal continuance of something.

³ The threat need not necessarily be directed towards the target of the act of cyber terrorism, but may be directed towards any person in whom the target has an interest.

⁴ The term cyber space used here extends to the entire virtual world, i.e. the Internet, stand alone computers, every bit of information stored in storage media - removable, non removable, physical and virtual.

⁵ The term intention implies the reason or purpose for which an act is committed, sought to be committed or threatened to be committed.

⁶ To intimidate means to put a person in fear and thereby compel him to do or not to do something that he does not desire to do.

⁷ The term person used here includes a human being, a corporate entity, a State, or a collection thereof.

The protestors also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same tactics against organizations using IGC services.

They demanded that IGC stop hosting the website for the Euskal Herria Journal, a New York-based publication supporting Basque independence.

Protestors said IGC supported terrorism because a section on the Web pages contained materials on the terrorist group ETA, which claimed responsibility for assassinations of Spanish political and security officials, and attacks on military installations. IGC finally relented and pulled the site because of the "mail bombings."

Illustration 3: In 2001, hackers broke into the U.S. Justice Department's web site and replaced the department's seal with a swastika, dubbed the agency the "United States Department of Injustice" and filled the page with obscene pictures.

Illustration 4: In 2005, US security consultants reported that hackers were targeting the U.S. electric power grid and had gained access to U.S. utilities' electronic control systems.

Illustration 5: In 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems.

Illustration 6: During the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with denial-of-service attacks by hacktivists protesting the NATO bombings.

In addition, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports. Web defacements were also common.

Illustration 7: Since December 1997, the Electronic Disturbance Theater (EDT) has been conducting Web sit-ins against various sites in support of the Mexican Zapatistas.

At a designated time, thousands of protestors point their browsers to a target site using software that floods the target with rapid and repeated download requests. EDT's software has also been used by animal rights groups against organizations said to abuse animals.

Electrohippies, another group of hacktivists, conducted Web sit-ins against the WTO when they met in Seattle in late 1999.

Illustration 9: In 1997, 35 computer specialists used hacking tools freely available on 1,900 web sites to shut down large segments of the US power grid. They also silenced the command and control system of the Pacific Command in Honolulu.

Illustration 10: In 2000, Asian School of Cyber Laws was regularly attacked by Distributed Denial of Service attacks by “hactivists” propagating the “right to pornography”. Asian School of Cyber Laws has spearheaded an international campaign against pornography on the Internet.

Illustration 11: In 2001, in the backdrop of the downturn in US-China relationships, the Chinese hackers allegedly released the Code Red virus into the wild. This virus infected millions of computers around the world and then used these computers to launch denial of service attacks on US web sites, prominently the web site of the White House.

21. Use of encryption by terrorists

A disturbing trend that is emerging nowadays is the increasing use of encryption, high-frequency encrypted voice/data links, encryption software like Pretty Good Privacy (PGP) etc by terrorists and members of organized crime cartels.

Strong encryption is the criminal’s best friend and the policeman’s worst enemy.

If a criminal were to use 512-bit symmetric encryption, how long would it take to decrypt the information using brute force techniques?

Suppose that every atom in the known universe (there are estimated to be 2^{300} of them) becomes a computer capable of checking 2^{300} keys per second, then it would take 2^{162} millennia to search 1% of the key space of a 512-bit key. The universe is believed to have come into existence less than 2^{24} years ago.

Illustration 1: Leary, who was sentenced to 94 years in prison for setting off fire bombs in the New York (USA) subway system in 1995, had developed his own algorithm for encrypting the files on his computer.

Illustration 2: The Cali cartel is reputed to be using (1) sophisticated encryption to conceal their telephone communications, (2) radios that distort voices, (3) video phones

which provide visual authentication of the caller's identity, and (4) instruments for scrambling transmissions from computer modems.

Illustration 3: The Italian mafia is believed to use PGP.

Illustration 4: On March 20, 1995, the Aum Supreme Truth cult dropped bags of sarin nerve gas in the Tokyo subway, killing 12 people and injuring 6,000 more.

Members of the cult had developed many chemical and biological weapons, including Sarin, VX, Mustard gas, Cyanide, botulism, anthrax and Q fever.

It is believed that preparations were underway to develop nuclear capability. The cult was also believed to be developing a "death ray" that could destroy all life!

The records of the cult had been stored in encrypted form (using the RSA algorithm) on computers.

The enforcement authorities were able to decrypt the information as the relevant private key was found in a floppy disk seized from the cult's premises. The encrypted information related to plans of the cult to cause mass deaths in Japan and USA.

Illustration 5: In 1997, a Bolivian terrorist organization had assassinated four U.S. army personnel.

A raid on one of the hideouts of the terrorists yielded information encrypted using symmetric encryption.

A 12-hour brute force attack resulted in the decryption of the information and subsequently led to one of the largest drug busts in Bolivian history and the arrest of the terrorists.

Illustration 6: James Bell was arrested for violating internal revenue laws of the USA. He did this by: (1) collecting the names and home addresses of agents and employees of the Internal Revenue Service (IRS) of the USA in order to intimidate them; (2) soliciting people to join in a scheme known as "Assassination Politics". Under this scheme those who killed selected government employees, including tax collectors, would be rewarded; (3) using false Social Security Numbers to hide his assets and avoid taxes; (4) contaminating an area outside IRS premises in many states of the USA with Mercaptan (a stink gas).

Investigators found on his computer documents relating to a plan to destroy electronic equipment with nickel-plated carbon fiber.

They also found an invoice for the purchase of the fiber at his residence, and a bundle of the material at the residence of his associate, Robert East. Bell had exchanged PGP-encrypted e-mail messages with some of his associates.

As part of his plea bargain, he turned over the passphrase to his private key. This allowed investigators to decrypt messages that he had received.

Illustration 7: Dutch organized crime syndicates use PGP and PGPfone to encrypt their communications. They also use palmtop computers installed with Secure Device, a Dutch software product for encrypting data with International Data Encryption Algorithm (IDEA).

In 1995, the Amsterdam Police captured a PC in possession of one organized crime member. The PC contained an encrypted partition, which they were able to recover only in 1997.

Illustration 8: An encryption case occurring in Vilseck, West Germany involved theft, fraud, and embezzlement of U.S. defense contractor and U.S. government funds from 1986 to 1988.

The accused had stored financial records relating to the crimes on a personal computer, the hard disk of which had been password protected.

The police used hacking software to defeat the password protection, only to find that some of the files listed in the directory had been encrypted.

They then found the encryption program on the hard disk and used brute force tools to decrypt the files.

Illustration 9: The Dallas Police Department in the USA encountered encryption in the investigation of a drug ring, which was operating in several states of the USA and dealing in Ecstasy.

A member of the ring, residing within their jurisdiction, had encrypted his address book. He turned over the password, enabling the police to decrypt the file.

Meanwhile, however, the accused was out on bail and alerted his associates, so the decrypted information was not as useful as it might have been.

The police noted that Ecstasy dealers were more knowledgeable about computers when compared with other types of drug

dealers, most likely because they were younger and better educated.

Illustration 10: Kevin Poulsen was a skilled hacker who rigged radio contests and burglarized telephone-switching offices and hacked into the telephone network in order to determine whose phone was being tapped and to install his own phone tapping devices.

Poulsen had encrypted files documenting everything from the phone tapping he had discovered to the dossiers he had compiled about his enemies. The files had been encrypted several times using the Data Encryption Standard.

A US Department of Energy supercomputer took several months to find the key, at a cost of millions of dollars. The result yielded nearly ten thousand pages of evidence.

Illustration 11: The mother of a 15-year old boy filed a complaint against an adult who had sold her son US \$ 1000 worth of hardware and software for one dollar.

The man had also given the boy lewd pictures on floppy disks.

The man subsequently mailed the boy pornographic material on floppy disks and sent pornographic files over the Internet.

When the accused was arrested it was found out that he had encrypted a directory on the system using PGP. The police were never able to decrypt the files.

2. Hacker Methodology

In this chapter we examine the methodology used by a hacker or cyber criminal. A hacker would usually begin with footprinting. This may involve a whois search, analysis of the robots.txt file of the website of the target organisation, web crawling and port scanning.

A hacker targeting an ecommerce website could use cookie manipulation and hidden field manipulation for eShoplifting. A web hacker could also use brute forcing software coupled with social engineering to carry out web defacement.

The use of Trojans by hackers and cyber criminals is also very common nowadays. The important issues pertaining to Trojans have been dealt with in the next chapter. These issues include types of Trojans, manipulating windows suffixes, mimicking file names, wrapper tools, Trojanizing software distribution sites and poisoning the source. Some Trojan related cases have also been discussed. The concept of Easter eggs has also been touched upon. Basic technical concepts of computer worms and computer viruses have also been covered in this book.

1. Footprinting

Footprinting is usually done for the purpose of finding ways to intrude into the target environment. It can reveal system vulnerabilities and improve the ease with which these can be exploited. The purpose is to learn as much as possible about the target.

Footprinting is the process of collecting data about a target organization's technology framework for the process of planning an attack (or for securing against an attack). Footprinting usually does not involve any active attack against the target, it only involves gathering of relevant information that can later be used to plan an attack.

1.1 Physical location and contact information

Source of information: (1) Corporate website (2) Business directories (3) online directories (4) annual reports (5) publications etc

Potential use / misuse: Can be used to plan a social engineering attack.

Illustration: The network administrator in a global software company received a set of beautifully packed CDs by courier. The CDs contained critical and non critical "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. A subsequent hacking attack

resulted in a millions of dollars worth of source code being stolen.

1.2 General information on the IT infrastructure

Source of information: 1. Red Herring Prospectus⁸ published by a company at the time of its Initial Public Offering (IPO).

Potential use / misuse: Can be used to plan a social engineering attack.

Illustration: The red herring prospectus of Deccan Aviation Ltd details its IT Infrastructure. The document discloses that Air Deccan has “centralised IT resources within its operations, under the coverage of an IT team which as of March 31, 2006 included 35 staff”. The document also discloses that its “CRS resides on servers hosted at InterGlobe’s data centre located in Gurgaon, India”.

An interesting extract from the prospectus is: “The servers are connected with redundant Internet connections leased from BSNL and Bharti, as well as by HCL wireless loop to help maximise network availability. Connectivity is maintained using an automated router that switches from a primary BSNL connection to a backup Bharti connection in case of failure. If both the leased connections fail the HCL wireless loop is used to keep the site live. ... the Air Deccan servers are kept isolated from other networks and a Cisco Pix 515e Firewall and LINUX firewall has been installed to extend network security”.

1.3 IP addresses of servers

Source of information: IP address of the web servers can be obtained by a whois search⁹. IP address of the name servers, mail servers etc can be obtained by performing a DNS Lookup¹⁰.

Potential use / misuse: Can be used to carry out port scanning to find out open ports, vulnerabilities etc. Can also be used to attack the computers using automated hacking and penetration testing software e.g. metasploit, backtrack etc.

1.4 IP addresses of individual computers

Source of information: (1) Analysis of the headers of emails sent by employees of the target organization. (2) Special ‘tracking’ emails sent to employees of the target organization¹¹.

⁸ These can be downloaded from: www.sebi.gov.in

⁹ Sites such as www.who.is can be used for this.

¹⁰ Sites such as www.uptools.com can be used for this.

¹¹ Sites such as www.readnotify.com can be used for this.

Potential use / misuse: Can be used to carry out port scanning to find out open ports, vulnerabilities etc. Can also be used to attack the computers using automated hacking and penetration testing software e.g. metasploit, backtrack etc.

1.5 Recent mergers, acquisitions, takeovers

Source of information: Information about the target organization's recent mergers, acquisitions, takeovers, can be obtained from the target's website and also from websites of regulatory bodies and stock exchanges¹² etc.

Potential use / misuse: This information is relevant as it takes months after a merger / acquisition for networks of the merging organizations to 'harmonize'. During this period these networks are vulnerable.

1.6 Websites

Source of information: Comments put by the web developers in the HTML or JavaScript code of the target website can be obtained from the target websites. The robots.txt file can be obtained from the website.

Advanced options of search engines such as www.google.com can be used to download word documents, excel files etc from the target website. These files can contain important information as well as deleted data that can be recovered. The entire website can be downloaded using tools such as websleuth.

Potential use / misuse: This information can point to vulnerabilities or loopholes that can be exploited.

1.7 Wireless network

Source of information: War-driving using a GPS enabled phone along with software such as AiroMap can reveal if the target has any open or weakly protected wireless networks.

Potential use / misuse: This information can point to vulnerabilities or loopholes that can be exploited.

1.8 Other information

Source of information: News items about any security breaches at the target organization can be obtained from news websites and specialized search engines such as www.data64.cc and www.bugs.ms

Statutory declarations made to the Registrar of Companies, Stock Exchange, SEBI etc may be available from the relevant websites or may

¹² Sites such as www.sebi.gov.in, www.bseindia.com, www.nseindia.com can be used for this.

have to be obtained from the authorities directly. Traceroute can also be performed.

Potential use / misuse: This information can point to vulnerabilities or loopholes that can be exploited. Traceroute is used to gather information about network infrastructure and IP ranges around a given host. Traceroute information can be used to map out the nodes available on a target's network architecture and later to exploit vulnerable or compromised nodes/computers.

2. Analyzing the robots.txt file

A robot is a program that automatically traverses the Internet by visiting a web page and then retrieving all linked files.

Web robots are sometimes referred to as Web Wanderers, Web Crawlers, or Spiders. These names are a bit misleading as they give the impression that the software itself moves between sites like a virus.

This is not the case. A robot simply visits sites by requesting documents from them¹³.

The quick way to prevent all robots from visiting a website is to put these two lines into the robots.txt file on the server:

```
User-agent: *
Disallow: /
```

Illustration

```
User-agent: webcrawler
Disallow: /tmp
Disallow: /logs
```

This indicates that the robot called webcrawler should not visit URLs starting with /tmp or /log.

A webmaster would usually create the robots.txt file in such a way that robots do not visit the portions of the website that contain sensitive information. A hacker can examine the robots.txt file and get an indication of which parts of the website he should target.

¹³ To see a list of active robots and their features, visit:
<http://www.robotstxt.org/wc/active.html>

3. Web crawling

Web crawling enables a hacker to download an entire website. It also enables him to search the website for useful information (such as email addresses, hidden fields, links to other servers etc)¹⁴.

4. Port scanning

Port has a dual definition in computers. There are many different ports on the computer itself: ports to plug in a mouse, keyboard, USB devices, printer, monitor, etc.

However, the types of ports that are more relevant to information security are the virtual ports found in Transmission Control Protocol / Internet Protocol (TCP/IP). TCP/IP is the basic communication language or protocol of the Internet.

Ports are like channels on your computer. Normal web or http (hyper text transfer protocol) traffic flows on port 80. POP3 (Post Office Protocol) email flows through port 110. By blocking or opening these ports into and out of your network you can control what kinds of data can flow through your network.

Scanning a port can be compared with a security guard traversing a neighbourhood and checking every door and window to assess which doors or windows are open and which are locked.

Port Scanning is the act of systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open “doors” to a computer. Port scanning has legitimate uses such as in managing networks, but can also be malicious in nature if someone is looking for a weakened access point to break into a computer.

Port scanning is also a prominent technique used to reveal what services are available (in order to plan an exploit involving those services), and to determine the operating system of a particular computer. A program that attempts to learn about the weaknesses of a computer or network edge device by repeatedly probing it with requests for information can be called a port scanner.

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are two of the protocols that make up the TCP/IP protocol suite which is used universally to communicate on the Internet. Each of these has ports 0 through 65535 available so essentially there are more than 65,000 “doors” to a computer.

¹⁴ Useful software for web crawling include *Sam Spade* and *Black Widow*.

The first 1024 TCP ports are called the Well-Known Ports and are associated with standard services such as, HTTP, FTP (File Transfer Protocol) SMTP (Simple Mail Transfer Protocol) or DNS (Domain Name System).

Some of the addresses over 1023 also have commonly associated services, but the majority of these ports are not associated with any service and are available for a program or application to use to communicate on¹⁵.

If a port scan is being conducted with malicious intent, the intruder would generally prefer to go undetected. Network security applications can be configured to alert administrators if they detect connection requests across a broad range of ports from a single host.

To get past this problem, intruders can scan the ports in strobe or stealth mode.

Strobing limits the ports to a smaller target set rather than blanket scanning of all 65536 ports. Stealth scanning utilizes techniques such as reducing the speed of the scan. By scanning the ports over a much longer period of time the chance that the target will sound an alarm also goes down.

There are a number of different methods to perform the actual port scans as well as tricks to hide the true source of a port scan¹⁶.

5. Cookie Manipulation

A cookie is a small file or text-only string registered in the memory of a web browser. It is used to identify a website user. The term originates from a well-known computer science term that is used when describing an opaque piece of data held by an intermediary.

Illustration: Sanya enters her username and password and logs into gmail.com. Gmail places a cookie in her browser.

Every time that Sanya connects to the gmail server (to send an email, read an email etc), gmail verifies her logged in status and identity based on the cookie in her browser.

Once Sanya logs out, the cookie is destroyed.

Websites use cookies to authenticate users (e.g. gmail.com) personalize data (e.g. My Yahoo or Excite), to assist customers with online sales or

¹⁵ For a detailed listing of port numbers please visit:
<http://www.iana.org/assignments/port-numbers>

¹⁶ Useful software for port scanning include *nmap*

services (e.g. eBay.com or Amazon.com) or merely for collecting statistical and demographic data (e.g. DoubleClick.com).

Cookies which are saved in the form of simple text files can be deleted. If you delete a cookie while your browser is open, it will be recreated when you close the browser. This is because all cookies are held in the memory of your browser till you close the browser.

You can set the options offered by your Internet browser to accept either all, some or none of the incoming cookies.

Your browser can be set to warn you before accepting cookies.

```
visitor=Name=sanya@www.asianlaws.net/1536136144588800300059503411794224129887631*
```

A demo cookie from asianlaws.net

Many sites use cookies to implement access control schemes of various sorts. For example, a subscription site that requires a user name and password might pass a cookie back to your browser the first time you log in.

Thereafter, the site will give you access to restricted pages if your browser can produce a valid cookie, basically using the cookie as an admission ticket. This can have several advantages for the site, not the least of which is that it can avoid the overhead of looking up your user name and password in a database each and every time you access a page.

However, unless this type of system is implemented carefully, it may be vulnerable to exploitation. For instance, a hacker could use a packet sniffer (discussed later in this book) to intercept the cookie as it passes from your browser to the server and then use it to obtain free access to the site.

There are 6 parameters in a cookie: (1) the name of the cookie (2) the value of the cookie (3) the expiration date of the cookie (4) The path the cookie is valid for (5) the domain the cookie is valid for (6) the requirement for a secure connection to use the cookie.

Out of these, two are compulsory (i.e. its name and its value). A semicolon [;] separates each parameter when it is set explicitly.

The *name* and the *value* of the cookie can be set by pairing them together. e.g., Name=Sanya

The *expires* parameter allows you to set the lifetime of the cookie. e.g. expires=Sat, 25-Apr-2011 18:30:00 GMT

If the ‘Expires’ parameter is not set clearly or is not set at all then by default the expiry gets set to the end of the session. Although the length of the session can depend on the browsers and the servers, usually the

length of a session is considered to be the time that the browser window remains open. This is the case even if the user is no longer at that website.

Out of the four optional settings or parameters of a cookie, the *path* is probably the most useful. This parameter establishes the URL path within which the cookie remains valid. If the user reaches pages which are not contained in this path then the browser can no longer use this cookie. e.g., path=/documents

Suppose the path of the cookie is not set explicitly, then by default it takes the path as the URL of the document that has created the cookie.

The *domain* parameter extends the path parameter a little. What happens if a site uses multiple servers for one domain? It is here that it becomes important to specify the Domain parameter in such a way so as to make the cookie accessible to any of the pages of these multiple servers. e.g., domain=www.asianlaws.net

It is possible to assign cookies to either an individual machine or to an entire Internet domain.

Remember that to be able to set a cookie for a domain, the server should be a member of that domain.

If the Domain parameter is not set explicitly, then by default the full domain of the document that has created the cookie is taken.

The *secure* parameter indicates that a cookie with this parameter should only be used under secure server condition, e.g. SSL (Secure Socket Layer).

Simple cookie manipulation

A simple cookie that is stored on the hard disk is used for saving basic user information and preferences. It is not used for authentication. We will discuss its manipulation using a simple illustration.

- (1) Visit <http://www.asianlaws.net/ceh/10/index.htm>
- (2) In the “name” field, enter “Sanya” and then click on “Sign in”. It automatically takes you to the web page
<http://www.asianlaws.net/ceh/10/read-cookie.php>
- (3) This page displays the text “Your name is Sanya”
- (4) When you clicked on “Sign in”, a cookie was created on your computer. When the read-cookie.asp page opened, it read that cookie to find the name (Sanya in this case) and displayed it.

- (5) Now install the *Cookie Editor* software¹⁷ on your computer. This is located in the “Web Hacking” folder of the CD ROM accompanying this book.
- (6) When you run the software, it will display all the cookies present on your computer. Double click on the cookie whose “Cookie Domain” is [www.asianlaws.net/](http://www.asianlaws.net)
- (7) Change the value “Sanya” to “Tanya” and click on “Save”.
- (8) Now shut your browser and open it up again.
- (9) Go directly to the web page:
<http://www.asianlaws.net/ceh/10/read-cookie.php>
- (10) The page displays the text “Your name is Tanya”. You have just manipulated the cookie and change the value from “Sanya” to “Tanya”.

Exercise: Use cookie manipulation to solve the case study at:

<http://www.asianlaws.net/realistic/3>

6. eShoplifting

Shoplifting is the act of stealing goods that are on display in a store. Simply put, e-shoplifting is the act of stealing goods that are available through an electronic store.

An eShop combines business logic and technology. Hackers target the vulnerabilities in the technology to buy products and services at lower prices (or even for free). Some of the major causes of weaknesses in eShops are:

- (1) Poor input validation – This implies that the input of the user is not being properly sanitized or checked. Instead of entering his username, a user could enter some malicious code that could exploit the system.
- (2) Inappropriate utilization of cookies – This implies that the cookies are vulnerable to exploitation. The hacker could manipulate important values stored in the cookies.
- (3) Improper session or state tracking – This implies that the methodology used to track logged in users and their activities is not adequate.
- (4) Weakness in client-side scripting – Client side scripting is the class of computer programs on the web that are executed “client-side” (by the user's web browser), instead of server-side (on the web server). A hacker

¹⁷ This can be downloaded from: <http://www.proxoft.com/CookieEditor.asp>

can manipulate the client side scripting to pass on malicious code to the eShop.

(5) Poor database integration – This implies that the database storing all the information is not securely integrated with the front end and other sections of the eShop. This can lead to information being stolen while it is being passed on to or from the database. It could also lead to the user passing malicious code into the database.

(6) Security flaws in third-party products – Flaws in third party products such as payment gateways can lead to the eShop being compromised.

7. Web defacement

Web defacement occurs when a hacker maliciously replaces a webpage with another page, usually containing provocative, pornographic or offending information.

The damage from a web defacement incident can be tremendous. Damage can range from loss of reputation, loss of customer trust and huge loss of revenue. Globally thousands of web defacement incidents take place annually targeting websites belonging to Governments, academic institutions, religious groups, ecommerce merchants etc.

Although it sounds simplistic, obtaining administrator usernames and passwords is a very popular and effective technique used by hackers to break into a site and deface it. To retrieve this information, hackers use the following:

- (1) information-gathering techniques, which exploit vulnerabilities in the system making use of publicly available information (e.g., domain registration records),
- (2) 'social engineering' tactics (e.g., emailing / calling an employee and posing as a system administrator),
- (3) brute force attacks, wherein a password cracking software is used to obtain the relevant usernames and passwords.

Illustration: The website of a major cyber crime cell in India was defaced a few years ago, allegedly by two hackers using a password cracking software named Brutus. Once they obtained the username and password using Brutus, they replaced the homepage of the website with pornographic information.

8. Using google as a hacking tool

Google, arguably the world's most popular and powerful search engine, can be easily misused by hackers. Malicious users can use the Google search engine extensively to gather confidential or sensitive information, which is not visible through common searches. There are several special commands of Google that can be used for critical information digging.

intitle:

The “intitle:” syntax helps Google restrict the search results to pages containing that word in the title. For example,

intitle: login password

will return links to those pages that has the word "login" in their title, and the word "password" anywhere in the page.

Similarly, if one has to query for more than one word in the page title then in that case “**allintitle:**” can be used instead of “intitle” to get the list of pages containing all those words in its title. For example using

intitle: login intitle: password

is same as querying allintitle: login password

These search syntax can be used to look for vulnerable sites

allintitle: “index of /root”

will list down the links to the web server which gives access to restricted directories like “root” through web. This directory sometimes contains sensitive information which can be easily retrieved through simple web requests.

allintitle: "index of /admin"

will list down the links to the websites which have index browsing enabled for restricted directories like “admin” through web. Most of the web applications sometimes use names like “admin” to store admin credentials in it. This directory sometimes contains sensitive information which can be easily retrieved through simple web requests.

Other illustrations are:

intitle:"Index of" .sh_history

```
intitle:"Index of" .bash_history  
intitle:"index of" passwd  
intitle:"index of" people.lst  
intitle:"index of" pwd.db  
intitle:"index of" etc/shadow  
intitle:"index of" spwd  
intitle:"index of" master.passwd  
intitle:"index of" htpasswd  
intitle:"index of" members OR accounts  
intitle:"index of" user_carts OR user_cart  
allintitle: sensitive filetype:doc  
allintitle: restricted filetype:mail  
allintitle: restricted filetype:doc site:gov
```

site:

The “site:” syntax restricts Google to query for certain keywords in a particular site or domain. For example:

```
courses site:asianlaws.org
```

will look for the keyword “courses” in those pages present in all the links of the domain “asianlaws.org”. There should not be any space between “site:” and the “domain name”.

inurl:

The “inurl:” syntax restricts the search results to those URLs containing the search keyword. For example:

```
inurl: passwd
```

will return only links to those pages that have "passwd" in the URL.

Similarly, if one has to query for more than one word in an URL then in that case “**allinurl:**” can be used instead of “inurl” to get the list of URLs containing all those search keywords in it. e.g.

```
allinurl: etc/passwd
```

will look for the URLs containing “etc” and “passwd”. The slash (“/”) between the words will be ignored by Google.

These search syntax can be used to look for vulnerable sites

allinurl:winnt/system32/

will list down all the links to the server which give access to restricted directories like “system32” through web. If access to cmd.exe in the “system32” directory is obtained, and if it can be executed, then the server can be compromised.

allinurl: wwwboard/passwd.txt

will list down all the links to the server which are vulnerable to “WWWBoard Password vulnerability”. To know more about this vulnerability, visit:

<http://www.securiteam.com/exploits/2BUQ4S0SAW.html>

inurl:.bash_history

will list down all the links to the server which give access to “.bash_history” file through web. This is a command history file.

This file includes the list of commands executed by the administrator, and sometimes includes sensitive information such as passwords typed in by the administrator. If this file is compromised and it contains the encrypted unix (or *nix) password then it can easily be cracked using tools like “John The Ripper”.

inurl: config.txt

will list down all the links to the servers which give access to “config.txt” file through web. This file contains sensitive information, including the hash value of the administrative password and database authentication credentials.

Other illustrations are:

- inurl:admin filetype:txt
- inurl:admin filetype:db
- inurl:admin filetype:cfg
- inurl:mysql filetype:cfg
- inurl:passwd filetype:txt
- inurl:iisadmin
- inurl:orders.txt

- inurl:"wwwroot/*."
- inurl:adpassword.txt
- inurl:webeditor.php
- inurl:file_upload.php
- inurl:gov filetype:xls "restricted"
- index of ftp +.mdb allinurl:/cgi-bin/ +mailto
- inurl:auth_user_file.txt

link:

“link:” syntax will list down webpages that have links to the specified webpage. E.g.

link:www.asianlaws.org

will list webpages that have links pointing to the AsianLaws.org homepage. Note there can be no space between the "link:" and the web page URL.

filetype:

This “filetype:” syntax restricts Google search for files on internet with particular extensions (i.e. doc, pdf or ppt etc). For example:

filetype:doc site:gov confidential

will look for files with “.doc” extension in all government domains with “.gov” extension and containing the word “confidential” either in the pages or in the “.doc” file. i.e. the result will contain the links to all confidential word document files on the government sites.

related:

The “related:” syntax will list web pages that are "similar" to a specified web page. e.g.

related:www.asianlaws.org

will list web pages that are similar to the AsianLaws.org site. Note there can be no space between the "related:" and the web page URL.

cache:

The query “cache:” will show the version of the web page that Google has in its cache. e.g.

cache:www.asianlaws.org

will show Google's cache of the AsianLaws.org homepage. Note there can be no space between the "cache:" and the web page URL.

If you include other words in the query, Google will highlight those words within the cached document. e.g.

cache:www.asianlaws.org courses

will show the cached content with the word "courses" highlighted.

intext:

The "intext:" syntax searches for words in a particular website. It ignores links or URLs and page titles. e.g.

intext:exploits

will return only links to those web pages that have the search keyword "exploits" in its webpage.

phonebook:

"phonebook" searches for U.S. street address and phone number information. e.g.

phonebook:Lisa+CA

will list down all names of person having "Lisa" in their names and located in "California (CA)". This can be used for collecting personal information for social engineering.

9. Packet sniffing

All network data travels across the Internet, and then into and out of PCs, in the form of individual, variable size, "data packets". Since the typical PC user never "sees" any of this raw data, many spyware systems covertly send sensitive information out of the user's computer without their knowledge.

Packet sniffing is a method of tapping each packet as it flows across the network i.e., it is a technique, in which a user sniffs data belonging to other users of the network. Packet sniffers can be used as an administrative tool or as a hacking tool. It depends on the user.

Network sniffers can capture passwords and other sensitive pieces of information passing through the network.

3. Trojans

1. Introduction to Trojans

In the 12th century BC, Greece declared war on the city of Troy. The dispute erupted when the prince of Troy abducted the queen of Sparta and declared that he wanted to make her his wife. This naturally angered the Greeks (and especially the queen of Sparta). The Greeks besieged Troy for 10 years but met with no success as Troy was very well fortified.

In a last effort, the Greek army pretended to be retreating, and left behind a huge wooden horse. The people of Troy saw the horse and thought it was a gift from the Greeks. They pulled the horse into their city, unaware that the hollow wooden horse had some of the best Greek soldiers hiding inside it.

Under the cover of night, the soldiers snuck out and opened the gates of the city, and later, together with the rest of the army, killed the entire army of Troy.

Similar to the wooden horse, a Computer Trojan (also referred to as Trojan Horse program) pretends to do one thing while actually doing something completely different.

**This chapter is based upon excerpts from writings of Ed Skoudis
provided courtesy of Addison Wesley Professional.**

A Trojan Horse program is a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality. Today's Trojan horses try to sneak past computer security fortifications (such as firewalls), by employing like-minded trickery. By looking like normal software, Trojan horse programs are used for the following goals:

- Duping a user or system administrator into installing the Trojan horse in the first place. In this case, the Trojan horse and the unsuspecting user becomes the entry vehicle for the malicious software on the system.
- Blending in with the “normal” programs running on a machine. The Trojan horse camouflages itself to appear to belong on the system so users and administrators continue their activity, unaware of the malicious code’s presence.

Attackers have devised a myriad of methods for hiding malicious capabilities inside their wares on your computer. These techniques include:

- employing simple, yet highly effective naming games,

- using executable wrappers,
- attacking software distribution sites,
- manipulating source code,
- co-opting software installed on your system, and
- disguising items using polymorphic coding techniques.

As we discuss each of these elements, we must bear in mind that the attackers' main goal is to disguise the malicious code so that the victims do not realize what the attacker is up to.

2. Types of Trojans

The most common types of Trojans found today are:

Remote Administration Trojans (RATs)

These are the most popular Trojans. They let a hacker access the victim's hard disk, and also perform many functions on his computer (shut down his computer, open and shut his CD-ROM drive etc.).

Modern RATs are very simple to use. They come packaged with two files - the server file and the client file. The hacker tricks someone into running the server file, gets his IP address and gets full control over the victim computer.

Some Trojans are limited by their functions, but more functions also mean larger server files. Some Trojans are merely meant for the attacker to use them to upload another Trojan to the target's computer and run it; hence they take very little disk space. Hackers also bind Trojans into other programs, which appear to be legitimate, e.g. a RAT could be bound with an e-greeting card.

Most RATs are used for malicious purposes - to irritate or scare people or harm computers. There are many programs that detect common Trojans. Firewalls and anti-virus software can be useful in tracing RATs.

RATs open a port on your computer and bind themselves to it (make the server file listen to incoming connections and data going through these ports). Then, once someone runs his client program and enters the victim's IP address, the Trojan starts receiving commands from the attacker and runs them on the victim's computer. Some Trojans let the hacker change this port into any other port and also put a password so only the person who infects the specific computer will be able to use the Trojan.

In some cases the creator of the Trojan would also put a backdoor within the server file itself so he'll be able to access any computer running his Trojan without the need to enter a password. This is called "a backdoor within a backdoor" e.g. CIA, Netbus, Back Orifice, Sub7.

Password Trojans

Password Trojans search the victim's computer for passwords and then send them to the attacker or the author of the Trojan. Whether it's an Internet password or an email password there is a Trojan for every password. These Trojans usually send the information back to the attacker via email.

Privileges-Elevating Trojans

These Trojans are usually used to fool system administrators. They can either be bound into a common system utility or pretend to be something harmless and even quite useful and appealing. Once the administrator runs it, the Trojan will give the attacker more privileges on the system. These Trojans can also be sent to less-privileged users and give the attacker access to their account.

Key loggers

These Trojans are very simple. They log all of the victim's keystrokes on the keyboard (including passwords), and then either save them on a file or email them to the attacker once in a while. Key loggers usually don't take much disk space and can masquerade as important utilities, thus becoming very hard to detect.

Joke Programs

Joke programs are not harmful. They can either pretend to be formatting your hard drive, sending all of your passwords to some hacker, turning in all information about illegal and pirated software you might have on your computer to the police etc. In reality, these programs do not do anything.

Destructive Trojans

These Trojans can destroy the victim's entire hard drive, encrypt or just scramble important files. Some might seem like joke programs, while they are actually destroying every file they encounter.

3. Manipulating Windows Suffixes

One very simple Trojan horse naming technique used by attackers against Windows systems is to trick victims by creating a file name with a bunch of spaces in it to obscure the file's type. The three-letter suffix (also known as an “extension”) of a file name in Windows is supposed to indicate the file's type and which application should be used to view that file. For example, executables have the .EXE suffix, whereas text files end in .TXT.

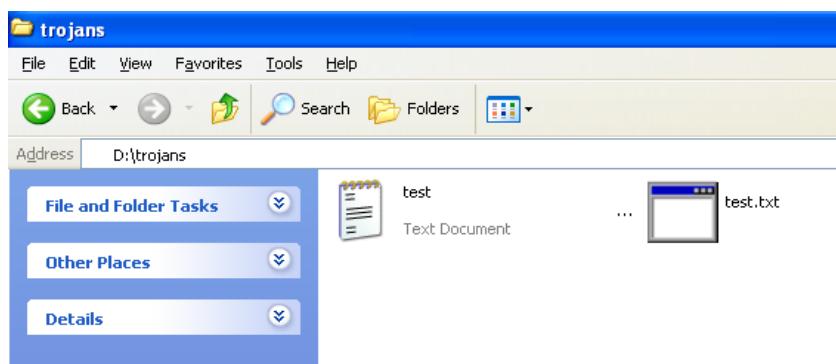
Vigilant users are wary of EXE files. So a hacker would need a trick to disguise an EXE file as something benign, such as a simple text file. An attacker could confuse a victim by naming a file with a bunch of spaces before its real suffix, like this:

just_text.txt

.exe

That .EXE at the end of the name after all of the spaces makes the program executable, but the unwary user might not notice the .EXE suffix. If users look at such a file with the Windows Explorer file viewer, it'll appear that the file might just be text. Most users would have no qualms about double-clicking such a file.

In the Windows Explorer, the display shows the file as something.txt followed by “...”. Those innocent-looking dots mean that the file name is actually longer than what is displayed.



The figure on the previous page illustrates two EXE files that have been disguised to look like TXT files.

It is also easy to configure the system so that an executable program type's icon actually appears as a .TXT icon. This can be accomplished by altering the icon using one of a variety of tools.

Alternatively, an attacker could choose a file type that is both executable and has an icon that looks quite similar to a text file, such as the Shell Scrap Object file type, with a .SHS extension. These .SHS files are used to bundle together commonly copied and pasted text and pictures, as well as commands, for various Windows programs.

The illustration below shows the icon for an SHS file (left) and a TXT file (right).



Numerous file suffixes could be used to deliver and contain malicious code on a target machine.

Table 1 below shows the different file types, developers use to hold binary, scripts, and other types of executable code.

In Windows, the operating system uses the suffix to determine which application to use when opening a document. For a detailed description of any type of file suffix, you can visit to <http://fileext.com>.

Table 1: Common file types used to hold executable code

File Extension	Purpose of This Type of File
.API	Acrobat Plug-in, for extending the capabilities of Adobe's Acrobat file viewing tool.
.BAT	Batch processing file, used to execute a series of contained commands in sequential order.
.BPL	Borland package libraries, containing chunks of shared code used in programs developed within the Delphi software language and environment.

.CHM	Compiled HTML Help file, which could include a link that would download and execute malicious code on a victim machine.
.COM	Command file, containing scripts or even executables for DOS and Windows systems.
.CPL	Windows Control Panel Extension, allowing new capabilities in your previously dull and monotonous control panels.
.DLL	Dynamic Link Library, executable code that is shared by other programs on the system.
.DPL	Delphi Package Library, used to add bundled together shared libraries of code developed in the Delphi programming environment.
.DRV	Device driver, used to extend the hardware support of a Windows machine, but could be abused to modify the kernel and completely control the victim machine.
.EXE	Windows binary executable program.
.HTA	HyperText application, a file that can run applications from an HTML document.
.JS	JavaScript, a scripting language that can be embedded in HTML or run through any JavaScript interpreter, including the Windows Scripting Host built into Windows systems.
.OCX	Object Linking and Embedding (OLE) control, used to orchestrate the interaction of several programs on a Windows machine.
.PIF	Program Information File, used to tell Windows how to run a non-Windows application.
.pl	Perl script, a powerful, high-level scripting language supported on most UNIX systems and some Windows machines.
.SCR	Screen saver program, which includes binary executable code.
.SHS	Shell Scrap Object file, a format used to hold frequently repeated commands, text, and pictures for Windows programs.
.SYS	System configuration file, normally used to establish system settings, but could be used by an attacker to reconfigure a victim machine.

.VBE	VBScript Encoded Script file, used to carry Visual Basic Scripts.
.VBS	Visual Basic Script, a scripting language built into many Windows machines.
.VXD	Virtual device driver, a device driver with direct access into a Windows kernel.
.WMA	Windows Media Audio file, used to store audio data, but has been exploited to carry a buffer overflow designed to execute malicious code embedded in the file.
.WSF	Windows Script File, designed to carry a variety of Windows script types.
.WSH	Windows Script Host Settings file, used to configure the script interpreter program on a Windows machine.

4. Mimicking File Names

These Trojan horse naming issues go far beyond just putting spaces between the name and its file extension on Windows systems. Often, to fool a victim, attackers create another file and process with exactly the same name as an existing program installed on the machine e.g. “iexplore”, a Windows process.

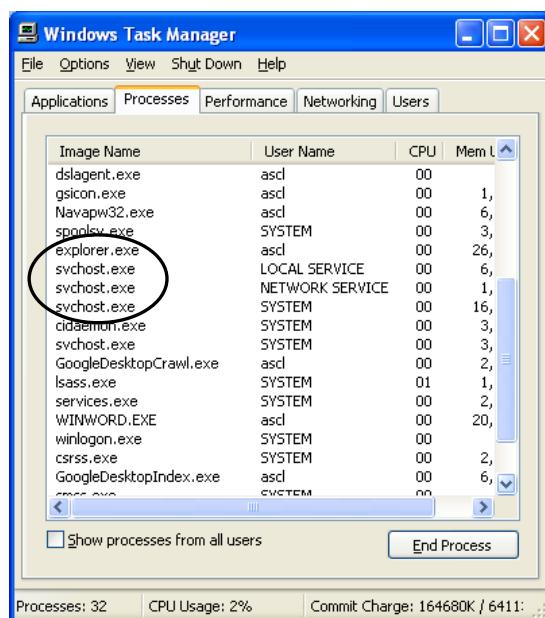
In this type of naming attack, the user could actually see two processes named “iexplore” running on his system: the normal “iexplore” that’s supposed to be there and another Trojan horse named “iexplore” by the attacker. A bunch of such naming schemes are possible. Table 2 lists common programs expected to be running on Windows operating systems whose names are frequently borrowed by attackers for malicious code.

Table 2: Common Names Given to Trojan Horses to Blend In

Name Given to Trojan Horse	Legitimate Program
win	Typically there is no legitimate process by this name on a Windows computer. However, attackers take advantage of the fact that many administrators might expect to see a process with this name.
iexplore	This executable is Microsoft’s Internet Explorer browser. On most Windows systems, a spare browser running every once in a while would go unnoticed.

notepad	This familiar editor frequently used on Windows systems is an ideal program for an attacker to impersonate. Several backdoor tools attempt to impersonate notepad.exe.
SCSI	Attackers sometimes name their Trojan horse processes SCSI, attempting to dupe an administrator into thinking that the program controls the SCSI chain. An administrator will hesitate to kill a process named SCSI for fear that it might disable the hard drive.
UPS	Sometimes, attackers name their processes UPS to fool administrators into thinking the program controls the uninterruptible power supply.

Note: Most of the processes named above are common on most Windows computers and their mere presence does not imply that the computer has been Trojanized. You can see the Windows Task Manager on a Windows 2003 system by hitting Ctrl-Alt-Delete and selecting Task Manager. Then by looking at the Processes tab, you can see the various processes running on the computer. If an attacker has installed another file with that name, then users will see a second copy of that process (say, svchost.exe) running in the Task Manager.



This is only a sample illustration. If you see multiple processes named svchost.exe on your computer, it does not necessarily mean that your computer has been Trojanized. A smart hacker can take advantage of an interesting characteristic of Windows 2000, XP, and 2003. In these operating systems, the Task Manager does not allow a user to kill processes that have certain names. If a process is named winlogon.exe, csrss.exe, or any other name shown in **Table 3** below, the system automatically assumes that it is a sensitive operating system process based solely on its name.

Table 3: Windows Process Names that cannot be killed with Task Manager

Windows Process Name	Purpose of Legitimate Process with This Name
csrss.exe	This is the environment subsystem process, which supports creating & deleting processes and threads and running console windows.
services.exe	This process is the Windows Service Controller, which is responsible for starting and stopping system services running in the background.
smss.exe	The Session Manager SubSystem on Windows machines is invoked during the boot process. Among numerous other tasks, it starts and supports the programs needed to implement the user interface, including the graphics subsystem and the log on processes.
System	This process includes most kernel-level threads, which manage the underlying aspects of the operating system.
System Idle Process	On a Windows system, this process is just a placeholder to indicate all of the CPU cycles consumed by idle tasks, when no specific other processes have a pressing need.
winlogon.exe	This process authenticates users on a Windows system by asking for user IDs and passwords, and interacting with other components to verify their validity.

If an attacker gives a backdoor a name from Table 3, Task Manager will refuse to kill it. The system believes that the backdoor process is really the vital system process. To prevent a user from accidentally killing a vital process and making the system unstable, Windows prevents users from killing any process with such a name.

Note: Under certain circumstances, you might legitimately have multiple copies of both csrss.exe and winlogon.exe running on a machine. If you use Windows Terminal Services or Citrix to allow multiple users to simultaneously log on to virtual desktops on a single Windows machine, each user will have a csrss.exe and winlogon.exe.

So, if there are two or more copies of these two processes running, you might not have been attacked; you're just looking at the processes created for different users.

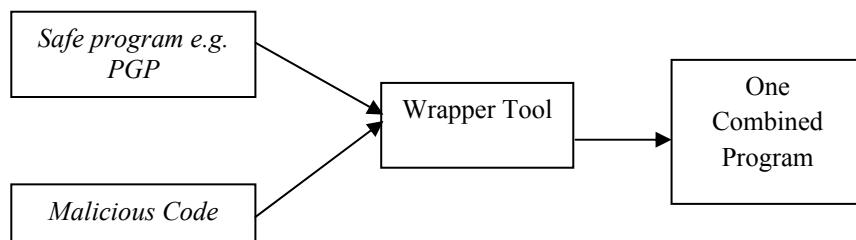
For the other processes listed in Table 3, however, only a single instance of the process should normally show up in Task Manager.

5. Wrapper Tools

A Trojan can be combined with an innocuous program to fool the victim. E.g. a Trojan can be combined with the PGP software. PGP or Pretty Good Privacy is a very popular encryption and digital signature software.

When an unsuspecting victim downloads PGP from a ‘dubious’ website, he receives the combined package (i.e. PGP and the Trojan). When he runs this Trojanized software, the malicious executable embedded in the package will typically run first (the vast majority of backdoors don’t display anything on the screen, so the victim will not see anything during this step, which usually takes less than a second).

After the backdoor is firmly lodged on the victim machine, the benign program (in this example PGP) runs. To combine two executables together, you need a **wrapper** tool (also called wrappers, binders, packers, EXE binders, and EXE joiners). The next figure illustrates how an attacker uses a wrapper program. Two programs enter and one program leaves with the combined functionality of both input programs.



In essence, these wrappers allow an attacker to take any executable backdoor program and combine it with any legitimate executable, creating a Trojan horse without writing a single line of new code! Even the most inexperienced attacker can easily create Trojan horses using this technique.

Wrapper tools combine two or more separate programs at a fundamental level into one package.

Some wrappers allow for combining two, six, nine, or even an arbitrary number of programs together. Others allow for the addition of static files into the mix. When the wrapper is run, it executes all included programs, and also unloads the bundled static files into the attacker's chosen places on the file system.

With such capabilities, these wrappers are actually becoming the functional equivalent of Setup programs. For most of the popular wrapper tools available today, when a combined package file is executed, the malicious program and benign program will each show up as separate running processes in Windows Task Manager. The two programs only live together in the file on the hard drive.

When a user is duped into running the package, the two wrapped programs become two separate processes. Therefore, to hide the malicious processes, attackers use wrappers together with the deceptive naming schemes discussed earlier.

Some wrappers go even further by encrypting the malicious code portion of the resulting package, so that antivirus programs on the target system have more difficulty detecting the malicious program.

Of course, to make the malicious program run on its target, the wrapper must add a decryption routine to the resulting package. Antivirus programs therefore look for the decryption code added by these popular wrapping tools.

Attackers sometimes also morph the decryption code, so that it dynamically alters itself to evade detection. Table 4 shows some of the most popular and powerful wrapper programs available.

Table 4: Popular Wrapper Tools

Wrapper Tool Name	Function of Wrapper Tool
AFX File Lace	This wrapper encrypts an executable and appends it to the end of another, unencrypted executable.

EliteWrap	<p>This program is the premier wrapper tool, with many features, including:</p> <ul style="list-style-type: none"> • The ability to bind together an unlimited number of executables. • A function to start programs in a specified order, with each program waiting for the other programs ahead of it to finish running before executing itself. • Built-in integrity checks to make sure the package hasn't been altered.
Exe2vbs	<p>This tool converts executable programs (in EXE format) into Visual Basic Scripts (VBSs or VBScripts). By packing the EXE inside of a VBScript, the attacker might be able to transmit a Trojan horse through e-mail filtering programs that block standard EXEs, but allow VBScripts to pass through.</p>
PE Bundle	<p>This program bundles together an executable with all the DLLs required by that executable to run. With this combined package, the malicious software will be able to run on the target system even if some critical DLLs are not installed there.</p>
Perl2Exe	<p>Using this tool, a developer can create standalone programs originally written in the Perl scripting language that do not require a Perl interpreter to run.</p> <p>Also, the original Perl code isn't included inside the resulting executable, making reverse engineering the functionality of the executable code significantly more difficult than simply analyzing more easily understood Perl scripts.</p> <p>This tool is available for both Windows and UNIX, turning a Perl script into an executable binary program. Binary executables can be created that will run on Windows or UNIX.</p>
Saran Wrap	<p>This easy-to-use GUI-based wrapper combines two executables together.</p>
TOPV4	<p>This so-called Teflon Oil Patch program combines up to nine executables together and sports a</p>

	simple GUI.
Trojan Man	This wrapper combines two programs, and also can encrypt the resulting package in an attempt to foil antivirus programs.

6. Trojaning Software Distribution Sites

One of the most lethal methods used by hackers to spread Trojans is to Trojanize a popular software and then watch as millions of unsuspecting people around the world download the software.

Take an example of a popular encryption and digital signature software like PGP. Everyday thousands of people from around the world download the PGP software. Imagine the impact if hackers are able to do the following:

- (1) Hack into the servers hosting PGP, and then
- (2) Replace the ‘pure’ PGP software with a Trojanized version of PGP (i.e. the PGP executable bound with a Trojan)

Subsequently the unsuspecting users who download and install PGP will end up infecting their own systems!

The conventional method

Imagine if the administrator of a large company receives an official looking CD ROM in an official looking package supposedly from Microsoft Corporation. The CD purports to contain the latest software updates.

Would the administrator install the ‘software updates’?

In 99 out of 100 cases, he would!

Well, the administrator would simply have installed a powerful backdoor into his company’s computer network. Sending Trojanized ‘software updates’, via conventional post or courier system is a very lethal weapon of information warfare.

It is surprisingly simple to fool even the most vigilant system administrators using official looking envelopes, letterheads, CDs etc.

The modern method

The conventional method of distributing Trojanized software is expensive. It also leaves a paper trail that the police can use to track down the hackers. The modern method of hacking into web servers, then Trojanizing popular software has the following plus points (for the hackers, not the victims!):

- (1) It is relatively inexpensive.
- (2) The impact is much greater (the more popular the software, the more the victims).
- (3) There is no paper trail. Instead there is a digital trail that is much easier to wipe out.

One of the earliest attacks of this kind involved the Washington University in USA in April 1994. In this incident an FTP server (wu-ftpd) was Trojanized. In 1999, a similar attack occurred involving the TCPWrapper distribution. (TCP Wrappers is a tool commonly used on Unix systems to monitor and filter connections to network services.)

Illustration 1: In May 2002, Monkey.org, a website that distributes popular security and hacking tools, was hacked into.

The hackers modified the following tools distributed through Monkey.org: the Dsniff sniffing program, the Fragroute IDS evasion tool and the Fragrouter IDS evasion tool.

The hackers replaced each tool with a Trojan horse version that created a backdoor on the systems of anyone who downloaded and installed these tools.

This attack was especially lethal as these tools are widely used by security professionals as well as by hackers.

Illustration 2: From July 30 to August 1, 2002, an attacker loaded a Trojan horse version of the Open Secure Shell (OpenSSH) security tool onto the main OpenSSH distribution Website (OpenSSH is widely used to provide tight security for remote access to a system).

However, diligent administrators who tried to protect their systems by downloading this security tool in late July 2002, unwittingly installed a backdoor.

Illustration 3: From September 28 until October 6, 2002, a period of more than one week, the distribution point for the most popular e-mail server software on the Internet was subverted.

The main FTP server that distributed the free, opensource Sendmail program was Trojanized with a backdoor.

Illustration 4: From November 11 to 13, 2002, tcpdump, the popular sniffing program, and libpcap, its library of packet capture routines, were replaced with a Trojan horse backdoor on the main tcpdump website.

Not only is the tcpdump sniffer widely used by security, network, and system administrators around the world, but the

libpcap (pronounced lib-pee-cap, which is short for “library for packet capture”) component is a building block for numerous other tools.

Administrators who installed tcpdump, libpcap, or any other package built on top of libpcap during this time frame were faced with a backdoor running on their systems.

7. Poisoning the Source

In this section, we will discuss a situation where a Trojan is implanted into a software product even before the product is released!

Hackers can Trojanize software programs during the software’s development and testing process. A hacker could join a software development company or contribute code to an open source software project.

As a developer or even a tester, the attacker could insert a relatively small backdoor of less than 100KB of code inside of hundreds of megabytes of legitimate code. This would be very difficult for anyone to uncover.

Any users purchasing the product would then unwittingly be buying a Trojan horse and installing it on their systems. The whole software product itself becomes the Trojan horse, doing something useful (that’s why you buy or download it), yet masking this backdoor.

Ken Thompson, noted UNIX co-creator and C programming language guru, discussed the importance of controlling source code and the possibility of planting backdoors in it in his famous 1984 paper titled *Reflections on Trusting Trust*¹⁸. In that classic paper, Thompson described modifying the source code for a compiler so that it built a backdoor into all code that it compiles.

The proposed attack was particularly dangerous, as even a brand new compiler that is compiled with a Trojan version of the old compiler would have the backdoor in it. Following is an extract from the paper:

You can't trust code that you did not totally create yourself.
(Especially code from companies that employ people like me.)
No amount of source-level verification or scrutiny will protect
you from using untrusted code. In demonstrating the possibility
of this kind of attack, I picked on the C compiler. I could have
picked on any program-handling program such as an
assembler, a loader, or even hardware microcode. As the level

¹⁸ See: <http://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf>

of program gets lower, these bugs will be harder and harder to detect. A well installed microcode bug will be almost impossible to detect.

This concern is even more disturbing than the Trojanizing of software distribution sites that we discussed in the last section. When an attacker Trojanizes a software distribution site, the developers of the software at least have a clean version of the software that they can compare against to detect the deception.

Solving problems is relatively easier after discovery, as a clean version of the software can be placed on the website for distribution. On the other hand, if an attacker embeds a Trojan horse during the software development process, the vendor might not even have a clean copy. If the attackers are particularly clever, they will intertwine a small, inconspicuous backdoor throughout the normal code, making eradication extremely difficult.

A software developer would have to scan enormous quantities of code to ensure the integrity of a whole product. The larger the software product, the more difficult detection and eradication become.

Most modern software tools are vast in scope. Detecting bugs in code, let alone backdoors, is very difficult and costly. To Trojanize a software product, an evil employee doesn't even have to actually write an entire backdoor into the product.

Instead, the malicious developer could purposefully write code that contains an exploitable flaw, such as a buffer overflow, that would let an attacker take over the machine. Effectively, such a purposeful flaw acts just like a backdoor. If the flaw sneaks past the software testing team, the developer would be the only one who knows about the hole initially. By exploiting that flaw, the developer could control any systems using his or her code.

Various analyses and surveys have revealed that, on average, a typical developer accidentally introduces between 100 and 150 defects per 1,000 lines of code. Although these defects are entirely unintentional, a single intentional flaw could be sneaked in as well.

Although many of these errors are simple syntactical problems easily discovered by a compiler, many of the remaining defects often result in gaping security holes. In fact, in essence, a security vulnerability is really just the very controlled exploitation of a bug to achieve an attacker's specific goal.

If the attacker can make the program fail in a way that benefits the attacker (by crashing the system, yielding access, or displaying

confidential information), the attacker wins. Estimating very conservatively, if only one in ten of the defects in software has security implications, that leaves between 10 and 15 security defects per 1,000 lines of code.

This looks even more dangerous when you consider that the Microsoft Windows XP operating system has approximately 45 million lines of code! Does this imply that Windows XP has about 450,000 security defects? Nobody knows for sure. What we do know is that the very same day that Windows XP was launched, Microsoft released 18 MB of patches for it!

8. Easter Eggs

The failure of software testing is open for all to see at the Easter Egg Archive (www.eeggs.com)

According to the Archive, an Easter egg is “a hidden feature or novelty that the programmers have put in their software. In general, it is any hidden, entertaining thing that a creator hides in their creation only for their own personal reasons. This can be anything from a hidden list of the developers, to hidden commands, to jokes, to funny animations”.

A true Easter egg must satisfy the following criteria:

- (1) It should be undocumented, hidden, and non-obvious

An Easter Egg can't be a legitimate feature of a product, or be an obvious part of a storyline. Easter Eggs will usually stand out either because they totally don't fit with their context (like a pinball game in a word processor), or because they have a deeper hidden personal meaning to the creators, so they threw it in for entertainment.

- (2) It must be reproducible

Every user with the same product or combination of products must be able to produce the same result given the instructions.

- (3) It must have been put there by the creators for personal reasons

The Egg must have been put there on purpose, and furthermore have a personal significance to the creators beyond just making a better product (movie, TV show, software program, etc).

By definition, Easter Eggs are intended to be entertaining and harmless. However, an Easter Egg might be accidentally harmful, e.g. maybe there was a bug in the programmer's Easter

Egg code, and in certain situations it might crash the program, or even the whole computer, forcing a reboot.

Illustration: Simply press Alt + Shift + 2 to win the Solitaire game on a Windows computer.

Illustration: Open a new word document using Microsoft Word. Type the following: =rand(200,99) and then press enter. In a few seconds, you will see hundreds of pages filled with the sentence “The quick brown fox jumps over the lazy dog” repeated over and over!

An Easter Egg is a form of Trojan horse. If software developers can sneak a benign Easter Egg past the software testing and quality assurance teams, there’s no doubt that they could similarly get a Trojan horse or intentional buffer overflow past them as well.

In fact, the attacker could even put the backdoor inside an Easter egg embedded within the main program.

The existence of Easter eggs proves quite clearly that a malicious developer or tester could put a nasty hidden functionality inside the product code and get it through product release without being noticed.

9. Trojan related cases

In an unreported case in India, a Trojan almost led to the death of a reporter!

A young lady was working on an article about ‘online relationships’. During the course of researching for the article, she befriended many strangers online. One of these people remotely implanted a Trojan on her home computer.

Staying in a small one-bedroom apartment in Mumbai, her computer was in one corner. Unknown to her, the Trojan had hijacked her web-camera and her microphone, both of which were attached to her computer.

Numerous pictures of her in compromising positions were ‘clicked’ by the hacker who then uploaded them on to a pornographic website. When the young lady came to know about it a year later, she attempted suicide. Fortunately she survived. This is a shocking reminder of the disastrous effects that a Trojan can have.

This section discusses two cases where Trojans had been used to frame innocent persons for having committed serious crimes.

(1) UK child porn case

A British citizen, Julian Green, was arrested in October 2002 after the police raided his home and found 172 indecent pictures of children on the hard disk of his home computer.

Green was an IT contractor in the UK defence industry. He was a divorcee with two children.

As a result of 13 paedophile related charges brought against him, he lost his job, was attacked and was unable to see his children.

Under British law the maximum sentence for possession of such images is ten years' imprisonment, and anyone convicted in such a matter would have become subject to registration with the police as a sex offender for a period of five years.

Green claimed that the pictures found on his computer had nothing to do with him and that he had no interest in paedophilia and had no pornographic magazines or videos at his home. He had no history of sexual offences and was an honest man trusted with a sensitive job that required security clearance.

An extensive examination of Green's computer hard disk showed the presence of 11 Trojan horse programs. These Trojans were set to log onto "inappropriate sites" without Green's permission whenever he accessed the Internet. These Trojans were believed to have come from unsolicited emails that Green opened before he deleted them.

The charges against him were finally dropped on account of the discovery of these Trojans on his computer.

In previous instances, the prosecution had been able to show that the Trojan defence was implausible. On behalf of the police, computer experts have been able to show that pictures were viewed and moved around the computer; that they did not appear in the locations that would indicate pop-ups; that there was no remaining indication of the spam email; and no evidence of any Trojan application.

Armed with this weight of evidence, courts have had no problem in dismissing the Trojan defence in other cases.

In this case, though, it was certain that there was evidence: the Trojan was indeed found and it was discovered that it referred to the paedophile pictures explicitly.

Experts were able to show that the defendant had not accessed the pictures and that he could not have known they were on his computer.

This final point is important. The actual offence under which most charges of computer paedophilia are brought is UK's 1988 Criminal Justice Act. Section 160 makes it an offence to be in possession of an indecent photograph of a child.

In this case there was no dispute about the fact that the pictures were indeed on his computer and were indeed indecent photographs of children.

There are, however, three defences: that the picture was in his possession for a legitimate reason; that he had not seen the picture or had any reason to believe it was indecent; and that it was unsolicited and not kept for any length of time.

The first defence is the one that gives permission for experts working on behalf of the courts to possess the pictures in the course of their investigations.

The second and third defences were claimed in this case: the pictures were not solicited and were not viewed.

The third defence also provides protection for those increasingly common situations in which extreme material - including paedophile content - is being transmitted in spam.

(2) The Texas port DoS case

Aaron Caffrey, a 19 year old UK citizen, was accused of crashing systems at the port of Houston in Texas, USA. He faced a charge of unauthorised modification of computer material at a UK court.

During the trial, it was claimed Caffrey had perpetrated a complex crime, involving computer hacking, identity theft and fraudulent financial-market trading.

The prosecutor in the case claimed that Caffrey hacked into the computer server at the port in order to target a female chatroom user called Bokkie, following an argument. It was said in court that they had argued over anti-US remarks she had made.

Caffrey, who suffers from a form of autism called Asperger's Syndrome, was said to be in love with an American girl called

Jessica. The court was told he named his computer after her and dedicated his "attack script" to her.

Scheduling computer systems, at the port, were bombarded with thousands of electronic messages on 20 September, 2001.

The attack froze the port's web service, which contained vital data for shipping, mooring companies and support firms responsible for helping ships navigate in and out of the harbour.

An investigation by US authorities traced the computer's IP address to a computer at Caffrey's home.

But the teenager claimed an unidentified third party had planted the instructions for the attack script on his website without his knowledge.

He also criticized the authorities for not uncovering the virus during their investigation. On the final day of the trial, Caffrey admitted being part of a group of hackers called Allied Haxor Elite, but denied he had ever illegally hacked into a computer.

The teenager told the court that hackers operated legally, but that people who entered computer systems illegally were known as "crackers". He said: "I have hacked into computers legally for friends to test their server security because they asked me to but never illegally."

Caffrey was found not guilty of computer crime after the jury accepted his story that attackers used an unspecified Trojan to gain control of his PC and launch the assault. The prosecution argued that no trace of Trojan infection was found on Caffrey's PC but the defence was able to counter this argument with testimony from Caffrey that it was possible for a Trojan to delete itself.

4. Computer Worms

1. Introduction

Computer viruses are programs that are designed to spread themselves from one file to another on a single computer. A virus might rapidly infect every application file on an individual computer, or slowly infect the documents on that computer, but it does not intentionally try to spread itself from that computer to other computers.

In most cases, that's where humans come in. We send e-mail document attachments, programs on CD ROMs, or copy files to file servers. When the next unsuspecting user receives the infected file or disk, they spread the virus to their computer, and so on.

Worms, on the other hand, rely less (or not at all) upon human behavior in order to spread themselves from one computer to others. The computer worm is a program that is designed to copy itself from one computer to another, using some network medium: e-mail, TCP/IP, etc.

The worm is more interested in infecting as many machines as possible on the network, and less interested in spreading many copies of itself on a single computer (like a computer virus). The prototypical worm infects (or causes its code to run on) a target system only once; after the initial infection, the worm attempts to spread to other machines on the network.

Illustration 1: The infamous Melissa only required a user to open a single infected document to spread itself to hundreds of thousands of users! IRC worms only require a simple user login to the IRC online chat system to spread themselves.

Illustration 2: The Explore.Zip worm could gain hold of thousands of machines with the launch of a single program. While humans exchange information at large time intervals with small groups of people, computer worms have no such restrictions. Computer worms can be classified based on the transport mechanism used by the worm to send itself.

(1) E-mail Worms use e-mail as its primary means of transport.

A *native e-mail worm* is one that is built in the native scripting language of the host e-mail system. Such a worm is carried in a proprietary form along with its associated e-mail message, as opposed to being carried as a file attachment. The native e-mail worm can only exist within the e-mail platform, and is not viable outside of the host e-mail system. A *parasitic e-mail worm* is one that leverages the transport capabilities of an e-mail system to spread itself. The parasitic e-mail worm, for

example, may use the e-mail program to send itself as an attachment to an e-mail. The parasitic e-mail worm can exist outside of the e-mail platform, and may actually use other techniques to spread itself. Of the recent worms, Melissa, ExploreZip and Happy99 would be considered parasitic e-mail worms.

(2) Arbitrary Protocol Worms spread themselves using one or more non e-mail based protocols, such as IRC's DCC protocol, the FTP protocol, or using simple TCP/IP sockets as its primary means of transport.

Computer worms can also be classified based on how the worm is actually launched on a computer system, how it actually gains control of a computer system and whether it requires user interaction (and how much).

Self launching worms are capable of spreading to a new system and actively running on that system. These worms do not require user interaction in order to gain control of a system; instead, they exploit some aspect of the host (operating system, application system, e-mail system) to cause their code to automatically execute upon introduction to a new system.

The Internet Worm and the IRC worms (described in later sections) are examples of self-launching worms. A subset of this category is the back door worm.

The back door worm is one that exploits a back door in a target system to gain entry and to ensure that it is launched, again without human intervention.

User launched worms require user intervention in order to execute on a new system e.g. in order for the Melissa worm / virus to infect a system, an infected attachment must be manually opened/viewed by a user. The worm cannot cause itself to launch on a system without user intervention.

Hybrid launch worms are capable of spreading using both mechanisms.

Illustration: ExploreZip, when sent in e-mail, required a user to launch the infected attachment to gain control of the system.

On the other hand, once running on a computer system, ExploreZip would automatically spread itself to other computers over the peer-to-peer network. These targeted machines would then become infected on the next reboot (without any known user intervention).

Three technological trends have had a huge impact on the spread of computer worms:

- (1) Infrastructural homogeneity: A vast majority of the world's desktop computers are running on the Windows platform, standard SMTP e-mail, standardized e-mail clients like Microsoft Outlook. This homogeneous environment allows worms to easily spread across the world.
- (2) Ubiquitous programmability: The availability of robust programming capabilities in the Microsoft Office product line, Microsoft has made the Office products the platform of choice for virus and Trojan creation. The simplicity of the macro programming language supported by Microsoft Office allows novices to develop powerful malicious macro programs.
- (3) Homogeneous communications mechanism: With more users on the Internet than ever before as potential targets, worms can now spread more quickly than ever. The worm exploits the communications infrastructure to send itself from one computer to another. Consequently, it can potentially spread itself thousands of times faster than a traditional virus.

2. A Brief History of Worms

The first computer worms were created in the labs of John Shock and Jon Hepps of Xerox's Palo Alto Research Center in the early 1980s. The team developed five different worms, each of which was designed to perform useful tasks on the network. These researchers quickly learned the danger of worms; one of the self-replicating programs had a bug that caused it to malfunction while running during non business hours.

The next morning, users found their computers crashed and found that resetting them did not help; the worm would continually re-infect the systems and quickly cause them to crash. After this event, the research group produced a "vaccine" (perhaps the first ever anti-virus) to prevent the worm from crashing systems and subsequent worm research died out.

Illustration: The CHRISTMA EXEC Worm: The First Widespread E-mail, User-launched Worm

In December of 1987, the first widespread computer worm was released into IBM VM/CMS systems. This worm, dubbed the CHRISTMA EXEC Worm, was a simplified predecessor to the Melissa virus/worm seen this year.

The worm was written in the REXX programming language, a common batch programming language on UNIX systems. When a user received this file as an e-mail attachment, they had to download the file to the hard drive and manually run the batch file to cause the worm to spread.

Once the worm was launched by the user, it displayed a character-based picture of a Christmas tree and then attempted to spread itself further over the IBM e-mail system.

The worm used entries in the audit trail file (that contained logs of all received and sent e-mail), as well as the user's personal address book to determine its next round of recipients.

Even though CHRISTMA required significant manual user intervention to spread, it clogged thousands of mailboxes and the underlying network with millions of copies of itself.

Illustration: The Internet Worm: The First Arbitrary Protocol, Back Door Worm

On November 2nd, 1988, the infamous Internet Worm (created by Robert Tappan Morris) wreaked havoc on the fledgling Internet.

Unlike the CHRISTMA EXEC Worm, this worm was designed to spread itself without any human intervention.

The Morris worm would spread to DEC VAX and Sun 3 machines running BSD UNIX by connecting to the target UNIX machine in one of three ways (to the e-mail service, the *finger* service, or by hacking passwords and performing a remote execution on a target machine).

Once it had penetrated the target computer, it would send over a small C program and cause the target host to compile and run this program.

Next, the compiled program would pull over the remaining worm components and launch them; at this point the worm had a foothold of the targeted computer and could spread to new computers on the Internet. It is estimated that the Morris worm affected more than 6,000 computers on the Internet using these techniques.

Illustration: The IRC Worms: The First Consumer-oriented Arbitrary Protocol, Self-Launching Worms

In 1997, standard end-users users encountered the first mainstream computer worms: IRC worms.

IRC, or Internet Relay Chat, is a chatting system available on the Internet. Users can connect to this system using an IRC client (e.g. a Windows program) and chat with thousands of other users about thousands of different topics.

One of the most popular IRC client programs, mIRC, was equipped with a fairly powerful scripting language that was targeted by the first IRC worms.

These scripts were programmed to send themselves to new users as they joined the IRC chat “channels.”

Once the recipient was infected, their mIRC program would execute the worm logic and also participate in the reproduction of the worm.

While many were benign, some of these worms were capable of other malicious actions.

For instance, users who spread the worms could send commands to infected systems and cause these systems to perform any number of malicious actions.

In essence, these were the first “remote control” worms ever created, since they allowed an attacker to remotely control and/or damage infected systems.

Illustration: The Happy99 Worm: The First Mainstream Consumer-oriented Worm

The Happy99 worm, released in early 1999, has arguably affected more home Internet users than any other worm in history. As of July 27th, 1999, the Symantec Antivirus Research Center has received over 4,200 submissions of Happy99.

Once the worm is received in e-mail and launched by the user, it displays a window with fireworks and, in the background, installs itself onto the system.

Subsequently, any time the user sends an e-mail (with the popular Internet SMTP protocol used by Eudora, Netscape mail, etc.), or posts a message to a USENET newsgroup, the worm will send an additional message to the same recipient(s), adding the worm as an attachment.

Illustration: The Melissa Virus + Worm: The First Mainstream Corporate Macro Hybrid (both a Virus and Worm)

The “Melissa Virus” is actually both a computer virus and a computer worm, or hybrid threat. Melissa is spread inside of Word 97 document files.

When a user receives and subsequently views a Melissa-infected document, the Melissa macros will run inside Word for Windows 97 and use the Outlook e-mail program (if present) to

send a copy of the infected document to the first fifty users in the Outlook address book.

Melissa will also infect the Word for Windows environment, allowing it to spread to other documents on the user's machine.

These second-generation infections are also fully infectious, and if shared with other users, will continue the infection process.

Based on the number of e-mail boxes that were flooded with copies of Melissa, it is without a doubt, the most prolific worm of all time.

Melissa spread itself prolifically during its short reign, filling up hundreds of thousands of e-mail inboxes.

However, due to the quick response of system and mail administrators, the actual number of computer users directly affected by Melissa was probably far less than the number of affected mailboxes.

In other words, most users probably did not actually launch Melissa, but might have found several copies of it in their inbox had they been able to access e-mail.

Melissa achieved such widespread distribution because when it spread, it sent itself to the first fifty entries in the Outlook address book.

While some of these entries might refer to typical end-user e-mail addresses, many corporations have entries such as "ASCL-Internal" among the top fifty entries.

An e-mail sent to the "ASCL-Internal" address would literally reach all the ASCL employees. Consequently, a small number of seed infections in a corporation could quickly clog hundreds of thousands of e-mail boxes with Melissa infections.

Illustration: The ExploreZip Worm: The First Widespread Hybrid-launch, Arbitrary Protocol Worm

Unlike Melissa or Happy99, the ExploreZip Worm spread itself to other computers using two distinct mechanisms.

First, like Melissa, ExploreZip was capable of leveraging Outlook, Outlook Express and Exchange e-mail programs to send itself over e-mail. Instead of sending itself to the first fifty users like Melissa, this worm sent itself to users that had recently sent e-mail to the infected user. In addition to spreading itself via e-mail, ExploreZip would also spread through all machines that are visible on a peer-to-peer Microsoft network.

The worm would copy itself to accessible machines and update a configuration file on the target machine to cause the machine to launch the ExploreZip worm during the next boot-up.

The worm continually searched for other peer machines to infect, and consequently, was difficult to eradicate from corporate networks. The moment an administrator would remove the worm from a machine, another copy would re-infect it.

In addition to infecting peer-to-peer networked machines, ExploreZip also deleted the contents of a variety of files from both local hard drives and the hard drives of networked peers.

The peer-to-peer capabilities of this worm clearly underscore the vulnerability of peer-to-peer networks in the enterprise.

5. Computer Viruses

A computer virus is a computer program which requires a host and infects other files so that it can “live” longer. Viruses most commonly delete or alter files on the infected system (e.g. the Nimda virus) or even destroy hardware (e.g. the CIH virus).

Illustration: CIH virus [W95/CIH.1003]

The CIH virus infects executable files under Windows 95/98A. Many CIH victims were infected after downloading files from Internet gaming sites.

The virus reprograms the flash BIOS in such a way that there is no cure but to replace the flash BIOS chip or even the motherboard.

The virus can also partially overwrite the hard disk and render it useless. It now exists in many different variants, some triggering on the 26th of the month.

Illustration: Nimda virus [W32/Nimda.A@mm]

The Nimda virus generates random Internet addresses and attempts to connect to them. If a connection is established, it attempts to hack the web server and copies itself to it. Visitors to web pages stored on this infected web server get infected by the virus and their information is destroyed.

The virus exploits a programming error in certain versions of Internet Explorer to be executed automatically as the web page (or mail body).

Viruses are of various types such as:

(1) Binary file viruses

These viruses infect executables (program files). They are able to infect over networks. Binary file viruses normally consist of instructions that are created for easy machine interpretation (machine code which is basically a row of numbers to be queued into the processor).

(2) Script viruses

A script virus is written as pure text and its source code is easily readable. As computers cannot understand text instructions directly, the text is first translated to machine code. This procedure, called “interpretation”, is performed by separate

programs e.g. Visual Basic Script (VBS) is interpreted by WSCRIPT.EXE.

Other scripting languages are JavaScript, Jscript, DOS BAT language, UNIX shell script, IRC scripts, Corel Draw, Visual Foxpro, SuperLogo, InstallShield etc.

(3) Macro viruses

Macro viruses infect data files like documents and spreadsheets. Many “data file types” have the possibility to include instructions along with the normal content e.g. Microsoft Word files can contain instructions that tells Word how to show a particular document, or instructions that tells Windows to do certain actions. Macro viruses are the most common type of viruses and exploit the fact that many applications now contain macro programming languages. These languages allow users to convert simple data files into programs.

The most targeted macro programming language is Visual Basic for Applications (VBA) which is used by Microsoft Word, Excel, Access, PowerPoint, Project, Visio etc

(4) Boot sector viruses

Boot viruses infect master boot sectors and system boot sectors of hard drives and floppy disks.

All physical hard drives such as hard disks and floppies have master boot sectors that contain information about how a physical disk is divided into logical disks. They also contain a short program that can find out where the system boot sectors (whose purpose is to find and run an operating system) are located. Boot sector viruses are not able to infect over networks.

(5) Multipartite virus

Multipartite viruses infect both executable files and boot sectors, or executable files and data files. These are able to infect over networks.

6. Cyber Crimes HIT LIST

It is easy to see the faults of others but not so easy to see one's own faults. These words of Gautam Buddha hold true even in today's digitalized world. The ability of criminals to easily misuse technology to commit crimes is blamed upon weaknesses in computer software. Rarely does the common man realize that the spread of cyber crime can be attributed more to his ignorance than to anything else.

Based upon 10 years of real world cyber crime investigations, ethical hacking and penetration testing, we at Asian School of Cyber Laws (ASCL) came to two very fundamental conclusions –

- (1) most cyber crimes are committed using one of 5 methods,
- (2) most cyber crimes can be prevented by user awareness of these 5 methods.

5. Computer Viruses & Worms

(Hit list item no. 5)

Not many people know that two brothers from Pakistan are (dis)credited with having created the world's first computer virus. From the humble beginnings of the Brain virus, today's computer virus packs quite a punch with artificial intelligence, encrypted source code and dynamic payloads.

Several viruses and worms have caught public attention with the sheer magnitude of their impact e.g. Melissa, Love Bug, SQL Slammer, Chernobyl, Nimda etc.

Viruses can be of various types such as polymorphic, stealth, multipartite, armored, companion etc. But deep down they are usually created for one primary purpose – to damage data. And most modern viruses have a highly successful track record.

Worms on the other hand are usually created to eat into your computer and network resources.

Of late a disturbing trend is the marriage of viruses, worms, Trojans and other malicious code to produce a highly evolved artificial intelligence enabled code that we at ASCL have nicknamed hydra (**HYbrid Data Raiding Agents**). So far hydra are confined to sophisticated information warfare attacks where national interest and high finance is the motivation. Hydra are in contrast to simpler viruses and worms which are primarily created to damage random computers. Hydra on the other hand are sent to carefully selected computers and are almost never found in the wild.

Because of this there is almost no known anti-virus program that is effective on hydra.

4. Trojans & Spyware **(Hit list item no. 4)**

The term Trojan has a rather romantic and violent origin in the unfortunate events surrounding Helen of Troy. True to the origins of the word, Computer Trojans are software programs that appear to be very useful, but in reality, enable malicious hackers to control the computers on which they are installed.

Script kiddies regularly use Trojans to cause serious damage to unsuspecting victims. Trojans are very easy to download and deploy and are most commonly sent as attachments to spoofed e-mails. The recipient of the e-mail believes that his friend / colleague has sent him an e-card or an important document and so he unsuspectingly downloads and runs the file on his computer.

Once the Trojan is installed on a computer the computer virtually becomes a free-for-all computer which people around the world can easily break into.

Case: A young lady reporter was working on an article about online relationships. The article focused on how people can easily find friendship and even love on the Internet. During the course of her research she made a lot of online friends. One of these ‘friends’ infected her computer with a Trojan.

This young lady stayed in a small one bedroom apartment and her computer was located in one corner of her bedroom. Unknown to her, the Trojan could activate her web camera and microphone even when the Internet was switched off. A year later she realized that hundreds of her pictures were posted on pornographic sites around the world!

Case: The network administrator in a global bank received a beautifully packed CD ROM containing “security updates” from the company that developed the operating system that ran his bank’s servers. He installed the “updates” which in reality was Trojanized software. Three years later, the effects are still being felt in the bank’s system!

Spyware and key loggers are regularly used to log all the strokes a victim makes on the keyboard. This assumes sinister proportions, if a key logger is installed on a computer which is regularly used for online banking and other financial transactions.

Key-loggers and spyware are most commonly found in public computers such as those in cyber cafes, hotels etc. Unsuspecting victims also end up downloading spyware when they click on “friendly” offers for free software.

Precautions

- (1) Do not download **email attachments** unless you are sure about the authenticity of the email.
- (2) Use good **anti-virus software** (many are available for free).
- (3) Regularly download **updates** for the anti-virus software. If your software has an auto update facility, use it.
- (4) Regularly apply updates and **security patches** to your operating system. For Windows users, the “automatic updates” option should be turned on.
- (5) Do not go “click happy” to download free software from pop-up advertisements. Almost always, there is a catch!
- (6) Use a **personal firewall** (e.g. ZoneAlarm) and enable the firewall and other safety options in your operating system.

3. Phishing & Spoofing attacks

(Hit list item no. 3)

Jasa dista tasa nasta mahnun jag phasta (old Marathi saying)

[Things are not what they seem and that is why the world gets conned]

In the 19th century, British comedian Arthur Roberts invented a game called Spoof, which involved trickery and nonsense. This gave the English speaking world a new word that today symbolizes a gamut of hacking technologies.

Spoofing attacks primarily include e-mail spoofing, SMS spoofing, IP spoofing, and web spoofing. Spoofing attacks are used to trick people into divulging confidential information (e.g. credit card data) or doing something that they would usually not do (e.g. installing malicious software on their own computers). Such use of spoofing attacks is commonly referred to as Phishing.

Sending an e-mail from somebody else's e-mail ID is the simplest form of Email spoofing. Innumerable tools exist on the Internet which can easily be used to send e-mails appearing to have been sent by somebody else. The effects are intense.

Case: Many customers received an email from their bank asking them to verify their usernames and passwords for the bank records. The emails were spoofed, but thousands of customers clicked on the link in the email and submitted the information at the webpage that opened up. On investigation, it was found that the emails had been sent by a disgruntled employee.

Case: Thousands of employees of a global IT company ended up installing viruses on their computers when they executed an attachment appearing to have been sent out by their officers. The employees even disabled the anti-virus software because the email said that “the attachment may be incorrectly detected as a virus!” On investigation, it was found that the emails had been sent out by a rival company.

SMS spoofing is very similar to e-mail spoofing. The major difference being that instead of an email ID, a cell phone number is spoofed and instead of a spoofed e-mail, a spoofed SMS is sent.

Case: A young lady received an SMS from her husband’s cell phone informing her that he had had an accident and was at the hospital and urgently needed money. On receiving the SMS, she rushed out of the house with the money. She was attacked and robbed by the person who had sent her the spoofed SMS.

An IP address (e.g. 75.125.232.93) is the primary identification of a computer connected to a network (e.g. the Internet). A criminal usually uses **IP spoofing** to bypass IP based authentication or to mislead investigators by leaving a trail of false evidence. IP spoofing can be accomplished using proxy servers and simple PHP scripts that are readily and freely available online.

Case: Internet users in many countries use proxy servers to bypass Government imposed Internet censorship. (We are not passing any comment on whether is it right or wrong to impose Internet censorship or bypass it, as the case may be.)

Case: A criminal hacked into the computer systems of a sensitive Government organization. The digital trail that he left behind led to a senior official of the same department. This officer would have been arrested immediately had it not been for his impeccable record. Detailed investigations proved that the digital trail was faked.

When you sit at a computer, open up a browser and type in www.asianlaws.org, you expect to reach the correct website (and most often you do!). This is because of the domain name system which

converts human readable domain names such as asianlaws.org into computer readable IP addresses such as 75.125.232.93

DNS spoofing involves manipulating the domain name system to take unsuspecting victims to fake websites (that look identical to the original ones). Sitting at the computer you may type in www.asianlaws.org but the site that opens up may be a fake site!

This can and has been done at the local organizational level (e.g. by host file rewriting or by a network administrator with malicious intentions) or at the national or international level (by hackers exploiting vulnerabilities in the BIND software that runs most of the world's domain name servers).

Case: Hundreds of employees at a global financial services company received emails from a popular online store about a huge discount on some popular books and DVDs. On clicking the link in the email, users were taken to what appeared to be the website of the online store. Most of the recipients of the emails placed orders using their credit cards. No one got the books / DVDs, but they all got hefty credit card bills at the end of the month.

On investigation it was uncovered that the network administrators had connived to carry out a simple Phishing attack. It was a fake email and a fake website. None of the victims (most of whom were advanced computer users) realized that something was amiss.

Precautions

- (1) Use **digital signatures** to authenticate your emails. This technology is very cheap (sometimes free!) and easy to use. Digitally signed documents enjoy legal validity in many countries.
- (2) Avoid accessing your primary email account(s) from a public computer. You can set up secondary email accounts for non critical work.
- (3) Treat with suspicion any email which makes an urgent request for your credit card or online banking account details.
- (4) If you suspect an email, do not click on the links in the email. Open up your browser and type in the URL.
- (5) Ensure that your operating system and Internet browser is updated regularly.

2. Packet Sniffing

(Hit list item no. 2)

On computer networks, data travels in the form of data packets. A packet sniffer can be used to read these packets while they are in transit.

On the legitimate side system administrators use this technology to monitor and troubleshoot network traffic. On the criminal side, this technology can easily be used to sniff out username and password information, credit card details etc.

Surprisingly, such sensitive information is generally transmitted in clear text from your computer to the web server. Such plain text information can easily be viewed with packet sniffing technology.

Case: A disgruntled former employee of a global trading corporation had installed Trojans in some of the company computers before resigning from his job. Subsequently, he used the Trojans to install packet sniffing software on the infected computers.

Using these compromised computers, he was able to view huge amounts of sensitive information. His earnings from selling this information to rival companies were more than that of the Chairman of the company!

Packet sniffers are not very difficult to install and use and are difficult to detect. With the growing popularity of wireless networks in companies and even in public places, the risks are even higher.

Case: ASCL recently conducted experiments near several software parks. The wireless networks of a whopping 90% of the software companies were leaking out sensitive information. A malicious hacker could easily sit in a parked car with a laptop; run some sniffing software and access huge amounts of sensitive data including source codes!

1. Greed

(Hit list item no. 1)

“We are all born brave, trusting and greedy, and most of us remain greedy.” - Mignon McLaughlin

Greed of the victim is the root of most cyber crimes.

If someone gets an email telling him that he has won a huge lottery, what is the first thing that he should do? Ask himself – did I even *buy* a ticket for this lottery? If you have not bought the ticket, how can you win the

lottery? If you still want to believe it and then even pay a “small” processing fee, whom can you blame if you get defrauded?

Every time that you download “free” software, that promises to change your very way of life, from a popup advertisement, you risk compromising your entire digital identity.

Today your computer holds the key to your digital life – your health records, bank accounts, online share trading accounts, email accounts, utility bills, credit card information, tax filings.... the list is endless.

Be CAREFUL.

7. Introduction to Cyber Crime Investigation

Cyber Crime Investigation is the collection, analysis and investigation of digital evidence and cyber trails.

These digital evidence and cyber trails may be found in computer hard disks, cell phones, CDs, DVDs, floppies, computer networks, the Internet etc.

Digital evidence and cyber trails can be hidden in pictures (steganography), encrypted files, password protected files, deleted files, formatted hard disks, deleted emails, chat transcripts etc.

Digital evidence and cyber trails can relate to online banking fraud, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, divorce cases, murder cases, organized crime, terrorist operations, defamation, pornography, extortion, smuggling etc.

The findings of a cyber crime investigation will be admissible in a court of law if the following basic rules are followed -

(1) The cyber crime investigators must be skilled competent professionals. This is essential so that they can properly conduct the investigation, collect the relevant evidence and instill confidence in the court about the admissibility of the evidence.

Digital evidence is highly fragile and can be destroyed by improper handling. Cyber crime investigators must be skilled competent professionals who understand the tools, techniques and methodologies of handling digital evidence.

A good cyber crime investigator should have: (a) excellent knowledge of the tools, techniques and methodology of cyber crime investigation and digital evidence analysis, (b) ability to competently handle a wide variety of software and hardware, (c) good communication and interpersonal skills, (d) an inquisitive mind and ability to think logically, (e) ability to handle a cross examination in a court of law.

(2) The original digital evidence must NEVER be tampered with or altered. As far as is practical, investigators must work on the image / clone of the original evidence. If that is not practical, then extreme care and caution must be taken while working on the original evidence.

Computer programs (especially operating systems) frequently alter the electronic contents. This usually happens without the knowledge of the user. This makes it necessary that, wherever practical, an image or clone

of the original storage medium (hard disk, floppy, USB drive etc) must be taken.

If the original data is very voluminous, then selected information can be copied or cloned.

In special circumstances where the investigator works upon the original evidence, a neutral and credible witness must be present. Without this, the evidence may not be admissible in court.

(3) A detailed and accurate audit trail must be maintained. The chain of custody forms and other audit trail documents must be meticulously maintained. Any lacuna in these documents casts suspicion on the entire findings of the investigation.

1. External Examination

The actual process of the investigation of any computer related crime begins with an external examination of the premises. Normally, for this part of the investigation, the rules and regulations of investigation and forensics related to traditional crimes also apply to some extent.

This part of the investigation basically assists the computer forensics expert in judging the strengths and vulnerabilities of the network. It also helps him in deciding the steps to be taken to investigate the crime and also the peculiarities of the incident.

The following are the steps to be taken and points to be borne in mind by the investigating officer. Let us take the example of the suspect computer or computer systems present in an organization.

- (1) The officer should have some members of a police team with him. They will assist him in maintaining order while the investigation is being carried out.
- (2) The team of experts should be prepared (with the required tools) for conducting any kind of examination on the suspected systems.
- (3) On reaching the scene of investigation, the police officers should seal the entrances and exits to the place.
- (4) They should ask the employees of the organization to move away from their machines. If possible, the employees should be made to gather in a room where no machines are present.
- (5) The employees should be retained till their statements (if required) have been taken.
- (6) The fingerprint experts should gather any fingerprints available from the machines, which are to be investigated. This may, at times, assist in revealing the person(s) who have used a computer. The results of the

fingerprinting exercise can then be compared with the access control policy of the organization to verify whether any unauthorized access has taken place.

(7) The computer experts should locate all the important servers and also understand the layout of the network. They should also make a chart of the network. At times, this assists in understanding the path for the flow of information.

(8) There should be regular and meticulous documentation of every step being taken. This will prove invaluable while proving the authenticity and accuracy of the investigation in a court of law.

2. Confiscation and seizure

Confiscation of computers and related peripherals is not always the practical approach.

Consider a situation where a denial of service attack on sensitive government websites has been traced to a large software company. In all likelihood, the evidence relating to the attack will be found on the computers in the company. Would it be practical to confiscate hundreds of computers along with tons of wiring and accessories?

A cyber crime investigator has to decide whether it is prudent to confiscate or to complete the investigation at the scene.

Confiscating and carrying out the investigation off-site would involve proper packaging and transporting of the computers and accessories, reassembling them at the laboratory and then recreating the network or configuration.

This can be a complex and sensitive issue and hence the cyber crime investigator must bear the following in mind before taking the decision on whether to confiscate and then investigate or whether to investigate on-site.

2.1 When to confiscate

This depends on the following factors:

Volume of evidence

As discussed above, seizing hundreds of computers and tons of accessories is not very practical. The cyber crime investigator must calculate whether it would be practical and feasible to confiscate, package, transport and then reassemble the confiscated material.

Technical issues

If the situation is such that the computers have to be sent to an outstation expert for examination, then confiscation would become necessary.

Infrastructure issues

If the situation is such that the cyber crime investigator does not possess the relevant tools for carrying out an onsite investigation, then it is prudent to confiscate the computers and carry out an extensive examination at the place where the infrastructure is present.

Attempting to examine the evidence without all the required tools (software and hardware) can lead to irretrievable loss of data.

Time available

At times it is essential to carry out an urgent investigation e.g. while tracking down a terrorist organization that is likely to carry out a major attack. In such situations there may not be enough time to confiscate and then investigate. It becomes imperative to examine the evidence with whatever tools and expertise are available.

Ultimately the decision to confiscate or not is best left to the judgment of the cyber crime investigator who is at the scene and knows all the relevant issues.

2.2 What to confiscate

Once a decision to confiscate has been taken, the next step is to decide on what all should be confiscated. This is a very important decision and must be well thought out. If the cyber crime investigator confiscates too much, some evidence may be damaged or lost while in transit or while reassembling and recreating the scenario.

If the cyber crime investigator confiscates too little, important evidence may be lost or recreation may not be possible.

The following may be borne in mind while deciding what to confiscate.

Confiscating hardware

While deciding on what hardware components to confiscate, one must remember that it is absolutely essential to confiscate the entire contents of the system cabinet without separating them.

This is because separating the hard disk may lead to damage if it is not packaged in anti-static material and carefully transported.

Moreover, some operating systems (like Windows NT) are very delicate. If the hard disk running Windows NT is removed from its original surrounding and later mounted on a laboratory computer, the operating system may crash if the RAM, motherboard or even the sound card is incompatible. It is an absolute must not to separate the hard disk from the original system unless authorized by an expert.

Decisions on whether to confiscate the keyboard, mouse, speakers and other related hardware would depend upon their nature. If these pieces of hardware were typical then there would be no need to confiscate them. But if they were special ones e.g. a keyboard that had an in-built storage device, then it would be prudent to confiscate them.

Consideration has to be given to fingerprints that can be found (especially on the keyboard and mouse). If such fingerprints are important for the prosecution, then naturally the equipment on which they are found should be confiscated.

Confiscating storage media

Storage media such as hard disks, floppies, CD ROMs, USB drives etc. can prove to be a valuable source of evidence. Not only may they contain incriminating information but also software, device drivers and other programs necessary for the investigation.

Confiscating peripherals

Some software does not function properly if the necessary peripherals (e.g. printers) are not connected. Hence it may be necessary to confiscate all the relevant peripheral devices like printers, scanners etc.

Confiscating documentation

Even experts need documentation while examining and operating the various types of hardware and software available. All documentation and books related to the hardware and software should preferably be confiscated so that reconstruction would be feasible. Moreover, passwords, passphrases and other secret information may be carelessly scribbled, by the user, on these documents or books.

Given below is a short list of hardware components and their evidentiary value.

Laser printers: On most laser printers it is possible to search for images of the last page printed. This can be done before the printer is moved. Therefore an expert must be present at the scene.

Hard disk print buffers: Some laser printers have hard drives that store information before it is printed. The information is stored till the printer runs out of memory space and overwrites it. The hard drive in such printers can be searched.

Print Spooler Device: This device holds information to be printed. The spooler may be holding a print job if the printer was not ready to print when the print command was given (e.g., the printer was not turned on or was out of paper). This device should be handled at the scene itself since the information can easily be lost.

Ribbon printers: Like old typewriter ribbons, printer ribbons contain impressions from printed jobs. These impressions can be recovered by examining the ribbon.

Keyboards: Normally keyboards don't store information. However, some keyboards are computer workstations and contain internal diskette drives.

Fax machines: Although some types of stand-alone fax machines simply scan and send data without storing it, other models can store the data (e.g., on a hard drive) before sending it. Significantly, the data remains in the machine's memory until overwritten. Some fax machines have enough memory to hold hundreds of pages of information.

Monitors: Any burning of the screen phosphorus on old technology monitors may reveal data or graphics commonly left on the screen.

2.3 Transporting confiscated material

Great care has to be taken while transporting computers from the crime scene to the investigation venue. The following points must be borne in mind while transporting computers:

The computers must be protected from damage: Care should be taken to properly pack the computers so that they will not be violently shaken while in transit. In one case in the USA, a hacker had put a very powerful magnetic coil on the top of his door. When the cyber crime investigators were carrying his computers out of the door, all the data on them was wiped out!

Computer parts must be carefully packed: If it is necessary to transport computer parts, they must be packed in sterile anti-static packaging.

The earlier configuration must be carefully documented: If the earlier configuration is not properly documented, it may not be possible to reassemble the computers as they were at the crime scene. All supporting documentation must be confiscated from the crime scene if possible. This will prove to be of great help in examination and recovery of evidence. Moreover, this will also preserve the integrity and accessibility of the data inside.

Before disconnecting any cables, all connections should be videotaped or photographed. A detailed diagrammatic representation of the wiring must be prepared.

Determine what needs more protection: Although all confiscated items need to be carefully handled, some components are more delicate than others. The cyber crime investigator must ascertain what component needs to be more carefully handled. E.g. if due to some reason the hard disk has to be removed, then the read / write heads must be secured to prevent damage.

Some systems secure (park) the heads automatically whenever the machine is not in use, but other systems may require that a specific command be executed or that the heads be secured mechanically. The manufacturer's operating manual specifies the proper procedure for each system.

Static electricity buildup can damage data in hard disks and other storage media and for this anti-static packaging must be used. The manufacturer's recommendations in relation to the environmental conditions (such as humidity, temperature etc.) must be carefully adhered to. Temperature between 5° C and 30° C, humidity between 20% and 80% and a smoke free and dust free environment is usually safe for storage of electronic media.

Most organizations keep all their data backed up on either CD-ROMs or floppies. At times this is done on a daily basis. This implies that all this information has to be confiscated.

All back up tapes and diskettes must be packed properly to avoid any alteration or corruption of the data contained on them. Special care should be taken to search the premises thoroughly so that no such media is missed out.

2.4 Chain of custody form

"Chain of custody" refers to the document or paper trail showing the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence.

A chain of custody is the process of validating how any kind of evidence has been gathered, tracked and protected. A piece of evidence is worthless without a chain of custody.

Chain of Custody Form

For storage media

Investigating Officer:

1. Case Number:	2. Evidence number:		
3. Date and time of Confiscation / recovery:	5. Place of Confiscation / recovery:		
4. Person from whom confiscated / recovered:			
6. Description of storage media: i. Model no: ii. Manufacturer: iii. Serial no: iv. Size: v. MD5 hash	7. If there were any unusual marks or scratches on the storage medium, please describe in detail:		
Chain of Custody			
Date & Time	Released by (Name & signature)	Released to (Name & signature)	Purpose of change of custody

A chain of custody form must answer the following questions:

- What is the evidence?
- How did the analyst get it?
- When was it collected?
- Who all have handled it?
- Why did the mentioned persons handle it?
- Where all has the evidence travelled?
- Where the evidence was ultimately stored?

An investigator must ensure that he knows at each step the person to whom the evidence was handed over. He must also make sure that such person has the proper authority to have the evidence in his custody.

If at any point this chain of custody is disrupted, it will weaken the case to a very large extent. Documenting each transfer of the collected evidence can also help in ensuring that the chain of custody is maintained.

The **packaging procedure** recommended by the Technical Working Group for Electronic Crime Scene Investigation of the U.S. Department of Justice is as under:

- Ensure that all collected electronic evidence is properly documented, labelled, and inventoried before packaging.
- Pay special attention to latent or trace evidence and take actions to preserve it.
- Pack magnetic media in antistatic packaging (paper or antistatic plastic bags).
- Avoid using materials that can produce static electricity, such as standard plastic bags.
- Avoid folding, bending, or scratching computer media such as diskettes, CD-ROMs, and tapes.
- Ensure that all containers used to hold evidence are properly labelled.

Note: If multiple computer systems are collected, label each system so that it can be reassembled as found (e.g., System A–mouse, keyboard, monitor, main base unit; System B–mouse, keyboard, monitor, main base unit).

The **transportation procedure** recommended by the Technical Working Group for Electronic Crime Scene Investigation of the U.S. Department of Justice is as under:

- Keep electronic evidence away from magnetic sources. Radio transmitters and speaker magnets are examples of items that can damage electronic evidence.
- Avoid storing electronic evidence in vehicles for prolonged periods of time. Conditions of excessive heat, cold, or humidity can damage electronic evidence.
- Ensure that computers and other components that are not packaged in containers are secured in the vehicle to avoid shock and excessive vibrations. For example, computers may be placed on the vehicle floor and monitors placed on the seat with the screen down and secured by a seat belt.
- Maintain the chain of custody on all evidence transported.

The storage procedure recommended by the Technical Working Group for Electronic Crime Scene Investigation of the U.S. Department of Justice is as under:

- Maintain the chain of custody on all evidence transported.
- Ensure that evidence is inventoried in accordance with departmental policies.
- Store evidence in a secure area away from temperature and humidity extremes. Protect it from magnetic sources, moisture, dust, and other harmful particles or contaminants.

Note: Be aware that potential evidence such as dates, times, and systems configurations may be lost as a result of prolonged storage. Since batteries have a limited life, data could be lost if they fail.

Therefore, appropriate personnel (e.g., evidence custodian, lab chief, forensic examiner) should be informed that a device powered by batteries is in need of immediate attention.

3. WHOIS search



Image courtesy: domaintools.com

WHOIS is commonly used to determine the owner of a domain name or an IP address on the Internet.

WHOIS lookups were traditionally made using a command line interface, but a number of simplified web-based tools now exist for looking up domain ownership details from different databases. WHOIS was standardized in the early 1980s to look-up domains, people and other resources related to domain and number registrations. Originally all domain registrations were handled by one organisation - the Defense Advanced Research Projects Agency in USA. Hence one centralized server was used for WHOIS queries and this made looking-up information very easy.

Early WHOIS servers would allow wild-card searches. A query on a keyword would display all registered domains containing that keyword. A query for a given administrative contact would display all domains associated with the said person. Now, there are many generic top-level domains and country-code top-level domains (e.g. com, net, org, edu, in, org.in, co.uk etc).

There is a complex network of domain name registrars and registrar associations and performing a WHOIS query on a domain requires knowing the correct, authoritative WHOIS server to use. Cross Registry Information Service Protocol is being developed as a successor to WHOIS.

www.Whois.net provides whois searching facility for more than 80 domain extensions.

Whois.net also provides a **search by domain or keyword option** e.g. using this option, a search for “cyber” displays thousands of websites containing the word “cyber” such as 007cybergadgets.com and 1588cyber.com



Whois.net also provides a **search deleted domains option** e.g. using this option to search for “cyber” displays thousands of domains containing the word “cyber” that were once registered but are now available such as 01cyberlink.com and 1800cybergift.com

Whois search for **globalroot-ca.com** using www.whois.net

Domain Name: globalroot-ca.com
 Registrant Contact:
 globalroot-ca.com Private Registrant
 globalroot-ca.com@proxy.dreamhost.com
 DreamHost Web Hosting
 417 Associated Rd #324
 Brea, CA 92821
 US
 +1.2139471032

Administrative Contact:
 globalroot-ca.com Private Registrant
 globalroot-ca.com@proxy.dreamhost.com
 DreamHost Web Hosting
 417 Associated Rd #324
 Brea, CA 92821
 US
 +1.2139471032
 Technical Contact:
 globalroot-ca.com Private Registrant
 globalroot-ca.com@proxy.dreamhost.com
 DreamHost Web Hosting
 417 Associated Rd #324
 Brea, CA 92821
 US

+1.2139471032

Billing Contact:
globalroot-ca.com Private Registrant
globalroot-ca.com@proxy.dreamhost.com
DreamHost Web Hosting
417 Associated Rd #324
Brea, CA 92821
US
+1.2139471032

Record created on 2007-12-03 04:54:26.
Record expires on 2008-12-03 04:54:26.

Domain servers in listed order:
ns1.dreamhost.com
ns2.dreamhost.com
ns3.dreamhost.com

Whois search for **208.113.199.97** using www.whois.net

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

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

OrgAbuseHandle: DAT5-ARIN
OrgAbuseName: DreamHost Abuse Team
OrgAbusePhone: +1-714-706-4182
OrgAbuseEmail: abuse@dreamhost.com
OrgNOCHandle: ZD69-ARIN
OrgNOCName: Network Operations
OrgNOCPhone: +1-714-706-4182
OrgNOCEmail: netops@dreamhost.com

OrgTechHandle: ZD69-ARIN
OrgTechName: Network Operations
OrgTechPhone: +1-714-706-4182
OrgTechEmail: netops@dreamhost.com

OrgTechHandle: MNA47-ARIN
OrgTechName: Nagel, Mark
OrgTechPhone: +1-714-706-4182
OrgTechEmail: mnagel@willingminds.com

Key Word Search Results for **cybercrime** using www.whois.net



Key Word Search Results:

New search: (advanced search)

Registered Domains: 94,546,719
On-Hold Domains: 37,650,475
Search Term: [cybercrime](#)
Matches Found: 170

1. aboutcybercrime.com	whois record / website
2. anti-cybercrime.com	whois record / website
anti-cybercrime.net	whois record / website
anti-cybercrime.us	whois record / website
3. casinocybercrime.com	whois record / website
4. computercybercrime.com	whois record / website
5. computercybercrimes.com	whois record / website
6. computerforensicscybercrime.com	whois record / website
7. countercybercrime.com	whois record / website
8. creditcardcybercrime.com	whois record / website
creditcardcybercrime.net	whois record / website
9. csicybercrimefbi.com	whois record / website



[Whois](#) [Domain Suggestions](#) [Web Search](#) [FAQ](#)

Who.is Search

Ex. name.com, sample.ca, example.co.uk, myname.mx

Your IP is 122.169.52.227

[Domain Generator](#) [ccTLDs Covered](#) [Whois Index](#) [IP Index](#)

©2005 - 2008 Who.is - Searching 364 Domain Extensions

With coverage of more than 360 domain extensions, www.who.is provides the widest whois searching facility. Domains searched by who.is include:

.aero	.biz	.com	.coop	.edu
.gov	.info	.int	.mil	.museum
.name	.net	.org	.pro	.ac
.ae	.ag	.ai	.am	.as
.asia	.at	.au	.be	.bg
.bi	.bj	.br	.br.com	.bz
.ca	.cc	.ch	.ck	.cl
.cn	.cn.com	.cz	.de	.de.com
.dk	.ee	.eu	.eu.com	.fi
.fo	.fr	.gb.com	.gb.net	.gg
.gl	.gm	.gr	.gs	.hk
.hm	.hu	.hu.com	.id	.ie
.il	.in	.io	.ir	.is
.it	.je	.jp	.jp.com	.ke
.kr	.kz	.la	.li	.lt
.lu	.lv	.ly	.mc	.md
.mn	.ms	.mx	.my	.na
.nl	.no	.no.com	.nu	.nz
.pl	.pm	.pt	.qc.com	.re
.ro	.ru	.ru.com	.sa	.sa.com
.sb	.se	.se.com	.se.net	.sg
.sh	.si	.sk	.sm	.sr
.st	.su	.tc	.tf	.th
.tk	.tm	.to	.tr	.tv
.tw	.ua	.ug	.uk	.uk.com
.uk.net	.us	.us.com	.uy.com	.uz
.va	.vc	.vg	.web.com	.wf
.ws	.yt	.za.com		

Whois search for **globalroot-ca.com** using www.who.is

Registry Whois

Domain Name: **globalroot-ca.com**
Status: ok
Registrar: NEW DREAM NETWORK, LLC
Whois Server: whois.dreamhost.com
Referral URL: <http://www.dreamhost.com>

Expiration Date: 2008-12-03
Creation Date: 2007-12-03
Last Update Date: 2007-12-03

Name Servers:

ns1.dreamhost.com
ns2.dreamhost.com
ns3.dreamhost.com

Extended Info

IP Address: 208.113.199.97
IP Location: United States
Website Status: active
Server Type: Apache/2.0.61 (Unix) PHP/4.4.7 mod_ssl/2.0.61 OpenSSL/0.9.7e mod_fastcgi/2.4.2 DAV/2 SVN/1.4.2
Cache Date: 2008-04-29 03:21:29 MST

Whois search for **208.113.199.97** using www.who.is

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

NetRange: 208.113.128.0 - 208.113.255.255
CIDR: 208.113.128.0/17
NetName: DREAMHOST-BLK6
NetHandle: NET-208-113-128-0-1
Parent: NET-208-0-0-0-0
NetType: Direct Allocation

NameServer: NS1.DREAMHOST.COM
NameServer: NS2.DREAMHOST.COM
NameServer: NS3.DREAMHOST.COM
Comment:
RegDate: 2006-04-12
Updated: 2007-11-01

OrgAbuseHandle: DAT5-ARIN
OrgAbuseName: DreamHost Abuse Team
OrgAbusePhone: +1-714-706-4182
OrgAbuseEmail: **No email specified**
OrgNOCHandle: ZD69-ARIN
OrgNOCName: Network Operations
OrgNOCPhone: +1-714-706-4182
OrgNOCEmail: **No email specified**

OrgTechHandle: ZD69-ARIN
OrgTechName: Network Operations
OrgTechPhone: +1-714-706-4182
OrgTechEmail: **No email specified**

OrgTechHandle: MNA47-ARIN
OrgTechName: Nagel, Mark
OrgTechPhone: +1-714-706-4182
OrgTechEmail: **No email specified**

www.DomainTools.com offers a very wide variety of services in addition to an excellent whois search facility. One of its services, **Reverse IP**, can be used to find all the .com, .net, .org, .biz, .us, and .info websites hosted on a given IP address. Since **phishing/scam sites** often come in groups, Reverse IP can be used to find the other scam sites hosted on the same server as the one being investigated.

Whois search for **globalroot-ca.com** using www.domaintools.com

Domain Name: globalroot-ca.com

Registrant Contact:
globalroot-ca.com Private Registrant
DreamHost Web Hosting
417 Associated Rd #324
Brea, CA 92821

US
+1.2139471032

Administrative Contact:
globalroot-ca.com Private Registrant
DreamHost Web Hosting
417 Associated Rd #324
Brea, CA 92821
US
+1.2139471032

Technical Contact:
globalroot-ca.com Private Registrant
DreamHost Web Hosting
417 Associated Rd #324
Brea, CA 92821
US
+1.2139471032

Billing Contact:
globalroot-ca.com Private Registrant
DreamHost Web Hosting
417 Associated Rd #324
Brea, CA 92821
US
+1.2139471032

Record created on 2007-12-03 04:54:26.
Record expires on 2008-12-03 04:54:26.

Domain servers in listed order:

ns1.dreamhost.com
ns2.dreamhost.com
ns3.dreamhost.com

Whois Record for Globalroot-ca.com (Global Root Ca)

Front Page Information

Website Title:	Globalroot CA
Title Relevancy	100%
AboutUs:	 Wiki article on Globalroot-ca.com
SEO Score:	81%
Terms:	272 (Unique: 138, Linked: 28)
Images:	3 (Alt tags missing: 0)
Links:	11 (Internal: 9, Outbound: 2)

Registry Data

ICANN Registrar:	NEW DREAM NETWORK, LLC
Created:	2007-12-03
Expires:	2008-12-03
Registrar Status:	ok
Name Server:	NS1.DREAMHOST.COM (has 684,968 domains)
Name Server:	NS2.DREAMHOST.COM
Name Server:	NS3.DREAMHOST.COM
Whois Server:	whois.dreamhost.com

Server Data

Server Type:	Apache/2.0.61 (Unix) PHP/4.4.7 mod_ssl/2.0.61 OpenSSL/0.9.7e mod_fastcgi/2.4.2 DAV/2 SVN/1.4.2
IP Address:	208.113.199.97     
IP Location	 - California - Brea - New Dream Network Llc
Response Code:	200
Blacklist Status:	Clear
Domain Status:	Registered And Active Website

DomainTools Exclusive

NS History:	1 change on 2 unique name servers over 1 year.
IP History:	1 change on 2 unique name servers over 1 years.
Whois History:	1 record has been archived since 2007-12-05.
Reverse IP:	18 other sites hosted on this server.
Monitor Domain:	 Set Free Alerts on globalroot-ca.com
Free Tool:	 Download DomainTools for Windows

Whois search for **208.113.199.97** using [www.domaintools.com](#)

Reverse IP - View all domain names hosted on an IP address

Look an IP Address

Enter an IP address or domain name into the form below and click "Look Up" to get a list of domains hosted on the same IP address.

IP/Domain Name:
Example: 192.168.% or 64.233.161.104

There are 4,375 domains hosted on this IP address.

Here are a few of them:

1. [Ezville.com](#)
2. [Acaffinatedlife.com](#)
3. [Al-ard-al-tayyiba.com](#)
4. [4372 more...](#)

4. DNS lookup

The Domain name system (DNS) implements a database for information associated with Internet domain names and addresses. Some of these DNS records are discussed in this section. The www.iptools.com website can be used for looking up the various DNS records associated with a particular domain name.

The screenshot shows the homepage of [iptools.com](http://www.iptools.com). The main navigation bar includes links for Home, Tools, Help, and Support. Below the navigation, there's a banner for "Free Magazines & Tech Papers Downloads". On the left, there's a sidebar with links for dns, ping, traceroute, domain info, rdns, url doob, urlbf, hex to dec, dec to hex, abuse, and whois. The main content area contains several lookup tools:

- DNS Lookup:** A form to look up DNS record(s) (ex: A, MX, NS). It shows results for noodlebank.com: A 208.113.204.184.
- Spam DB Lookup:** A form to check against spammer databases.
- Whois Lookup(Domain):** A form to contact info for a domain.
- Reverse DNS Lookup:** A form to check if your IP has a reverse DNS entry.
- Decimal to hex:** A form to convert a decimal IP to hex.
- ISP Cached DNS:** A form to check cached DNS at major ISPs.
- IP Routing Lookup:** A form to show IP routing information from RADB.

On the right side of the page, there's an advertisement for "WEBSITE for your company" with a price of 1690/- per year, including domain, webspace and (IMAP) email. There's also a link to "chilly domains.in".

There are many types of records that can be used in DNS. Here are the most common.

A records - address data

An “A” record is used to map a hostname to an IP address. This example shows that the IP address for noodlebank.com is 208.113.204.184

```
noodlebank.com. IN A 208.113.204.184
```

MX records - mail exchange information

An “MX” record indicates which server(s) are responsible for handling mail for the domain. Consider the following illustrative MX record for noodlebank.com:

```
noodlebank.com. IN MX 0 aspmx.l.google.com.  
noodlebank.com. IN MX 10 mail.noodlebank.com.
```

A numerical priority (10 and 10 in this example) determines the order in which servers are to be used.

The server with the lowest priority is the primary. In this example, google.com handles mail for noodlebank.com. If however, google.com is down, then mail.noodlebank.com will also accept mail for noodlebank.com

NS records – name server record

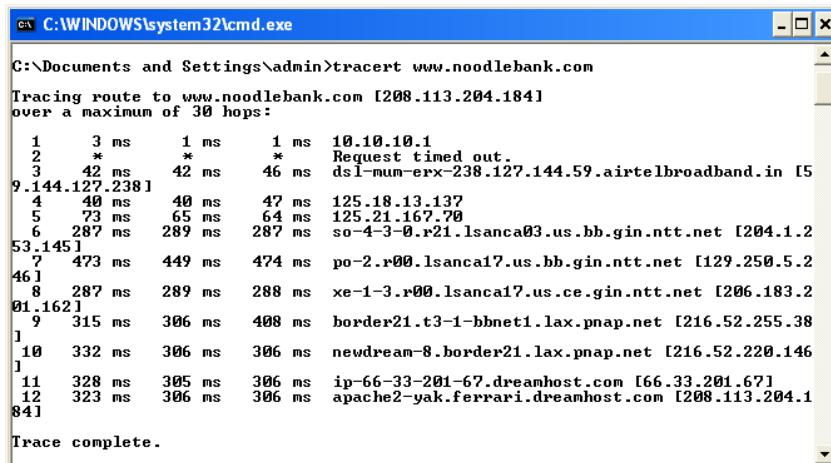
NS records indicate which nameservers are responsible for the domain. In this example, the noodlebank.com domain has the nameservers at Dreamhost.

```
noodlebank.com. IN NS ns1.dreamhost.com.  
noodlebank.com. IN NS ns2.dreamhost.com.  
noodlebank.com. IN NS ns3.dreamhost.com.
```

5. Traceroute

Traceroute is used to gather information about network infrastructure and IP ranges around a given host. Traceroute information can be used to map out the nodes available on a target's network architecture and later to exploit vulnerable / compromised nodes/computers.

The illustration below is a traceroute (to www.noodlebank.com) carried out using the *tracert* command on a Windows computer.



```
C:\WINDOWS\system32\cmd.exe  
C:\Documents and Settings\admin>tracert www.noodlebank.com  
Tracing route to www.noodlebank.com [208.113.204.184]  
over a maximum of 30 hops:  
 1  3 ms    1 ms    1 ms  10.10.10.1  
 2  *         *         * Request timed out.  
 3  42 ms    42 ms    46 ms  dsl-mun-erx-238.127.144.59.airtelbroadband.in [5  
9.144.127.238]  
 4  40 ms    40 ms    47 ms  125.18.13.137  
 5  73 ms    65 ms    64 ms  125.21.167.70  
 6  287 ms   287 ms   287 ms  so-4-3-0.r21.lsanca03.us.bb.gin.ntt.net [204.1.2  
53.145]  
 7  473 ms   449 ms   474 ms  po-2.r00.lsanca17.us.bb.gin.ntt.net [129.250.5.2  
46]  
 8  287 ms   289 ms   288 ms  xe-1-3.r00.lsanca17.us.ce.gin.ntt.net [206.183.2  
01.162]  
 9  315 ms   306 ms   408 ms  border21.t3-1-bbnet1.lax.pnap.net [216.52.255.38]  
10  332 ms   306 ms   306 ms  newdream-8.border21.lax.pnap.net [216.52.220.146]  
11  328 ms   305 ms   306 ms  ip-66-33-201-67.dreamhost.com [66.33.201.67]  
12  323 ms   306 ms   306 ms  apache2-yak.ferrari.dreamhost.com [208.113.204.1  
84]  
Trace complete.
```

The illustration below is a traceroute (to www.noodlebank.com) carried out using www.ip-tools.com

```
traceroute to noodlebank.com (208.113.204.184), 30 hops max, 40 byte packets
1 f9.8d.5646.static.theplanet.com (70.86.141.249) 8.001 ms 1.310 ms 1.346 ms
2 1d.fe.5746.static.theplanet.com (70.87.254.29) 0.356 ms 0.348 ms 0.226 ms
3 po52.dsro2.dllstx3.theplanet.com (70.85.127.109) 0.356 ms 0.359 ms 0.353 ms
4 et3-2.ibr03.dllstx3.theplanet.com (70.87.253.17) 0.236 ms 0.231 ms 0.228 ms
5 xe-4-4.r03.dllstx09.us.bb.gin.ntt.net (157.238.225.5) 0.488 ms 0.351 ms 0.353 ms
6 ae-2.r20.dllstx09.us.bb.gin.ntt.net (129.250.2.153) 0.613 ms 0.600 ms 0.478 ms
7 as-0.r20.hstntx01.us.bb.gin.ntt.net (129.250.3.130) 8.107 ms 6.224 ms 10.260 ms
8 ae-0.r21.hstntx01.us.bb.gin.ntt.net (129.250.3.25) 6.170 ms 6.081 ms 6.221 ms
9 as-1.r21.lsanca03.us.bb.gin.ntt.net (129.250.3.121) 48.116 ms 48.062 ms 48.060 ms
10 po-2.r00.lsanca17.us.bb.gin.ntt.net (129.250.5.246) 48.236 ms 48.047 ms *
11 xe-1-3.r00.lsanca17.us.ce.gin.ntt.net (206.183.201.162) 40.396 ms 40.392 ms 40.451 ms
12 border21.t4-1-bbnet2.lax.pnap.net (216.52.255.102) 41.104 ms 40.767 ms 40.699 ms
13 newdream-8.border21.lax.pnap.net (216.52.220.146) 40.832 ms 40.558 ms 40.585 ms
14 ip-66-33-201-67.dreamhost.com (66.33.201.67) 41.233 ms 40.936 ms 41.336 ms
15 apache2-yak.ferrari.dreamhost.com (208.113.204.184) 41.209 ms 40.935 ms 41.088 ms
```

6. IP tracing

In most investigations it is required to trace the computer or person behind an IP address e.g. analyzing a log file or the header of an email reveals the IP address of the suspect computer.

A WHOIS search reveals the organisation that has registered a particular IP address or a group of IP addresses. In many cases this organisation is an Internet Service Provider (ISP). The suspect may be one of the subscribers of the ISP. In such a scenario, the ISP has to be requested to provide details of the customer to whom they had allotted the suspect IP address at the relevant date and time.

Relevant formats for such request letters are provided in Chapter 16.

7. Investigating server logs

In many cyber crime cases (especially web defacement cases), analysis of FTP and web server logs yields the most crucial evidence – the IP address of the suspect. This book provides a simple guide to analyzing FTP and web server logs. The basic configuration of an FTP server, web server as well as a DNS server is provided in the annexure for reference.

To understand the relation between the FTP server and a web server, especially from the point of view of a web defacement attack, let us consider an example.

Illustration:

Sanya provides web hosting facilities to people around the world. For this, she has a powerful computer running the Microsoft® Windows® 2008 Server (Enterprise Edition) operating system. This computer has 24x7 Internet connectivity and power backup. This computer has a static IP address 67.19.217.53

Sanya has dedicated the “D” drive of her computer for storing the websites of her clients.

She configures the Web Server and DNS server provided by Microsoft® on this computer. (This process has been discussed in more detail in chapter 4 and 6 respectively). She also configures the Bullet Proof FTP Server (This process has been discussed in more detail in chapter 2).

Roheena is an interior designer who wants to host her website with Sanya. The steps that would be followed are as under:

- (1) Roheena first books a suitable domain name e.g. www.internomoda.com using the domain registration service provider www.data64.net.
- (2) While booking her domain name, Roheena sets the name servers to point to the IP address 67.19.217.53 as this is the IP address of Sanya’s computer.
- (3) Once Sanya receives the relevant payment from Roheena, she will set up the hosting service.
- (4) Sanya first creates a folder named “internomoda” in the “D” drive of her computer.
- (5) Sanya then creates an account on her FTP server with the username “roheena” and password “TopSecret2153”. This account will enable Roheena to connect to the FTP server and upload relevant files directly onto the “D:\internomoda” folder of Sanya’s computer.
- (6) Sanya then configures her web server to display the www.internomoda.com website using the files stored in the D:\internomoda folder of her computer.
- (7) Roheena then creates the web pages for her site. She then uploads these pages to the “D:\internomoda” folder of Sanya’s computer using an FTP client such as FireFTP.
- (8) Gopal is a businessman who needs an interior designer for his new house. He has heard about Roheena’s expertise and

decides to visit her website. He starts up his laptop and types in www.internomoda.com in his browser. Since Gopal is using an Airtel Internet connection, his laptop requests Airtel's DNS server for the location of Roheena's website.

(9) The Airtel DNS server informs Gopal's laptop that the website www.internomoda.com is located on the web server running on the IP address 67.19.217.53.

(10) Gopal's browser then connects to the web server on 67.19.217.53 and the web server picks up the files (html files, image files etc) from the "D:\internomoda" folder and servers them to Gopal.

(Note: This is a simplified explanation of the actual process.)

The issue of analyzing FTP and web server logs is discussed in detail in Chapter 9.

8. Email tracking and tracing

Cyber crime investigation frequently involves email tracking and tracing. When only the email ID of the suspect is known and it is required to track the person using the email account, then services such as www.ReadNotify.com can be used. This is known as email tracking.

When a particular email is to be traced, to ascertain from which IP address it has been sent, the email header needs to be examined. This is known as email tracing.

The concepts of email tracking and tracing have been dealt with in detail in Chapter 8.

9. Recovering deleted evidence

It is a common misconception that once a file is deleted on a Windows computer, it cannot be retrieved. Deleting a file, emptying the recycle bin and even formatting a drive do not really destroy the information stored there.

This issue is discussed in detail in Chapter 10.

10. Password Breaking

File passwords are usually considered an effective method of protecting the information kept in a file. In most cyber crime investigations, the investigator would be required to confront password-protected files.

Fortunately, cracking the passwords of these files is not very difficult. There are two basic methods of cracking a file password. These are:

(1) Dictionary Attack: The dictionary attack attempts to check the file password against any predefined set of words. This set may be a set of Indian names, a set of Russian names, a set of names of breeds of dogs, a set of words from the English language etc.

(2) Brute Force Attack: In a brute force attack, the tool will check the password of the file against every possible combination of alphabets, numbers, special symbols and spaces, till it retrieves the password.

This implies that a brute force attack, although it may take longer to crack a password, cannot fail (if the range is specified accurately).

Another type of password that an investigator may be confronted with is operating system password. e.g. when a suspect computer running Windows XP operating system is started up.

These issues are dealt with in Chapter 11.

11. Handling Encrypted Files

A disturbing trend that is emerging nowadays is the increasing use of encryption, high-frequency encrypted voice/data links, Pretty Good Privacy (PGP) etc by terrorists and members of organized crime cartels.

In many cases, the investigator will be confronted with encrypted files. The process of cracking encrypted files is very time consuming.

The relevant concepts are discussed in detail in Chapters 11 and 14.

12. Handling Steganography

Centuries ago, when a king wanted to send a confidential message to his generals in another country, he would shave the head of a messenger and tattoo a message or image on the messenger's head. Then the hair would be allowed to grow for a few days. The messenger would then travel to far off lands carrying the message safely hidden on his scalp!

This method of "hidden writing" is also called steganography.

One of the first documents describing steganography is from the Histories of Herodotus. In ancient Greece, text was written on wax-covered tablets.

In one story Demeratus wanted to notify Sparta that Xerxes intended to invade Greece. To avoid capture, he scraped the wax off of the tablets and wrote a message on the underlying wood. He then covered the

tablets with wax again. The tablets appeared to be blank and unused so they passed inspection by sentries without question.

Another common form of invisible writing is through the use of Invisible inks. Such inks were used with much success as recently as World War II. An innocent letter may contain a very different message written between the lines.

Early in World War II, steganographic technology consisted almost exclusively of invisible inks. Common sources for invisible inks are milk, vinegar, fruit juices and urine. All of these darken when heated.

Steganography simply takes one piece of information and hides it within another. Computer files (images, sounds recordings, even disks) contain unused or insignificant areas of data. Steganography takes advantage of these areas, replacing them with information (encrypted mail, for instance).

The files can then be exchanged without anyone knowing what really lies inside of them. An image of Priyanka Chopra might contain a private letter to a friend. Steganography can also be used to place a hidden "trademark" in images, music, and software, a technique referred to as watermarking. Of late, steganography has been discussed a lot, especially since it was suspected that terrorists connected with the September 11, 2001 attacks might have used it for covert communications. Although no such connection has been conclusively proven, this discussion goes a long way to evince the efficacy of steganography. In addition to encryption, steganography is one of the fundamental ways by which data can be kept hidden.

In contemporary terms, steganography has evolved into a digital strategy of hiding a file in some form of multimedia, such as an image, an audio file (like a .wav or mp3) or even a video file.

Watermarking, another kind of steganography, has taken on a new importance in the digital era. Images, video, music, text, and software are all easily copied and illegally distributed, causing the authors to lose out on considerable income in royalties. By embedding identifying information in a file, watermarking software enables authors to control the distribution of and to verify ownership of their digital information. It essentially "copyrights" digital information.

Like many security tools, steganography can be used for a variety of reasons.

Legal purposes can include things like watermarking images for reasons such as copyright protection. Digital watermarks (also known as fingerprinting, significant especially in copyrighted material) are similar

to steganography in that they are overlaid in files, which appear to be part of the original file and are thus not easily detectable by the average person. Steganography can be used to maintain the confidentiality of valuable information, to protect the data from possible sabotage, theft, or unauthorized viewing.

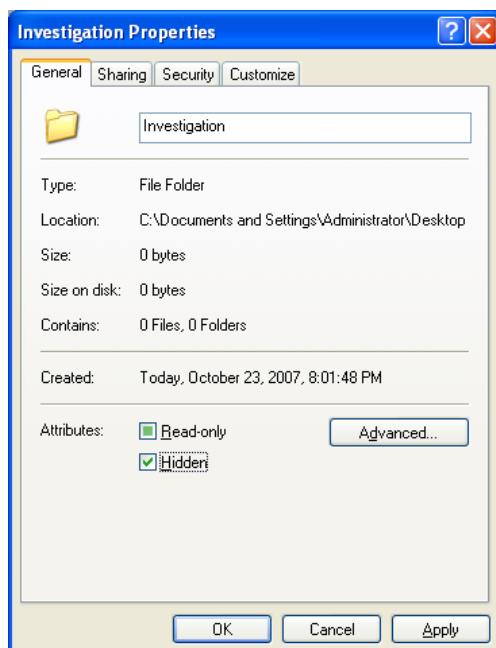
Unfortunately, steganography can also be used for illegal purposes. For example, if someone was trying to steal information, they could hide it in another file or files and send it out as an innocuous looking email or file transfer. Additionally, a person who saves pornography, or worse, to their hard drive, may choose to hide the evidence through the use of steganography. And, as was pointed out earlier, it can also be used as a means for covert communication. This issue is discussed further in Chapter 11.

13. Handling hidden data

Technology savvy criminals use various methods to hide incriminating information.

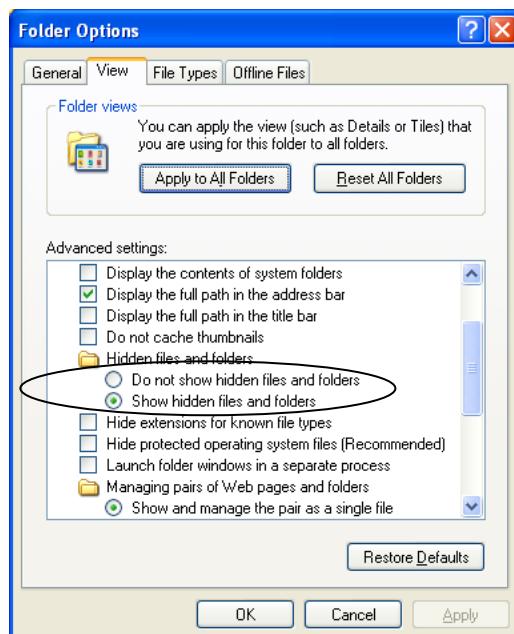
(1) Hidden files and folders

One of the simplest methods is “hidden files and folders” option of windows. To use this facility simply right click on a file or folder and click on “Properties”. Then check the “Hidden” option and click on “Apply”.



This file or folder will now be hidden from normal view. To display the file or folder, open Windows Explorer and click on “Tools”, then “Folder Options” and then “View”.

Under the “Hidden files and folders” heading there is an option named “Show hidden files and folders”. Check this option and click on “OK”. This will display all hidden files and folders.



(2) System files

A slightly more advanced option is to convert a confidential file into a system file so that Windows does not display the file even if the “Show hidden files and folders” option is selected.

Let us take an illustration to see how a file (e.g. sanya.txt) can be converted into a system file:

- Open up the Windows command prompt (Click Start, then Run, type in “cmd” and then click on OK).
- Let us presume that the sanya.txt file is stored in the root of the “d” drive of the computer. In the command prompt type in **d:**
- The command prompt will now display something like **D:>**

- (d) Type in **attrib +h +s sanya.txt**
- (e) The file would now be treated by Windows as a system file and would be hidden from view.
- (f) To display the file or folder, open Windows Explorer and click on “Tools”, then “Folder Options” and then “View”. There is an option named “Hide protected operating system files”. Uncheck this option and click on “OK”. This will display all system files.

(3) Alternate data streams (ADS)

Alternate data streams (ADS) are a very interesting feature of the NTFS file system. They can be used to “hide” one file inside another file.

Let us take a simple illustration that shows how to “hide” an MS Word file named “sanya.doc” in a text file named “tanya.txt”. Both these files are in the “G” drive.

- (a) Open up the Windows command prompt (Click Start, then Run, type in “cmd” and then click on OK).
- (b) In the command prompt type in **g:**
- (c) The command prompt will now display something like **G:\>**
- (d) Now type the following –

```
type g:\sanya.doc>g:\tanya.txt:sanya.doc
```

- (e) That’s it!
- (f) In order to run the “hidden” doc file, type the following:

```
start g:\tanya.txt:sanya.doc
```

14. Using keyloggers for investigation

Consider a case in which the police know which cyber café a suspected terrorist is going to use to send emails to his contacts. They are not sure about the identity of the terrorist or the exact computer in the cyber café that he would use. In such a situation they could install a keylogger in all the computers in the cyber café.

The logs generated by the keylogger could then be regularly examined to identify the email addresses being used by the suspect. All the information being emailed by the suspect would also be obtained.

Illustration: The police suspected Sameer to be a terrorist. They needed to have access to Sameer’s personal emails to recover evidence. An undercover police woman got a job as a maid servant in Sameer’s house. While working there she managed to install a keylogger in his laptop. The keylogger was configured

to regularly email keystroke logs to the police. During the next few weeks the police were able to crack down on the entire group of suspected terrorists using the information from the keystroke logs.

15. Searching for keywords

Keyword searching is a powerful technique during a cyber forensic investigation. Forensic investigations often involve analysis of a large quantity of data for particular keywords.

However, in most cases the investigator is not aware of the correct keyword to search for. E.g. the hard disk of a suspected drug peddler is seized. Would searching for the word “drugs” really help? Most probably not. The peddler may have used code words like “snow”, or “stuff” etc. He also may have misspelled “drugs” as “druggs”

Specialized keyword software is essential for cyber crime investigators. This software supports various types of search options including:

- (1) *Fuzzy searching* which will find a word even if it is misspelled. E.g. a fuzzy search for “money” will find “moneey”. Fuzzy searching is very useful when searching text that may contain typographical errors, or for text that has been scanned using optical character recognition (OCR). The level of fuzziness can be adjusted i.e. the number of differences between the search term and the matched term can be adjusted e.g. 1 difference (money and monay), 2 differences (money and monaw) etc.
- (2) *Phonic searching* which looks for a word that sounds like the searched word and begins with the same letter e.g. kite and kyte.
- (3) *Stemming* which extends a search to cover grammatical variations on a word e.g. a search for “run” would also find “running” and “ran”.
- (4) *Synonym searching* which finds synonyms of a word that is searched for. E.g. a search for “money” would also find “cash”.
- (5) *Numeric range search* which searches for any numbers that fall within a range. E.g. a search for numbers between 12 and 75. An advanced numeric search could be used to find instances where the word “money” comes within 10 words of a number between 10 and 70.

8. Investigating emails

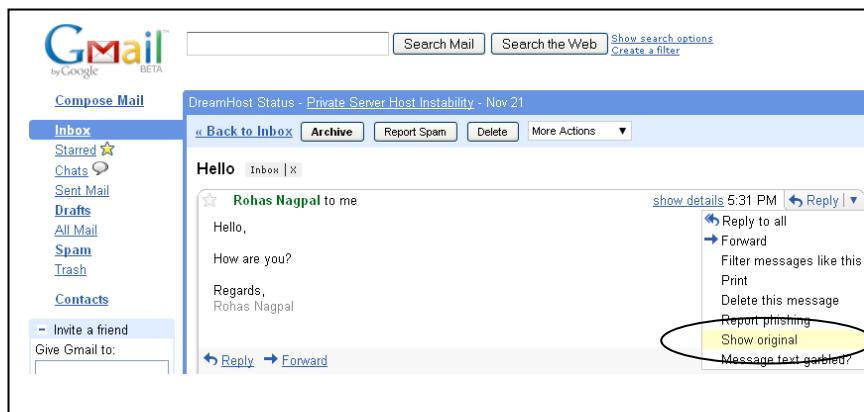
This chapter covers the following issues:

- (1) Analysis of the *Gmail* header
- (2) Analysis of the *Rediffmail* header
- (3) Analysis of the *Yahoo* header
- (4) Analysis of the *Thunderbird* email client header
- (5) Online email header analysis tools
- (6) Tracking email accounts
- (7) Case Study

Also relevant are the Common Internet Message Headers provided in the Annexure to this book.

1. Analysis of the Gmail header

To see the full header for a particular email, log into your gmail account and open up the email. Then click on the arrow button next to the “Reply” option. Finally, click on “Show Original” (as illustrated below):



This will open the email with the detailed header in a new window.

Now let us take the illustration of an email sent from tanya.777@rediffmail.com to sanyanagpal@gmail.com having the subject “Re: Email header analysis”.

The detailed header of the email is as under:

```

Delivered-To: sanyanagpal@gmail.com
Received: by 10.143.14.2 with SMTP id r2cs422355wfi;
          Sat, 13 Oct 2007 07:53:42 -0700 (PDT)
Received:       by      10.114.134.1      with      SMTP      id
h1mr4864975wad.1192287222686;
          Sat, 13 Oct 2007 07:53:42 -0700 (PDT)
Return-Path: <tanya.777@rediffmail.com>
Received: from rediffmail.com ([202.54.124.145])
          by mx.google.com      with      SMTP      id
z20si2553641pod.2007.10.13.07.53.41;
          Sat, 13 Oct 2007 07:53:42 -0700 (PDT)
Received-SPF: pass (google.com: domain of tanya.777@rediffmail.com
designates 202.54.124.145 as permitted sender) client-ip=202.54.124.145;
Authentication-Results: mx.google.com; spf=pass (google.com: domain of
tanya.777@rediffmail.com designates 202.54.124.145 as permitted sender)
smtp.mail=tanya.777@rediffmail.com
Received: (qmail 18986 invoked by uid 510); 13 Oct 2007 14:52:16 -0000
Date: 13 Oct 2007 14:52:16 -0000
Message-ID: <20071013145216.18983.qmail@webmail30.rediffmail.com>
MIME-Version: 1.0
To: <sanyanagpal@gmail.com>
Received: from unknown 122.169.11.181 by rediffmail.com via HTTP; 13
Oct 2007 14:52:16 -0000
Subject: Re: Email header analysis
From: "Tanya " <tanya.777@rediffmail.com>
Content-Type: multipart/alternative;
  boundary="=_7d001a0d1af346f974274cce90d3f126"
--=_7d001a0d1af346f974274cce90d3f126
Content-Type: text/plain; charset="ISO-8859-1"
Content-Transfer-Encoding: 7bit
Hi, Lets meet up at the Asian School of Cyber Laws office tomorrow.
Regards, Tanya
--=_7d001a0d1af346f974274cce90d3f126
Content-Type: text/html; charset="ISO-8859-1"
Content-Transfer-Encoding: quoted-printable
--=_7d001a0d1af346f974274cce90d3f126--

```

Let us now analyse this header. [Note: The original header is shown in **bold** font and the analysis is in normal font]

Delivered-To: sanyanagpal@gmail.com

This signifies that this email was delivered to the account sanyanagpal@gmail.com

Received: by 10.143.14.2 with SMTP id r2cs422355wfi;

Sat, 13 Oct 2007 07:53:42 -0700 (PDT)

Received: by 10.114.134.1 with SMTP id h1mr4864975wad.1192287222686;

Sat, 13 Oct 2007 07:53:42 -0700 (PDT)

This is the trace of the MTAs (Message Transfer Agents), which this email has passed along with the relevant date and time. An MTA, commonly referred to as the mail server program, is the program responsible for receiving incoming e-mails and delivering the messages to individual users. The MTA transfers messages between computers.

UNIX sendmail and Microsoft Exchange Server are two examples of MTAs. Hidden from the average user, it is responsible for routing messages to their proper destinations. MTAs receive messages from both Mail User Agents (MUAs) and other MTAs.

Mail user agent is the software that allows a user to access and manage e-mail, including reading, composing, disposing, and printing and displaying e-mail messages. The MUA provides the interface between the user and the MTA. Eudora and Outlook are two popular MUAs.

PDT stands for Pacific Daylight Time and -0700 signifies that the time mentioned is 7 hours behind GMT. To convert PDT to IST (Indian Standard Time) simply add 12 hours and 30 minutes. E.g. 07:53:42 PDT is 20:23:42 IST i.e. 42 seconds past 8.23 pm.

If you perform a Whois search ([using www.whois-search.com](http://www.whois-search.com)) for the IP addresses **10.143.14.2** and **10.114.134.1** mentioned above, you would be informed that the block of IP addresses from 10.0.0.0 through 10.255.255.255 is reserved for special purposes.

This part of the header is not of much interest to us as far as investigation is concerned; hence we will not elaborate on the purposes for which these IP addresses are blocked. RFC 1918 titled "Address Allocation for Private Internets" provides further details on this issue¹⁹.

Return-Path: <tanya.777@rediffmail.com>

In the event that the email is rejected by the recipient server it would bounce to the email ID mentioned here i.e. tanya.777@rediffmail.com

Received: from rediffmail.com ([202.54.124.145])

by mx.google.com with SMTP id z20si2553641pod.2007.10.13.07.53.41;

Sat, 13 Oct 2007 07:53:42 -0700 (PDT)

¹⁹ This RFC can be downloaded from <ftp://ftp.rfc-editor.org/in-notes/rfc1918.txt>

This signifies that the email was received by a Simple Mail Transfer Protocol (SMTP) server at Google called mx.google.com at the abovementioned time from the rediffmail.com server that has the IP address 202.54.124.145. On performing a Whois search for this IP (using www.whois-search.com) we can ascertain that the IP is that of Videsh Sanchar Nigam Limited, an Internet Service Provider based in India. Rediffmail.com appears to have taken Internet services from Videsh Sanchar Nigam Limited.

Received-SPF: pass (google.com: domain of tanya.777@rediffmail.com designates 202.54.124.145 as permitted sender) client-ip=202.54.124.145;

Authentication-Results: mx.google.com; spf=pass (google.com: domain of tanya.777@rediffmail.com designates 202.54.124.145 as permitted sender) smtp.mail=tanya.777@rediffmail.com

SPF stands for Sender Policy Framework, an extension of SMTP that stops e-mail spammers from forging the “From” fields in an e-mail. As SMTP itself does not carry an authenticating mechanism, the SPF extension provides the authentication scheme by specifying which computers are authorized to send email from a specific domain.

In order to use SPF, the domain sending e-mails must establish an SPF record that is published in DNS records. When the e-mail passes through the DNS server, it is compared to the SPF record for that domain to determine if the sender is indeed authorized to transmit e-mails from that sender's address. If the e-mail comes from a domain that is not authorized, the DNS server will not forward the e-mail to the expected destination. SPF is one method that can be used to stop spam from being sent using unauthorized domain names. However, it should be noted that SPF only stops the spammer from forging the “From” field in the e-mail and does not stop the spammer from sending e-mails from a domain in which it is a member. SPF was formerly called Sender Permitted Form, but the name was later changed while the abbreviation remained the same. In this case, since it is a genuine email, the SPF status is “pass”. If the SPF status was “failed”, the email would directly have gone to the spam folder of Sanya's email account i.e. sanyanagpal@gmail.com

Received: (qmail 18986 invoked by uid 510); 13 Oct 2007 14:52:16 -0000

This indicates that the program called qmail is running on the mail server, shows the version and the time of the processing. The mail server is showing the time stamp in GMT.

Date: 13 Oct 2007 14:52:16 -0000

Message-ID: <20071013145216.18983.qmail@webmail30.rediffmail.com>

MIME-Version: 1.0

To: <sanyanagpal@gmail.com>

Received: from unknown 122.169.11.181 by rediffmail.com via HTTP; 13 Oct 2007 14:52:16 -0000

From an investigation point of view this is probably the most important part of the email header. The conclusions that we can draw from this part of the header are:

- (1) The email was sent from a computer having IP address **122.169.11.181**
- (2) The email was sent from the above-mentioned computer on 13 October, 2007 at **14:52:16 -0000** GMT i.e. **20:22:16 IST**
- (3) The Rediffmail server has stamped the following unique Message ID to this email: **20071013145216.18983.qmail@webmail30.rediffmail.com**

Performing a Whois search (using <http://www.whois-search.com>) displays that the IP address information can be obtained from Asia Pacific Network Information Centre (APNIC).

It can be ascertained (by performing a Whois search at the apnic.net website that the IP Address 122.169.11.181 is registered to Bharti Airtel Ltd - Broadband & Telephone Services, an Internet Service Provider (ISP) based in India.

As an Internet Service Provider, Bharti Airtel Ltd has a large number of IP addresses. As its customers log on to the Internet, Airtel allots them an IP address from its pool of IP addresses. Once a user logs off the Internet, the IP address allotted to him would be allotted to another user.

Thus we can see that only Bharti Airtel Ltd would be able to provide information as to who is the user who had been allotted this IP address at that particular time. In conclusion we can see that the cooperation of the ISP is essential for tracing the exact sender of an email.

MIME-Version: 1.0

Multipurpose Internet Mail Extensions (MIME) refers to an official Internet standard that specifies how messages must be formatted so that they can be exchanged between different email systems. MIME is a very flexible format, permitting one to include virtually any type of file or document in an email message. Specifically, MIME messages can contain text, images, audio, video, or other application-specific data.

Subject: Re: Email header analysis

This is the subject of the email.

From: "Tanya " <tanya.777@rediffmail.com>

This signifies that the mail was sent by tanya.777@rediffmail.com who gives her name as **Tanya**. Please remember that this can be spoofed very easily. *DO NOT rely on this part of the header while investigating an email.*

Content-Type: multipart/alternative;

boundary="=_7d001a0d1af346f974274cce90d3f126"

==_7d001a0d1af346f974274cce90d3f126

Content-Type: text/plain; charset="ISO-8859-1"

Content-Transfer-Encoding: 7bit

The multipart/alternative content type is used when the same information is presented in different body parts in different forms.

The body parts are ordered by increasing complexity. For example, a message that consists of a heavily formatted Microsoft® Word 97 document might also be presented in Microsoft Word version 6.0 format, rich text format, and a plain text format.

In this case the plain text would be presented as the first alternative body part. The rich text version would follow, then the Word 6.0, then the most complex, Word 97. Placing the plain text version first is the friendliest scheme for users with non-MIME-compliant User Agents, because they will see the recognizable version first.

The MIME-compliant User Agents should present the most complex version that they can recognize or give the user a choice of which version to view.

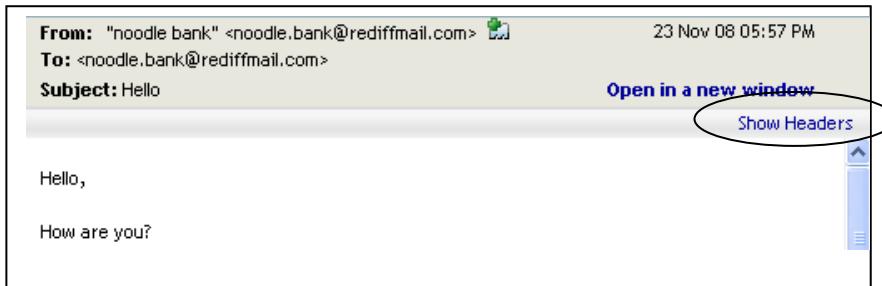
Hi, Lets meet up at the Asian School of Cyber Laws office tomorrow.

Regards,Tanya

This is the plain text representation of the body of the email.

2. Analysis of the Rediffmail header

To see the full header for a particular email, log into your rediffmail account and open up the email. Then click on the “Show Headers” option near the top of the email. (as illustrated below):



This will open the detailed email header email in a new window.

Let us take the illustration of an email sent from nagpalsanya@yahoo.com to tanya.777@rediffmail.com. The subject of the email is – “Re: Email header analysis”

This email is sent from a yahoo.com account to a rediffmail.com email account. The header of the email is as under:

```
Return-Path: <nagpalsanya@yahoo.com>
Delivered-To: tanya.777@f1.p4.mail.in.rediffmail.com
Received: (qmail 9288 invoked from network); 15 Oct 2007 10:15:59 -0000
Received: from unknown (HELO rediffmail.com) (220.226.195.203)
by 0 with SMTP; 15 Oct 2007 10:15:59 -0000
Received: (qmail 14680 invoked from network); 15 Oct 2007 10:15:58 -0000
Received: from unknown (HELO n9.bullet.ukl.yahoo.com) (217.146.182.189)
by 0 with SMTP; 15 Oct 2007 10:15:58 -0000
Received: from [217.12.4.214] by n9.bullet.ukl.yahoo.com with NNFMP; 15
Oct 2007 10:17:16 -0000
Received: from [216.252.122.217] by t1.bullet.ukl.yahoo.com with NNFMP; 15
Oct 2007 10:17:16 -0000
Received: from [69.147.84.114] by t2.bullet.sp1.yahoo.com with NNFMP; 15
Oct 2007 10:17:16 -0000
Received: from [127.0.0.1] by omp203.mail.sp1.yahoo.com with NNFMP; 15
Oct 2007 10:17:16 -0000
X-Yahoo-Newman-Property: ymail-3
```

```
X-Yahoo-Newman-Id: 610847.72799.bm@omp203.mail.sp1.yahoo.com
Received: (qmail 39035 invoked by uid 60001); 15 Oct 2007 10:17:16 -0000
DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws;
s=s1024; d= yahoo.com;
h=X-Ymail-OSG:Received:Date:From:Subject:To:MIME-Version:Content-
Type:Content-Transfer-Encoding:Message-ID;
b=zonuVU93WbuPdzLNnl6Ky26duwQ3WaYLDJ/t226xGtagY2hWYO9aIW4s
GsViX2muK3vjgHfO0ZWO5/BSUIKAzazltl2DmkWEyoEAa96lPt3NFBHTGu
hYauHrE1eLAbyyU8FlmDO/JaZSQvz1OtpDK404kD/s7cZXmn8vXO2qpHQ=
;
X-Ymail-OSG:
ajdT7VQVM1k4SkCx.MfjoBwiZuKhbtgxUzRt2W.Wv3ZsH0W5_Rj3F8Kld6ii
Om70U3ocVlsXjrh1dlbNR3wvyQQmg5u3hjfj02D8hoVeeWUovD5braNXn3G.
aA-
Received: from [122.169.35.25] by web45603.mail.sp1.yahoo.com via HTTP;
Mon, 15 Oct 2007 03:17:16 PDT
Date: Mon, 15 Oct 2007 03:17:16 -0700 (PDT)
From: Sanya Nagpal <nagpalsanya@yahoo.com>
Subject: test
To: tanya.777@rediffmail.com
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="0-1285962384-
1192443436=:38368"
Content-Transfer-Encoding: 8bit
Message-ID: <343993.38368.qm@web45603.mail.sp1.yahoo.com>
```

Let us now analyse this header. **[Note:** The original header is shown in **bold** font and the analysis is in normal font]

Return-Path: <nagpalsanya@yahoo.com>

In the event that the email is rejected by the recipient server it would bounce to the email ID mentioned here i.e. nagpalsanya@yahoo.com

Delivered-To: tanya.777@f1.p4.mail.in.rediffmail.com

This signifies that this email was delivered to the account tanya.777 maintained in the rediffmail server named f1.p4.mail.in.

Return-Path: <nagpalsanya@yahoo.com>

Delivered-To: tanya.777@f1.p4.mail.in.rediffmail.com

Received: (qmail 9288 invoked from network); 15 Oct 2007 10:15:59 -0000
Received: from unknown (HELO rediffmail.com) (220.226.195.203)
by 0 with SMTP; 15 Oct 2007 10:15:59 -0000
Received: (qmail 14680 invoked from network); 15 Oct 2007 10:15:58 -0000
Received: from unknown (HELO n9.bullet.ukl.yahoo.com)
(217.146.182.189)
by 0 with SMTP; 15 Oct 2007 10:15:58 -0000
Received: from [217.12.4.214] by n9.bullet.ukl.yahoo.com with NNFMP; 15
Oct 2007 10:17:16 -0000
Received: from [216.252.122.217] by t1.bullet.ukl.yahoo.com with NNFMP;
15 Oct 2007 10:17:16 -0000
Received: from [69.147.84.114] by t2.bullet.sp1.yahoo.com with NNFMP;
15 Oct 2007 10:17:16 -0000
Received: from [127.0.0.1] by omp203.mail.sp1.yahoo.com with NNFMP;
15 Oct 2007 10:17:16 -0000

This is the trace of the MTAs (Message Transfer Agents), which this email has passed along with the relevant date and time. An MTA, commonly referred to as the mail server program, is the program responsible for receiving incoming e-mails and delivering the messages to individual users. The MTA transfers messages between computers.

UNIX sendmail and Microsoft Exchange Server are two examples of MTAs. Hidden from the average user, it is responsible for routing messages to their proper destinations. MTAs receive messages from both Mail User Agents (MUAs) and other MTAs.

Mail user agent is the software that allows a user to access and manage e-mail, including reading, composing, disposing, and printing and displaying e-mail messages. The MUA provides the interface between the user and the MTA. Eudora and Outlook are two popular MUAs.

-0000 signifies that the time mentioned is GMT. To convert GMT to IST (Indian Standard Time) simply add 5 hours and 30 minutes. E.g. 10:17:16 PDT is 15:47:16 IST i.e. 16 seconds past 3.47 pm.

If you perform a Whois search (using www.whois-search.com) for the IP addresses **217.146.182.189**, **216.252.122.217** and **69.147.84.114** mentioned above, you would be informed that they are registered to Yahoo Inc. 127.0.0.1 is an internal network IP address and has no relevance to our analysis.

This part of the header is not of much interest to us as far as investigation is concerned.

X-Yahoo-Newman-Property: ymail-3

X-Yahoo-Newman-Id: 610847.72799.bm@omp203.mail.sp1.yahoo.com

Received: (qmail 39035 invoked by uid 60001); 15 Oct 2007 10:17:16 -0000

**DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws; s=s1024;
d=yahoo.com;**

**h=X-Ymail-OSG:Received:Date:From:Subject:To:MIME-
Version:Content-Type:Content-Transfer-Encoding:Message-ID;**

**b=zonuVU93WbuPdzLNnl6Ky26duwQ3WaYLDJ/t226xGtagY2hWYO9aIW4sGsViX2muK3vjqHfO0ZWO5/BSUIKAzazltl2DmkWEyoEAa96lPt3NF
BHTGuhYauHrE1eLAbyyU8FlmDO/JaZSQvz1OtpDK404kD/s7cZXmn8v
XO2qpHQ=; X-Ymail-OSG:
ajdT7VQVM1k4SkCx.MfjoBwiZuKhbtgxUzRt2W.Wv3ZsH0W5_Rj3F8KId6iiOm70U3ocVlsXjrh1dlbNR3wvyQQmg5u3hjfj02D8hoVeeWUovD5bra
NXn3G.aA=**

Parts of the header beginning with **X-** are internal Yahoo stamped information and are not relevant to our analysis. Domain keys are a Yahoo patented technology to control email spoofing. For more information on Domain keys please visit the URL – <http://antispam.yahoo.com/domainkeys>

**Received: from [122.169.35.25] by web45603.mail.sp1.yahoo.com via
HTTP; Mon, 15 Oct 2007 03:17:16 PDT**

Date: Mon, 15 Oct 2007 03:17:16 -0700 (PDT)

From an investigation point of view this is probably the most important part of the email header. The conclusions that we can draw from this part of the header are:

- (1) The email was sent from a computer having IP address 122.169.35.25
- (2) The email was sent from the above-mentioned computer on 15 October, 2007 at 03:17:16 -0700 PDT. i.e. 15:47:16 Indian Standard Time. PDT stands for Pacific Daylight Time and -0700 signifies that the time mentioned is 7 hours behind GMT. To convert PDT to IST (Indian Standard Time) simply add 12 hours and 30 minutes. It can be ascertained (by performing a Whois search at the apnic.net website that the IP Address 122.169.11.181 is registered to Bharti Airtel Ltd – Broadband & Telephone Services, an Internet Service Provider (ISP) based in India.

As an Internet Service Provider, Bharti Airtel Ltd has a large number of IP addresses. As its customers log on to the Internet, Airtel allots them

an IP address from its pool of IP addresses. Once a user logs off the Internet, the IP address allotted to him would be allotted to another user.

Thus we can see that only Bharti Airtel Ltd would be able to provide information as to who is the user who had been allotted this IP address at that particular time. In conclusion we can see that the cooperation of the ISP is essential for tracing the exact sender of an email.

From: “Sanya Nagpal “ <nagpalsanya@yahoo.com>

This signifies that the mail was sent by nagpalsanya@yahoo.com who gives her name as Sanya Nagpal. Please remember that this can be spoofed very easily. DO NOT rely on this part of the header while investigating an email.

Subject: Re: Email header analysis

This is the subject of the email.

MIME-Version: 1.0

Multipurpose Internet Mail Extensions (MIME) refers to an official Internet standard that specifies how messages must be formatted so that they can be exchanged between different email systems.

MIME is a very flexible format, permitting one to include virtually any type of file or document in an email message. Specifically, MIME messages can contain text, images, audio, video, or other application-specific data.

Content-Type: multipart/alternative; boundary=”0-1285962384-1192443436=:38368” **Content-Transfer-Encoding:** 8bit

The multipart/alternative content type is used when the same information is presented in different body parts in different forms.

The body parts are ordered by increasing complexity. For example, a message that consists of a heavily formatted Microsoft® Word 97 document might also be presented in Microsoft Word version 6.0 format, rich text format, and a plain text format.

In this case the plain text would be presented as the first alternative body part. The rich text version would follow, then the Word 6.0, then the most complex, Word 97. Placing the plain text version first is the friendliest scheme for users with non-MIME-compliant User Agents, because they will see the recognizable version first.

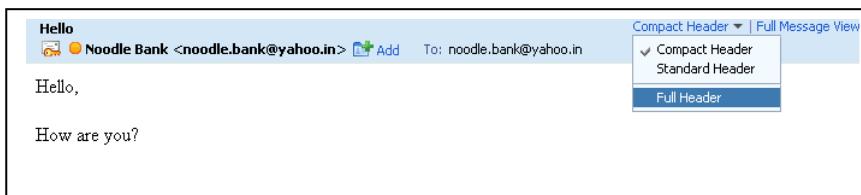
The MIME-compliant User Agents should present the most complex version that they can recognize or give the user a choice of which version to view.

Message-ID: <343993.38368.qm@web45603.mail.sp1.yahoo.com>

The Yahoo server has stamped the following unique Message ID to this email: **343993.38368.qm@web45603.mail.sp1.yahoo.com**

3. Analysis of the Yahoo header

To see the full header for a particular email, log into your yahoo account and open up the email. Then click on the “Full Header” option on the top right hand corner as illustrated below.



This will open the detailed email header.

Let us take the illustration of an email sent from tanya.777@rediffmail.com to nagpalsanya@yahoo.com. The subject of the email is – “Re: Email header analysis”

This email is sent from a rediffmail.com account to a yahoo.com email account. The detailed email header is as under:

```
X-Apparently-To: nagpalsanya@yahoo.com via 68.180.197.144; Mon, 15
Oct 2007 03:05:26 -0700
X-YahooFilteredBulk: 203.199.83.33
X-Originating-IP:[203.199.83.33]
Return-Path: <tanya.777@rediffmail.com>
Authentication-Results: mta276.mail.mud.yahoo.com from=rediffmail.com;
domainkeys=neutral (no sig)
Received: from 203.199.83.33 (HELO rediffmail.com) (203.199.83.33) by
mta276.mail.mud.yahoo.com with SMTP; Mon, 15 Oct 2007 03:05:26 -0700
Received: (qmail 19445 invoked by uid 510); 15 Oct 2007 10:04:00 -0000
Date: 15 Oct 2007 10:04:00 -0000
Message-ID: <20071015100400.19441.qmail@f4mail203.rediffmail.com>
MIME-Version: 1.0
To: nagpalsanya@yahoo.com
Received: from unknown 122.169.35.25 by rediffmail.com via HTTP; 15
Oct 2007 10:04:00 -0000
Subject: hi
From: "Tanya " <tanya.777@rediffmail.com>
Content-Type: multipart/alternative;
boundary="=_1c8583417c3d8e8c4872024d66556d24"
Content-Length: 815
```

Let us examine the header. [Note: The original header is in **bold** font and the analysis is in normal text.]

X-Apparently-To: nagpalsanya@yahoo.com via 68.180.197.144;
Mon, 15 Oct 2007 03:05:26 -0700

This is an Internal Yahoo header and is not relevant for our analysis. It can be ascertained (by performing a Whois search at the www.whois-search.com website that the IP Address 68.180.197.144 is registered to Yahoo Inc.

X-YahooFilteredBulk: 203.199.83.33

This is a special header used by Yahoo mail to filter spam.

X-Originating-IP: [203.199.83.33]

This is NOT the IP address of the computer where the email originated. It can be ascertained (by performing a Whois search using <http://www.whois-search.com>) that the IP Address that of Videsh Sanchar Nigam Limited (VSNL), an Internet Service Provider (ISP) based in India.

It can also be ascertained that this IP address is part of the pool of IP addresses used by Rediffmail, which is the email service provider used to send this email.

Authentication-Results: mta276.mail.mud.yahoo.com
from=rediffmail.com; domainkeys=neutral (no sig)

Domain keys are a Yahoo patented technology to control email spoofing. For more information on Domain keys please visit the URL – <http://antispam.yahoo.com/domainkeys>

**Received: from 203.199.83.33 (HELO rediffmail.com)
(203.199.83.33) by mta276.mail.mud.yahoo.com with SMTP; Mon,
15 Oct 2007 03:05:26 -0700**

**Received: (qmail 19445 invoked by uid 510); 15 Oct 2007 10:04:00 -
0000**

Date: 15 Oct 2007 10:04:00 -0000

This is the trace of the MTAs (Message Transfer Agents), which this email has passed along with the relevant date and time.

An MTA, commonly referred to as the mail server program, is the program responsible for receiving incoming e-mails and delivering the messages to individual users. The MTA transfers messages between computers. UNIX sendmail and Microsoft Exchange Server are two examples of MTAs.

Hidden from the average user, it is responsible for routing messages to their proper destinations. MTAs receive messages from both Mail User Agents (MUAs) and other MTAs.

Mail user agent is the software that allows a user to access and manage e-mail, including reading, composing, disposing, printing and displaying e-mail messages. The MUA provides the interface between the user and the MTA. Eudora and Outlook are two popular MUAs.

**Message-ID:
<20071015100400.19441.qmail@f4mail203.rediffmail.com>**

This signifies that the Rediffmail server has allotted the unique message ID <20071015100400.19441.qmail@f4mail203.rediffmail.com> to this email.

MIME-Version: 1.0

Multipurpose Internet Mail Extensions (MIME) refers to an official Internet standard that specifies how messages must be formatted so that they can be exchanged between different email systems. MIME is a very

flexible format, permitting one to include virtually any type of file or document in an email message.

Specifically, MIME messages can contain text, images, audio, video, or other application-specific data.

Received: from unknown 122.169.35.25 by rediffmail.com via HTTP; 15 Oct 2007 10:04:00 -0000

From an investigation point of view this is probably the most important part of the email header. The conclusions that we can draw from this part of the header are:

The email was sent from a computer having IP address 122.169.35.25

The email was sent from the above-mentioned computer at **10:04:00** GMT i.e. **15:34:00** Indian Standard Time i.e. 3.34 pm.

It can be ascertained (by performing a Whois search at the apnic.net website that the IP Address 122.169.11.181 is registered to Bharti Airtel Ltd – Broadband & Telephone Services, an Internet Service Provider (ISP) based in India.

As an Internet Service Provider, Bharti Airtel Ltd has a large number of IP addresses. As its customers log on to the Internet, Airtel allots them an IP address from its pool of IP addresses. Once a user logs off the Internet, the IP address allotted to him would be allotted to another user.

Thus we can see that only Bharti Airtel Ltd would be able to provide information as to who is the user who had been allotted this IP address at that particular time. In conclusion we can see that the cooperation of the ISP is essential for tracing the exact sender of an email.

From: "Tanya" <tanya.777@rediffmail.com>

This signifies that the mail was sent by tanya.777@rediffmail.com who gives her name as Tanya.

Please remember that this can be spoofed very easily using email spoofing software. **DO NOT rely on this part of the header while investigating an email.**

**Content-type: multipart/alternative;
boundary="=_1e8583417c3d8e8c4872024d66556d24"**

The multipart/alternative content type is used when the same information is presented in different body parts in different forms.

The body parts are ordered by increasing complexity. For example, a message that consists of a heavily formatted Microsoft® Word 97 document might also be presented in Microsoft Word version 6.0 format, rich text format, and a plain text format.

In this case the plain text would be presented as the first alternative body part. The rich text version would follow, then the Word 6.0, then the most complex, Word 97. Placing the plain text version first is the friendliest scheme for users with non-MIME-compliant User Agents, because they will see the recognizable version first.

The MIME-compliant User Agents should present the most complex version that they can recognize or give the user a choice of which version to view.

4. Analysis of email sent from Thunderbird Client

Thunderbird is a free, open-source and cross-platform mail client for most operating systems including, but not limited to, Windows, Linux and Macintosh. It is based on the Mozilla codebase. It is a robust and easy to use client, similar to competing products like Outlook Express.

Let us take the illustration of an email sent from demo1@vault64.net to sanyanagpal@gmail.com. The subject of the email is – “Hi”. This email is sent from a vault64.net account configured on a Thunderbird client to a gmail.com email account. The detailed email header is as under:

```
Delivered-To: sanyanagpal@gmail.com
Received: by 10.143.14.2 with SMTP id r2cs20437wfi;
          Mon, 15 Oct 2007 04:28:44 -0700 (PDT)
Received: by 10.66.222.9 with SMTP id u9mr7814334ugg.1192447722928;
          Mon, 15 Oct 2007 04:28:42 -0700 (PDT)
Return-Path: <demo1@vault64.net>
Received: from smtp1.infomaniak.ch (smtp1.infomaniak.ch [84.16.68.89])
          by mx.google.com with ESMTP id z33si3136254ikz.2007.10.15.04.28.41;
          Mon, 15 Oct 2007 04:28:42 -0700 (PDT)
Received-SPF: pass (google.com: domain of demo1@vault64.net designates
84.16.68.89 as permitted sender) client-ip=84.16.68.89;
Authentication-Results: mx.google.com; spf=pass (google.com: domain of
demo1@vault64.net designates 84.16.68.89 as permitted sender)
smtp.mail=demo1@vault64.net
Received: from [10.10.10.4] (ABTS-MH-dynamic-025.35.169.122.airtelbroadband.in
[122.169.35.25] (may be forged))
          (authenticated bits=0)
          by smtp1.infomaniak.ch (8.13.6/8.13.6) with ESMTP id l9FBSda6016996
          for <sanyanagpal@gmail.com>; Mon, 15 Oct 2007 13:28:41 +0200
Message-ID: <47134EDB.1000707@vault64.net>
Date: Mon, 15 Oct 2007 16:58:27 +0530
From: Data64 Demo <demo1@vault64.net>
User-Agent: Thunderbird 1.5.0.12 (Windows/20070509)
MIME-Version: 1.0
To: sanyanagpal@gmail.com
Subject: Hello
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit
X-Antivirus: Dr.Web (R) for Mail Servers on smtp1 host
X-Antivirus-Code: 100000
X-Infomaniak-Spam: ham
X-Spam-Score: 0
Hi, Lets meet up at the Asian School of Cyber Laws office tomorrow. Regards, Tanya
```

Given below is the analysis of the header from an email sent from demo1@vault64.net using **Thunderbird** email client to sanyanagpal@gmail.com

Note: The original header is in **bold** font and the analysis is in normal text.

Delivered-To: sanyanagpal@gmail.com

This signifies that this email was delivered to the account sanyanagpal@gmail.com

Received: by 10.143.14.2 with SMTP id r2cs20437wfi;

Mon, 15 Oct 2007 04:28:44 -0700 (PDT)

Received: by 10.66.222.9 with SMTP id u9mr7814334ugg.1192447722928;

Mon, 15 Oct 2007 04:28:42 -0700 (PDT)

This is the trace of the MTAs (Message Transfer Agents), which this email has passed along with the relevant date and time. An MTA, commonly referred to as the mail server program, is the program responsible for receiving incoming e-mails and delivering the messages to individual users. The MTA transfers messages between computers.

UNIX sendmail and Microsoft Exchange Server are two examples of MTAs. Hidden from the average user, it is responsible for routing messages to their proper destinations. MTAs receive messages from both Mail User Agents (MUAs) and other MTAs.

Mail user agent is the software that allows a user to access and manage e-mail, including reading, composing, disposing, and printing and displaying e-mail messages. The MUA provides the interface between the user and the MTA. Eudora and Outlook are two popular MUAs.

PDT stands for Pacific Daylight Time and -0700 signifies that the time mentioned is 7 hours behind GMT. To convert PDT to IST (Indian Standard Time) simply add 12 hours and 30 minutes. If you perform a Whois search (using www.whois-search.com) for the IP addresses **10.143.14.2** and **10.66.222.9** mentioned above, you would be informed that the block of IP addresses from 10.0.0.0 through 10.255.255.255 is reserved for special purposes.

This part of the header is not of much interest to us as far as investigation is concerned; hence we will not elaborate on the purposes for which these IP addresses are blocked. RFC 1918 titled "Address Allocation for Private Internets" provides further details on this issue. This RFC can be downloaded from

<ftp://ftp.rfc-editor.org/in-notes/rfc1918.txt>

Return-Path: <demo1@vault64.net>

In the event that the email is rejected by the recipient server it would bounce to the email ID mentioned here i.e. demo1@vault64.net

Received: from **smtp1.infomaniak.ch** (**smtp1.infomaniak.ch [84.16.68.89]**)
by **mx.google.com** with **ESMTP** **id**
z33si3136254ikz.2007.10.15.04.28.41;
Mon, 15 Oct 2007 04:28:42 -0700 (PDT)

This signifies that the email was received by a Simple Mail Transfer Protocol (SMTP) server at Google called mx.google.com at the abovementioned time from the infomaniak.ch server that has the IP address 84.16.68.89.

On performing a Whois search for this IP (using www.whois-search.com) we can ascertain that the IP is that of Infomaniak, a Switzerland based Internet Service Provider. Vault64.net appears to have taken Internet services from Infomaniak.

Received-SPF: pass (google.com: domain of demo1@vault64.net designates 84.16.68.89 as permitted sender) client-ip=84.16.68.89;

Authentication-Results: mx.google.com; spf=pass (google.com: domain of demo1@vault64.net designates 84.16.68.89 as permitted sender) smtp.mail=demo1@vault64.net

SPF stands for Sender Policy Framework, an extension of SMTP that stops e-mail spammers from forging the “From” fields in an e-mail. As SMTP itself does not carry an authenticating mechanism, the SPF extension provides the authentication scheme by specifying which computers are authorized to send email from a specific domain.

In order to use SPF, the domain sending e-mails must establish an SPF record that is published in DNS records. When the e-mail passes through the DNS server, it is compared to the SPF record for that domain to determine if the sender is indeed authorized to transmit e-mails from that sender's address. If the e-mail comes from a domain that is not authorized, the DNS server will not forward the e-mail to the expected destination.

SPF is one method that can be used to stop spam from being sent using unauthorized domain names.

However, it should be noted that SPF only stops the spammer from forging the “From” field in the e-mail and does not stop the spammer from sending e-mails from a domain in which it is a member.

SPF was formerly called Sender Permitted Form, but the name was later changed while the abbreviation remained the same.

In this case, since it is a genuine email, the SPF status is “pass”. If the SPF status was “failed”, the email would directly have gone to the spam folder of Sanya’s email account i.e. sanyanagpal@gmail.com

Received: from [10.10.10.4] (ABTS-MH-dynamic-025.35.169.122.airtelbroadband.in [122.169.35.25] (may be forged) (authenticated bits=0) by smtp1.infomaniak.ch (8.13.6/8.13.6) with ESMTP id I9FBSDa6016996 for <sanyanagpal@gmail.com>; Mon, 15 Oct 2007 13:28:41 +0200

From an investigation point of view this is probably the most important part of the email header. The conclusions that we can draw from this part of the header are:

1. The email was sent from a computer having IP address **122.169.35.25**
2. The email was sent from the above-mentioned computer on 15 October, 2007 at **13:28:41 +0200** i.e. 16:58:41 Indian Standard Time.
3. The email was sent from a computer having an internal IP address 10.10.10.4. This additional information would help in tracking the computer from which the mail was sent, if the mail has been sent from an internal network like a LAN.
4. It can be ascertained (by performing a Whois search at the apnic.net website that the IP Address 122.169.35.25 is registered to Bharti Airtel Ltd - Broadband & Telephone Services, an Internet Service Provider (ISP) based in India.

5. As an Internet Service Provider, Bharti Airtel Ltd has a large number of IP addresses. As its customers log on to the Internet, Airtel allots them an IP address from its pool of IP addresses. Once a user logs off the Internet, the IP address allotted to him would be allotted to another user.
6. Thus we can see that only Bharti Airtel Ltd would be able to provide information as to who is the user who had been allotted this IP address at that particular time. In conclusion we can see that the cooperation of the ISP is essential for tracing the exact sender of an email.

Message-ID: <47134EDB.1000707@vault64.net>

The vault64.net server has stamped the following unique Message ID to this email:
47134EDB.1000707@vault64.net

Date: Mon, 15 Oct 2007 16:58:27 +0530

The email was sent on 15 October, 2007 at **16:58:27** Indian Standard Time. In one of the previous headers, the time was calculated as 16:58:41. This difference of 14 seconds is on account of the slow Internet speed.

From: Data64 Demo <demo1@vault64.net>

This signifies that the mail was sent by demo1@vault64.net who gives its name as **Data64 Demo**. Please remember that this can be spoofed very easily. **DO NOT rely on this part of the header while investigating an email.**

User-Agent: Thunderbird 1.5.0.12 (Windows/20070509)

A mail user agent (MUA) or User-Agent functions by connecting to a mailbox into which e-mail has been fetched and stored in a particular format. It typically presents a simple user interface to perform tasks with the mail. An MUA by itself is incapable of sending or retrieving mail.

Here Thunderbird is a MUA having version 1.5.0.12 which was used for sending a mail. Another good example of MUA is MS Outlook Express.

MIME-Version: 1.0

Multipurpose Internet Mail Extensions (MIME) refers to an official Internet standard that specifies how messages must be formatted so that they can be exchanged between different email systems.

MIME is a very flexible format, permitting one to include virtually any type of file or document in an email message. Specifically, MIME messages can contain text, images, audio, video, or other application-specific data.

Content-Type: text/plain; charset=ISO-8859-1; format=flowed

Content-Transfer-Encoding: 7bit

The multipart/alternative content type is used when the same information is presented in different body parts in different forms.

The body parts are ordered by increasing complexity. For example, a message that consists of a heavily formatted Microsoft® Word 97 document might also be presented in Microsoft Word version 6.0 format, rich text format, and a plain text format.

In this case the plain text would be presented as the first alternative body part. The rich text version would follow, then the Word 6.0, then the most complex, Word 97. Placing the plain text version first is the friendliest scheme for users with non-MIME-compliant User Agents, because they will see the recognizable version first.

The MIME-compliant User Agents should present the most complex version that they can recognize or give the user a choice of which version to view.

X-Antivirus: Dr.Web (R) for Mail Servers on smtp1 host

X-Antivirus-Code: 100000

X-Infomaniak-Spam: ham

X-Spam-Score: 0

These are internal vault64.net headers and are not relevant to our investigation. It appears that the valt64.net servers are using Dr. Web anti-virus services to filter all email for viruses.

5. Online email header analysis tools

There are several tools that can automate the process of email header analysis. One such tools is available online at: <http://cyberforensics.in/OnlineEmailTracer/index.aspx> and is illustrated below.

The screenshot shows the 'Online EmailTracer' page from the 'Resource Centre for Cyber Forensics - India'. The top navigation bar includes links for 'Web', 'site', 'Home', 'About C-DAC', and 'Research'. The main content area has a heading 'Online EMailTracer' and a sub-section 'Paste Email Header here'. Below this, a large block of email header text is displayed, starting with 'Delivered-To: rohasnagpal@gmail.com'. At the bottom of the page are buttons for 'Start Tracing', 'EMail Crimes', and 'How to extract EMail Header?'. On the left side, there is a sidebar with sections for 'Members Area', 'Navigation' (Incident Reporting, E-MailTracer, Forums, Procedure, Mail to Expert, White Papers), 'Featured' (Press Release, Laws and Rules, FAQ, Contact Us), and a logo for 'CyberCheck Suite Cyber forensics Tools'.

```
Delivered-To: rohasnagpal@gmail.com
Received: by 10.141.5.15 with SMTP id h15cs263386rvi;
Tue, 9 Dec 2008 20:35:55 -0800 (PST)
Received: by 10.110.41.17 with SMTP id o17mr1293983tio.1.1228883754389;
Tue, 09 Dec 2008 20:35:54 -0800 (PST)
Return-Path: <kjacquelyn_nn@uswest.net>
Received: from cfozk ([189.123.183.119])
by mx.google.com with ESMTP id b4si2095590tic.2.2008.12.09.20.35.50;
Tue, 09 Dec 2008 20:35:54 -0800 (PST)
Received-SPF: neutral (google.com: 189.123.183.119 is neither permitted nor denied
record for domain of kjacquelyn_nn@uswest.net) client-ip=189.123.183.119;
Authentication-Results: mx.google.com; spf=neutral (google.com: 189.123.183.119 is
permitted nor denied by best guess record for domain of kjacquelyn_nn@uswest.net)
smtp.mail=kjacquelyn_nn@uswest.net
To: <rohasnagpal@gmail.com>
Subject: NO Degree NO Job?? Buy a Genuine College Degree at cheap price & deliver
weeks, No study needed jne 40r
Date: Tue, 09 Dec 2008 21:00:43 -0700
In-Reply-To: <86a301c95549$0f876ec0$5dae2262@kg9nmr3>
X-Sender: <kjacquelyn_nn@uswest.net>
Reply-To: "Kim Jacquelyn" <kjacquelyn_nn@uswest.net>
```

The header of the email to be traced must be pasted in the relevant area as illustrated above. Then click on “**Start Tracking**”.

The report generated by this tool is illustrated below:

Details extracted from Mail Header

The mail appears to be originated from the computer with IP address
189.123.183.119

The contact information of the ISP for the above IP address is,

whois-contact@lacnic.net

Montevideo

URUGUAY

The sender's email address is kjacquelynn_nn@uswest.net

The message-id of the mail is <1228881643.7851@uswest.net>.

Received By	Received From	Date
rohasnagpal@gmail.com	[10.141.5.15]	--
[10.141.5.15]	--	Tue, 9 Dec 2008 20:35:55 -0800 (PST)
--	mx.google.com	Tue, 09 Dec 2008 20:35:54 -0800 (PST)
mx.google.com	cfozk [189.123.183.119]	Tue, 09 Dec 2008 20:35:54 -0800 (PST)
cfozk [189.123.183.119]	kjacquelynn_nn@uswest.net	Tue, 09 Dec 2008 21:00:43 -0700

Domain / Registrant	IP	Registry	Country	City / Address	ISP
	10.141.5.15	**	**	**	**
cfozk / Latin American and Caribbean IP address Regional Registry	189.123.183.119 / Latin American and Caribbean IP address Regional Registry	ARIN	URUGUAY	Montevideo	Latin American and Caribbean IP address Regional Registry

** Private IP address

189.123.183.119/Latin American and Caribbean IP address Regional Registry

OrgName: Latin American and Caribbean IP address Regional Registry

OrgID: LACNIC

Address: Rambla Republica de Mexico 6125

City: Montevideo

StateProv:
PostalCode: 11400
Country: UY

ReferralServer: whois://whois.lacnic.net

NetRange: 189.0.0.0 - 189.255.255.255

CIDR: 189.0.0.0/8

NetName: NET189

NetHandle: NET-189-0-0-0-1

Parent:

LACNIC

NetType: Allocated to

NameServer: NS.LACNIC.NET
NS2.DNS.BR

NameServer:

NameServer: NS3.AFRINIC.NET
SEC3.APNIC.NET

NameServer:

NameServer: TINNIE.ARIN.NET
SEC.RIPE.NET

NameServer: NS-

Comment: This IP address range is under LACNIC responsibility for
further

Comment: allocations to users in LACNIC region.

Comment: Please see <http://www.lacnic.net/> for further details, or check
the

Comment: WHOIS server located at <http://whois.lacnic.net>

RegDate: 2005-06-17 Updated: 2007-12-17

OrgTechHandle: LACNIC-ARIN

OrgTechName: LACNIC Whois Info OrgTechPhone:

OrgTechEmail: whois-contact@lacnic.net

ARIN WHOIS database, last updated 2008-12-13 19:10

Enter ? for additional hints on searching ARIN's WHOIS database.

Another tool for online email header analysis is available at:

<http://whatismyipaddress.com/staticpages/index.php/trace-email-source-IP-address>

The screenshot shows a web-based tool for tracing email sources. At the top, there's a text input field labeled "Headers:" containing an email header. Below the input field is a large text area displaying the parsed header information. At the bottom of the page, there's a button labeled "Get Source".

Headers:

```
by mx.google.com with ESMTP id b4si2095590tic.2.2008.12.09.20.35.50;
Tue, 09 Dec 2008 20:35:54 -0800 (PST)
Received-SPF: neutral (google.com: 189.123.183.119 is neither permitted nor denied by best guess record for domain of kjacquelynn_nn@uswest.net) client-ip=189.123.183.119;
Authentication-Results: mx.google.com; spf=neutral (google.com: 189.123.183.119 is neither permitted nor denied by best guess record for domain of kjacquelynn_nn@uswest.net) smtp.mail=kjacquelynn_nn@uswest.net
To: <rohasnagpal@gmail.com>
Subject: NO Degree NO Job?? Buy a Genuine College Degree at cheap price &
deliver to you in 2 weeks, No study needed jne 40r
Date: Tue, 09 Dec 2008 21:00:43 -0700
In-Reply-To: <86a301c95549$0f876ec0$5dae2262@kg9nmr3>
X-Sender: <kjacquelynn_nn@uswest.net>
Reply-To: "Kim Jacquelyn" <kjacquelynn_nn@uswest.net>
Message-ID: <1228881643.7851@uswest.net>
From: "Kim Jacquelyn" <kjacquelynn_nn@uswest.net>
Content-Type: text/plain;
charset="iso-8859-2"
Content-Transfer-Encoding: 8bit
```

The header of the email to be traced must be pasted in the relevant area as illustrated above. Then click on “**Get Source**”.

The report generated by this tool is illustrated below:

Source

The source host name is "bd7bb777.virtua.com.br" and the source IP address is 189.123.183.119.

Geo-Location Information

Country	Brazil
State/Region	18
City	Curitiba
Postal Code	
Latitude	-25.4167
Longitude	-49.25
Area Code	

Whois:

The IP address 189.123.183.119 appears to have been assigned by the Latin American and Caribbean IP address Regional Registry (LACNIC). LACNIC is the Regional Internet Registry (RIR) for Latin America and some Caribbean Islands.

For details, see the additional information about IP address 189.123.183.119 at LACNIC.

6. Tracking email accounts

Note: It is advised that you obtain a free account at <http://www.ReadNotify.com> before proceeding with this section. This would enable you to try out the various options mentioned here. Please enter **data64** as the “promotion code” while signing up for the account.

Disclaimer:

Although ASCL experts have successfully used ReadNotify.com for several cyber crime investigations; Asian School of Cyber Laws does not in any way suggest that the reports generated by ReadNotify.com are 100% authentic and reliable.

You are requested to exercise due caution while relying upon the reports generated by ReadNotify.com.

All information pertaining to ReadNotify.com in this book has been obtained from ReadNotify.com and Asian School of Cyber Laws is not liable for any errors or omissions contained therein.

ReadNotify is a powerful and reliable email tracking service. It tracks an email as to when it was read / re-opened / forwarded and much more. In cases where only an email ID is obtained as a clue to track the sender of an email, services like ReadNotify.com can prove very helpful.

Sending tracked emails via ReadNotify is very easy. You simply have to add ‘readnotify.com’ to the end of your recipients email address (they won’t see this) - or install one of their ‘Active Tracker plug-ins’ to add the tracking.

The email is then directed to pass through their server, where it assigns it a tracking code, and sends it on to the recipient. When your recipient opens the email, the assigned tracking code sends their server a message, which allows them to report the details (such as the IP address of the computer where the email was read) to you.

The following basic features are available using ReadNotify:

With current defaults

This will activate the settings you have chosen as your defaults. (This will be ‘Invisible’ tracking unless you have changed this since initial registration).

Invisible

Your recipient will not be aware from your email that you are tracking it. Sending emails this way can decrease the reliability of getting return receipts - but this is rare. Invisible tracking cannot be used in conjunction with any other special tracking feature.

Certified + Notarised

This option will digitally sign your email and insert a timestamp certificate. This certificate links the body and headers of an email to the date and time they were dispatched.

Ensured / Retractable

Ensured emails are stored on the ReadNotify server until accessed by the recipient - so they cannot be opened without guaranteeing a return receipt.

The body of emails sent using their Ensured feature, may also be retracted by the sender prior to them being opened by the recipient. This 'retract' option is available in the 'Personal Tracking Page'.

Self-Destructing/Retractable

Emails sent with this feature must be accessed via a link and will automatically get destroyed in the time selected by the sender. The email will also self-destruct immediately if the recipient tries to copy, print or forward it.

Sending emails using the Self-Destruct feature allows you to retract the body of your email prior to it being opened by your recipient. This 'retract' option is available from the "Personal Tracking Page".

Block print & copy

You are able to block the recipients from printing or copying your emails. Keep in mind that this does not guarantee that your recipients will not be able to retain a copy using another format - for example, they could photograph the screen!

The following advanced tracking features are available using ReadNotify:

The default ReadNotify settings work the best in most situations. If you are unsatisfied with the tracking results, you can alter some settings.

(These are available to from "My Account" under Member Utilities when you log in.)

Encoded in base64

Improves the tracking reliability for emails sent to recipients using very old email clients.

HTML format only

Increases the reliability of receiving tracking reports on emails sent to recipients who accept Text-Only emails. This can, however, decrease the reliability of accurately tracking any "forwards" [Note: This tracking technique must be activated if you wish to track certified emails]

Insert tracking code into text

This technique works by inserting tracking code into the text portion of your sent email, which increases the reliability of tracking whether or not your email was forwarded. It may also increase the chance that your recipient will know you are tracking the email.

Include secure tracking code

Some recipients open their emails through a secure connection. By including secure tracking code into your sent email, your read-notifications will be more accurate. This may cause a generic warning message to appear if the recipient is not on a secure connection.

Advanced tracking - include "frames"

Frames provide additional tracking which increases the reliability of receiving accurate read-notifications. Please note that some email filters give your recipients the option of blocking frames.

Global Identifiers

This option uses "global identifiers" to improve the ability of identifying the computer on which your email was opened

Style tracking

This includes additional tracking that may improve the reliability of your Notifications.

Embed tracking

This includes additional tracking that may improve the reliability of your Notifications.

Script tracking

This includes additional tracking that may improve the reliability of your Notifications.

The ReadNotify tracking reports

You may choose to receive your tracking reports via email (called ReadNotifications) as well as in your Personal Tracking Page. These are sent upon initial opening - so if you wish to check on any up-to-date tracking, you will need to log in and visit your Personal Tracking Page. (As long as your Sent emails are still listed - then it is still tracking them.)

Your ReadNotifications / Tracking Records may include the following information regarding the tracked emails you send:

Date and time opened

This is the date and time when the recipient first opens your email, and is reported back to you in your own time zone.

Location

This is the location of your recipient's ISP - which is usually in the same city as your recipient. It will also give a percentage of accuracy regarding this.

Map

A map regarding original opening location is included in your ReadNotifications and Tracking Records. If your recipient lives in a remote location for which their map service does not exist for, then just the place name will be reported.

Recipients IP address

Your recipients IP address will be reported on all openings and forwards. An 'IP' address is a number allocated by your recipients Internet Service Provider for their connection to the Internet.

Recipients email address

If it can, it will let you know the email addresses of the people to whom your message was forwarded. This is only an **apparent** address as determined from the details on your recipient's computer - and may not necessarily be correct (especially if more than one person uses - or has used the computer your email is opened on).

Referrer

If your recipient opened your email via a third party source (e.g.; Hotmail)

Track URL's

If you include any URL's in your emails, it can track whether or not your recipient 'clicked' on them. The option to track URL clicks is available from "My Account" under Member Utilities when you log in.

Track how long an email is opened for

It shall endeavour to let you know how long your email was opened for. Sometimes though, this information is not available to them. Some reasons for this could be that your recipient either opened, or closed your email off-line; or that your email was only opened for a very short time (e.g.; a few seconds) - not long enough for ReadNotify to record the 'length of time reading'.

Track how many times your email was opened

It will let you know if your email was opened more than once.

Track forwards

Your Tracking Records (from your Personal Tracking Page) will let you know if, and when your email was forwarded.

It counts 'forwarded' emails as those opened on a different computer than the original recipient.

Note: If your recipient 'replies' to your tracked email (i.e. sends your email back to you with their reply) then you may be recorded as the recipient of the 'forwarded' email.

Step by step guide to using Readnotify

To sign up for a ReadNotify account, visit www.readnotify.com. Please enter **data64** as the “promotion code” while signing up for the account.

Ensure that you select the “Time Zone” accurately e.g. for India it is suggested to select the *Asia / Calcutta* option.

ReadNotify.com - Free trial signup.

• Please complete all the boxes to register. ○ Free trials last for two weeks or 25 emails (whichever comes first).
• Don't forget to read our [terms](#) first. ○ Remember to enter your real email address or you won't be able to send mail or receive confirmations.

Your Main Email Address:
(You can add additional email addresses later if you wish)

First Name:
Last Name:
Password:
Confirm Password:
Country: 
Language: 
Time Zone: 

Once you create your account, the following page will open up. You can set up your default settings from here. The recommended settings are illustrated in the next few pages:

Re@adNotify  **Default Settings**

 **ReadNotify.com - Default Settings** 

Choose your Default Settings

Click either of the buttons below to configure your account to use ReadNotify suggested default tracking settings. Choosing from either of these options will restore your advanced tracking techniques also.

Recommended Tracking Defaults **Invisible Tracking Defaults**

We also offer some overrides to our recommended or invisible tracking settings which you can change manually if desired:

Use traditional Message Disposition Notifications: MDN's (recommended)

Highly Recommended - this option improves tracking reliability, and can sometimes let you know when your email was deleted without being read.
MDN's are usually invisible to WebMail users (such as Yahoo and Hotmail etc) but non-webmail users may be asked to confirm reading the email you sent (by their own email program - not by ReadNotify).
MDN's do **not** mention you are tracking the email.
MDN's are sometimes ambiguously referred to as "Return Receipts", and are available in most email clients and automatically enabled (without prompting the recipient) by many business users.

Choose an optional banner to include in your outgoing email:

- Select this option if you do not wish to include any banner on your emails
- ReadNotify.com** This was a receipt-requested email.
Click here to acknowledge reading.
- ReadNotify.com** Click here to acknowledge reading this receipt-requested email.
- ReadNotify.com** ここをクリックしてこのメッセージを受信したことを送信者に確認させてください。
- ReadNotify.com** has confirmed the delivery of this email.
- ReadNotify** このメッセージの送信者はあなたが読んだことの確認を求めています。
これをクリックして確認してください。
- ReadNotify** The sender of this email requested a notification upon opening.
This notification has already been generated and sent to them.
- ReadNotify.com** Click here to confirm to sender that you read this message.
- ReadNotify.com** Click here to confirm to sender that you read this message.

Choose a message to display (shows up if the reader sees unformatted email text, or moves the mouse over the banner)

- The sender of this message requests confirmation when you read it. Click here to confirm.
- Click here to confirm to the sender that you received this message.
- none
- Other: Please specify:

Note: this message goes out with all mail you send using ReadNotify

Insert "X-Read-Notification: Courtesy of ReadNotify.com..." into outgoing email headers

- As a courtesy to your readers, this mentions (in your expanded headers) that you sent the email via our service.

Track URL Clicks

- If the emails you send include any URL's (clickable links to web pages) this option will track whether or not your recipient clicked on them.
- Although not apparent to the majority of your recipients, this feature is not entirely invisible. You must activate or de-activate URL tracking from here (ie; it is not affected by the Tracking Defaults' buttons above).

Stay logged on

- Select this if you do not want our web site to "log you out". This will save you from having to type your password every time you visit our web site.
- Do not use this option if you share your computer with other people.

Track Attached PDF Documents



- Check this box to automatically add tracking to your PDF files. You must activate or de-activate PDF tracking from here (ie; it is not affected by the Tracking Defaults' buttons above).
- You can read more about Document Tracking [here](#).

- Check this box if you would like us to send you a reminder about PDF Document Tracking the next time you send a trackable document (recommended).



Track Attached MS Word Documents

- Check the above box to automatically add tracking to your MS Word documents.

Check this box if you would like us to send you a reminder about MS Word Tracking the next time you send a trackable document (recommended).



Track Attached MS Excel Documents

- Check the above box to automatically add tracking to your MS Excel documents.

Check this box if you would like us to send you a reminder about MS Excel Tracking the next time you send a trackable document (recommended).



Track Attached MS PowerPoint Presentations and Shows

- Check the above box to automatically add tracking to your MS PowerPoint Presentations and Shows.

Check this box if you would like us to send you a reminder about MS PowerPoint Tracking the next time you send a trackable document (recommended).

Save Changes

After selecting the options as illustrated above, click on the “**Save Changes**” option.

Click on the Member Utilities→Configuration Wizard to configure your readnotify account.

The screenshot shows a dropdown menu titled "Member Utilities" with the following options:

- ✓ Sign-In
- Log Out
- Personal Tracking Page
- Subscribe (pay)
- Configuration Wizard** (highlighted with a blue border)
- My Account

A tooltip for the "Configuration Wizard" option states: "This wizard leads you step by step through some of the popular tracking options you can choose from".

At the bottom of the menu, there are three links: "about Re@dNotify", "business solutions", and "member utilities".

The recommended settings are illustrated in the next few pages:



ReadNotify Configuration Wizard

Message Dispositions

Do you want to prompt your recipient to send you a manual return-receipt when they read your email?

Yes - prompt them
 No - don't prompt

configuration Message Dispositions

ReadNotify Configuration Wizard

Certified Email

Do you want to certify your emails (attaches published proof-of-posting certificates to them, and sends you posting receipts)

Yes - use certified emails and send me proof-of-posting certificates
 No - not certified.

configuration Certified Email

Re@Notify Configuration Wizard

← Previous **Next →**

Proof of opening

Do you want digitally signed read-notifications? (verifiable, irrefutable evidence your email was opened)

Yes please
 No thanks

configuration Proof of opening

Re@Notify Configuration Wizard

← Previous **Next →**

Track Clickthroughs

Do you want to know if they clicked on URLs you emailed to them?

Yes please
 No thanks

configuration Track Clickthroughs

Re@Notify Configuration Wizard

← Previous **Next →**

Use power tracking

Power tracking is recommended. Disable this if you get email sending problems, or a recipient who alleges they cannot read your tracked emails

Enabled (recommended)
 Disabled

configuration Use power tracking

ReadNotify Configuration Wizard

← Previous **Next →**

Self-Destructing

Do you want your email to delete itself after it gets read, and to inhibit printing/saving/forwarding etc.

Yes - I want all my emails to self-destruct
 No.

(note: you can always send individual self-destructing emails by adding _selfdestructing.readnotify.com on the end of your recipient email address)

configuration Self-Destructing

ReadNotify Configuration Wizard

← Previous **Next →**

Ensured-Receipt

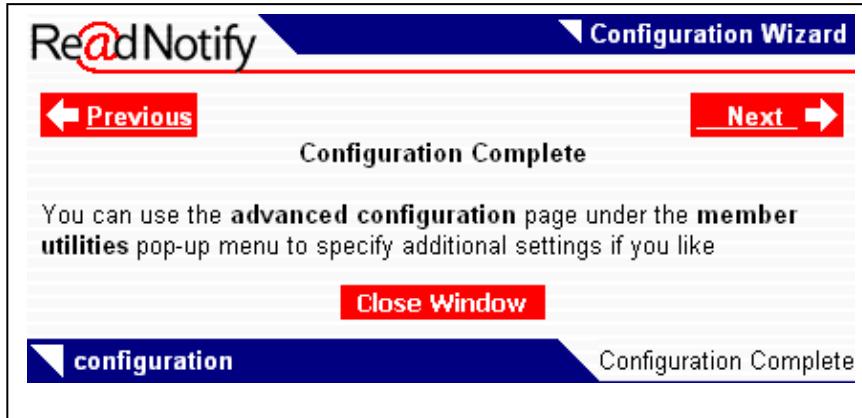
Do you want to block your readers from accessing your email until a successful read-notification can be sent to you?

Yes, use ensured-receipt
 No, just send ordinary emails

(Note: this stores a copy of your email on the ReadNotify ensured-receipt server.)

configuration Ensured-Receipt

After making the recommended settings as illustrated above, click on the “Close Window” button as illustrated below:



Now click on Member Utilities→Email Quick Send to send out a tracking email.



The screen illustrated below will open up. Create the tracking email as illustrated below.

Notice that although the receiver's email ID is rohasnagpal@gmail.com, it is entered as rohasnagpal@gmail.com.readnotify.com

The *.readnotify.com* part has to be entered at the end of the recipient's email address so that the email can go through the readnotify servers and be properly tracked.

Re@adNotify

ReadNotify Tracked-Email Quick-Send Form.
You can send ReadNotify email directly from here, OR, you can use your [normal](#) email program.

From: Samairah Nagpal <samairahnagpal@yahoo.in> [▼](#)

To: rohasnagpal@gmail.com.readnotify.com

Subject: Hello

CC: BCC:

Send Options: (You may select as many send options as you like for this email.)
 Send certified email Send self-destructing email Use ensured-receipt
 Send a copy of this email to my own mail Inbox.

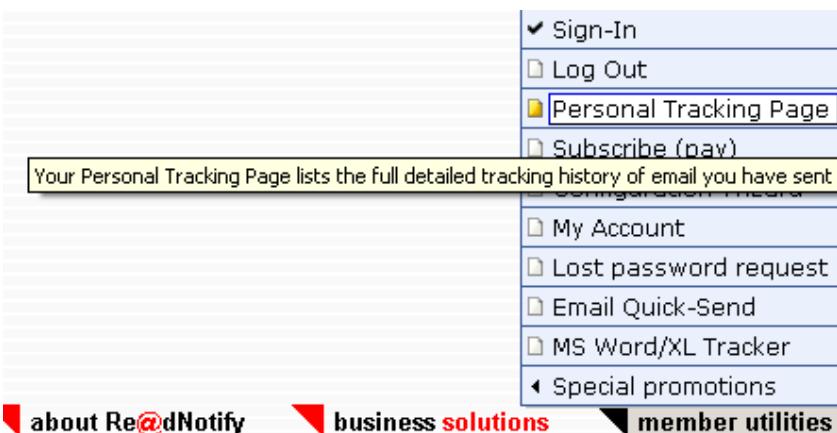
Hello,

How are you?

Samairah|

Send

Once you have sent the email, go to Member Utilities→Personal Tracking Page to track the email.



Once the recipient clicks on the email sent by you, your personal tracking page will show a date and time as illustrated below:

The screenshot shows the "Personal Tracking Page" of ReadNotify. At the top, there is a header bar with the "Re@dNotify" logo, a "Refresh Display" button, and a "Personal Tracking Page" link. Below the header, there is a section titled "Emails that you have sent using ReadNotify". This section contains a table with four columns: "Date", "Recipient", "Subject", and "Opened?". There is one row in the table with the following data: Date: 23-Nov, Recipient: rohsnagpal@gmail.com, Subject: Hello, and Opened?: 23-Nov-08 20:14:08. To the left of the table, there are two buttons: "Delete Selected" and "Select all". To the right of the table, there is a note: "All times converted to "Asia/Calcutta" time." Above the table, there is a small box containing account information: account: samairahnagpal@yahoo.in, limit: 25, used: 1, expiry: 08-Dec-08, and a "My Acct" link.

Date	Recipient	Subject	Opened?
23-Nov	rohsnagpal@gmail.com	Hello	23-Nov-08 20:14:08

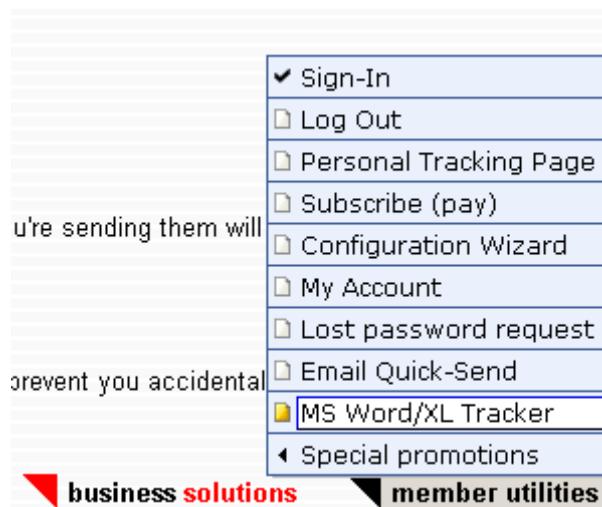
Clicking on the date and time link in the screen illustrated above will open up a screen similar to the one illustrated below:

ReadNotify Refresh Display Close Window

To rohanagnpal@gmail.com	
From samairahagnpal@yahoo.in	
Subject Hello	
Sent on 23-Nov-08 at 20:09:35pm 'Asia/Calcutta' time	
1st Open 23-Nov-08 at 20:09:37pm +05:30	
Tracking Details	
Opened	
Opened 23-Nov-08 at 20:09:37pm (UTC +05:30) - 2secs after sending	
Location Mumbai, Maharashtra, India (86% likelihood)	
Opened on ABTS-mum-Dynamic-034.19.170.122.airtelbroadband.in (12.170.19.34:1998)	
Language of recipient's PC: en-us (English/United States), en;q=0.5 (English)	
Browser used by recipient: Moz5.0 (Win; U; Windows NT 5.1; en-US; rv:1.9.0.4) Gecko/2008102920 Firefox/3.0.4	
Accepts files browser can open: if/png,*;q=0.8,*;q=0.5	
Referrer http://mail.google.com/mail/?ui=2&view=bsp&ver=1qygcgurkoy	
Last log No more activity after 23-Nov-08 at 20:14:08pm (UTC +05:30) - Log data indicates email was read for at least 4mins31secs (approx.)	
Summary - as at 23-Nov-08 at 20:17:35pm (UTC +05:30) - 8mins after sending	
Total Opened 1 time by 1 reader	

This screen shows us that the email was opened on 23-Nov-2008 at 20:09:37 Indian standard Time on a computer having the IP address 12.170.19.34 (this is a fictitious IP address shown only as an example. In a real life scenario it will display the actual IP address of the recipient.)

To use the Microsoft® Word ® tracker, click on Member Utilities→MS Word/XL Tracker as illustrated below:



In the screen that open up, enter the document subject, recipient email address and document type as illustrated below.

ReadNotify  Document Tracking Service

 MS Word  MS Excel  MS PowerPoint Other OLE documents To track PDF

Follow these steps to create a tracked document:

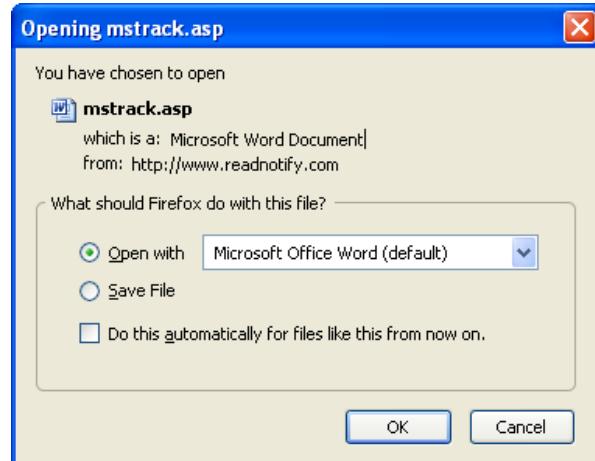
- 1. Subject** - Enter a subject or short sentence to identify this document (if you are also trac
Test Document for tracking
- 2. To: Email** - Enter the email address of your recipient
noodle.bank@yahoo.in
- 3. Document Type** - What kind of document do you want to track?
 Microsoft Word Document
 Microsoft XL Spreadsheet
 Microsoft PowerPoint presentation
 Other document supporting OLE
[Adobe PDF](#)
- 4. Add tracking to your document** - Click the "Track it" button below; then follow the instruc
to the minimum size gives optimal tracking results)

Track It!

Then: **Save** your document ... & **Give** it to the recipient.
(e.g. **send** it by email, put it on a **disc**, copy it onto your **server**, FTP it, etc)

Then click on the “**Track It**” button.

A screen as illustrated below will automatically open up:



Click on “Open with” and then click “OK”. The following Microsoft® Word® document will open up:

Microsoft Word Document tracking

Instructions: Here is your Microsoft Word document tracker. Drag the indicated transparent tracking graphic below, and drop it into your Word document that you want to track. For best results, place it somewhere that is visible when the document is first opened.

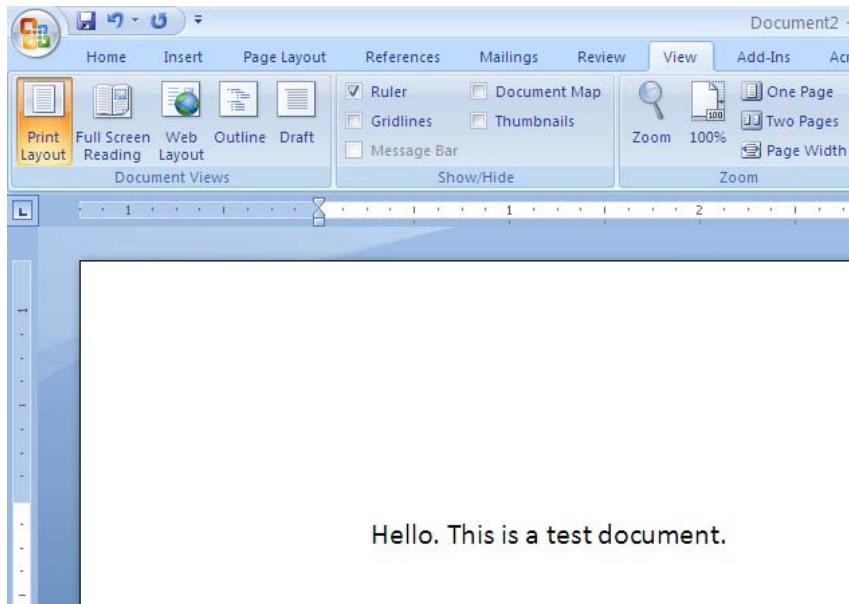
Drag & Drop graphic =>  <= Drag & Drop graphic

You can resize the tracking graphic if you wish. Note: tracking will commence only when your document is opened on a different computer, or, in one hours time; whichever comes first.

Note: The tracking graphic will turn invisible (transparent) when you drop it into your document.

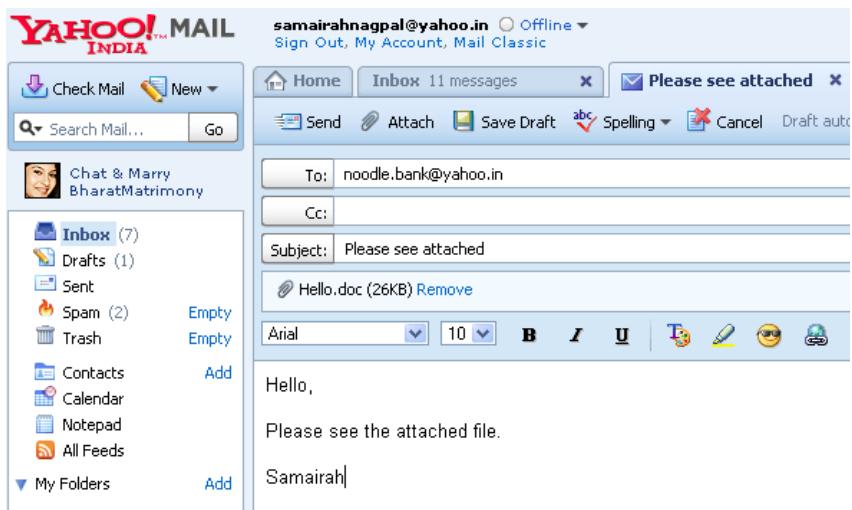
Open a new Microsoft® Word® document and write some message in it e.g. "Hello. This is a test document."

Then select the arrow image in the screen above and drag and drop it in the newly created Microsoft® Word® document. The arrow will become invisible. The newly created Microsoft® Word® document will look as illustrated below.



Although the tracking image has been embedded into the above newly created Microsoft® Word® document, the image will not be visible.

Now simply email the newly created Microsoft® Word® document as an attachment to the recipient as illustrated below:



Once you have sent the email, go to Member Utilities→Personal Tracking Page to track the email.

- Sign-In
- Log Out
- Personal Tracking Page
- Subscribe (nav)
- My Account
- Lost password request
- Email Quick-Send
- MS Word/XL Tracker
- Special promotions

Your Personal Tracking Page lists the full detailed tracking history of email you have sent

about Re@dNotify **business solutions** **member utilities**

Once the recipient clicks on the email sent by you, your personal tracking page will show a date and time as illustrated below:

ReadNotify email tracking history	
To	needle.bank@yahoo.in
From	samarahnaqbal@yahoo.in
Subject	Test Document for tracking
Sent on	23-Nov-08 at 20:49:39pm 'Asia/Calcutta' time
1st Open	23-Nov-08 at 20:51:50pm +05:30
Tracking Details	
Opened	
Doc Opened	23-Nov-08 at 20:51:50pm (UTC +05:30) - 2mins11secs after sending
Location	Mumbai, Maharashtra, India (86% likelihood)
Opened on	ABTS-mum-Dynamic-034.19.170.1.22.airtelbroadband.in (12.170.19.34:2339)
Doc Opened	Tracked document opened at 23-Nov-08 at 20:51:50pm (UTC +05:30), 23-Nov-08 at 20:52:14pm (UTC +05:30), 23-Nov-08 at 20:52:27pm (UTC +05:30)
Browser used by recipient:	Moz4.0 (MSIE 7.0; WinNT 5.1; MSOffice 12)
Last log	No more activity after 23-Nov-08 at 20:52:27pm (UTC +05:30) - Log data indicates email was read for at least 37secs (approx.)
Re-Opened	
Opened	24-Nov-08 at 10:51:45am (UTC +05:30) - 14hours2mins6secs after sending
Location	Mumbai, Maharashtra, India (86% likelihood)
Opened on	ABTS-mum-dynamic-224.87.169.122.airtelbroadband.in (12.169.87.224:1088)
Doc Opened	Tracked document opened at 24-Nov-08 at 10:51:46am (UTC +05:30)
Browser used by recipient:	Moz4.0 (MSIE 7.0; WinNT 5.1; MSOffice 12)
Re-Opened	
Opened	24-Nov-08 at 12:47:24pm (UTC +05:30) - 15hours57mins45secs after sending
Location	Mumbai, Maharashtra, India (86% likelihood)
Opened on	ABTS-mum-dynamic-224.87.169.122.airtelbroadband.in (12.169.87.224:1678)
Doc Opened	Tracked document opened at 24-Nov-08 at 12:47:25pm (UTC +05:30)
Browser used by recipient:	Moz4.0 (MSIE 7.0; WinNT 5.1; MSOffice 12)
Summary	- as at 24-Nov-08 at 13:14:10pm (UTC +05:30) - 16hours24mins31secs after sending
Total	Opened 3 times by 1 reader

Details of the various computers on which the document was opened (such as IP address, operating system, version of Microsoft® Office® etc) as well as the date and time are displayed in the screen illustrated above.

7. Case Study

Note: The names of people, Case Numbers, email IDs and IP addresses have been changed in order to protect the privacy of the individuals concerned. All names, case numbers, IP addresses, email IDs are fictitious and any resemblance to any person / organization are purely co- incidental.

1. The Complaint

On 14th April 2007, 22 years old Rashmi Pandya entered the Cyber Crime Cell and lodged a complaint stating that she was receiving obscene and pornographic emails from someone at her email ID, rashmi_is@hotmail.com. She was able to provide the police with only the email ID of the person who was sending these emails. This email ID was badman22@yahoo.com.

She also stated in her complaint that the emails mentioned that this person had seen her at various places in Pune while she had been out with friends and family. After verifying the emails that had been received by Rashmi, the police registered a complaint under Section 67 of the Information Technology Act 2000.

2. The legal provisions

Section 67 of the Information Technology Act, 2000 is as under:

67. Publishing of information which is obscene in electronic form.

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

3. Analysis of the Email Header

The Police, first, analyzed the pornographic emails that Rashmi had been receiving. The header of one such email is reproduced below:

From : Joe Smith <badman22@yahoo.com>
Sent : Saturday, April 12, 2007 11:57:57 AM
To : rashmi_is@hotmail.com
Subject : Come and meet me
MIME-Version: 1.0
Received: from web52101.mail.yahoo.com ([206.190.39.70]) by mc7-f42.hotmail.com with Microsoft SMTPSVC(5.0.2195.6713); Sat, 12 Apr 2007 04:57:58 -0700
Received: from [204.69.234.1] by web52101.mail.yahoo.com via HTTP; Sat, 12 Apr 2007 04:57:57 PDT
X-Message-Info: 6sSXyD95QpV20hZk0u1hNvFQdOeyTq7i
Message-ID: <20071016115757.55743.qmail@web52101.mail.yahoo.com>
Return-Path: badman22@yahoo.com
X-OriginalArrivalTime: 12 Apr 2007 11:57:58.0640 (UTC)
FILETIME=[61328F00:01C4B377]

The police then identified that the email had originated from a computer having the IP address 204.69.234.1. The police conducted a Whois search using the website <http://www.who.is> to ascertain details about this IP address.

The results of the Whois search indicated that the IP address 204.69.234.1 had been allotted to Nile Corporation, a Germany based company. The police then sent the following request (by email as well as by post) to the Chairman of Nile Corporation:

22nd April 2007

To,
Mark Janison,
CTO, Nile Corporation

Subject: IP Address query

Respected Mr. Janison,

This is in respect of case number ITA/2003/CCC/0345 registered with us on 14th April 2007. This case has been filed by Ms. Rashmi Pandya under Section 67 of Information Technology Act, 2000.

The complainant in this case has received several pornographic emails. One such email appears to have originated on Sat, 12 Apr 2007 04:57:57 PDT from a computer having the IP address 204.69.234.1.

Your kind assistance and co-operation is sought in identifying the person who was operating the said computer at the said date and time.

Regards,
Mr. Suraj Khan
Officer-in-charge,
Cyber Crime Cell

Despite several follow-ups, no relevant information was received from Nile Corporation. Investigation into the case came to a complete standstill as nothing could be done without the information sought from Nile Corporation.

At this stage the police sought the assistance of Asian School of Cyber Laws (ASCL). Vikram Jaiswal was the ASCL cyber crime investigator who was deputed to assist the police in investigating this case.

4. Assistance from Asian School of Cyber Laws

Based upon experience of solving similar cases, Vikram was of the opinion that the person responsible for sending the emails was residing in the same city as Rashmi. Vikram was of the view that the emails were being composed by this local person who was then sending the emails to his friend working at Nile Corporation. This friend was then sending the emails to Rashmi.

Vikram decided to focus upon the email address badman22@yahoo.com rather than upon the IP address 204.69.234.1.

Vikram created a free account with ReadNotify.com in the name of “Priety Singh” by using the email ID prietysingh@hotmail.com.

Using the above ReadNotify.com account, Vikram sent an email to badman22@yahoo.com with the subject “Thanks for the lovely evening”. The email is reproduced below:

Hi there...

Remember me? This is just a small note to say thank you for a really great date. I am really looking forward to meeting you again..

Email me! I'm waiting!

Priety



Vikram was of the view that when this email was received by the person(s) operating the email account badman22@yahoo.com, the person(s) would be tempted to click on the email. After all it is very difficult for a man to resist an email from a lady thanking him for “a lovely evening”!

Vikram's plan worked. Within 12 hours, the email had been opened three times, twice from a computer at Nile Corporation and once from a computer at XOTech Software.

When Rashmi was asked if she knew anybody at XOTech Software, she told the police that she had been working at XOTech till a few months ago. She also told the police that Sameer, a senior programmer at XOTech used to harass her a lot as she had refused to go out for dinner with him.

The police immediately planned and executed a search and seizure operation at the premises of XOTech Software.

The first thing that was done during the operation was to examine the computer used by Sameer at XOTech. Using advanced cyber forensic techniques, Vikram was able to ascertain that Sameer's computer had been used to access the email account *badman22@yahoo.com* several times in the recent past!

Despite questioning from the police, Sameer refused to cooperate. He denied that he had anything to do with the email account *badman22@yahoo.com*. Vikram then asked Sameer to make a list of all the email accounts, personal and official, operated by him as well as their passwords.

The list provided by Sameer was as under:

Email ID	Password
1. Sameer@mail.com	xygz+563in
2. Sameer@xotech.com	xygz+563in
3. programguru@rediffmail.com	xygz+563in
4. sam_22@hotmail.com	xygz+563in

Vikram noticed that Sameer had kept the same password for all his email accounts. On a hunch, Vikram tried to access the email account *badman22@yahoo.com* using the password *xygz+563in*

It worked! The password for the email account *badman22@yahoo.com* was *xygz+563in*

Vikram then examined the folders in the *badman22@yahoo.com* email account. The tally of emails in each folder was as under:

Folder	No. of Emails
Inbox -	33
Deleted -	29
Sent -	03
Bulk -	06

In the presence of the witnesses, printouts were taken of all these emails by the police. It was ensured that each printout was taken in such a manner that the detailed header of the email was clearly visible.

The printouts were taken so that even in case the emails were deleted, the evidence would not be destroyed. The next day, the police began to trace the IP addresses of all the emails that they had recovered.

After days of investigation, the police traced one email to a certain Pallavi Jain from Mumbai, India. The email pertained to some technical books that Pallavi had sought to buy from Sameer.

When Pallavi was shown a photograph of Sameer, she immediately recognized him. She said that she had seen an advertisement put up by Sameer at an online auction website. Pursuant to the advertisement she had sent an email to *badman22@yahoo.com* to the effect that she was interested in purchasing the books advertised for sale by Sameer.

Pallavi also said that subsequent to the email exchange, she had met Sameer in Mumbai and they had carried out the transaction relating to the books. Once Pallavi's statement was taken by the police the evidence was complete and Sameer was arrested. The case is now under trial.

The chain of evidence that was collected by the police with the assistance of ASCL expert Vikram was as under:

- (1) The result of the ReadNotify email that showed that the *badman22@yahoo.com* email account was accessed from a computer at XOTech Software.
- (2) The cyber forensic examination that showed that the *badman22@yahoo.com* email account had been operated from Sameer's official computer several times.
- (3) The statement by Pallavi that she had communicated with Sameer using the *badman22@yahoo.com* email account.

9. Investigating server logs

1. FTP server logs

Let us take the illustration of an FTP Server running on port 21 of a computer having the IP address 10.10.10.111. The following are extracts from logs generated by this FTP Server. The FTP Server logs explained in this section are in standard format. The format of these logs can be different for some FTP servers. A list of raw FTP commands and FTP Status and Error Codes are provided in the annexure to this book.

1.1 Connecting to a closed FTP server

Following is an extract of the log when someone (from IP address 10.10.10.222) attempts to access an FTP Server which is closed to connections. This means that although the FTP server is online, it is not accepting connections from users e.g. the administrator may be carrying out some changes and does not want users to connect at this time.

```
11/14/2008 7:20:46 AM - FTP Server On-line : IP(s) 10.10.10.111, on port 21
11/14/2008 7:21:12 AM - (not logged in) (10.10.10.222) > connected to ip :
10.10.10.111
11/14/2008 7:21:12 AM - (not logged in) (10.10.10.222) > 421 Server is
closed, no more connections are allowed.
11/14/2008 7:21:12 AM - (not logged in) (10.10.10.222) > connection failed :
No more connections allowed, server is closed.
11/14/2008 7:21:12 AM - (not logged in) (10.10.10.198) > disconnected.
```

Let us examine the above extract in detail.

11/14/2008 7:20:46 AM - FTP Server On-line : IP(s) 10.10.10.111, on port 21

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:20:46 AM	This is the time
FTP Server On-line	This indicates that the FTP Server is online
IP(s) 10.10.10.111,	This indicates the IP address of the FTP server i.e. 10.10.10.111
on port 21	This indicates that the server is running on port number 21

11/14/2008 7:21:12 AM - (not logged in) (10.10.10.222) > connected to ip : 10.10.10.111

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:21:12 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
connected to ip :	This indicates the IP address of the FTP server i.e. 10.10.10.111

11/14/2008 7:21:12 AM - (not logged in) (10.10.10.222) > 421 Server is closed, no more connections are allowed.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:21:12 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
421 Server is closed, no more connections are allowed.	This indicates that the server is closed and is not accepting connections. The “421” error code is used in the following cases: (1) Service not available, closing control connection. (2) User limit reached (3) You are not authorized to make the connection (4) Max connections reached (5) Max connections exceeded

11/14/2008 7:21:12 AM - (not logged in) (10.10.10.222) > connection failed : No more connections allowed, server is closed.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:21:12 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
connection failed : No more connections allowed, server is closed.	This indicates that the server is closed and is not accepting connections.

1.2 FTP server is started up

Following is the log entry generated when the FTP Server is started up.

11/14/2008 7:21:56 AM - FTP Server opened to new connections.

Let us examine the above extract in detail.

<i>Field</i>	<i>Explanation</i>
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:21:56 AM	This is the time
FTP Server opened to new connections	This indicates that the FTP Server is now open to accepting new connections.

1.3 Password cracking attempt

Following is a small extract from the log documenting a password cracking attempt. Two unsuccessful attempts are displayed in the log. Such log entries are usually generated under the following circumstances: (1) A malicious hacker is attempting to obtain the password by using a brute force or dictionary attack (e.g. using Brutus) (2) A genuine user, who has forgotten his password, is attempting to guess his password by trying out some possible passwords.

```
11/14/2008 7:40:27 AM - (not logged in) (10.10.10.222) > connected to ip : 10.10.10.111
11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > sending welcome message.
11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > 220 Welcome to Noodle Bank FTP
Server
11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > USER noodle-admin
11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > 331 Password required for noodle-
admin.
11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > PASS *****
11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > 530 Login or Password incorrect.
11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > disconnected.
(000009) 11/14/2008 7:40:30 AM - (not logged in) (10.10.10. 222) > connected to ip : 10.10.10.198
(000009) 11/14/2008 7:40:30 AM - (not logged in) (10.10.10. 222) > sending welcome message.
(000009) 11/14/2008 7:40:30 AM - (not logged in) (10.10.10. 222) > 220 Welcome to Noodle
Bank FTP Server
(000009) 11/14/2008 7:40:30 AM - (not logged in) (10.10.10. 222) > USER noodle-admin
(000009) 11/14/2008 7:40:30 AM - (not logged in) (10.10.10. 222) > 331 Password required for
noodle-admin.
(000009) 11/14/2008 7:40:30 AM - (not logged in) (10.10.10. 222) > PASS *****
(000009) 11/14/2008 7:40:30 AM - (not logged in) (10.10.10.198) > 530 Login or Password
incorrect.
(000009) 11/14/2008 7:40:30 AM - (not logged in) (10.10.10. 222) > disconnected.
```

The above extract displays two unsuccessful attempts. The following extract shows the log entries for one unsuccessful attempt:

11/14/2008 7:40:27 AM - (not logged in) (10.10.10.222) > connected to ip : 10.10.10.111
11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > sending welcome message.
11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > 220 Welcome to Noodle Bank FTP Server
11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > USER noodle-admin
11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > 331 Password required for noodle-admin.
11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > PASS *****
11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > 530 Login or Password incorrect.
11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > disconnected.

Let us examine the above extract in detail.

11/14/2008 7:40:27 AM - (not logged in) (10.10.10.222) > connected to ip : 10.10.10.111

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:40:27 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
connected to ip :	This indicates that the user is making a connection with the IP address 10.10.10.111

11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > sending welcome message.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:40:27 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
sending welcome message.	This indicates that the FTP server is sending a welcome message. This does not indicate that the user has been successful in logging in.

11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > 220 Welcome to Noodle Bank FTP Server

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:40:27 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
220	Service ready for new user.
Welcome to Noodle Bank FTP Server	This is the customized welcome message sent by this FTP server. This does not indicate that the user has been successful in logging in.

11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > USER noodle-admin

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:40:27 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
USER noodle-admin	This indicates that the username “noodle-admin” has been sent by the client

11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > 331 Password required for noodle-admin.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:40:27 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
331	This signifies that the user name is correct and that a password is needed. However, this status code is usually seen even if the username is invalid.
Password required for noodle-admin.	The FTP server requires a password for the username “noodle-admin”

11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > PASS *****

<i>Field</i>	<i>Explanation</i>
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:40:27 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
PASS *****	This indicates that a password has been sent by the client. The actual password is not logged in this case (this depends upon the settings on the particular FTP server).

11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > 530 Login or Password incorrect.

<i>Field</i>	<i>Explanation</i>
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:40:27 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
530	This error code means that the user is not logged in. This usually occurs when the correct user name and password combination has not been entered.
Login or Password incorrect.	This indicates that either the username, or password or both are incorrect.

11/14/2008 7:40:27 AM - (not logged in) (10.10.10. 222) > disconnected.

<i>Field</i>	<i>Explanation</i>
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:40:27 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
disconnected.	The user has been disconnected.

1.4 Logging onto an FTP Server

Following is a small extract from the log documenting a successful attempt to log into the FTP Server. The user having username “noodle-admin” is logging into the FTP Server from a computer having the IP address 10.10.10.222

```
11/14/2008 7:22:00 AM - (not logged in) (10.10.10.222) > connected to ip :  
10.10.10.111  
11/14/2008 7:22:00 AM - (not logged in) (10.10.10.222) > sending  
welcome message.  
11/14/2008 7:22:00 AM - (not logged in) (10.10.10.222) > 220 Welcome to  
Noodle Bank FTP Server  
11/14/2008 7:22:00 AM - (not logged in) (10.10.10.222) > USER noodle-  
admin  
11/14/2008 7:22:00 AM - (not logged in) (10.10.10.222) > 331 Password  
required for noodle-admin.  
11/14/2008 7:22:00 AM - (not logged in) (10.10.10.222) > PASS *****  
11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > logged in.  
11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > 230 User noodle-  
admin logged in.  
11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > FEAT  
11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > 211-Extensions  
supported:  
11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > CLNT  
11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > MDTM  
11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > PASV  
11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > SIZE  
11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > 211 End.
```

Let us examine the above extract in detail.

**11/14/2008 7:22:00 AM - (not logged in) (10.10.10.222) > connected to ip :
10.10.10.111**

<i>Field</i>	<i>Explanation</i>
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:22:00 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
connected to ip :	This indicates that the user is making a connection with the IP address 10.10.10.111

11/14/2008 7:22:00 AM - (not logged in) (10.10.10. 222) > sending welcome message.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:22:00 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
sending welcome message.	This indicates that the FTP server is sending a welcome message. This does not indicate that the user has been successful in logging in.

11/14/2008 7:22:00 AM - (not logged in) (10.10.10. 222) > 220 Welcome to Noodle Bank FTP Server

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:22:00 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
220	Service ready for new user.
Welcome to Noodle Bank FTP Server	This is the customized welcome message sent by this FTP server. This does not indicate that the user has been successful in logging in.

11/14/2008 7:22:00 AM - (not logged in) (10.10.10. 222) > USER noodle-admin

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:22:00 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
USER noodle-admin	This indicates that the username “noodle-admin” has been sent by the client

11/14/2008 7:22:00 AM - (not logged in) (10.10.10. 222) > 331 Password required for noodle-admin.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:22:00 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
331	This signifies that the user name is correct and that a password is needed. However, this status code is usually seen even if the username is invalid.
Password required for noodle-admin.	The FTP server requires a password for the username “noodle-admin”

11/14/2008 7:22:00 AM - (not logged in) (10.10.10. 222) > PASS *****

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:22:00 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
PASS *****	This indicates that a password has been sent by the client. The actual password is not logged.

11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > logged in.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:22:00 AM	This is the time
noodle-admin	This indicates that the user is logged in as noodle-admin
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
Logged in	This indicates that the user is logged into the FTP Server.

11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > 230 User noodle-admin logged in.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:22:00 AM	This is the time
noodle-admin	This indicates that the user is logged in as noodle-admin
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
230	This indicates “user logged in, proceed”. This status code appears after the client sends the correct password. It indicates that the user has successfully logged on.
User noodle-admin logged in.	This indicates that the user “noodle-admin” is logged into the FTP Server.

11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > FEAT

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:22:00 AM	This is the time
noodle-admin	This indicates that the user is logged in as noodle-admin
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
FEAT	The FEAT command causes the FTP server to list all new FTP features that the server supports beyond those described in the basic FTP standards mentioned in RFC 959 (http://www.rfc-editor.org/rfc/rfc959.txt).

11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > 211-Extensions supported:

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:22:00 AM	This is the time
noodle-admin	This indicates that the user is logged in as noodle-admin
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
211	This code stands for the system status, or system help reply.
Extensions supported:	These are the extensions supported by the FTP Server.

11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > MDTM

11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > PASV

11/14/2008 7:22:00 AM - noodle-admin (10.10.10.222) > SIZE

These lines show a list of extension supported by the FTP Server. In this case, the extensions are:

(1) MDTM which returns the modification time of a file. The syntax is MDTM *remote-filename*. Returns the last-modified time of the given file on the remote host in the format:

"YYYYMMDDhhmmss":

YYYY is the four-digit year,

MM is the month from 01 to 12,

DD is the day of the month from 01 to 31,

hh is the hour from 00 to 23,

mm is the minute from 00 to 59, and

ss is the second from 00 to 59.

(2) PASV which tells the server to enter "passive mode". The syntax is PASV. In the passive mode, the server will wait for the client to establish a connection with it rather than attempting to connect to a client-specified port.

(3) SIZE which returns the size of a file. The syntax is SIZE *remote-filename*.

1.5 Attempting to connect from a banned IP

Following is a small extract from the log documenting an attempt to log into the FTP Server from an IP address which has specifically been banned. The administrator of the FTP Server can ban a particular IP address (or a group of IP addresses). This is usually done if the administrator suspects that such IP addresses are being used for malicious activities.

11/14/2008 7:45:50 AM - (not logged in) (10.10.10.222) > connected to ip : 10.10.10.111

11/14/2008 7:45:50 AM - (not logged in) (10.10.10.222) > sending welcome message.

11/14/2008 7:45:50 AM - (not logged in) (10.10.10.222) > 220 Welcome to Noodle Bank FTP Server

11/14/2008 7:45:50 AM - (not logged in) (10.10.10.222) > USER noodle-admin

11/14/2008 7:45:50 AM - (not logged in) (10.10.10.222) > 331 Password required for noodle-admin.

11/14/2008 7:45:50 AM - (not logged in) (10.10.10.222) > PASS *****

11/14/2008 7:45:50 AM - (not logged in) (10.10.10.222) > 530 Not logged in, access denied.

11/14/2008 7:45:50 AM - (not logged in) (10.10.10.222) > disconnected.

Let us examine the above extract in detail.

11/14/2008 7:45:50 AM - (not logged in) (10.10.10.222) > connected to ip : 10.10.10.111

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:45:50 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
connected to ip :	This indicates that the user is making a connection with the IP address 10.10.10.111

11/14/2008 7:45:50 AM - (not logged in) (10.10.10. 222) > sending welcome message.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:45:50 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
sending welcome message.	This indicates that the FTP server is sending a welcome message. This does not indicate that the user has been successful in logging in.

11/14/2008 7:45:50 AM - (not logged in) (10.10.10. 222) > 220 Welcome to Noodle Bank FTP Server

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:45:50 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
220	Service ready for new user.
Welcome to Noodle Bank FTP Server	This is the customized welcome message sent by this FTP server. This does not indicate that the user has been successful in logging in.

11/14/2008 7:45:50 AM - (not logged in) (10.10.10. 222) > USER noodle-admin

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:45:50 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
USER noodle-admin	This indicates that the username “noodle-admin” has been sent by the client

(00001) 11/14/2008 7:45:50 AM - (not logged in) (10.10.10. 222) > 331 Password required for noodle-admin.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:45:50 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
331	This signifies that the user name is correct and that a password is needed. However, this status code is usually seen even if the username is invalid.
Password required for noodle-admin.	The FTP server requires a password for the username “noodle-admin”

11/14/2008 7:45:50 AM - (not logged in) (10.10.10. 222) > PASS *****

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:45:50 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
PASS *****	This indicates that a password has been sent by the client. The actual password is not logged.

11/14/2008 7:45:50 AM - (not logged in) (10.10.10. 222) > 530 Not logged in, access denied..

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:45:50 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
530	This error code means that the user is not logged in. This usually occurs when the correct user name and password combination has not been entered. Some servers use this code instead of 421 when the user limit is reached.
Not logged in, access denied.	This indicates that the FTP Server has denied access to the user.

11/14/2008 7:45:50 AM - (not logged in) (10.10.10. 222) > disconnected.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:45:50 AM	This is the time
(not logged in)	This indicates that the user is not logged in
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
disconnected.	The user has been disconnected.

1.6 Attempting to upload a banned file

Following is a small extract from the log documenting an attempt to download a banned file. The administrator of the FTP Server can ban particular file types. This is usually done to prevent spreading of pirated music (e.g. mp3 files), viruses (e.g. exe or vbs files) etc.

```
11/14/2008 7:54:42 AM - noodle- user (10.10.10. 222) > STOR songs.mp3
11/14/2008 7:54:42 AM - noodle- user (10.10.10. 222) > 550-File is banned
on server !
11/14/2008 7:54:42 AM - noodle- user (10.10.10. 222) > 550 Cannot STOR.
No permission.
```

Let us examine the above extract in detail.

11/14/2008 7:54:42 AM - noodle-user (10.10.10. 222) > STOR songs.mp3

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:54:42 AM	This is the time
noodle-user	This indicates that the user is logged in as “noodle-user”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
STOR	This basically stands for “store a file on the remote host”. The syntax is: STOR <i>remote-filename</i> which in this case is STOR <i>songs.mp3</i>
songs.mp3	This is the file sought to be transferred to the FTP Server.

11/14/2008 7:54:42 AM - noodle-user (10.10.10. 222) > 550-File is banned on server !

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:54:42 AM	This is the time
noodle-user	This indicates that the user is logged in as “noodle-user”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
550	This error code basically signifies that the requested action was not taken, or the file is unavailable, not found, not accessible etc.
File is banned on server !	This indicates that this file type is banned on this FTP Server.

11/14/2008 7:54:42 AM - noodle-user (10.10.10. 222) > 550-File is banned on server !

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:54:42 AM	This is the time
noodle-user	This indicates that the user is logged in as “noodle-user”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
550	This error code basically signifies that the requested action was not taken, or the file is unavailable, not

	found, not accessible etc.
Cannot STOR. No permission.	This indicates that there is no permission to store this file type on this FTP Server.

1.7 Uploading a file

Following is a small extract from the log documenting the upload of the file *style.css*

```

11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > STOR style.css
11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > asked to upload
'style.css' in 'S:\websites\noodlebank_com' --> Access allowed.
11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > 150 Data
connection accepted from 10.10.10.222:49249; transfer starting for
style.css.
11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > started
uploading 'style.css' in 'S:\websites\noodlebank_com'.
11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > 226 File
received ok.
11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > finished
uploading 'style.css' in 'S:\websites\noodlebank_com' - (00:00:01 - 3.254
KB - 3.254 KBytes/s).
11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > TYPE A
11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > 200 Type set to
A.
11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > PASV
11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > 227 Entering
Passive Mode (10,10,10,222,98,70)

```

Let us examine the above extract in detail.

11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > STOR style.css

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:26:34 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle-admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
STOR	This basically implies "store a file on the remote host".
style.css	This is the file sought to be transferred to the FTP Server.

11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > asked to upload 'style.css' in 'S:\websites\noodlebank_com\' --> Access allowed.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:26:34 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle-admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
asked to upload 'style.css' in 'S:\websites\noodlebank_com\' --> Access allowed.	This basically means that the <i>style.css</i> file is sought to be uploaded to a particular folder (S:\websites\noodlebank_com) on the computer on which the FTP Server is running.

11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > 150 Data connection accepted from 10.10.10.222:49249; transfer starting for style.css.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:26:34 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle-admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
150	This code signifies that the file status is okay and the FTP Server is about to open a data connection. FTP uses two ports: 21 for sending commands, and 20 for sending data. A status code of 150 indicates that the server is about to open a new connection on port 20 to send some data.
Data connection accepted from 10.10.10.222:49249;	This means that a connection has been accepted from port 49249 of the user's computer having IP address 10.10.10.222
transfer starting for style.css.	This means that the transfer of <i>style.css</i> to the FTP server is starting.

11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > started uploading 'style.css' in 'S:\websites\noodlebank_com\'.

<i>Field</i>	<i>Explanation</i>
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:26:34 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle- admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
started uploading 'style.css' in 'S:\websites\noodlebank_com\'.	This signifies the start of the uploading of the <i>style.css</i> file to the S:\websites\noodlebank_com folder on the computer on which the FTP Server is running.

11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > finished uploading 'style.css' in 'S:\websites\noodlebank_com\' - (00:00:01 - 3.254 KB - 3.254 KBytes/s).

<i>Field</i>	<i>Explanation</i>
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:26:34 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle- admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
finished uploading 'style.css' in 'S:\websites\noodlebank_com\'	This signifies the completion of the uploading of the <i>style.css</i> file to the S:\websites\noodlebank_com folder on the computer on which the FTP Server is running.
00:00:01	This signifies that the upload took 1 second
3.254 KB	This signifies that the size of the uploaded file was 3.254 KB
3.254 KBytes/s	This signifies that the speed of the upload was 3.254 KB per second.

11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > TYPE A

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:26:34 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle-admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
TYPE A	TYPE sets the type of file to be transferred. Various options are: A - ASCII text E - EBCDIC text I - image (binary data) L - local format

11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > PASV

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:26:34 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle-admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
PASV	PASV tells the server to enter "passive mode". In the passive mode, the server will wait for the client to establish a connection with it rather than attempting to connect to a client-specified port.

11/14/2008 7:26:34 AM - noodle-admin (10.10.10.222) > 227 Entering Passive Mode (10,10,10,222,98,70)

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:26:34 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle-admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
227 Entering Passive Mode	This indicates that the FTP Server is entering passive mode
(10,10,10,222,98,70)	This indicates the users IP address and port number. The format is as under:

	<p>The first four numbers represent the IP address i.e. 10,10,10,222 means 10.10.10.222</p> <p>For calculating the port number, multiply the fifth number by 256 and then add to it the sixth number. In this case the fifth and sixth numbers are 98 and 70. So the port number will be:</p> $= (98*256) + 70$ $= 25158$
--	---

1.8 Renaming a file

Following is a small extract from the log documenting the renaming of the file *accounts.doc* to *accounts2009.doc*.

11/14/2008 8:08:12 AM - noodle-admin (10.10.10.222) > RNFR /accounts.doc
11/14/2008 8:08:12 AM - noodle-admin (10.10.10.222) > asked to rename 'S:\websites\noodle_net\accounts.doc' --> Primary access allowed, waiting destination name.
11/14/2008 8:08:12 AM - noodle-admin (10.10.10.222) > 350 File exists, ready for destination name.
11/14/2008 8:08:12 AM - noodle-admin (10.10.10.222) > RNTO /accounts2009.doc
11/14/2008 8:08:12 AM - noodle-admin (10.10.10.222) > asked to rename 'S:\websites\noodle_net\accounts.doc' to 'S:\websites\noodle_net\accounts2009.doc' --> Access allowed.
11/14/2008 8:08:12 AM - noodle-admin (10.10.10.222) > 250 File '/accounts.doc' renamed to '/accounts2009.doc'.
11/14/2008 8:08:12 AM - noodle-admin (10.10.10.222) > PASV

Let us examine the above extract in detail.

11/14/2008 8:08:12 AM - noodle-admin (10.10.10.222) > RNFR /accounts.doc

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
8:08:12 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle-admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
RNFR	This refers to "rename from".
/accounts.doc	This is the filename that is sought to be renamed.

11/14/2008 8:08:12 AM - noodle-admin (10.10.10.222) > asked to rename 'S:\websites\noodle_net\accounts.doc' --> Primary access allowed, waiting destination name.

<i>Field</i>	<i>Explanation</i>
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
8:08:12 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle-admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
asked to rename 'S:\websites\noodle_net\accounts.doc'	This signifies that the file "accounts.doc" in the 'S:\websites\noodle_net folder of the computer running the FTP Server is sought to be renamed.
Primary access allowed, waiting destination name.	This signifies that the necessary access is allowed and the final name (after renaming) is awaited.

11/14/2008 8:08:12 AM - noodle-admin (10.10.10.222) > 350 File exists, ready for destination name.

<i>Field</i>	<i>Explanation</i>
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
8:08:12 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle-admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
350	Requested file action pending further information.
File exists, ready for destination name.	This indicates that the file that is sought to be renamed, exists. The FTP Server is now ready for destination name.

**11/14/2008 8:08:12 AM - noodle-admin (10.10.10.222) > RNTO
 /accounts2009.doc**

<i>Field</i>	<i>Explanation</i>
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
8:08:12 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle- admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
RNTO	This refers to: “rename to”.
/accounts2009.doc	This is the revised name sought to be given to the file.

**11/14/2008 8:08:12 AM - noodle-admin (10.10.10.222) > asked to rename
 'S:\websites\noodle_net\accounts.doc' to
 'S:\websites\noodle_net\accounts2009.doc' --> Access allowed.**

<i>Field</i>	<i>Explanation</i>
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
8:08:12 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle- admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
asked to rename 'S:\websites\noodle_net\accounts.doc' to 'S:\websites\noodle_net\accounts2009.doc'	This signifies that the file “accounts.doc” in the 'S:\websites\noodle_net folder of the computer running the FTP Server is sought to be renamed to accounts2009.doc
Access allowed	This indicates that access is allowed.

11/14/2008 8:08:12 AM - noodle-admin (10.10.10.222) > 250 File '/accounts.doc' renamed to '/accounts2009.doc'.

<i>Field</i>	<i>Explanation</i>
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
8:08:12 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle-admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
250	This code indicates that the requested file action has been completed.
File '/accounts.doc' renamed to '/accounts2009.doc'.	This signifies that the file "accounts.doc" has been renamed to accounts2009.doc

11/14/2008 8:08:12 AM - noodle-admin (10.10.10.222) > PASV

<i>Field</i>	<i>Explanation</i>
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
8:08:12 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle-admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
PASV	This indicates that the server has entered "passive mode". In the passive mode, the server will wait for the client to establish a connection with it rather than attempting to connect to a client-specified port.

1.9 Deleting a file

Following is a small extract from the log documenting the deletion of the index.html file. In many cases of web defacement, the index.html file is deleted by a malicious hacker.

```
11/14/2008 7:28:32 AM - noodle-admin (10.10.10.222) > DELE index.html
11/14/2008 7:28:32 AM - noodle-admin (10.10.10.222) > asked to delete
'S:\websites\noodlebank_com\index.html' --> Access allowed.
11/14/2008 7:28:32 AM - noodle-admin (10.10.10.222) > 250 File/Dir '/index.html'
deleted.
11/14/2008 7:28:32 AM - noodle-admin (10.10.10.222) > PASV
```

Let us examine the above extract in detail.

11/14/2008 7:28:32 AM - noodle-admin (10.10.10.222) > DELE index.html

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:28:32 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle-admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
DELE	This indicates that a file on the FTP Server is sought to be deleted.
index.html	This is the file that is sought to be deleted.

11/14/2008 7:28:32 AM - noodle-admin (10.10.10. 222) > asked to delete 'S:\websites\noodlebank_com\index.html' --> Access allowed.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:28:32 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle- admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
asked to delete 'S:\websites\noodlebank_com\index.html' --> Access allowed.	This indicates that the <i>index.html</i> file in the 'S:\websites\noodlebank_com folder (of the computer running the FTP Server) is sought to be deleted.

11/14/2008 7:28:32 AM - noodle-admin (10.10.10. 222) > 250 File/Dir '/index.html' deleted.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:28:32 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle-admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
250	This code signifies that the requested file has been completed.
File/Dir '/index.html' deleted.	This indicates that the <i>index.html</i> file has been deleted.

11/14/2008 7:28:32 AM - noodle-admin (10.10.10. 222) > PASV

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:28:32 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle-admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
PASV	This indicates that the server has entered "passive mode". In the passive mode, the server will wait for the client to establish a connection with it rather than attempting to connect to a client-specified port.

1.10 Downloading a file

Following is a small extract from the log documenting the downloading of the *style.css* file.

```
11/14/2008 7:31:28 AM - noodle-admin (10.10.10.222) > RETR style.css
11/14/2008 7:31:28 AM - noodle-admin (10.10.10.222) > asked to download
'S:\websites\noodlebank_com\style.css' --> Access allowed.
11/14/2008 7:31:28 AM - noodle-admin (10.10.10.222) > 150 Data connection accepted
from 10.10.10.222:49254; transfer starting for style.css (3332 bytes).
11/14/2008 7:31:28 AM - noodle-admin (10.10.10.222) > started downloading
'S:\websites\noodlebank_com\style.css'.
11/14/2008 7:31:28 AM - noodle-admin (10.10.10.222) > finished downloading
'S:\websites\noodlebank_com\style.css' - (00:00:01 - 3.254 KB - 3.254 KBytes/s)
11/14/2008 7:31:28 AM - noodle-admin (10.10.10.222) > 226 Transfer ok
```

Let us examine the above extract in detail.

11/14/2008 7:31:28 AM - noodle-admin (10.10.10.222) > RETR style.css

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:31:28 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle-admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
RETR	This basically signifies retrieving a remote file.
style.css	This is the file sought to be retrieved from the FTP Server.

11/14/2008 7:31:28 AM - noodle-admin (10.10.10.222) > asked to download 'S:\websites\noodlebank_com\style.css' --> Access allowed.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:31:28 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle- admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
asked to download 'S:\websites\noodlebank_com\style.css' --> Access allowed.	This basically means that the <i>style.css</i> file is sought to be downloaded from a particular folder (S:\websites\noodlebank_com) on the computer on which the FTP Server is running.

11/14/2008 7:31:28 AM - noodle-admin (10.10.10.222) > 150 Data connection accepted from 10.10.10.222:49254; transfer starting for style.css (3332 bytes).

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:31:28 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle- admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
150	This code signifies that the file status is okay and the FTP Server is about to open a data connection. FTP uses two ports: 21 for sending commands, and 20 for sending data. A status code of 150 indicates that the server is about to open a new connection on port 20 to send some data.
Data connection accepted from 10.10.10.222:49254;	This means that a connection has been accepted from port 49254 of the user's computer having IP address 10.10.10.222
transfer starting for style.css	This means that the transfer of <i>style.css</i> from the FTP server is starting and the size of the file is 3332 bytes.

11/14/2008 7:31:28 AM - noodle-admin (10.10.10.222) > started downloading 'S:\websites\noodlebank_com\style.css'.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:31:28 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle- admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
started downloading 'S:\websites\noodlebank_com\style.css'.	This signifies the start of the downloading of the <i>style.css</i> file from the S:\websites\noodlebank_com folder on the computer on which the FTP Server is running.

11/14/2008 7:31:28 AM - noodle-admin (10.10.10.222) > finished downloading 'S:\websites\noodlebank_com\style.css' - (00:00:01 - 3.254 KB - 3.254 KBytes/s)

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:31:28 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle- admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
finished downloading 'S:\websites\noodlebank_com\style.css'	This signifies the completion of the downloading of the style.css file from the S:\websites\noodlebank_com folder on the computer on which the FTP Server is running.
00:00:01	This signifies that the download took 1 second.
3.254 KB	This signifies that the size of the downloaded file was 3.254 KB.
3.254 KBytes/s	This signifies that the speed of the download was 3.254 KB per second.

11/14/2008 7:31:28 AM - noodle-admin (10.10.10.222) > 226 Transfer ok

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:31:28 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle- admin”

(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
226	This code signifies that the requested file action was successful (file download in this case) and also signifies the closing of the data connection.
Transfer ok	This signifies that the transfer was successfully carried out.

1.11 Creating a directory

Following is a small extract from the log documenting the creation of a directory named *test*.

```
11/14/2008 7:32:51 AM - noodle-admin (10.10.10. 222) > MKD test
11/14/2008 7:32:51 AM - noodle-admin (10.10.10. 222) > asked to create dir
'S:\websites\noodlebank_com\test' --> Access allowed.
11/14/2008 7:32:51 AM - noodle-admin (10.10.10. 222) > made dir 'test' in
'S:\websites\noodlebank_com\'.
11/14/2008 7:32:51 AM - noodle-admin (10.10.10. 222) > 257 '/test':
directory created.
11/14/2008 7:32:51 AM - noodle-admin (10.10.10. 222) > PASV
```

Let us examine the above extract in detail.

11/14/2008 7:32:51 AM - noodle-admin (10.10.10. 222) > MKD test

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:32:51 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle-admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
MKD	This stands for making a remote directory
test	This is the name of the directory sought to be made / created

11/14/2008 7:32:51 AM - noodle-admin (10.10.10. 222) > asked to create dir 'S:\websites\noodlebank_com\test' --> Access allowed.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:32:51 AM	This is the time

noodle-admin	This indicates that the user is logged in as “noodle- admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
asked to create dir 'S:\websites\noodlebank_com\test' --> Access allowed.	This signifies that a directory named <i>test</i> is sought to be created in the S:\websites\noodlebank_com folder of the computer running the FTP Server.

11/14/2008 7:32:51 AM - noodle-admin (10.10.10. 222) > made dir 'test' in 'S:\websites\noodlebank_com\'.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:32:51 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle- admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
made dir 'test' in 'S:\websites\noodlebank_com'.	This signifies that a directory named <i>test</i> has been created in the S:\websites\noodlebank_com folder on the computer on which the FTP Server is running.

11/14/2008 7:32:51 AM - noodle-admin (10.10.10. 222) > 257 '/test': directory created.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:32:51 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle- admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
257	This signifies that a “PATHNAME” has been created
'/test': directory created.	This signifies that a directory named <i>test</i> has been created

11/14/2008 7:32:51 AM - noodle-admin (10.10.10. 222) > PASV

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:32:51 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle-

	admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
PASV	This indicates that the server has entered "passive mode". In the passive mode, the server will wait for the client to establish a connection with it rather than attempting to connect to a client-specified port.

1.12 Deleting a directory

Following is a small extract from the log documenting the deletion of a directory named *test*.

```
11/14/2008 7:33:15 AM - noodle-admin (10.10.10.198) > RMD test
11/14/2008 7:33:15 AM - noodle-admin (10.10.10.198) > asked to delete
'S:\websites\noodlebank_com\test\' --> Access allowed.
11/14/2008 7:33:15 AM - noodle-admin (10.10.10.198) > 250 '/test': directory
removed.
11/14/2008 7:33:15 AM - noodle-admin (10.10.10.198) > PASV
```

Let us examine the above extract in detail.

11/14/2008 7:33:15 AM - noodle-admin (10.10.10.222) > RMD test

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:33:15 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle-admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
RMD	This signifies that a remote directory is sought to be removed
test	This signifies that the name of the remote directory is <i>test</i>

11/14/2008 7:33:15 AM - noodle-admin (10.10.10.222) > asked to delete 'S:\websites\noodlebank_com\test\' --> Access allowed.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008

7:33:15 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle- admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
asked to delete 'S:\websites\noodlebank_com\test\' --> Access allowed.	This signifies that a directory named test in the S:\websites\noodlebank_com folder on the computer on which the FTP Server is running is sought to be deleted.

11/14/2008 7:33:15 AM - noodle-admin (10.10.10.222) > 250 '/test': directory removed.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:33:15 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle- admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
250	This code signifies that the requested file has been completed.
'/test': directory removed.	This signifies that the directory named <i>test</i> has been removed.

11/14/2008 7:33:15 AM - noodle-admin (10.10.10.222) > PASV

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:33:15 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle- admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
PASV	This indicates that the server has entered "passive mode". In the passive mode, the server will wait for the client to establish a connection with it rather than attempting to connect to a client-specified port.

1.13 Making a directory writable by public

Following is a small extract from the log documenting the change in properties of a directory named *secret*. Prior to the change, the contents of this directory could not be changed by users. After the change, the directory can be written to by users, implying that its contents can be altered by users.

11/14/2008 7:35:46 AM - noodle-admin (10.10.10.222) > SITE CHMOD 0757 secret
11/14/2008 7:35:46 AM - noodle-admin (10.10.10.222) > 200 CHMOD command successful.
11/14/2008 7:35:46 AM - noodle-admin (10.10.10.222) > PASV

Let us examine the above extract in detail.

11/14/2008 7:35:46 AM - noodle-admin (10.10.10.222) > SITE CHMOD 0757 secret

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:35:46 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle-admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
SITE CHMOD 0757	The chmod command (abbreviated from change mode) can change permissions of files and directories.
secret	This is the folder whose permissions are to be changed (from read only to writable in this example)

11/14/2008 7:35:46 AM - noodle-admin (10.10.10.222) > 200 CHMOD command successful.

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:35:46 AM	This is the time
noodle-admin	This indicates that the user is logged in as “noodle-admin”
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
200	Site-specific commands
CHMOD command successful	The chmod command (abbreviated from change mode) has been successful (in this case it signifies that the permission has been changed for the <i>secret</i> directory)

11/14/2008 7:35:46 AM - noodle-admin (10.10.10.222) > PASV

Field	Explanation
11/14/2008	This is the date in mm/dd/yyyy format i.e. 14 th November, 2008
7:35:46 AM	This is the time
noodle-admin	This indicates that the user is logged in as "noodle-admin"
(10.10.10.222)	This indicates the IP address of the user i.e. 10.10.10.222
PASV	This indicates that the server has entered "passive mode". In the passive mode, the server will wait for the client to establish a connection with it rather than attempting to connect to a client-specified port.

1.14 List of raw FTP commands

Command	Brief description	Details
ABOR	abort a file transfer	Syntax: ABOR Aborts a file transfer currently in progress.
CWD	change working directory	Syntax: CWD <i>remote-directory</i> Makes the given directory be the current directory on the remote host.
DELE	delete a remote file	Syntax: DELE <i>remote-filename</i> Deletes the given file on the remote host.
LIST	list remote files	Syntax: LIST [<i>remote-filename</i>] If <i>remote-filename</i> refers to a file, sends information about that file. If <i>remote-filename</i> refers to a directory, sends information about each file in that directory. <i>remote-filename</i> defaults to the current directory. This command must be preceded by a PORT or PASV command.
MDTM	return the modification time of a file	Syntax: MDTM <i>remote-filename</i> Returns the last-modified time of the given file on the remote host in the format "YYYYMMDDhhmmss": YYYY is the four-digit year, MM is the month from 01 to 12, DD is the day of the month from 01 to 31, hh is the hour from 00 to 23, mm is the minute from 00 to 59, and ss is the second from 00 to 59.
MKD	make a remote directory	Syntax: MKD <i>remote-directory</i> Creates the named directory on the remote host.
NLST	name list of remote directory	Syntax: NLST [<i>remote-directory</i>] Returns a list of filenames in the given directory (defaulting to the current directory), with no other information.

		Must be preceded by a PORT or PASV command.
PASS	send password	<p>Syntax: PASS <i>password</i></p> <p>After sending the USER command, send this command to complete the login process. (Note, however, that an ACCT command may have to be used on some systems.)</p>
PASV	enter passive mode	<p>Syntax: PASV</p> <p>Tells the server to enter "passive mode". In passive mode, the server will wait for the client to establish a connection with it rather than attempting to connect to a client-specified port. The server will respond with the address of the port it is listening on, with a message like:</p> <p>227 Entering Passive Mode (a1,a2,a3,a4,p1,p2)</p> <p>where a1.a2.a3.a4 is the IP address and p1*256+p2 is the port number.</p>
PORT	open a data port	<p>Syntax: PORT <i>a1,a2,a3,a4,p1,p2</i></p> <p>Specifies the host and port to which the server should connect for the next file transfer. This is interpreted as IP address <i>a1.a2.a3.a4</i>, port <i>p1*256+p2</i>.</p>
PWD	print working directory	<p>Syntax: PWD</p> <p>Returns the name of the current directory on the remote host.</p>
QUIT	terminate the connection	<p>Syntax: QUIT</p> <p>Terminates the command connection.</p>
RETR	retrieve a remote file	<p>Syntax: RETR <i>remote-filename</i></p> <p>Begins transmission of a file from the remote host. Must be preceded by either a PORT command or a PASV command to indicate where the server should send data.</p>

RMD	remove a remote directory	Syntax: RMD <i>remote-directory</i> Deletes the named directory on the remote host.
RNFR	rename from	Syntax: RNFR <i>from-filename</i> Used when renaming a file. Use this command to specify the file to be renamed; follow it with an RNTO command to specify the new name for the file.
RNTO	rename to	Syntax: RNTO <i>to-filename</i> Used when renaming a file. After sending an RNFR command to specify the file to rename, send this command to specify the new name for the file.
SITE	Site-specific commands	Syntax: SITE <i>site-specific-command</i> Executes a site-specific command.
SIZE	return the size of a file	Syntax: SIZE <i>remote-filename</i> Returns the size of the remote file as a decimal number.
STOR	store a file on the remote host	Syntax: STOR <i>remote-filename</i> Begins transmission of a file to the remote site. Must be preceded by either a PORT command or a PASV command so the server knows where to accept data from.
TYPE	set transfer type	Syntax: TYPE <i>type-character</i> [<i>second-type-character</i>] Sets the type of file to be transferred. <i>type-character</i> can be any of: <ul style="list-style-type: none"> * A - ASCII text * E - EBCDIC text * I - image (binary data) * L - local format For A and E, the <i>second-type-character</i> specifies how the text should be interpreted. It can be: <ul style="list-style-type: none"> * N - Non-print (not destined for

		<p>printing). This is the default if second-type-character is omitted.</p> <ul style="list-style-type: none"> * T - Telnet format control (<CR>, <FF>, etc.) * C - ASA Carriage Control <p>For L, the <i>second-type-character</i> specifies the number of bits per byte on the local system, and may not be omitted.</p>
USER	send username	<p>Syntax: USER <i>username</i></p> <p>Send this command to begin the login process. <i>username</i> should be a valid username on the system, or "anonymous" to initiate an anonymous login.</p>
ACCT	send account information	<p>Syntax: ACCT <i>account-info</i></p> <p>This command is used to send account information on systems that require it. Typically sent after a PASS command.</p>
APPE	append to a remote file	<p>Syntax: APPE <i>remote-filename</i></p> <p>Append data to the end of a file on the remote host. If the file does not already exist, it is created. This command must be preceded by a PORT or PASV command so that the server knows where to receive data from.</p>
CDUP	CWD to the parent of the current directory	<p>Syntax: CDUP</p> <p>Makes the parent of the current directory be the current directory.</p>
HELP	return help on using the server	<p>Syntax:</p> <p>If a command is given, returns help on that command; otherwise, returns general help for the FTP server (usually a list of supported commands).</p>
MODE	set transfer mode	<p>Syntax: MODE <i>mode-character</i></p> <p>Sets the transfer mode to one of:</p> <ul style="list-style-type: none"> * S - Stream * B - Block * C - Compressed <p>The default mode is Stream.</p>

NOOP	do nothing	Syntax: NOOP Does nothing except return a response.
REIN	reinitialize the connection	Syntax: REIN Reinitializes the command connection - cancels the current user/password/account information. Should be followed by a USER command for another login.
STAT	return server status	Syntax: STAT [<i>remote-filename</i>] If invoked without parameters, returns general status information about the FTP server process. If a parameter is given, acts like the LIST command, except that data is sent over the control connection (no PORT or PASV command is required).
STOU	store a file uniquely	Syntax: STOU Begins transmission of a file to the remote site; the remote filename will be unique in the current directory. The response from the server will include the filename.
STRU	set file transfer structure	Syntax: STRU <i>structure-character</i> Sets the file structure for transfer to one of: <ul style="list-style-type: none"> * F - File (no structure) * R - Record structure * P - Page structure The default structure is File.
SYST	return system type	Syntax: SYST Returns a word identifying the system, the word "Type:", and the default transfer type (as would be set by the TYPE command). For example: UNIX Type: L8

Source: <http://www.nsftools.com/tips/RawFTP.htm>

1.15 FTP Status and Error Codes

Code	Description	Possible Solutions
100 Series	The requested action was initiated; expect another reply before proceeding with a new command.	
110	Restart marker reply.	(Informational)
120	Service ready in <i>nn</i> minutes.	(Informational)
125	Data Connection already open, transfer starting.	(Informational)
150	File status okay, about to open data connection. FTP uses two ports: 21 for sending commands, and 20 for sending data. A status code of 150 indicates that the server is about to open a new connection on port 20 to send some data.	(Informational)
200 Series	The requested action has been successfully completed.	
200	Command okay.	(Informational)
202	Command not implemented, superfluous at this site.	(Informational)
211	System status, or system help reply.	(Informational)
212	Directory status.	(Informational)
213	File status.	(Informational)
214	Help message.	(Informational)
215	NAME system type. (Where NAME is an official system name from the list in the Assigned Numbers document.)	(Informational)
220	Service ready for new user.	(Informational)
221	Service closing control connection. Logged out if appropriate.	(Informational)
225	Data connection open; no transfer in progress.	(Informational)
226	Closing data connection. Requested file action successful (for example; file transfer or file abort). The command opens a data connection on port 20 to perform an action, such as transferring a file. This action successfully completes, and the data connection is closed.	(Informational)

227	Entering Passive Mode.	(Informational)
230	User logged in, proceed. This status code appears after the client sends the correct password. It indicates that the user has successfully logged on.	(Informational)
250	Requested file action okay, completed.	(Informational)
257	"PATHNAME" created.	(Informational)
300 Series	The command has been accepted, but the requested action is on hold, pending receipt of further information.	
331	User name okay, need password.	You see this status code after the client sends a user name, regardless of whether the user name that is provided is a valid account on the system.
332	Need account for login.	Provide login credentials
350	Requested file action pending further information.	(Informational)
400 Series	The command was not accepted and the requested action did not take place, but the error condition is temporary and the action may be requested again.	
421	Error 421 Service not available, closing control connection. Error 421 User limit reached Error 421 You are not authorized to make the connection Error 421 Max connections reached Error 421 Max connections exceeded	Try logging in later.
425	Cannot open data connection.	Change from PASV to PORT mode, check your firewall settings, or try to connect via HTTP.
426	Connection closed; transfer aborted. The command opens a data connection to perform an action, but that action is canceled, and the data connection is closed.	Try logging back in; contact your hosting provider to check if you need to increase your hosting account; try disabling the firewall on your PC to see if that solves the problem. If not, contact your hosting provider or ISP.

450	Requested file action not taken. File unavailable (e.g., file busy).	Try again later.
451	Requested action aborted: local error in processing.	Ensure command and parameters were typed correctly.
452	Requested action not taken. Insufficient storage space in system.	Ask FTP administrator to increase allotted storage space, or archive/delete remote files.
500 Series	The command was not accepted and the requested action did not take place.	
500	Syntax error, command unrecognized, command line too long.	Try switching to passive mode.
501	Syntax error in parameters or arguments.	Verify your input; i.e., make sure there are no erroneous characters, spaces, etc.
502	Command not implemented.	The server does not support this command.
503	Bad sequence of commands.	Verify command sequence.
504	Command not implemented for that parameter.	Ensure entered parameters are correct.
530	User not logged in.	Ensure that you typed the correct user name and password combination. Some servers use this code instead of 421 when the user limit is reached.
532	Need account for storing files.	Logged in user does not have permission to store files on remote server.
550	Requested action not taken. File unavailable, not found, not accessible.	Verify that you are attempting to connect to the correct server/location. The administrator of the remote server must provide you with permission to connect via FTP.

552	Requested file action aborted. Exceeded storage allocation.	More disk space is needed. Archive files on the remote server that you no longer need.
553	Requested action not taken. File name not allowed.	Change the file name or delete spaces/special characters in the file name.
10,000 series	Common Winsock Error Codes)	
10054	Connection reset by peer. The connection was forcibly closed by the remote host.	(Informational)
10060	Cannot connect to remote server (Generally a time-out error).	Try switching from PASV to PORT mode, or try increasing the time-out value.
10061	Cannot connect to remote server. The connection is actively refused by the server.	Try switching the connection port.
10066	Directory not empty. The server will not delete this directory while there are files/folders in it.	If you want to remove the directory, first archive or delete the files in it.
10068	Too many users, server is full.	Try logging in at another time.

Source: <http://kb.globalscape.com/article.aspx?id=10142>

2. Web server logs

Following is an extract of the log when someone (from IP address 10.10.10.222) accesses the *menu.gif* image on the website www.noodlebank.com.

```
#Software: Microsoft Internet Information Services 7.0
#Version: 1.0
#Date: 2008-11-22 23:13:25
#Fields: date time s-computername s-ip cs-method cs-uri-stem cs-uri-query
s-port cs-username c-ip cs-version cs(User-Agent) cs(Cookie) cs(Referer)
cs-host sc-status sc-substatus sc-win32-status sc-bytes cs-bytes time-taken
2009-1-13 00:45:26 ASCL 10.10.10.111 GET /images/menu.gif - 80 -
10.10.10.222 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.0;+SLCC1;+.NET+
CLR+2.0.50727;+.NET+CLR+3.0.04506) - http://www.noodlebank.com/
www.noodlebank.com 200 0 0 625 315 62
```

The relevant part of the log is as below:

```
2009-1-13 00:45:26 ASCL 10.10.10.111 GET /images/menu.gif - 80 -
10.10.10.222 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.0;+SLCC1;+.NET+CL
R+2.0.50727;+.NET+CLR+3.0.04506) - http://www.noodlebank.com/
www.noodlebank.com 200 0 0 625 315 62
```

The explanation of the log entry is as below:

Log entry	Field name	Description
2009-1-13	date	Date i.e. the date on which the activity occurred.
00:45:26	time	Time i.e. the time, in coordinated universal time (UTC), at which the activity occurred.
ASCL	s-computername	Server Name i.e. the name of the server on which the log file entry was generated.
10.10.10.111	s-ip	Server IP Address i.e. the IP address of the server on which the log file entry was generated.

GET	cs-method	Method i.e. the requested action, for example, a GET method.
/images/menu.gif	cs-uri-stem	URI Stem i.e. the target of the action, e.g. in this case menu.gif as the user downloaded the image file menu.gif
-	cs-uri-query	URI Query i.e. the query, if any, that the client was trying to perform. A Universal Resource Identifier (URI) query is necessary only for dynamic pages.
80	s-port	Server Port i.e. the server port number that is configured for the service. This is usually 80.
-	cs-username	User Name i.e. the name of the authenticated user who accessed your server. Anonymous users are indicated by a hyphen as in this case.
10.10.10.222	c-ip	Client IP Address i.e. the IP address of the client that made the request.
HTTP/1.1	cs-version	Protocol Version i.e. the protocol version that the client used.
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.0;+SLCC1;+.NET+CLR+2.0.50727;+.NET+CLR+3.0.04506)	cs(User-Agent)	User Agent i.e. the browser type that the client used.
-	cs(Cookie)	Cookie i.e. the content of the cookie sent or received, if any. If none, then it is indicated by a hyphen as in this case.

http://www.noodlebank.com /	cs(Referrer)	Referrer i.e. the site that the user last visited. This site provided a link to the current site.
www.noodlebank.com	cs-host	Host i.e. the host header name, if any.
200	sc-status	HTTP Status i.e. the HTTP status code.
	sc-substatus	Protocol Substatus i.e. the substatus error code.
	sc-win32-status	Win32 Status i.e the Windows status code.
625	sc-bytes	Bytes Sent i.e. the number of bytes that the server sent.
315	cs-bytes	Bytes Received i.e. the number of bytes that the server received.
62	time-taken	Time Taken i.e the length of time that the action took, in milliseconds.

10. Cyber Forensics

1. Introduction

Cyber Forensics is a wide term that encompasses computer forensics (gathering evidence from computer media seized at the crime scene) and network forensics (gathering digital evidence that is distributed across networks).

As per the definition provided by the Computer Emergency Response Team of the Asian School of Cyber Laws (ASCL-CERT):

Cyber Forensics is the discovery²⁰, analysis²¹, and reconstruction²² of evidence²³ extracted²⁴ from and / or contained in a computer, computer system, computer network, computer media or computer peripheral.

Broadly speaking, Cyber Forensics involves:

- (1) finding²⁵ and decrypting password protected information, encrypted information and steganographic content,
- (2) tracking software piracy,
- (3) recovering deleted data,
- (4) matching information to computers that created them,
- (5) remotely monitoring computers and
- (6) preserving digital evidence for presentation in court.

Digital evidence is the foundation of any case involving computers. Searching, examining, collecting, and preserving digital evidence has to be done in such a manner that the court can rely upon the evidence to deliver its judgment. Any errors in gathering, developing, or presenting digital evidence can adversely affect the trial.

²⁰ Discovery implies recovery of something previously unknown or unrecognized.

²¹ Analysis is the detailed examination of something made in order to understand its nature or determine its essential characteristics.

²² Reconstruct means to construct again, to rebuild, and to form again or anew.

²³ Evidence refers to all documents including electronic records produced for the inspection of the Court.

²⁴ Extract means to take out or derive.

²⁵ E.g. the American case of *MacPherson v. Buick Motor Co* (217 N.Y. 382 (N.Y. 1916)) demonstrates the use of search words using specialized software to search for up to fifty target words simultaneously.

As computers become more prevalent and networks permeate our lives, they will contain an ever-increasing amount of evidence of witness, victim, and criminal activity. Even traditional crimes such as homicide and rape can involve a computer, either directly or incidentally.

For instance, in one homicide, the victim's home computer contained hundreds of e-mail messages that provided the crucial link between the victim and the murderer. Before these e-mails were found, investigators believed that they were dealing with a low risk victim and, without these e-mails; it is unlikely that the investigators would have found the offender²⁶.

Acquisition of digital evidence begins when the information and / or the physical items that are collected in the course of cyber crime investigation are collected and / or stored for the purpose of examination.

A distinction may be drawn between original digital evidence and duplicate digital evidence. Original digital evidence includes the physical items and the associated electronic data at the time of acquisition or seizure. Duplicate digital evidence is the accurate digital reproduction of all electronic records contained on an original physical item of evidence.

Examining a computer to discover exactly what data is stored on it is a time consuming and painstaking process. It is important that it can be proved that the examination had been performed thoroughly. There are many types of information in a computer that are valuable from the evidentiary point of view. These are normal files, deleted files, password protected information, hidden files, data in free space, file slack, RAM slack, drive slack space and unallocated space²⁷.

The most important point to be borne in mind is that the information on the original computer is not altered by any of the examination processes (i.e. the entire examination is non-invasive).

The original computer should be treated with great caution as it may contain viruses, logic bombs, booby traps etc. that can alter the data contained therein (or sometimes even format the entire hard disk!). Usually while examining the data stored on any of the storage media associated with a computer, the original evidence is not used. This implies that the investigator first makes an image copy of all the data on the computer storage and then examines this while retaining the original evidence in its initial form. This ensures that tampering of the original evidence does not occur.

²⁶ Casey, E. "Criminal Profiling, Computers, and the Internet," Journal of Behavioral Profiling, May, 2000, Vol. 1, No. 2

²⁷ See key terms at the end of this chapter for the meanings of these terms

Making a mirror image of the entire data stored on a computer assists in this process. This mirror image is known as a **bit-stream image**.

This method of examination of the data stored on a computer ensures that the original evidence is not tampered with. Also, when a bit stream is created, it makes a mirror image of the slack created in the various files and also of the unallocated storage space, thus providing the investigator with an exact copy of the data or information stored there.

A US Court, in Northwest Airlines, et al v. Local 2000, et al.²⁸, directed the plaintiff's expert to make mirror images of the drives in the defendant's computers. The original drives were not released but were entered as evidence.

In Gates Rubber Co. v. Bando Chemical Industries, Ltd.²⁹, a US Court ordered investigation of some computerized files. Due to mishandling of the evidence the Court then passed a stricture on one of the parties for not having made an image copy of a drive at the outset.

The Court ruled that while collecting evidence for judicial purposes the investigating party had "a duty to utilize the method which would yield the most complete and accurate results".

It must be borne in mind that **digital evidence is easily misinterpreted**. All possible explanations for a given piece of evidence must be considered before drawing a conclusion.

Illustration: A log entry may indicate that a suspect was using the Internet at a certain time. In reality it is possible that the suspect's young son was using his father's Internet account.

Illustration: The presence of a pornographic URL in a suspect's web browser history or cookie file indicates that the suspect visited these sites. In fact, it is possible that the URL was the result of advertisements embedded in non-pornographic web pages. In this case, it is possible that the suspect never visited pornographic web sites.

2. Key Terms

File Slack - When a file is created its length depends upon its contents. When this file is saved to the disk any system using DOS, Windows or Windows NT saves it in the form of blocks of data.

These blocks are of a fixed length and are known as clusters. Most of the time, the contents of files do not exactly match the size of these clusters.

²⁸ C.A. No. 00-08DWF/AJB (D.Minn. 2000) (Case settled without trial)

²⁹ 167 F.R.D. 90 (D. Colo 1996)

The space that remains from the end of the file contents to the end of the last cluster assigned to the file is called File Slack. To fill in this space, randomly selected data from the computer's memory is used. File Slack is created at the time when a file is saved to the disk. Due to this, it may contain and assist investigators in identification of network logon names, passwords and other sensitive information associated with computer usage.

File slack can also be analyzed to identify prior uses of the suspected computer and such legacy data can help the investigator.

Fragments of prior email messages and word processing documents can be found in file slack. It potentially contains evidence that may have been thought to be lost.

RAM Slack - Clusters are made up of blocks of sectors. Now if the contents of the file do not fill up the last sector assigned to a file, then any DOS / Windows based system fills up the remaining space by using a system of padding.

The data used for this padding is taken from the memory buffers of the system. This data originates from the memory of the computer and hence is called RAM Slack. RAM slack pertains only to the last sector of a file.

RAM Slack can contain any information that may have been created, viewed, modified, downloaded or copied during the past work sessions since the computer was last booted.

Thus, if the computer has not been shut down for several days, the data stored in file slack can come from work sessions that occurred in the past. Such information could help investigators gather evidence of the files on which a suspect may have worked.

Drive Slack - In certain situations, more or additional sectors need to be added to fill out the blocks of the last cluster assigned to a particular file. In such a case, a different kind of slack has to be created. This is known as Drive Slack. This is then stored in the sectors needed to fill up the last cluster for a file. Drive Slack contains data from what was previously stored on that particular storage device.

The data or information contained in the Drive Slack is derived from what was previously stored or data from the format pattern associated with disk storage space that has yet to be used by the computer. The perpetrator of the crime may assume these files to be completely deleted or wiped, but remnants of these may be procured from the Drive Slack.

Secure wiping is used to erase the contents of one or more files irrevocably, such that they cannot be restored by data recovery software. Each selected file is overwritten according to the current settings, shortened to a length of zero and then deleted. This command is applied to confidential files which are to be destroyed.

This concept is used to prepare “forensically sterile media” on which the analyst can clone the evidence disk.

Splitting - In real world cases, a large size evidence image may need to be **split** into smaller files (e.g. to save the image of a 120 GB hard disk onto multiple 650 MB CD ROMs). Splitting creates several destination files using the contents of a single source file. The source file is not affected by this function.

Concatenation is the process when several source files are to be copied into one destination file. The source files are not affected.

3. ASCL Best Practices for Cyber Forensics

Asian School of Cyber Laws (ASCL) Best Practices for Cyber forensics provide guidelines on the **collection and archival of digital evidence** for cyber crime and incident response purposes. A systematic and correctly followed procedure for digital evidence collection and archival enhances the probability of success of prosecution.

All through the various stages of evidence collection and archival, detailed notes should be kept of the steps being taken. A detailed note should be, as far as possible, chronological and contain the exact time of various procedures and then authenticated by the person conducting the investigation.

The **chain of custody** must be well documented and maintained. Someone should always be accountable for possessing any piece of evidence in his custody and there should be some physical proof of this custody.

Practically speaking, this would imply that a police officer or an investigator will take a piece of evidence into his custody, document this custody and only then hand it over to a clerk for safe storage.

Just as the police officer has documented the custody of the evidence, similarly every time the evidence changes hands, from the collection of the evidence to its presentation in a court, it must be properly documented.

3.1 Guidelines for Evidence collection

- (1) The system configuration (including the system and application software programs installed) should be accurately captured.
- (2) If specialized software is being used to record dates and times, then the resultant file should be stored on a media that is not a part of the original evidence.
- (3) Documentation (notes, printouts etc) should contain the time at which a particular document was made and should be authenticated by the person creating the document. Any difference between the system time and the actual time should be noted and the time zone whether ahead or behind GMT should be indicated on the document itself [e.g. Indian Standard Time (IST) is 5½ hours ahead of Greenwich Mean Time (GMT)].
- (4) It is natural for electronic information to undergo changes as it is being collected. Certain changes may only relate to access time of files and directories rather than the information contained in any file. Even then due care must be taken to see that such changes are minimal.

(5) As far as possible, procedures should be automated with minimum human intervention. These procedures should be easily implemented. This can be confirmed by subjecting such procedures to prior testing.

(6) Collection of evidence should be methodical and systematic. The task should be divided among the members of a team to reduce time taken.

(7) Collection of evidence should be in such a manner that it is collected from storage media before such evidence is lost. Collection should start from the most volatile storage medium moving on to the least volatile medium.

A computer system stores information in the following decreasing order of volatility.

- (a) Registers and cache memory
- (b) Routing tables, Address Resolution Protocol cache, process table and Operating System statistics
- (c) Temporary file systems
- (d) Hard disk drive
- (e) Remote logging and monitoring data with respect to the system being examined
- (f) Information relating to physical configuration and network topology
- (g) Archival media

(8) Since accessing a file changes its access time each time it is accessed, any forensic examination of a file should be done on a copy of the file instead of the original file. A bit-wise image of the file is considered as the most authentic copy of the file for forensic examination.

(9) Important steps in the collection of evidence are:

- (a) It is important to determine the relevance of the evidence being collected. The following factors should be kept in mind while collecting evidence from a computer system. (i) Admissibility of the evidence in a court of law (ii) Genuineness of the evidence (iii) Entirety of the evidence (iv) Reliability of the evidence.
- (b) The order of volatility for each computer system is different. This order should be ascertained for each system before starting to collect evidence.
- (c) Any possibilities of change in information contained in a system under examination, as far as possible, have to be removed.

- (d) The use of software tools for evidence recovery should be according to the order of volatility determined for the system.
 - (e) Each step taken for evidence recovery should be documented.
 - (f) The evidence collected should be mathematically authenticated and signed so that the chain of custody is easily established and the veracity of the evidence is preserved.
- (10) Precautionary measures for evidence collection are
- (a) A computer system being examined for evidence should be shutdown only when evidence collection is complete. This is to avoid execution of small software programs that might have been installed by the suspect, which may destroy information during the start-up or shutdown process.
 - (b) Forensic software utilities should be executed not from the system but from a write protected storage medium. Don't trust the programs on the system. Ideally, programs that change the access times of files and directories should be avoided.
 - (c) Before a system is taken off a network or disconnected from the Internet, it is important to verify the existence of software triggers that detect such disconnection and wipe evidence.

3.2 Guidelines for Evidence archival

The following guidelines should be followed for archiving evidence.

- (1) The collected evidence must be archived in a manner that rules out any possibility of tampering.
- (2) Digital Hash functions such as MD5 or SHA-1 should be used to prove the integrity of the digital evidence.

Hash functions are used for mathematical authentication of data. A one-way hash function takes variable-length input — say, a message of any length — and produces a fixed-length output; say, 160-bits. The hash function ensures that, if the information is changed in any way — even by just one bit — an entirely different output value is produced.

The table below shows some sample output values using SHA-1 (Standard Hash Algorithm 1):

sanya	c75491c89395de9fa4ed29affda0e4d29cbad290
Sanya	4c391643f247937bee14c0bcc9ffb985fc0d0ba
sAnya	ed7e05ab380e4142f0f100332c8ab633b57a532c
SANYA	33fef490220a0e6dee2f16c5a8f78ce491741adc

[To use SHA please visit: www.asianlaws.org/sha]

It can be seen from the table above that the hash value for **sanya** is
c75491c89395de9fa4ed29affda0e4d29cbad290

while the hash value for **Sanya** is
4c391643f247937bee14c0bcc9ffb985fc0d0ba

By changing the input from **sanya** to **Sanya**, an entirely different hash value is generated. What must be kept in mind is that irrespective of the size of the input, the hash output will always be of the same size. Two things must be borne in mind with regard to one-way hash functions:

- (a) It is computationally infeasible to find two different input messages that will yield the same hash output.
 - (b) It is computationally infeasible to reconstruct the original message from its hash output.
- (3) The chain of custody through which the evidence has passed should be properly documented in such a manner that such documentation would reveal the location, collection and subsequent handling of the evidence.
- Documentation of Chain of custody means documentation of the following.
- (a) Where, when, and by whom was the evidence discovered and collected?
 - (b) Who had custody of the evidence and during what period?
 - (c) How was it stored?
 - (d) When the evidence changed custody, when and how did the transfer occur?
- (4) High quality DVDs or CDRs (Compact Disc-Recordable) are preferable to CDRW (Compact Disc Re-Writable) for archiving evidence. After archival, access to the digital evidence should be entirely need based and documented in a manner, which makes it possible to detect any unauthorized access.

3.3 Guidelines for Hard disk examination

The following procedures must be followed for examining computer hard disks.

- (1) The media used for the examination process should be virus free.
- (2) The original media should not be used for the examination. Only a bit-stream image of the original hard disk should be used. The bit-stream image should be taken in a non-invasive manner.
- (3) The bit-stream image should be verified by MD-5 or SHA-1 hash value.

- (4) The boot record data, command files such as the CONFIG.SYS file and the AUTOEXEC.BAT should be examined.
- (5) All recoverable deleted files should be restored.
- (6) All the files contained on the hard disk should be listed.
- (7) The unallocated storage space and slack space should be examined.
- (8) Attempts should be made to decrypt password-protected files.

3.4 Guidelines for USB drive / floppy disk examination

The following procedures must be followed for examining floppy disks:

- (1) The media used for the examination process should be virus free.
- (2) A duplicate image of the original floppy disk should be made on another floppy disk.
- (3) A copy of the original floppy disk should be logically examined and all information contained therein should be documented.
- (4) All recoverable deleted files should be restored.
- (5) All the files contained on the floppy disk should be listed.
- (6) The unallocated space and slack space should be examined.
- (7) Attempts should be made to decrypt password-protected files.

3.5 Using Forensic software

The CD accompanying this book contains a step-by-step guide to using the Winhex, Trace and dtSearch software. The trial versions of the software are also included in the CD.

11. Password Breaking

1. Breaking file passwords

File passwords are usually considered an effective method of protecting the information kept in a file. In most computer investigations, the investigator would be required to confront password-protected files (usually Word and WinZip files).

There are two primary ways of password recovery / cracking:

- (1) The Dictionary attack attempts to check the file password against any predefined set of words. This set may be a set of Indian names, a set of Russian names, a set of names of different breeds of dogs, a set of words from the English language etc.
- (2) The brute force attack checks the password of the file against every possible combination of alphabets, numbers, special symbols and spaces, till it retrieves the password. This implies that a brute force attack, although it may take longer to crack a password, cannot fail (if the range is specified accurately).

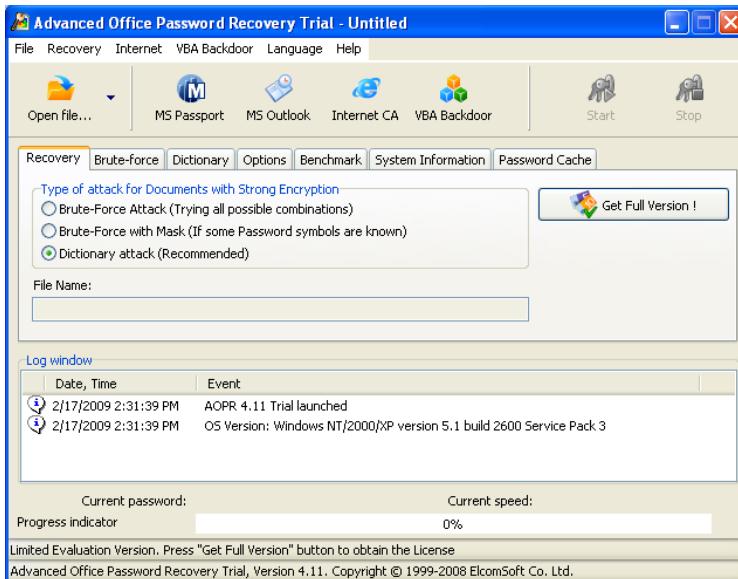
1.1 Using Advanced Office Password Recovery software

The trial version of Advanced Office Password Recovery software (AOPR) is provided in the CD accompanying this book. The software can also be downloaded from www.elcomsoft.com

AOPR can be used for recovering passwords for the following applications:

1. Microsoft® Word®
2. Microsoft® Excel®
3. VBA Project Password
4. Microsoft® Access®
5. Microsoft® Outlook®
6. Microsoft® PowerPoint®
7. Microsoft® OneNote®
8. Microsoft® Visio®
9. Microsoft® Project®
10. Microsoft® Money
11. Microsoft® Backup
12. Microsoft® Schedule+
13. Microsoft® Mail
14. Microsoft® Internet Explorer
15. All Applications with VBA

The main interface of the software is illustrated below:



Let us assume that we have a password protected Microsoft® Word® document titled “Secret-1.doc”. To break the password, the first step is to click on “Open File” in the main interface and then browse to the relevant document. If the password is simple (in this case it is *abc*), it is immediately recovered by AOPR, as illustrated below:



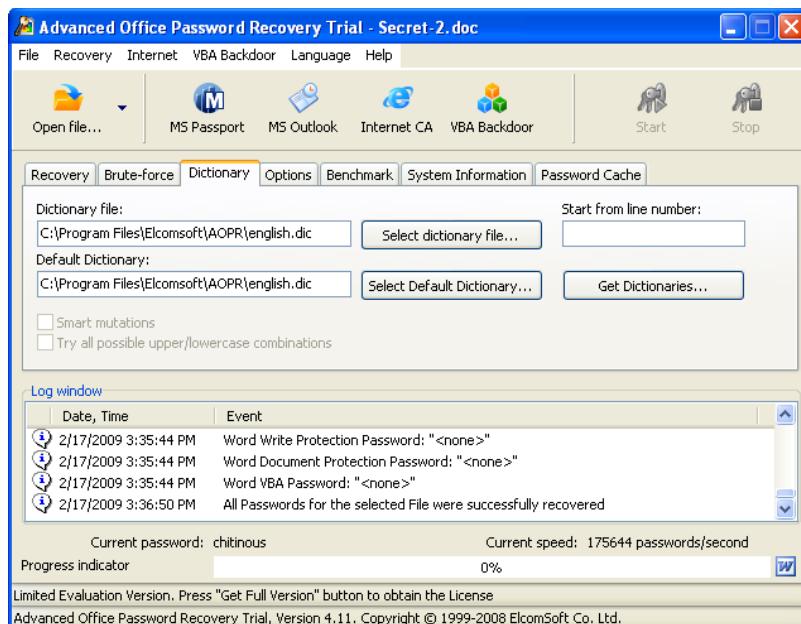
Dictionary Attack

As discussed earlier, the dictionary attack attempts to check the file password against any predefined set of words. This set may be a set of Indian names, a set of Russian names, a set of names of different breeds of dogs, a set of words from the English language etc.

A large collection of dictionaries is provided in the CD accompanying this book.

To configure the dictionary to be used for a particular attack, click on the “**Dictionary**” tab in the main interface.

This is illustrated below:



Let us presume that we have a password protected Microsoft® Word® document titled “Secret-2.doc”. To break the password, the first step is to click on “**Open File**” in the main interface and then browse to the relevant document. Once the dictionary attack is complete and if the password is recovered, it will be displayed as illustrated below:



In the dictionary attack, you can select an option "**Smart mutations**" or "**Try all possible upper/lower case combinations**". For example, let's assume that the next word in dictionary is «PASSword» (the case, actually, doesn't matter here). With the second option enabled, the program will just try all possible combinations, like:

password
passworD
passwoRd
password
passwOrd

...

PASSWORD
PASSWORD

However, checking all such combinations takes a lot of time: in the example above, the program will check 2^8 words (i.e. 256) instead of one. With Smart Mutations, you can eliminate a number of "virtually impossible" combinations, and here are all the words which will be checked:

PASSword	(as is)
passWORD	(reversed)
password	(all lower case)
PASSWORD	(all upper case)
Password	(first uppercase, rest lowercase)
pASSWORD	(first lower case, rest uppercase)
PaSSWoRD	(elite: vowels in lc, others in uc)
pAsswOrd	(noelite)
PaSsWoRd	(alt/1)
pAsSwOrD	(alt/2)

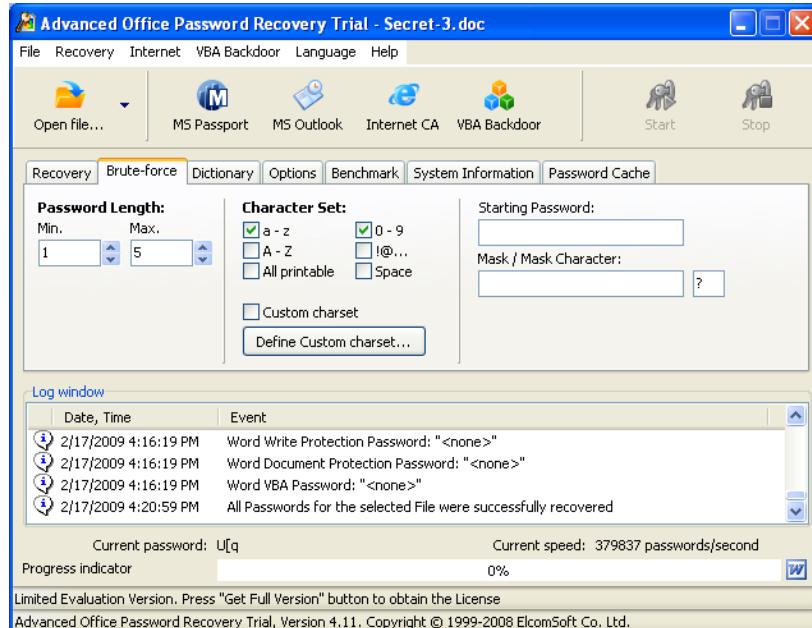
So, it makes only 10 combinations for each word.

Brute Force Attack

As discussed earlier, a brute force attack checks the password of the file against every possible combination of alphabets, numbers, special symbols and spaces, till it retrieves the password. This implies that a brute force attack, although it may take longer to crack a password, cannot fail (if the range is specified accurately).

Click on the “Brute-force” tab in the main interface.

This is illustrated below:



A brute-force attack will try all possible characters combinations in the specified Range. The Range is defined by Password Length and Brute-Force Range Options.

AOPR allows you to set a **Password Length** range by defining the Minimal and Maximal Length. These values can be set using the "Password Length" controls at the "Brute-Force" tab. The minimal length cannot be set to a value greater than maximal one. In this case the appropriate error message will be displayed.

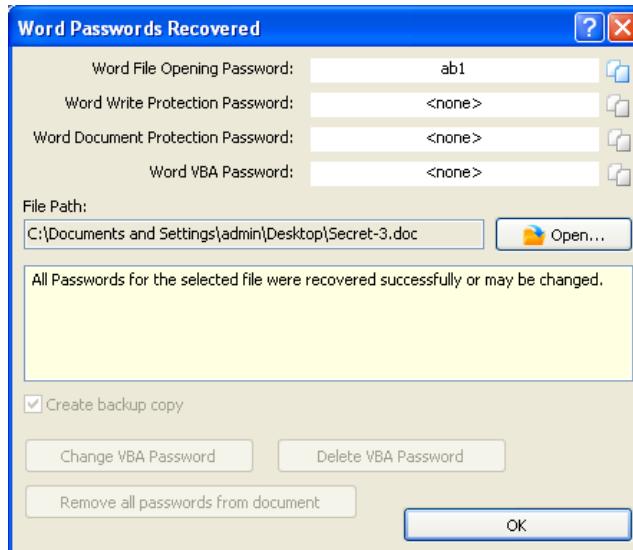
If the Minimum password length and Maximum password length is not the same, the program tries the shorter passwords first. For example, if you set Minimal=3 and Maximal=7, the program will start from 3-character Passwords, then try 4-character ones and so on -- up to 7. While AOPR is running, it shows the current Password Length, as well as the current Password, Average Speed, Elapsed and Remaining Time, and Total and Processed number of passwords (some of these Parameters are displayed in the "Extended Statistics" Dialog).

In MS Office documents passwords may contain the following Characters: Latin letters (both small and capital), digits, special symbols (like @, #, \$ etc) and national languages symbols. You can select these Ranges separately, or define your own **Password Range**. To define your own range, check the box "Custom charset" and press the "Custom charset..." button.

The Predefined Passwords Ranges contain the following Characters:

- "a - z": abcdefghijklmnopqrstuvwxyz
- "A - Z": ABCDEFGHIJKLMNOPQRSTUVWXYZ
- "0 - 9": 0123456789
- "!@...": (special characters): !@#\$%^&*()_+=<>,./?[]{}~:;`|"\`
- "All Printable": contains all Ranges defined above

Let us presume that we have a password protected Microsoft® Word® document titled “Secret-3.doc”. To break the password, the first step is to click on “**Open File**” in the main interface and then browse to the relevant document. Once the brute-force attack is complete and the password is recovered, it will be displayed as illustrated below:



Brute-Force with Mask

This attack is useful when you remember a part of the password. For example if you remember that length of your password was 5 characters and password begins from "A", you can define the mask "A?????" and save the time by trying 4 symbols instead of 5. A Password Mask must be defined to use this Attack.

If you already know some characters in the Password, you can specify the Mask to decrease the total number of passwords to be verified. At the moment, you can set the Mask only for fixed-length Passwords, but doing this can still help.

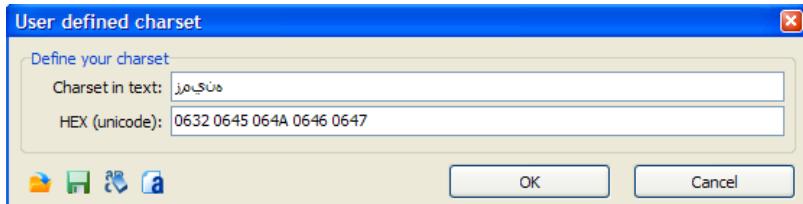
For example, you know that the Password contains 8 characters, starts with 'x', and ends with '99'; the other symbols are small or capital letters. So, the Mask to be set is "x?????99", and the charset has to be set to All caps and All small. With such options, the total number of the passwords that AOPR will try will be the same as if you're working with 5-character passwords which don't contain digits; it is much less than if the length were set to 8 and the All Printable option were selected. In the above example, the '?' characters indicate the unknown symbols.

If you know that the Password contains an occurrence of the Mask character '?', you can choose a different Mask Character to avoid having one character, '?', represent both an unknown pattern position and a known character. In this case, you could change the Mask Symbol from

'?' to, for example, '#' or '*', and use a mask pattern of "x#####?" (for mask symbol '#') or "x*****?" (for mask symbol '*').

The Mask and Mask Symbol can be defined in the "Mask / Mask Character" control at the "Brute-Force" tab.

You can define your own Character Set for the Brute-Force Attack. Click the "Define Custom Charset" button at the "Brute-Force" tab. The following Dialog will appear:



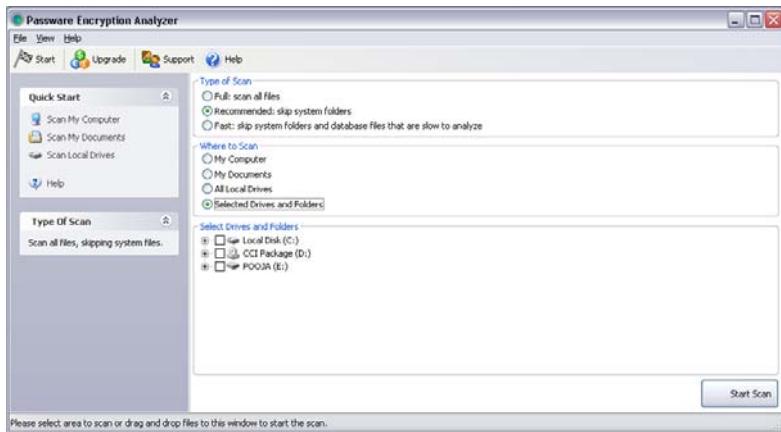
You can enter the Custom charset either in text and HEX format. In HEX format the Unicode symbols must be separated by Spaces. You can Load, Save, Clear and Add Charset by pressing the corresponding buttons. After entering the Charset AOPR checks for duplicate characters and removes it automatically.

The following charsets are included in AOPR distribution: Arabic (all Arabic symbols according to Unicode standard), Armenian, Czech (split to caps and small letters), French (split to caps and small letters), German (split to caps and small letters), Greek (all symbols according to Unicode standard), Greek (letters only), Hebrew, Japanese (Katakana), Japanese (Hiragana), Korean (Hangul Jamo) and Russian (Cyrillic).

1.2 Using Encryption Analyzer

The free version of Passware Encryption Analyzer is provided in the CD accompanying this book. The software can also be downloaded from www.lostpassword.com

The main interface of the software is illustrated below:



Encryption Analyzer is used to scan a computer (or a network) to locate all the password protected and encrypted files.

Type of Scan

Encryption Analyzer offers three types of scans. Which one you use depends on what type of password-protected file you are looking for, and how fast you want the scan to run.

<i>Scan Type</i>	<i>When to use</i>
Fast	Since this scan skips system folders and files with unknown extensions, it is appropriate when you know the file is not a system file, and you're sure the file type resides in the Windows Registry.
Recommended	This scan will find most password-protected files, unless the file type is not registered with Windows.
Full	Use this scan if you are not sure if you need to scan system files and you're not sure if the file type is registered with Windows.

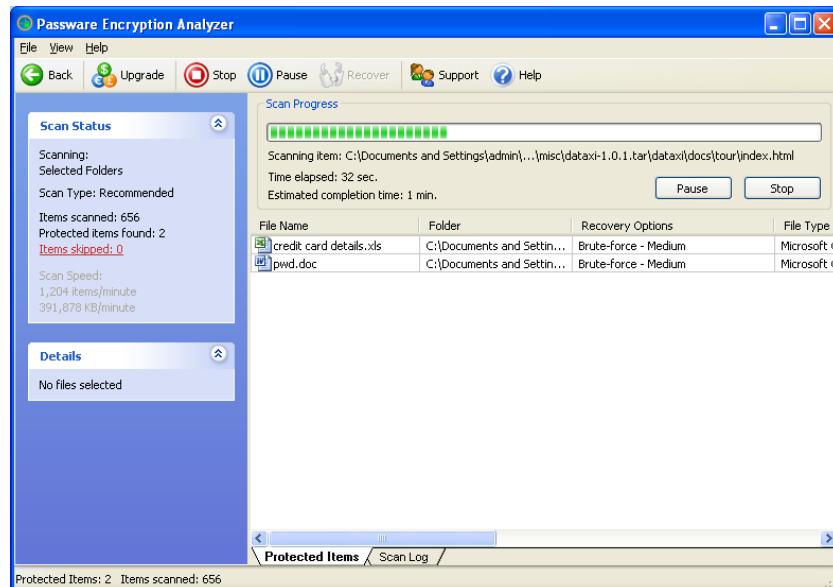
Choosing What to Scan

Encryption Analyzer is flexible - it allows you to limit your scan to a single drive or folder, or to scan your entire computer system.

During a scan, Encryption Analyzer keeps you up-to-date as to the progress of the scan in several ways:

The Scan Progress area at the top of the main window displays a graphical progress bar, and lists time elapsed and time-to-completion.

A sample Scan Progress area is shown here:



Once the scan is over, Encryption Analyzer displays both - a list of password-protected files (in the right pane of the window) and a summary of the scan results (in the Last Scan area on the left side of the window).

A sample scan result is shown below:

File Name	Folder	Recovery Options	File Type	Document Type	Protection Flags
credit card details.xls	C:\Documents and Settings\...	Brute-force - Medium	Microsoft Office Excel 97-2003 ...	MS Excel 2000/97	Open Password
pwd.doc	C:\Documents and Settings\...	Brute-force - Medium	Microsoft Office Word 97 - 2003 ...	MS Word 2003	Open Password
rec.moodle.zip	C:\Documents and Settings\...	Brute-force - Slow	Compressed (zipped) Folder	Zip 2.0	Extraction Password, AES Encryption
rec.moodle.zip	C:\Documents and Settings\...	Brute-force - Slow	Compressed (zipped) Folder	Zip 2.0	Extraction Password, AES Encryption
Secret-1.doc	C:\Documents and Settings\...	Brute-force - Medium	Microsoft Office Word 97 - 2003 ...	MS Word 97	Open Password
Secret-2.doc	C:\Documents and Settings\...	Brute-force - Medium	Microsoft Office Word 97 - 2003 ...	MS Word 97	Open Password
Secret-3.doc	C:\Documents and Settings\...	Brute-force - Medium	Microsoft Office Word 97 - 2003 ...	MS Word 97	Open Password
Secret-4.doc	C:\Documents and Settings\...	Brute-force - Medium	Microsoft Office Word 97 - 2003 ...	MS Word 97	Open Password
Secret-doc.doc	C:\Documents and Settings\...	Brute-force - Medium	Microsoft Office Word 97 - 2003 ...	MS Word 97	Open Password
Secret.doc	C:\Documents and Settings\...	Brute-force - Medium	Microsoft Office Word 97 - 2003 ...	MS Word 97	Open Password

The 'Last Scan' panel on the left shows 'Actions' like 'Save File List' and 'Start a New Scan'. It also displays 'Selected Folders' with 'Scan Type: Recommended' and 'Scan Time: 59 sec.'. The 'Scan Status' section shows 'Items scanned: 2,030', 'Protected items found: 9', and 'Items skipped: 4'. The 'Details' panel indicates 'Scan Speed: 2,438 items/minute'.

Clicking on the “Items skipped” option in the left pane above displays a list of files that have been skipped by Encryption Analyzer. It also shows the reasons for skipping the file e.g. the file is damaged. This is illustrated below.

Type	Time	Item	Details	File Type	Folder
Information	2/19/2009 6:08:57 AM	credit card details.xls	Protected item found	MS Excel 98/97...	C:\Documents and Setti...
Information	2/19/2009 6:09:17 AM	TOCQ.xls	Protected item found	Microsoft Office Excel 97-2...	C:\Documents and Setti...
Warning	2/19/2009 6:09:21 AM	FCAGLJ_1.xls	File damaged	Microsoft Word document	C:\Documents and Setti...
Information	2/19/2009 6:09:24 AM	gvd.doc	Protected item found	MS Word 2003	C:\Documents and Setti...
Information	2/19/2009 6:09:25 AM	transacted15.zip	File damaged	Zip Unknown	C:\Documents and Setti...
Warning	2/19/2009 6:09:32 AM	sec module.zip	Protected item found	Zip 2.0	C:\Documents and Setti...
Information	2/19/2009 6:09:32 AM	Thumbs.db	Skipped	Data Base File	C:\Documents and Setti...
Information	2/19/2009 6:09:33 AM	Thumbs.db	Skipped	Data Base File	C:\Documents and Setti...
Information	2/19/2009 6:09:36 AM	Thumbs.db	Skipped	Data Base File	C:\Documents and Setti...
Information	2/19/2009 6:09:43 AM	Secret1.doc	Protected item found	MS Word 97	C:\Documents and Setti...
Information	2/19/2009 6:09:47 AM	Secret2.doc	Protected item found	MS Word 97	C:\Documents and Setti...
Information	2/19/2009 6:09:47 AM	Secret3.doc	Protected item found	MS Word 97	C:\Documents and Setti...
Information	2/19/2009 6:09:47 AM	Secret4.doc	Protected item found	MS Word 97	C:\Documents and Setti...
Information	2/19/2009 6:09:47 AM	secret.doc.doc	Protected item found	MS Word 97	C:\Documents and Setti...
Information	2/19/2009 6:09:47 AM	Secret4.doc	Protected item found	MS Word 97	C:\Documents and Setti...
			Scan complete		

1.3 Using Passware Kit Enterprise

The demo version of Passware Kit Enterprise is provided in the CD accompanying this book. The software can also be downloaded from www.lostpassword.com

The software supports the following files:

1. ACT!
2. Acrobat
3. BestCrypt
4. FileMaker
5. ICQ
6. Lotus 1-2-3
7. Lotus Notes
8. Lotus Organizer
9. Lotus WordPro
10. MS Access
11. MS Backup
12. MS Excel
13. MS Mail
14. MS Money
15. MS OneNote
16. MS Outlook
17. MS Pocket Excel
18. MS PowerPoint
19. MS Project

20. MS Schedule+
21. MS SQL
22. MS Word
23. MYOB
24. Norton Backup
25. Paradox
26. PeachTree
27. Quattro Pro
28. QuickBooks
29. Quicken
30. RAR
31. Remote Desktop Connection
32. VBA
33. WordPerfect
34. Zip

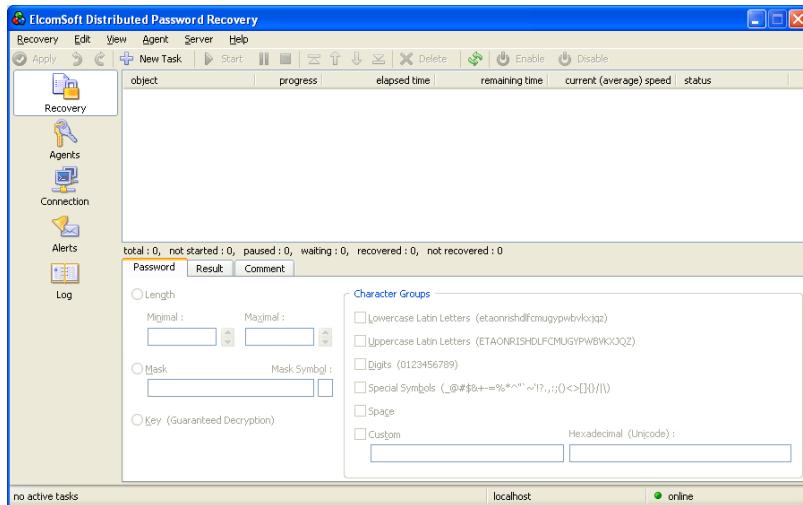
1.4 Using EDPR

Elcomsoft Distributed Password Recovery (EDPR) supports the following applications and file formats:

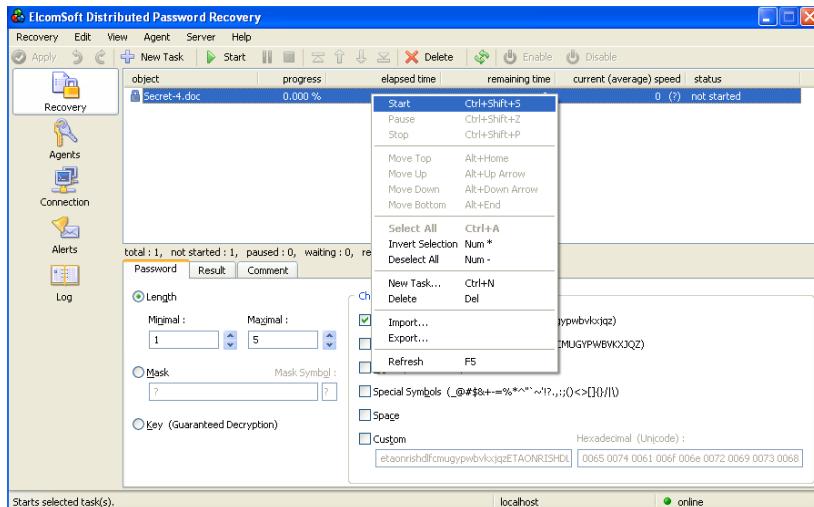
- Microsoft Word/Excel/PowerPoint XP/2003 (.DOC, .XLS)
- Microsoft Word/Excel 97/2000 (.DOC, .XLS) (password recovery - "open" password only)
- Microsoft Word/Excel 97/2000 (.DOC, .XLS) (guaranteed decryption)
- Microsoft Money (.MNY, .MBF) (password recovery)
- Microsoft OneNote (.ONE) (password recovery)
- PGP zip archives (.PGP) (password recovery)
- PGP secret key rings (.SKR) (passphrase recovery)
- PGP disks with conventional encryption (.PGD) (password recovery)
- PGP self-decrypting archives (.EXE) (password recovery)
- PGP Whole Disk Encryption (.WDE) (password recovery)
- Personal Information Exchange certificates - PKCS #12 (.PFX, .P12) (password recovery)
- Adobe Acrobat PDF with 128-bit encryption ("user" and "owner" password recovery)
- Adobe Acrobat PDF with 40-bit encryption ("user" and "owner" password recovery)
- Adobe Acrobat PDF with 40-bit encryption (guaranteed decryption)
- Windows Logon LM/NTLM passwords
- Intuit Quicken (.QDF) (password recovery)
- Lotus Notes (.ID, ADMINDATA.XML) (password recovery)
- MD5 Hashed Password (.MD5) (password recovery)

The trial version of this software is provided to you in the CD accompanying this book.

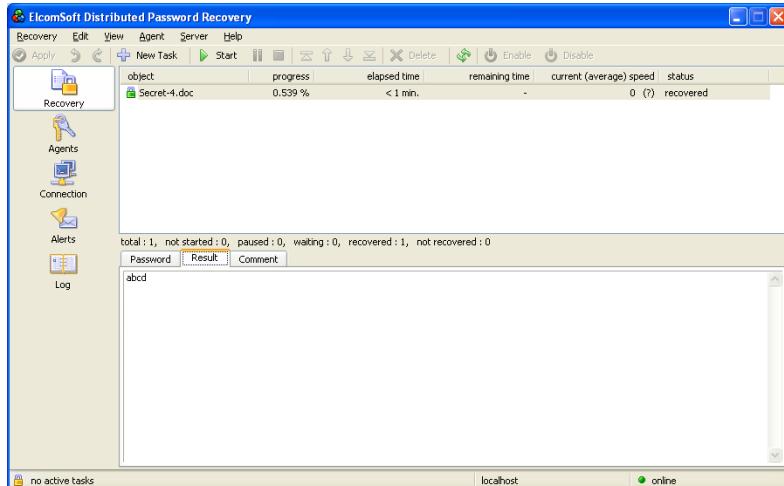
The main interface of the “server” console of this software is illustrated below:



Let us presume that we have a password protected Microsoft® Word® document titled “Secret-4.doc”. To break the password, the first step is to click on “New Task” in the main interface and then browse to the relevant document. Then right-click on the document and click on “Start” as illustrated below:



Once the password is cracked, it is displayed as illustrated below:



1.5 Using Decryptum

www.Decryptum.com is the first instant online Microsoft Excel and Microsoft Word password recovery and removal service. Decryption time is a few seconds, regardless of password length.

The main interface of the website is illustrated below:

A screenshot of the Decryptum website. The top navigation bar includes links for About Decryptum, Try, Buy, FAQ, and Support, along with language selection buttons. The main content area features a large graphic of a document with a 'W' logo and the text 'Lost password for MS Word/Excel document?.. Decrypt it!'. In the center, there are two main buttons: 'START DECRYPTION' with a play icon and 'DOWNLOAD YOUR FILE' with a download icon. To the right, a sidebar lists features like 'Easy online password recovery', 'Instant decryption - works in seconds, regardless of file password', 'Free preview', 'Secure service - all file submissions are encrypted by SSL protocol', and 'No software to download - service is web-only'. At the bottom, sections include 'What is Decryptum?' (explaining it's an online service), 'How to proceed?' (instructions for upload and download), 'News' (with links to recent press releases), and 'Our Customers Say' (a testimonial section). A 'DECRYPTUM GUIDE' link is also present.

Decryptum is not a free service. However, it displays the first few lines of the password protected file for free.

Once you have verified that your file can actually be cracked by Decryptum, you can purchase a credit for cracking the file. After that Decryptum allows you to download a non-password protected copy of the file.

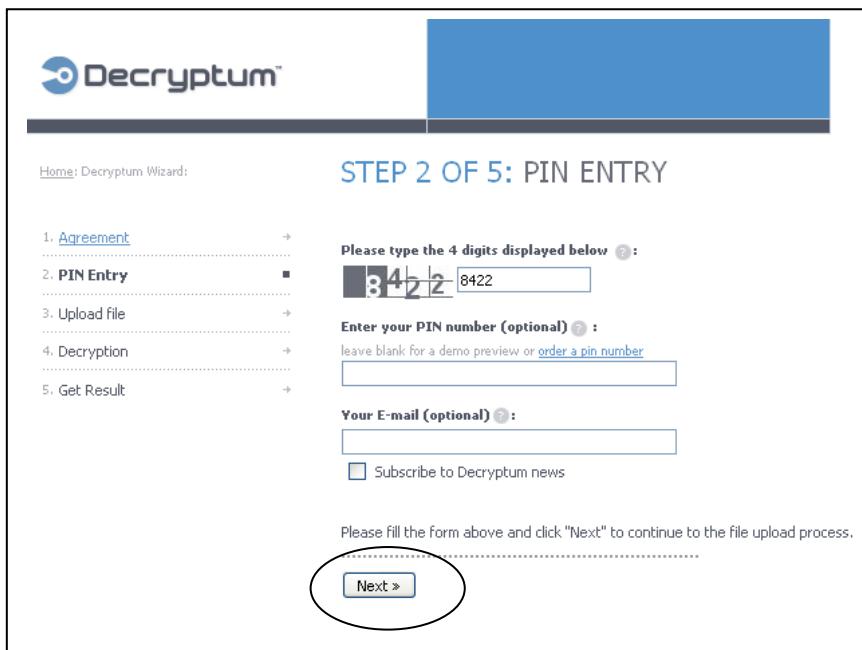
Note: Decryptum does not recover the password of the file. It cracks the file and creates a non password protected copy of the file.

To use Decryptum, click on “**Start Decryption**” in the screen above. The following screen will open up:

The screenshot shows the 'Decryptum Wizard' interface. At the top, there's a navigation bar with tabs: Home, Decryptum Wizard, and a third tab which is partially visible. Below the navigation bar, the title 'STEP 1 OF 5: SERVICE AGREEMENT' is centered. To the left, a sidebar lists five steps: 1. Agreement (selected), 2. PIN Entry, 3. Upload file, 4. Decryption, and 5. Get Result. Each step has a small arrow icon next to it. The main content area contains instructions for step 1: 'To decrypt your file please accept the Agreement below and follow these easy steps:' followed by a bulleted list of three items. Below this, a note says 'If you have any questions regarding Decryptum, please visit our [Frequently Asked Questions](#) or contact [Support](#)'. A section titled 'Service And Confidentiality Agreement:' follows, containing a detailed legal text about the agreement between the user and Passware Inc. A scroll bar is visible on the right side of this section. At the bottom of the page, there's a large oval containing a blue button labeled 'I agree >'. Above the 'I agree' button, a note says 'Please acknowledge that you have read, understand and agree to the above conditions. To use the service, click the "I agree" button.' There are also two small checkboxes at the very bottom of the page.

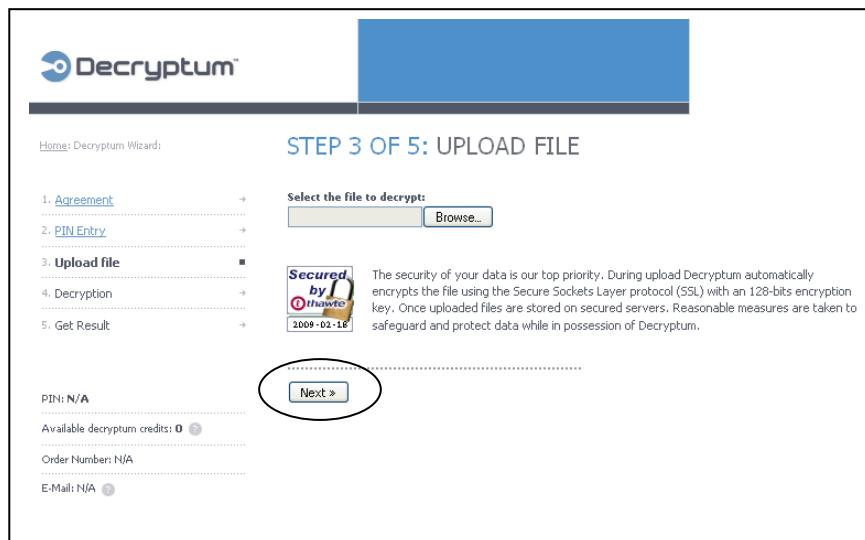
Click on “**I agree**”.

The following screen will open up:



The screenshot shows the 'Decrypturn' logo at the top left. Below it, a navigation menu on the left lists steps: 1. Agreement, 2. PIN Entry (which is selected and highlighted with a square icon), 3. Upload file, 4. Decryption, and 5. Get Result. To the right of the menu, the title 'STEP 2 OF 5: PIN ENTRY' is displayed in blue. A large blue rectangular area is present on the right side of the page. Below the title, there is a text field labeled 'Please type the 4 digits displayed below' with a question mark icon. Inside the field, the digits '8422' are entered. Below this, there is a text input field labeled 'Enter your PIN number (optional)' with a question mark icon, containing the placeholder text 'leave blank for a demo preview or [order a pin number](#)'. Further down, there is a text input field labeled 'Your E-mail (optional)' with a question mark icon, and a checkbox labeled 'Subscribe to Decrypturn news'. At the bottom, a note says 'Please fill the form above and click "Next" to continue to the file upload process.' Below this note is a 'Next >' button, which is circled with a red oval.

Enter the 4 digits and click on “Next”.



The screenshot shows the 'Decrypturn' logo at the top left. Below it, a navigation menu on the left lists steps: 1. Agreement, 2. PIN Entry (selected), 3. Upload file (highlighted with a square icon), 4. Decryption, and 5. Get Result. To the right of the menu, the title 'STEP 3 OF 5: UPLOAD FILE' is displayed in blue. A large blue rectangular area is present on the right side of the page. Below the title, there is a text input field labeled 'Select the file to decrypt:' with a 'Browse...' button to its right. To the right of this field, there is a small 'Secured by iThawte' logo with the text '2009-02-18'. Below the logo, a note states: 'The security of your data is our top priority. During upload Decrypturn automatically encrypts the file using the Secure Sockets Layer protocol (SSL) with an 128-bits encryption key. Once uploaded files are stored on secured servers. Reasonable measures are taken to safeguard and protect data while in possession of Decrypturn.' Below the logo, there is a 'Next >' button, which is circled with a red oval. At the bottom left, there are several status messages: 'PIN: N/A', 'Available decryptum credits: 0', 'Order Number: N/A', and 'E-Mail: N/A'.

Click on “**Browse**” and navigate to the file you want to crack. This file is then uploaded to the Decryptum servers and the following screen is displayed.

STEP 4 OF 5: PROCESSING FILE

Your file has been successfully uploaded and decryption has been started.

File **secret-doc.doc** is being processed now.
Decryption Job ID **50406-38018-24724-5839**

Warning! Please write down and keep Job ID confidential because this is the only authentication token required to download decrypted file from the server.

Processing your file.
This usually takes up to several minutes...

PIN: N/A
Available decryptum credits: 0

Order Number: N/A
E-Mail: N/A

Once the decryption is complete, the following screen is displayed:

STEP 5 OF 5: DEMO PREVIEW

SUCCESSFUL DECRYPTION!

File: **secret-doc.doc**
Decryption Job ID **50406-38018-24724-5839**

Partial content of your file:

File:secret-doc.doc

File passwords are usually considered an effective method of protecting the information kept in a file. In most computer investigations, the investigator would be required to confront password-protected files (usually)

...

Buy & Download

Need to decrypt more files? We have [discounts](#) for multiple credits.

Preview [another file](#) or [order PIN](#) to instantly download decrypted file.

PIN

We strongly recommend you to [delete the demo preview now](#).

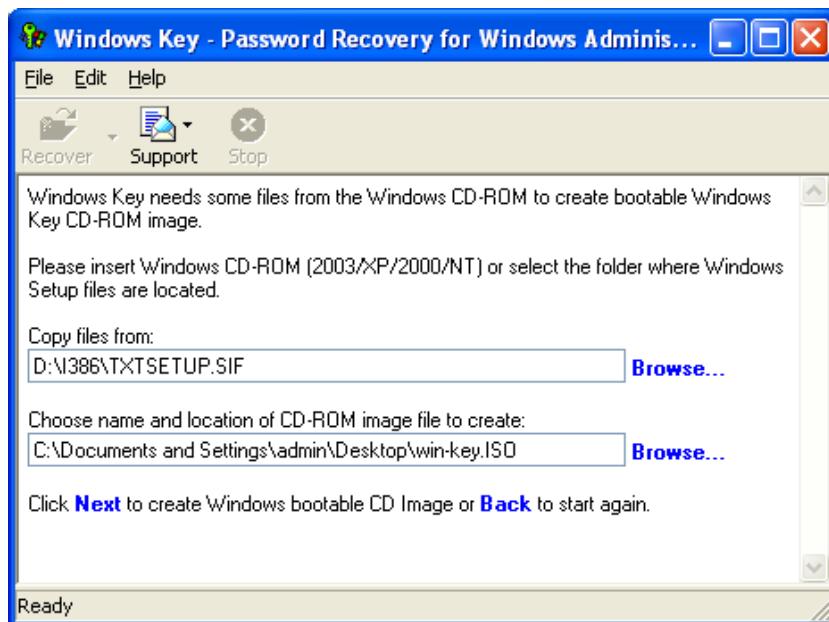
The demo preview displays the first few lines of the file, as illustrated above.

2. Breaking operating system passwords

Windows Key is an easy-to-use tool to gain access into any Microsoft Windows system if a login password is lost. The software allows you to reset passwords in a matter of minutes - no need to reinstall the system.

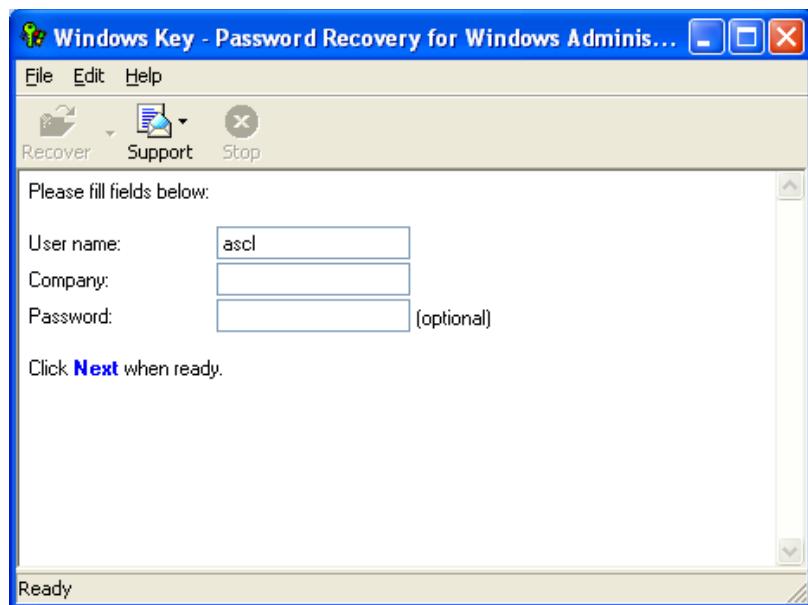
Windows Key creates a password reset CD, USB Flash Drive or a driver floppy that work during the boot process and instantly reset Administrator or other account passwords and Windows security settings that prevent you from logging in.

The main interface of the software is illustrated below:



Click on “**Next**” after you have selected the relevant options as illustrated above.

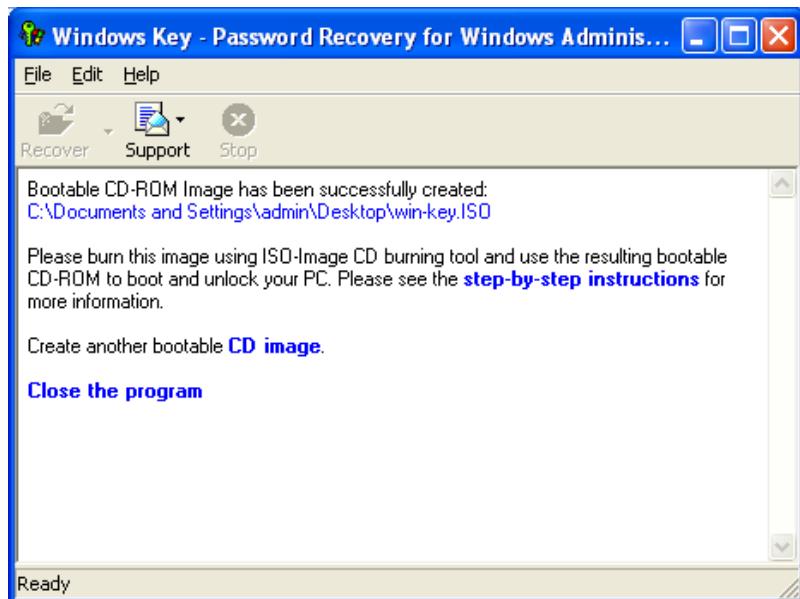
Enter the information in the next screen as illustrated below:



The progress will be displayed as illustrated below:



Once the process is complete, the following screen will be displayed:



Once the win-key.iso file is created, you will need to use the Nero Burning Rom software and select the "Recorder|Burn image" option. Browse for the WindowsKey.iso file. Press "OK".

If you use Roxio CD Creator, please select the "File|Record Disk from Image" option and browse for the WindowsKey.iso file. Press "OK".

Now the Windows Key bootable CD-ROM is ready. Follow the step-by-step guide below:

- (1) Reboot the computer (whose password you want to reset) with this CD-ROM.
- (2) Windows Setup process starts. After all the required files are loaded from the bootable CD, Windows Key starts working. It displays your license info and asks to enter the password that you set for the bootable CD.
- (3) Enter the password that you have set for the Windows Key bootable media.
- (4) Select the Windows installation to be unlocked.

- (5) Windows Key asks: "Undo Windows Key changes? (Y/N)". Press "N" if you want to reset the password or "Y" if you want to leave the original passwords and cancel the program changes.
- (6) Select the account to reset the password for (e.g. 'Administrator').
- (7) Windows Key asks: "Reset 'account_name' password? (Y/N)". Press "Y" to reset the password or "N" to leave the original password.
- (8) Windows Key asks: "Reset password for another account? (Y/N)". Press "Y" to reset password for another account or "N" to quit Windows Key.
- (9) Remove the Windows Key bootable media and restart your computer.

3. Handling Encrypted Files

A disturbing trend that is emerging nowadays is the increasing use of encryption, high-frequency encrypted voice/data links, Pretty Good Privacy (PGP) etc by terrorists and members of organized crime cartels.

Notable examples are:

- (1) Ramsey Yousef, who was behind the bombing of the World Trade Center in the USA in 1993 and an aircraft belonging to Manila Air in 1995.
- (2) Leary, who was sentenced to 94 years in prison for setting off fire bombs in the New York (USA) subway system in 1995. Leary had developed his own algorithm for encrypting the files on his computer.
- (3) The Cali cartel, which is reputed to be using sophisticated encryption to conceal their telephone communications, radios that distort voices, video phones which provide visual authentication of the caller's identity, and instruments for scrambling transmissions from computer modems.
- (4) The Italian mafia that uses PGP.

Strong encryption is the criminal's best friend and the investigator's worst enemy. If a criminal were to use 512-bit symmetric encryption, how long would it take to decrypt the information using brute force techniques? Suppose that every atom in the known universe (there are estimated to be 2^{300} of them) becomes a computer capable of checking 2^{300} keys per second, then it would take 2^{162} millennia to search 1% of the key space of a 512-bit key. The universe is believed to have come into existence less than 2^{24} years ago. The table below summarizes how long a brute force attack will take for various key sizes.

Key size (in bits)	1% of key size	50% of key space
56	1 second	1 minute
57	2 seconds	2 minutes
58	4 seconds	4 minutes
64	4.2 mins	4.2 hours
72	17.9 hours	44.8 days
80	190.9 days	31.4 days
90	535 years	321 centuries
108	140,000 millennia	8 million millennia
128	146 billion millennia	8 trillion millennia

3.1 How cryptography works

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

While cryptography is the science of securing data, **cryptanalysis** is the science of analyzing and breaking secure communication (breaching security measures).

Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers.

Cryptology embraces both cryptography and cryptanalysis.

A cryptographic algorithm, or **cipher**, is a mathematical function used in the encryption and decryption process. This mathematical function works in combination with a key — a very large number — to encrypt the plaintext (the original message).

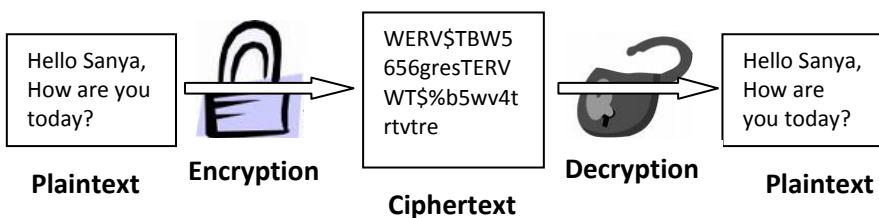
Data that can be read and understood without any special measures is called plaintext or clear text. Data which requires some special function to be performed on it before it can be read and understood, is called **cipher text**.

The same plaintext, encrypted by using different keys, will result in different cipher text. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a cryptosystem.

Encryption is used to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plaintext is called **decryption**.

The figure below illustrates the process of encryption and decryption.



The fundamental objective of cryptography is information security. Simply put, it is to ensure the following:

- (1) *Confidentiality* is used to keep the content of information secret from unauthorized persons. This is achieved through symmetric and asymmetric encryption.
- (2) *Data integrity* addresses the unauthorized alteration of data. This is addressed by hash functions.
- (3) *Authentication* is related to identification. This function applies to both entities and information itself. This is achieved through digital signature certificates and digital signatures.
- (4) *Non-repudiation* prevents someone from denying previous commitments or actions. This is achieved through digital signature certificates and digital signatures.

3.2 Keys

A key is a value that works with a cryptographic algorithm to produce a specific cipher text. Keys are basically very, very, very big numbers. Key size is measured in bits. In public key cryptography, the bigger the key, the more secure the cipher text. However, public key size and conventional cryptography's symmetric key size are totally unrelated.

The algorithms used for each type of cryptography are very different and are very difficult to compare.

Although the public and private keys are mathematically related, it is very difficult to derive the private key by analysing the public key (this is explained later in this chapter). Keys are stored by cryptographic software in an encrypted form. These files are called key rings.

The figure below illustrates a 512-bit RSA public key

```
3048 0241 00FC DBDF 80FA 0121 AD3F 8FFF B101 A19D 52E8  
A4A4 E79D E9A2 BE37 EFED 8126 8A03 7130 F4E2 3644 1BE0  
5CFE 613B 4400 CEE4 8E27 B971 ECCA 78C5 F714 FAE5 B2A2  
1E01 FF02 0301 0001
```

A 512-bit RSA public key

The figures below illustrate a 1024 bit RSA key pair generated using the PGP (Pretty Good Privacy) digital signature and encryption software.

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
IQHgBD5vDDEBBAC+UMHKr9YL1W0OYzL9gK/AERegEtzoFiveSzbeFQtNhxDIOSPJc60Y8v2n
TecI0R5Y6Z55uzakcPBZmTJ+kWrFR4NZPApiOFXhUrkHF0DmmrEpa5UpHjpO3sD+Hlvg84N6j
HjAIRMINMAYrg/e4i6ABGzAuxYbJCs6ax9mxdrFAQARAQABAwtDcK53Fr79Ss3v83ZR7g1DgF
fY3oo97XWbmJ02BdRGy/C+aluu3wMRNqmPo5w118VVCjIM02eqSr0+8mbLLX0Dwqbn33QiG
W34Upt6EI+f0ObKbjRi2Hc62813mi+jsskvQ8oavtSJL2/jxTEtL+wqvObcFxlsyjpH5N1wY7xQ5B
PSNjYLFZ99MXYcFhee14V2YdQv0pZFrJnvCQFWXLAIx1L9AH5DgwmXLtNCpBIQnRwyLPyW
SOT4yH8e6ibqBvhMphGe4WOAZQccHL6jjZrokVrBbu50Z6EqGFkzS8X6iygvSATOjr3L/X9EW7F
w098CcVK3iDB93peXR+U370nV+OfgXQqUzQ3SJ6vZwdlwy6cmjZOWmd/YrbGLOyyW+zFFS
ZFdiG480ELozMfMsqp3OJvElvhRgS/tbA/94jpOtzhWV9Du0pd7otCBBYmhpbmF2IEJoYXR0IDxh
YkBhc2lhbmxhd3Mu3JnP0B4AQ+bwwyAQQAQAmkqdApHtWspZdNfqeEROxctZKLxdvtXBnaO1J
1sS6jKjx2qGj3yxLrnW+N4QUAgm+eNNsTrqZZjJUP526dOTK8RmxV4QJeh2Q0bsLps6SXTIPw
fBWPPt+U/kfrSt8ZJF5IWROjaJG2hE3dBiussPa+6cJUDuQnYCVCHZARCKLcAEQEAAQPT8PB
QW4y8b4C7VbhjnGAATQliwRajv6uWmfUFcl+DPdtAZh3yb9EKWmS8vSkSnz+pWG1dEkuURyv
BGJMDxs/FB+CmoutQejhA11h05blas8HnoNPeqv1x9Xas+lr1j2AmfrLWwKEQAUH9di+d9DR
U6YHxy1ocIHZELXR9ECsSP0C1iSeujn+u4HLP3y4uBhcGRdhLRUJSCJ0tXd2meRAxw4dsZlD
Aeb21i2Tj+l0SngTEzFj8fSuvAxoXrv30gq5Vlbh5WdbJah5n688THMAUIUC5dIG8MMXMgmUe
887lwKEqSvLqCk5ymHmCdZiJQQEpAxVbXb9bkKs2UhxN1zRnug4OcR411XOqlvlBwsk121yY7
606mZ7r+icnXvLLEvezmegXsN8mlhAnb+p629HPZSMFOShgX3CwhlwTKDaMxZBft94Fk8w3l/
NBuwQJYg==Emf5
-----END PGP PRIVATE KEY BLOCK-----
```

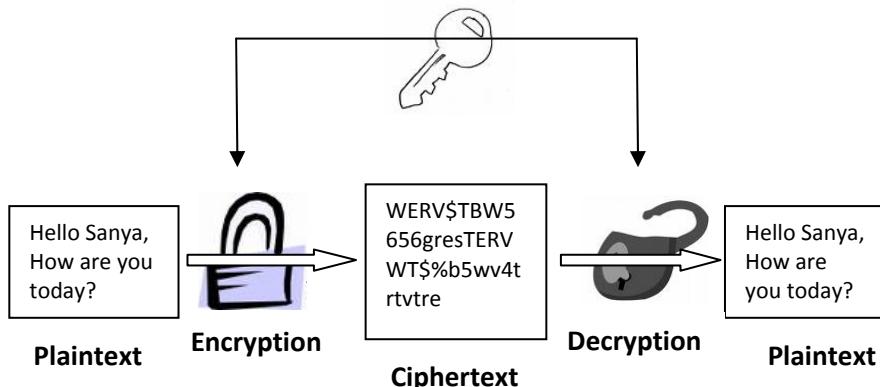
A 1024 bit RSA private key generated using the PGP (Pretty Good Privacy) digital signature and encryption software.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQCNCBD5vDDEBBAC+UMHKr9YL1W0OYzL9gK/AERegEtzoFiveSzbeFQtNhxDIOSPJc60Y8
v2nTecI0R5Y6Z55uzakcPBZmTJ+kWrFR4NZPapiOFXhUrkHF0DmmrEpa5UpHjpO3sD+Hlvg
84N6jHjAIRMINMAYrg/e4i6ABGzAuxYbJCs6ax9mxdrFAQARAQABtCBYmhpbmF2IEJoYXR
0IDxhYkBhc2lhbmxhd3Mu3JnP0AtAQQAQIAHgUCPm8MMQUJAeKFAAgLAwklBwlBCgIZA
QuBawAAAAAKCRDRPtuuStKFCIJwA/9t1Cjpi+hjVaWjJx1BZpoGv4b+t/Qb03J9ABFUatbyPU
X5jmMmCUT7h3TgiCgT5F4imvjm4+uCDeoHz0Uj+nPfvW8guMd805s/+3oU+FT4R2qYvEX6
MAQVex67TJ0pHvmiV55Mn/apNvTdvgsXJbQfHuza9u1QPEUm+LIVdOZx7kAjQQ+bwwyAQ
QAmkqdApHtWspZdNfqeEROxctZKLxdvtXBnaO1J1sS6jKjx2qGj3yxLrnW+N4QUAgm+eNNs
TrqZZjJUP526dOTK8RmxV4QJeh2Q0bsLps6SXTIPwfBWPPt+U/kfrSt8ZJF5IWROjaJG2hE3d
BiussPa+6cJUDuQnYCVCHZARCKLcAEQEAAyKaqAQYQAQIAEgUCPm8MMgUJAeKFAAUb
DAAAAAAKCRDRPtuuStKFCADiA/0csZOSY9Ztyvw2iVSJqf9g4u3z+ePmEcwy2RK5tuOXU2p
7HvEBMKeLIG9Dxg0xwy7cVvHejjAn4LxMPG9j26TinLCAfqHs7C1og8an1tHstrM4lcw7pWx5fl
RLiqQLqEc/RVFLBKU3nMAjgu0E9wjHicWFwsxUfeF5qD9kAsl0Og==kITT
-----END PGP PUBLIC KEY BLOCK-----
```

A 1024 bit RSA public key generated using the PGP (Pretty Good Privacy) digital signature and encryption software.

3.3 Symmetric Cryptography

In conventional cryptography, also called secret-key or symmetric-key encryption, the **same key is used both for encryption and decryption**. The figure below is an illustration of the conventional encryption process.



Caesar's Cipher

When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the “shift by 3” rule could decipher his messages.

For example, if we want to encode the word “SECRET” using Caesar’s key value of 3, we offset the alphabet so that the 3rd letter down, (D), begins the alphabet.

So starting with

ABCDEFGHIJKLMNOPQRSTUVWXYZ

and sliding everything up by 3, you get

DEFGHIJKLMNOPQRSTUVWXYZABC

where D=A, E=B, F=C, and so on.

Using this scheme, the plaintext, “SECRET” encrypts as “VHFUHW”. To allow someone else to read the cipher text, you tell him or her that the key is 3.

Conventional encryption has certain benefits. It is very fast. It is especially useful for encrypting data that is not to be transmitted anywhere. So, if you want to store information so that no one can read it without your authorization, it would be a good idea to use conventional encryption.

For a sender and recipient to communicate securely using conventional encryption, they must agree upon a key and keep it secret between themselves. If they are in different physical locations, they must trust a courier or some other secure communication medium.

This is to prevent the disclosure of the secret key during transmission. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all information encrypted or authenticated with that key.

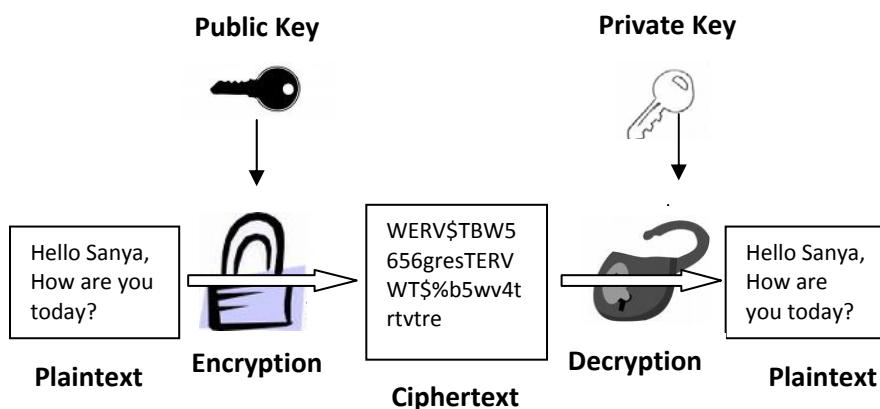
The persistent problem with conventional encryption is key distribution: how do you get the key to the recipient without someone intercepting it? The problems of key distribution in conventional encryption are solved by public key cryptography, a concept that was introduced by Whitfield Diffie and Martin Hellman in the U.S.A in the 1970s.

3.4 Asymmetric Cryptography

Public key cryptography is an asymmetric scheme that uses a pair of keys: a **public key**, which encrypts data, and a **corresponding private key**, or secret key for decryption.

Each user has a key pair given to him. The public key is published to the world while the private key is kept secret. Anyone with a copy of the public key can then encrypt information that only the person having the corresponding private key can read. It is **computationally infeasible to deduce the private key from the public key**. Anyone who has a public key can encrypt information but cannot decrypt it.

Only the person who has the corresponding private key can decrypt the information. The figure below illustrates the process of asymmetric encryption.



The primary benefit of public key cryptography is that it allows people who have no pre-existing security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared.

Some examples of public-key cryptosystems are ElGamal (named for its inventor, Taher ElGamal), RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman), Diffie-Hellman (named for its inventors), and DSA, the Digital Signature Algorithm (invented by David Kravitz).

Because conventional cryptography was once the only available means for relaying secret information, the expense of secure channels and key distribution relegated its use only to those who could afford it, such as governments and large banks. Public key encryption is the technological revolution that provides **strong cryptography to the masses**.

3.5 Hash function

A one-way hash function takes variable-length input – e.g a message of any length – and produces a fixed-length output; say, 160-bits. The hash function ensures that, if the information is changed in any way – even by just one bit – an entirely different output value is produced. The table below shows some sample output values using SHA (Standard Hash Algorithm)³⁰.

sanya	c75491c89395de9fa4ed29affda0e4d29cbad290
SANYA	33fef490220a0e6dee2f16c5a8f78ce491741adc
Sanya	4c391643f247937bee14c0bcc9ff985fc0d0ba

It can be seen from the table above that the hash value for **sanya** is
c75491c89395de9fa4ed29affda0e4d29cbad290
while the hash value for **SANYA** is
33fef490220a0e6dee2f16c5a8f78ce491741adc

³⁰ To use SHA please visit <http://www.asianlaws.org/sha>

By changing the input from **sanya** to **SANYA**, an entirely different hash value is generated. What must be kept in mind is that irrespective of the size of the input, the hash output will always be of the same size.

Two things must be borne in mind with regard to one-way hash functions:

- (1) It is computationally infeasible to find two different input messages that will yield the same hash output.
- (2) It is computationally infeasible to reconstruct the original message from its hash output.

3.6 Digital Signatures

A major benefit of public key cryptography is that it provides a method for employing digital signatures.

Digital signatures enable the recipient of the information to verify the authenticity of the information's origin, and also verify that the information is intact. Thus, digital signatures provide authentication and data integrity.

A digital signature also provides non-repudiation, which means that it prevents the sender from later claiming that he or she did not actually send the information. These features are every bit as fundamental to cryptography as privacy, if not more.

A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A digital signature is superior to a handwritten signature in that it is nearly impossible to counterfeit, plus it attests to the contents of the information as well as the identity of the signer.

Illustration: Sameer uses computer software to generate two keys, a public key and private key. These keys are nothing but extremely large numbers. Although the keys are mathematically related, it is almost impossible to obtain the private key by using the public key.

Sameer will give his public key to the whole world but will keep his private key to himself. Now Sameer wants to enter into a transaction with Pankaj. He composes an electronic document containing the words:

“I, Sameer, owe Pankaj the sum of Rs. 500 only.”

Using his computer Sameer runs this document through a hash function.

The hash function software produces a fixed length of alphabets, numbers and symbols for any document. This is known as the hash result. However, the contents of this fixed length are never the same for two different documents.

If even one letter in the document is altered, an entirely different hash result will be generated.

When using a particular hash function, the length of the output is always the same, whether the input document is one word or 1-lakh words. Moreover, the hash function software will always produce the same hash result for a particular message. It is practically impossible to reconstruct the original message from the hash result. That is why it is known as a one-way hash function.

Sameer now uses his computer to “sign” the hash result of his document. His computer software uses his private key to perform some calculations upon the hash result. This produces a signature, which consists of some digits. This set of digits is attached to the hash result.

Sameer now sends the original message and the signed message digest (hash result) to Pankaj. Pankaj has the same hash function software on his computer. He also has Sameer’s public key. When Pankaj receives Sameer’s email, he runs the original document through the hash function software and generates a hash result.

He compares this hash result with the one that was sent to him by Sameer. If the two hash results are the same, it means that the message is unaltered. Pankaj also verifies whether Sameer’s private key was actually used to sign the hash result. For this Pankaj’s computer uses Sameer’s public key. Only a message signed by Sameer’s private key can be verified using Sameer’s public key.

The public key and private key are basically two very large numbers that are mathematically related to each other. If a particular private key was used to “sign” a message, then only the corresponding public key will be able to verify the “signature”.

The digital signature creation and verification process achieves the following legal requirements:

Signer authentication: A person’s digital signature cannot be forged unless his private key is stolen. This means that if a digital signature can be verified by Sanya’s public key, then it must have been created by

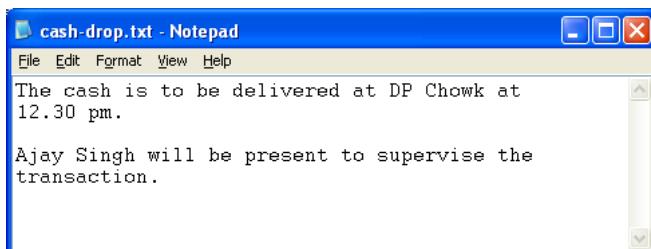
Sanya's private key. The digital signature verification process thus authenticates the identity of the signer.

Message authentication: A digital signature is based upon the hash value (or message digest) of the actual message. Thus a digital signature is unique for each message and automatically authenticates the message.

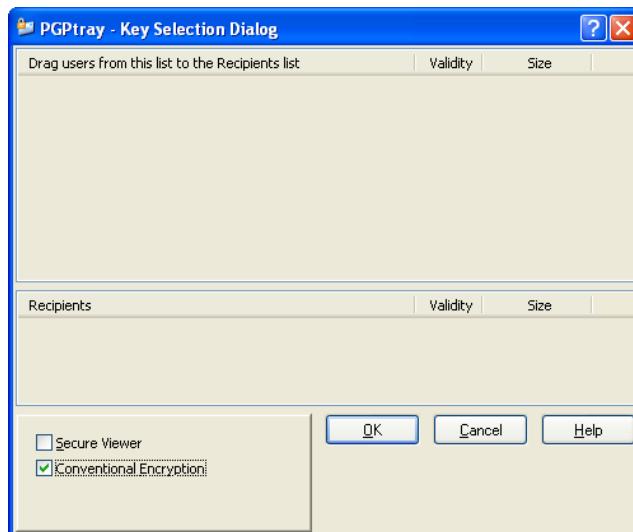
Affirmative act: The process of digital signature creation requires the signer to use his private key (usually by entering a password). This overt act alerts the signer that he is initiating a transaction that may have legal consequences.

3.7 Using PGP

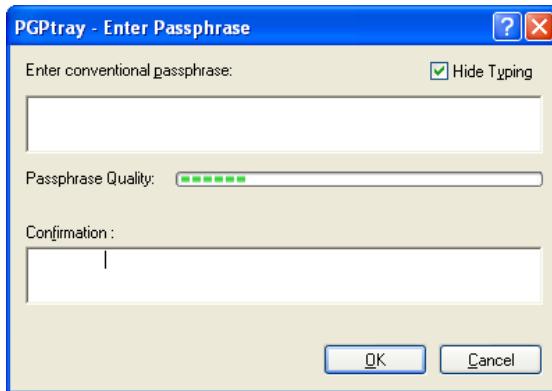
The trial version of PGP is provided in the CD accompanying this book. Let us take an example of a simple message that needs to be **encrypted using symmetric encryption**. The figure below illustrates the message.



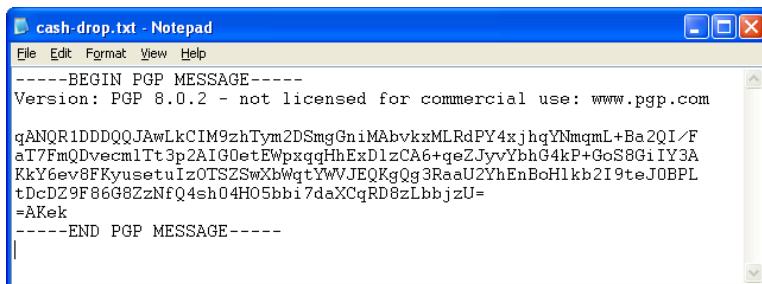
Right click the PGP icon and click on Current Window → Encrypt. In the next screen select the “**Conventional Encryption**” option, as illustrated below:



In the next window (illustrated below), enter the passphrase (this can be alphabets, numbers, symbols etc) e.g. 12345678. Then click on “OK”.



The message has now been encrypted and is illustrated below:



This message can be emailed to the recipient. The recipient can then use PGP and the passphrase (12345678 in this case) to decrypt it and read the original message.

Let us take an example of an Microsoft Word document that needs to be converted to a **self-decrypting archive**.

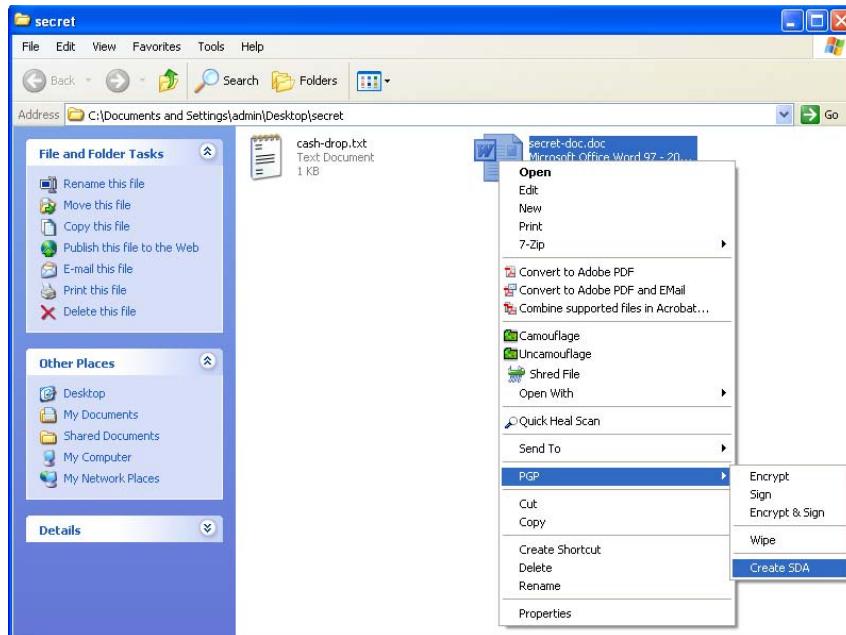
A self-decrypting archive (SDA) is a self-decrypting executable file that is conventionally encrypted using a passphrase you specify. The resulting file can be decrypted simply by double clicking it and entering the correct passphrase.

SDAs are valuable for situations where you need to send encrypted data to someone who does not have PGP. SDAs can be a single file, multiple files, a directory, multiple directories, or even an entire drive.

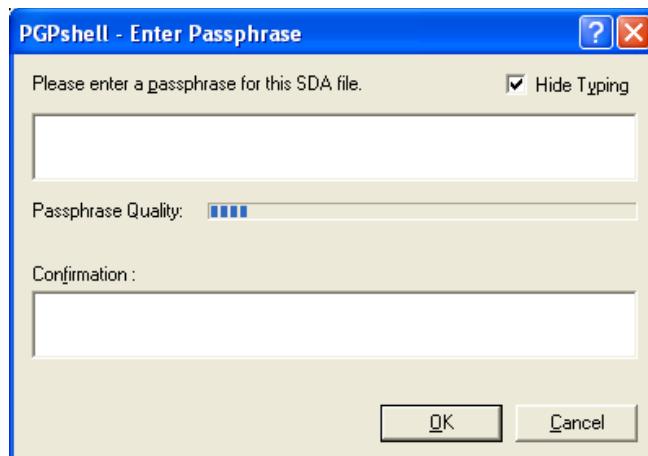
Note: SDAs can only be opened under the same operating system as they were created under. In other words, you cannot open an SDA on a

Macintosh if it was created by the Windows version of PGP, and vice versa.

To create an SDA, select the files, directories, or drive you want to include in the SDA. Right-click on your selection, slide down to PGP, then over and down to Create SDA. This is illustrated below:



The Enter Passphrase screen appears.



Enter the passphrase you want to use for this SDA, then enter it again for confirmation. Note: You must be able to securely communicate this passphrase to the person who is going to be decrypting the SDA.

If you're creating an SDA with a file or files specifically selected (that is, not on the drive or in a directory, but specifically selected), you'll be prompted to confirm the filename and location of the SDA. If no file or files are specifically selected, you won't be prompted for a filename or location.

Click Save. PGP creates the SDA with the contents you specified.

The default filename for an SDA with a file or files specifically selected is the name of one of the files in the SDA with .sda.exe appended. The default filename for an SDA with no files specifically selected (that is, just directories or drives) is the name of one of the directories or drives with .sda.exe appended. Unless you specified otherwise, the SDA is saved in the same location as the original files.



To open an SDA, double-click the executable file (the file should have a .SDA.EXE extension) Enter the correct password and specify a location in which to save the decrypted file. The SDA opens.

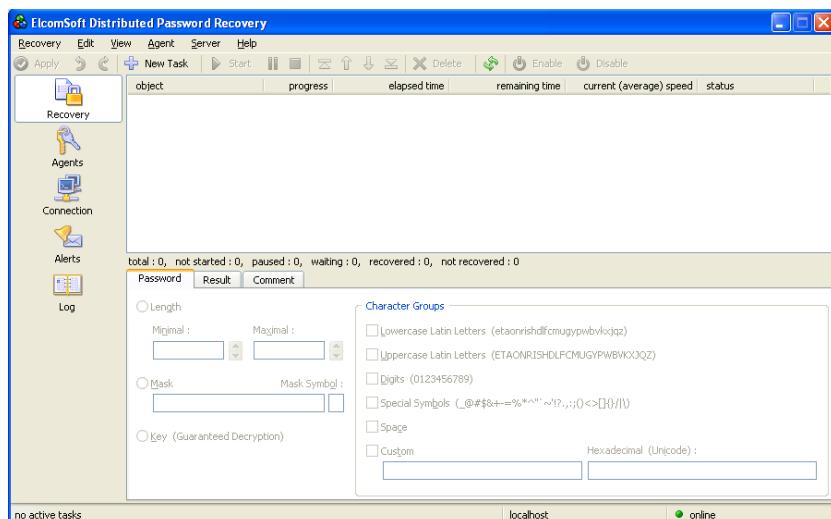


3.8 Using EDPR to crack PGP passwords

Elcomsoft Distributed Password Recovery (EDPR) supports the following PGP passwords:

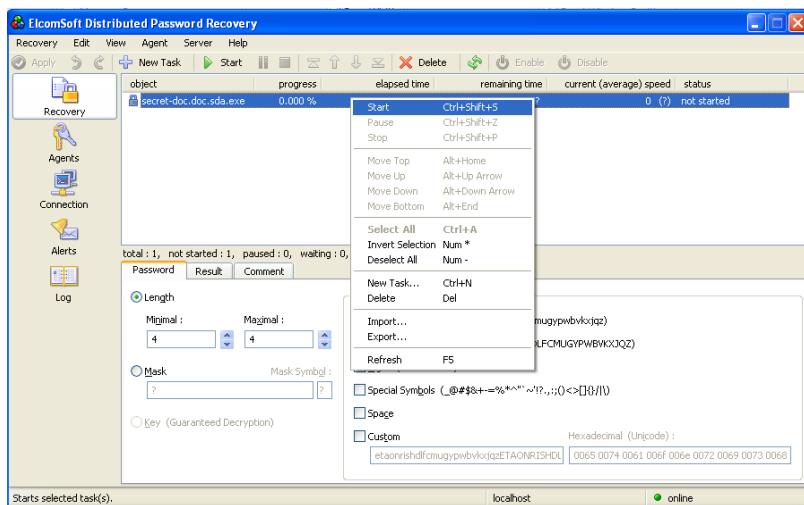
- PGP zip archives (.PGP) (password recovery)
- PGP secret key rings (.SKR) (passphrase recovery)
- PGP disks with conventional encryption (.PGD) (password recovery)
- PGP self-decrypting archives (.EXE) (password recovery)
- PGP Whole Disk Encryption (.WDE) (password recovery)

The trial version of this software is provided to you in the CD accompanying this book. The main interface of the “server” console of this software is illustrated below:

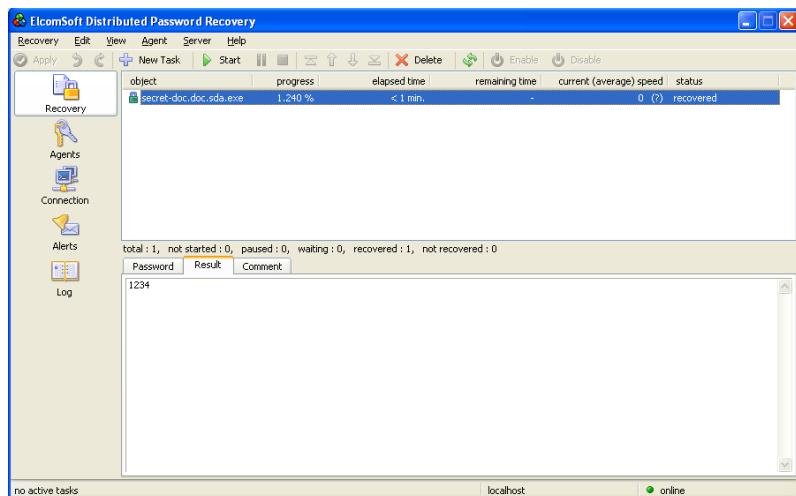


Let us presume that we have a PGP Self Decrypting Archive titled “**secret-doc.doc.sda.exe**”.

To break the password, the first step is to click on “New Task” in the main interface and then browse to the relevant document. Then right-click on the document and click on “Start” as illustrated below:



Once the passphrase is cracked, the following screen opens up.



3.9 Using MD5 hashes to protect passwords

In many applications, the passwords of a user are not stored in the database. Instead, the MD5 hash of the password is stored. This ensures that even if the database is compromised by a hacker, the passwords are not visible.

(Note: To generate MD5 hashes, you can use the free online MD5 hash calculator available at: <http://www.rohasnagpal.com/projects/md5-calculator>)

For this example, we calculate the MD5 hash for the word *coffee99* using the free online MD5 hash calculator mentioned above. The hash is *8e98836b70893b7bf64cdaba0cfdecb2*

Suppose Sanya has an online banking account with Noodle Bank. The bank stores the hash of passwords and not the actual passwords.

In this case we presume that Sanya's username is *sanya* and her password is *coffee99*. The bank's database may look like this:

username	password	customer-name
sanya	8e98836b70893b7bf64cdaba0cfdecb2	Sanya Nagpal

When Sanya visits the NoodleBank website, she enters her username as *sanya* and password as *coffee99* (as illustrated below):



As soon as she presses the "login" button, her password is then converted into the MD5 hash *8e98836b70893b7bf64cdaba0cfdecb2* and then passed on the NoodleBank servers. The server checks whether the username-password combination:

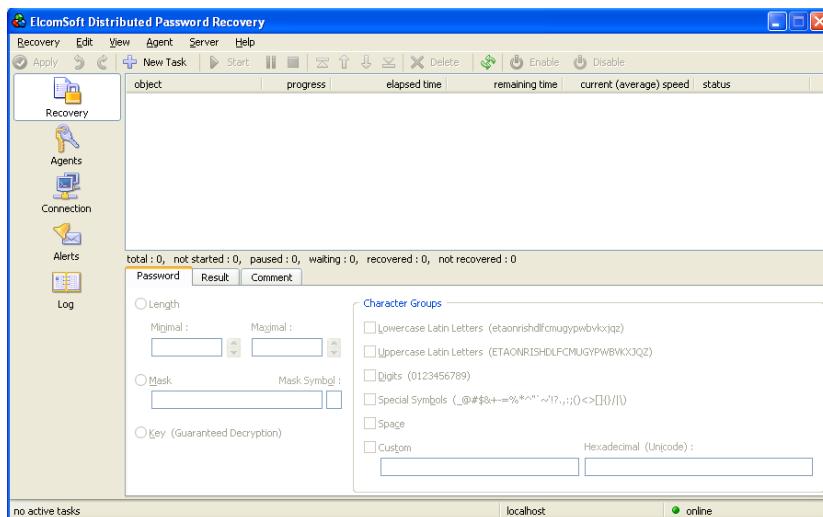
sanya-8e98836b70893b7bf64cdaba0cfdecb2

matches the record stored in the database. If its matches, Sanya is logged into her account. This means that even the administrator of the NoodleBank servers cannot come to know Sanya's password. All he can get to know is that the MD5 hash of her password is *8e98836b70893b7bf64cdaba0cfdecb2*

3.10 Using EDPR to crack MD5 hashes

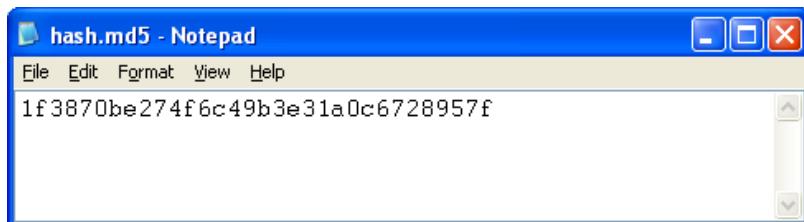
Elcomsoft Distributed Password Recovery (EDPR) supports the cracking of MD5 hashes.

The trial version of this software is provided to you in the CD accompanying this book. The main interface of the “server” console of this software is illustrated below:



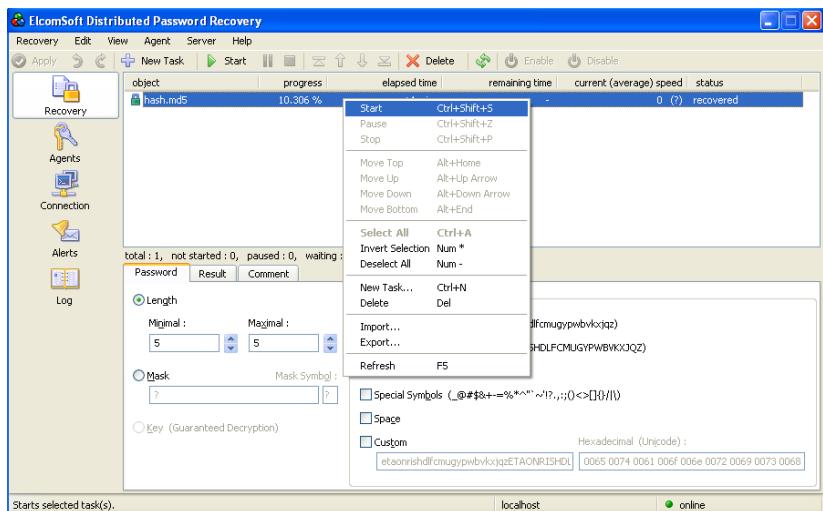
Suppose that we want to crack the hash
1f3870be274f6c49b3e31a0c6728957f

Create a text file containing the above hash, as illustrated below:

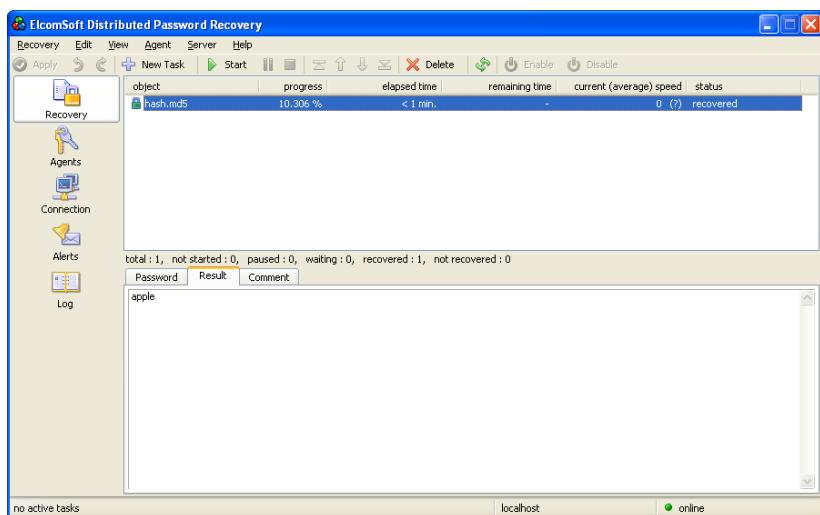


(Note: The file is saved with a .md5 extension)

To break the password, the first step is to click on “New Task” in the main interface and then browse to the relevant document (*hash.md5* in this case). Then right-click on the entry and click on “Start” as illustrated below:



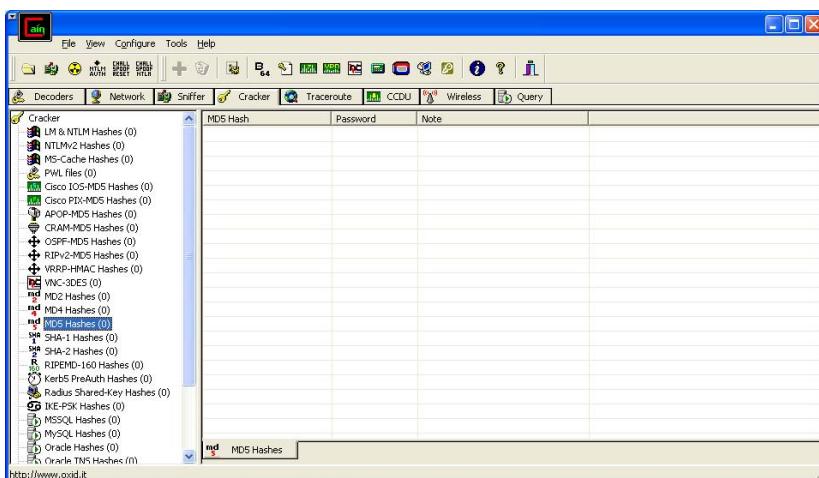
Once the hash is cracked, it is displayed as illustrated below:



3.11 Using Cain & Abel to crack MD5 hashes

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of several kinds of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

This chapter discusses the use of Cain for cracking an MD5 hash. The main interface of the software is illustrated below:

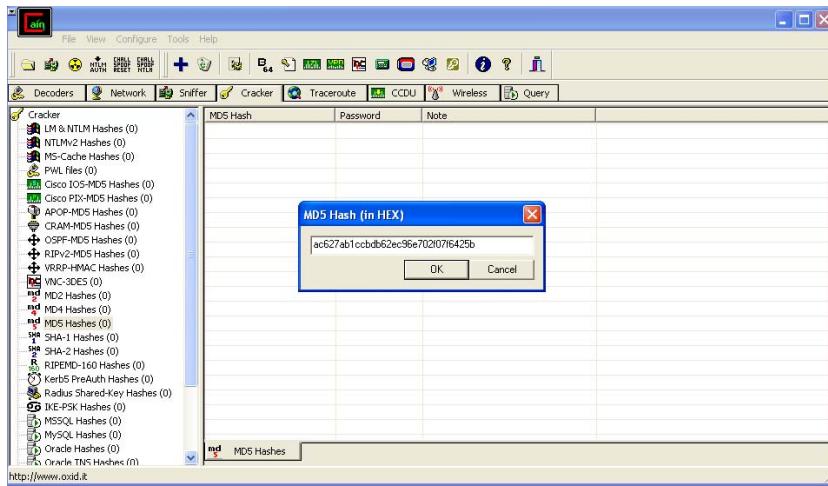


Click on File → Add to list.

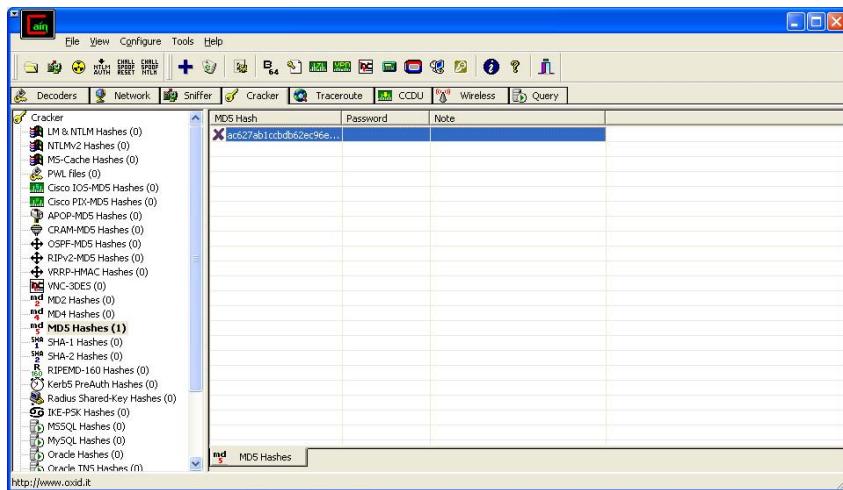
The interface illustrated below open up. Enter the MD5 hash that is sought to be cracked. (Note: To generate MD5 hashes, you can use the free online MD5 hash calculator available at: <http://www.rohasnagpal.com/projects/md5-calculator>)

For this example, we calculate the MD5 hash for the number 99 using the free online MD5 hash calculator mentioned above. The hash is ac627ab1ccbdb62ec96e702f07f6425b

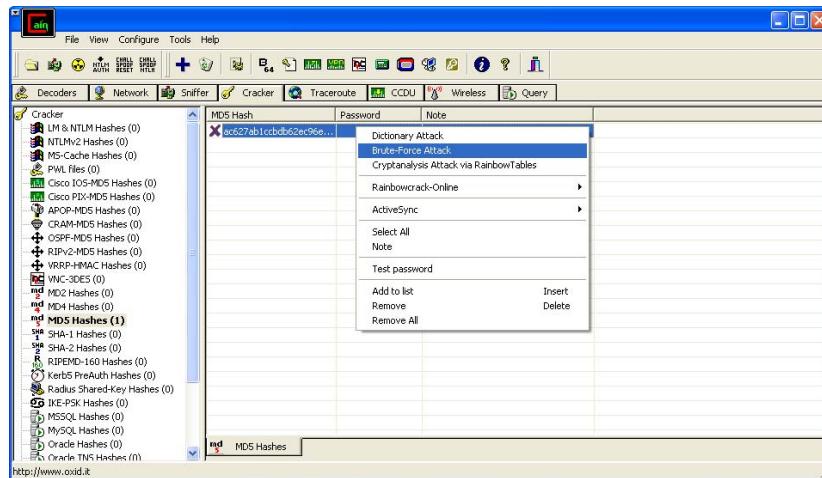
Enter this hash into the Cain interface as illustrated below:



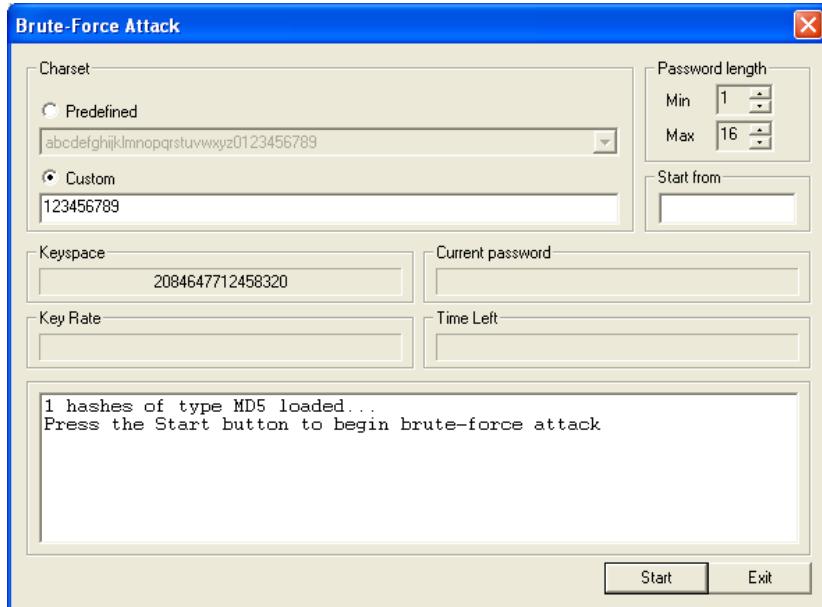
Click on “OK” in the screen illustrated above. The following screen will open up:



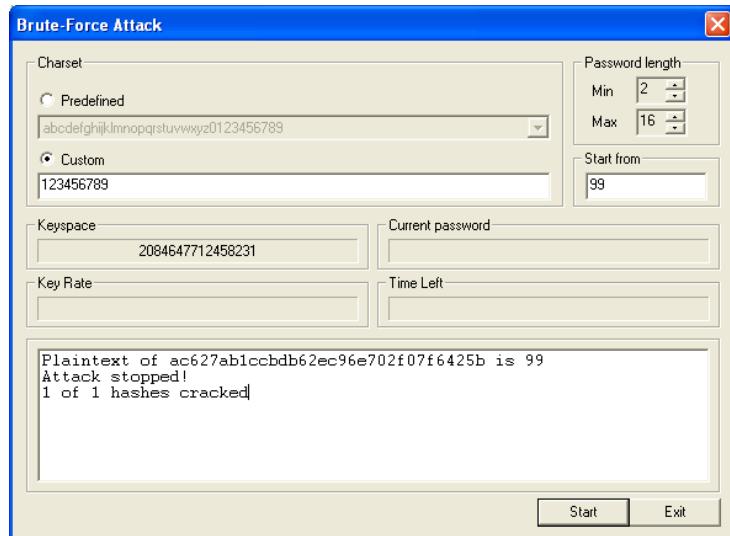
Right click on the hash value and choose “**Brute Force Attack**” as illustrated below:



Now set the options for the attack. Since this is a simple example, set the Charset as “123456789” i.e. Cain will check hash values for all combinations of these digits only. Click on “Start”.



Once the hash is cracked, it is displayed as illustrated below:



3.12 Using gdata to crack MD5 hashes

GData is an online MD5 Hash Database that can be accessed from www.gdataonline.com

Simply enter the hash value and press “Submit”, as illustrated below:

Hash look up:
(For multiple hashes, separate by a semicolon)*

Submit

* up to five(5) hashes at a time

Within a few seconds, the hash is cracked and the result is displayed as illustrated below:

RESULTS:	
Hash	Pass
1fc89d430c040962b8172b349ea88a7d	rohas

Note: The hash database is limited and may not always be able to crack the hash.

4. Handling Steganography

4.1 What is Steganography?

Throughout history, a multitude of methods and variations have been used to hide information.

One of the first documents describing steganography is from the Histories of Herodotus. In ancient Greece, text was written on wax-covered tablets.

In one story Demeratus wanted to notify Sparta that Xerxes intended to invade Greece. To avoid capture, he scraped the wax off the tablets and wrote a message on the underlying wood. He then covered the tablets with wax again. The tablets appeared to be blank and unused so they passed inspection by sentries without question.

Another ingenious method was to shave the head of a messenger and tattoo a message or image on the messenger's head. After allowing his hair to grow, the message would be undetected until the head was shaved again.

Another common form of invisible writing is through the use of invisible inks. Such inks were used with much success as recently as WWII. An innocent letter may contain a very different message written between the lines.

Early in World War II, steganographic technology consisted almost exclusively of invisible inks. Common sources for invisible inks are milk, vinegar, fruit juices and urine. All these darken when heated.

With improvement in technology and the ease of decoding these invisible inks, more sophisticated inks were developed which reacted to various chemicals. Some messages had to be "developed" much as photographs are developed with a number of chemicals in processing labs.

Steganography simply takes one piece of information and hides it within another. Computer files (images, sound recordings, even disks) contain unused or insignificant areas of data. Steganography takes advantage of these areas, replacing them with information (encrypted mail, for instance).

The files can then be exchanged without anyone knowing what really lies inside them. An image of the girl next door might contain a private letter to a friend. Steganography can also be used to place a hidden "trademark" in images, music, and software, a technique referred to as watermarking

Of late, steganography has been discussed a lot, especially since it was suspected that terrorists connected with the September 11 attacks might have used it for covert communications. Although no such connection has been conclusively proven, this discussion goes a long way to evince the efficacy of steganography. In addition to encryption, steganography is one of the fundamental ways by which data can be kept hidden.

4.2 What is Steganography used for?

Like many security tools, steganography can be used for a variety of reasons, some good, some not so good. Legal purposes can include things like watermarking images for reasons such as copyright protection. Digital watermarks (also known as fingerprinting, significant especially in copyrighted material) are similar to steganography in that they are overlaid in files, which appear to be part of the original file and are thus not easily detectable by the average person.

Steganography can also be used as a way to make a substitute for a one-way hash value (where you take a variable length input and create a static length output string to verify that no changes have been made to the original variable length input). Further, steganography can be used to tag notes to online images (like post-it notes attached to paper files).

Finally, steganography can be used to maintain the confidentiality of valuable information, to protect the data from possible sabotage, theft, or unauthorized viewing.

Unfortunately, steganography can also be used for illegal purposes. For example, if someone was trying to steal information, they could hide it in another file or files and send it out as an innocuous looking email or file transfer.

Additionally, a person who saves pornography, or worse, to their hard drive, may choose to hide the evidence through the use of steganography. And, as was pointed out earlier, it can also be used as a means for covert communication.

4.3 Using Camouflage

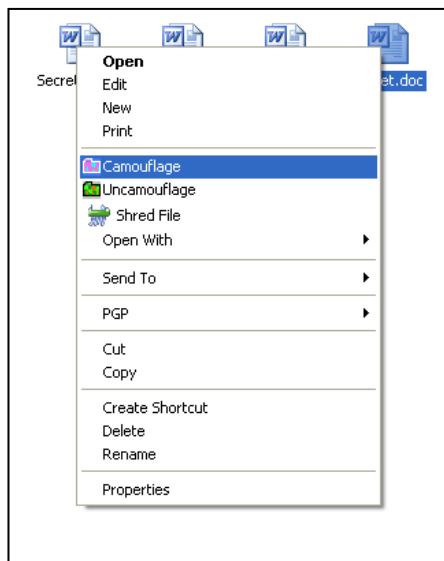
Camouflage is provided in the CD accompanying this book. Camouflage allows you to hide files by scrambling them and then attaching them to the file of your choice. This camouflaged file then looks and behaves like a normal file, and can be stored or emailed without attracting attention. For example, you could create a picture file that looks and behaves exactly like any other picture file but contains hidden encrypted

files, or you could hide a file inside a Word document that would not attract attention if discovered. Such files can later be safely extracted.

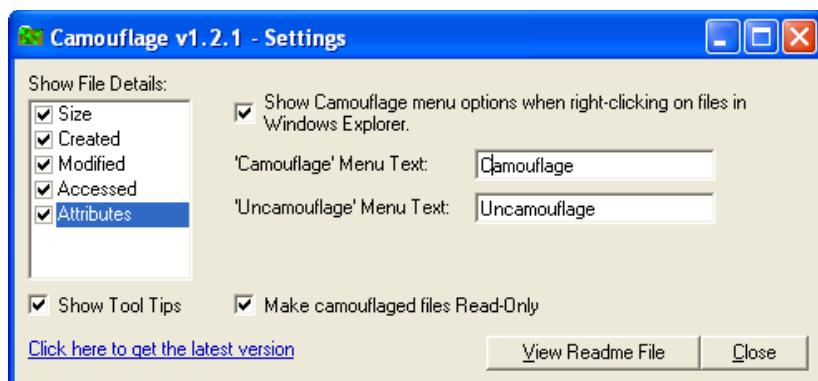
For additional security you can password protect your camouflaged file. This password will be required when extracting the files within. You can even camouflage files within camouflaged files.

Camouflaging Files

After installing Camouflage you will find two new menu options when right-clicking files in Windows Explorer; 'Camouflage' and 'Uncamouflage'.



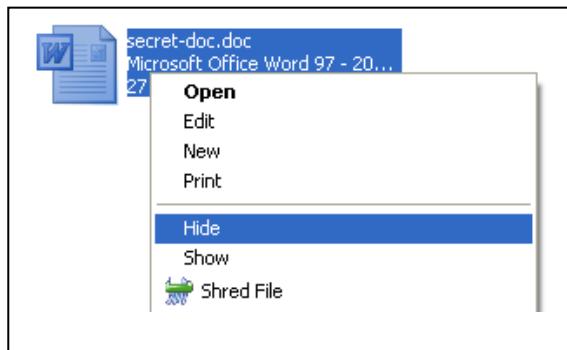
These options (i.e. Camouflage and Uncamouflage) can be renamed from the program settings. The default settings are illustrated below:



Altered settings are illustrated below:

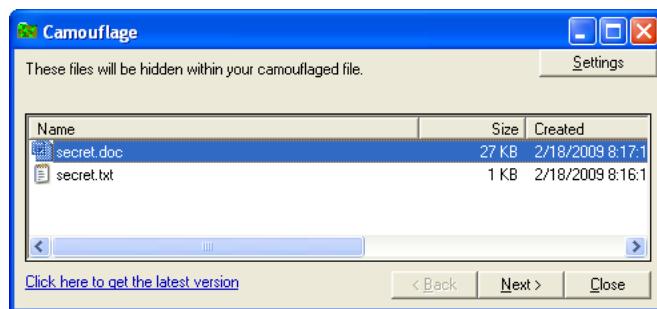


After changing the settings, the two new menu options when right-clicking files in Windows Explorer are illustrated below:



You can camouflage a file or several files at a time by highlighting them in Windows Explorer, then clicking the right mouse button and choosing 'Camouflage' from the pop-up menu.

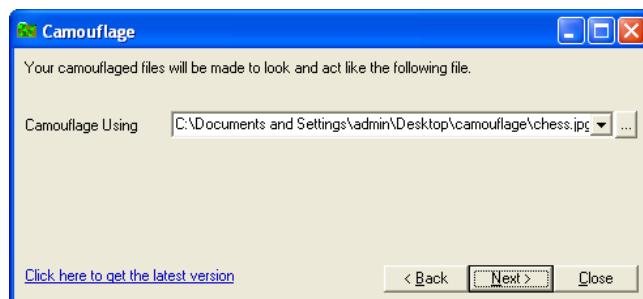
A list of the files chosen is displayed in the Camouflage dialog, as illustrated below:



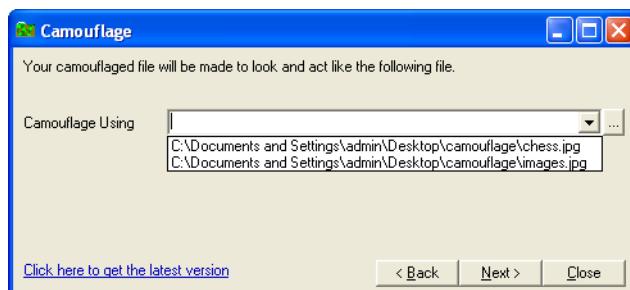
You can view/edit the files by double-clicking them with the mouse, or by highlighting and right-clicking them, then choosing 'Open' from the pop-up menu. Selecting 'Properties' from this menu will display an information page similar to that in Windows Explorer.

To continue click 'Next'.

In the second screen choose a file to be used as camouflage. This can be any type of file, but some files work better than others. For example, avoid choosing a text file because Notepad would display the entire contents of it, including the scrambled files attached. Most other files work well.



Camouflage remembers the last 10 files used and you can reuse one of them by selecting it from the drop-down list.

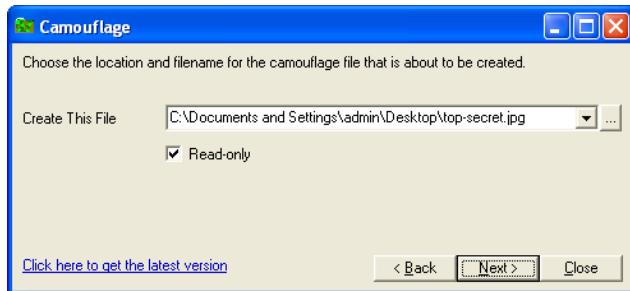


Note that Camouflage will simply use a copy of the selected file. The original chosen file will not be altered in any way.

Once you have selected a file, click 'Next'.

From the third screen choose the folder and filename of the camouflaged file that will be created. The default folder is the folder where you selected the files in Windows Explorer, and the default filename is the name of the file you selected for use as camouflage in the previous screen.

Check 'Read-only' to create the camouflaged file with its 'Read-Only' attribute set. This is recommended because it makes the file safer, and prevents other applications from modifying it and destroying the camouflaged section.



Click 'Next'.

From the final screen you can type in a password if you wish. This password will be required when extracting files from your camouflaged file. If you do not wish to add a password just click 'Finish'.



Clicking 'Finish' will create the camouflaged file and then exit.

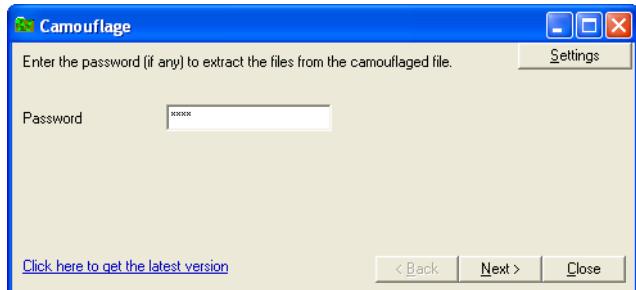
Uncamouflaging Files

To extract the files hidden within a camouflaged file, right-click it in Windows Explorer and choose 'Uncamouflag' from the pop-up menu.

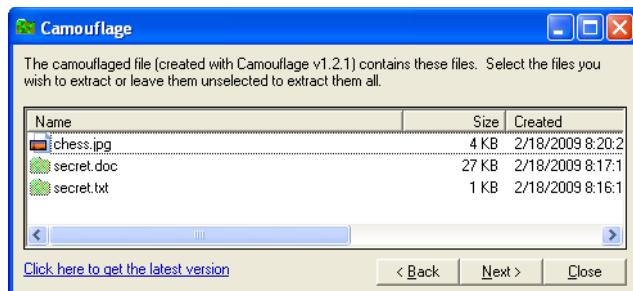
A password prompt appears in the Uncamouflag dialog. If this file was created with a password, type it in.

Note that Camouflage was designed so that it doesn't reveal camouflaged files to the casual observer. For this reason the password screen is always displayed whether the file is a camouflaged file or not, or whether or not it contains a password.

Once you have entered the correct password (if applicable), click 'Next'.



The second screen displays a list of the files hidden within the camouflaged file. The first file in the list is the file originally used as camouflage.



Name	Size	Created
chess.jpg	4 KB	2/18/2009 8:20:2
secret.doc	27 KB	2/18/2009 8:17:1
secret.txt	1 KB	2/18/2009 8:16:1

[Click here to get the latest version](#) | [Back](#) | [Next >](#) | [Close](#)

To extract all files from the camouflaged file, either select them all, or just click 'Next' without selecting any files. You can extract certain files by selecting them, then clicking 'Next'. Note that you can deselect files by holding down CTRL and left-clicking them with the mouse.

You can view the files by double-clicking them with the mouse, or by highlighting and right-clicking them, then choosing 'Open' from the pop-up menu. Note that files modified in this way will not be changed in the archive. You can display further information about the files by choosing 'Properties' from this menu.

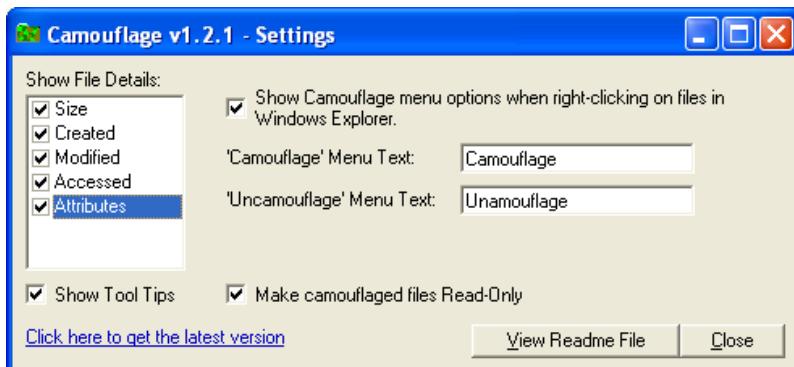
From the final screen, choose the folder where the files are to be extracted. If you're not extracting the first file in the list (the file originally used as camouflage), the default folder will be the folder where you right-clicked on the camouflaged file in Windows Explorer.

Click 'Finish' to extract the files and exit.

Configuring Camouflage Settings

You can modify Camouflage settings by running Camouflage from the Windows Start Menu shortcut, by opening the folder where you installed Camouflage and double-clicking Camouflage.exe from Windows Explorer, or by clicking the 'Settings' button on the first screen.

The Camouflage Settings screen will appear. The version number is displayed in the title bar.



You can add or remove columns in the file selection screens (Size, Creation Date/Time, Modified Date/Time, Accessed Date, File Attributes) by checking or unchecking items in the 'Show File Details' area.

You can switch the pop-up help messages on or off by checking or unchecking 'Show Tool Tips'.

You can hide Camouflage from Windows Explorer by unchecking 'Show Camouflage menu options when right-clicking on files in Windows Explorer'.

When checked, Camouflage is enabled and you can right-click on files in Windows Explorer to use the Camouflage options.

When unchecked, Camouflage is disabled and the menu options do not appear when right-clicking on files in Windows Explorer.

By checking 'Make camouflaged files Read-Only', all files created by Camouflage have their Read-Only attribute set by default. This is highly recommended and prevents the camouflaged file from being modified by certain applications when you open it.

Tips for Using Camouflage

Although they do work well, text files are not recommended to be used as camouflage. Files with '.txt' extensions are usually opened with Notepad by default. Notepad will display the entire file, including the encrypted camouflaged section which might give the game away.

Most other applications will just open their part of the file, and ignore the camouflaged section.

Certain files, for example, Microsoft Excel files, are often modified by their native application when opened by it. It is recommended that you always make camouflaged files Read-Only. This prevents these applications from modifying the camouflaged file and therefore destroying the camouflaged section.

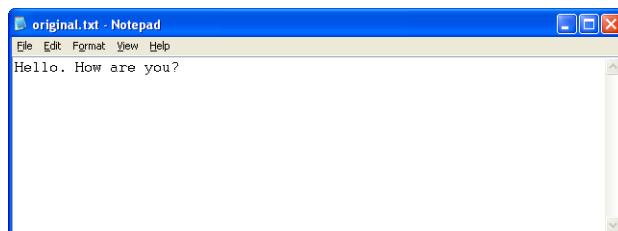
Be careful when uploading camouflaged files (especially text files) to an FTP site. Many FTP applications will 'auto-detect' the transfer type, and will upload text files as ASCII.

This would destroy the binary section of the file (the camouflaged section), so you must make sure that when uploading camouflaged files, you always set the transfer type to BINARY.

4.4 Using SNOW

SNOW allows the hiding of text within text by using blank spaces and tabs. SNOW is provided in the CD accompanying this book.

Suppose we have a text file named *original.txt* that has the following text: *Hello. How are you?*



Now, we want to hide the following text in it:

Cash has been received

We also want to use the password *apple125* while hiding this text. We will need to follow the steps mentioned below:

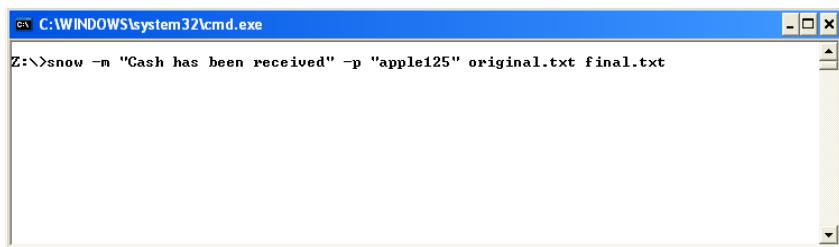
- (1) Place the snow.exe file in a suitable location (z drive in this example).

(2) Place the original.txt file in the same location (z drive in this example).

(3) Run the following command from the command prompt (Note: in a Windows computer, click Start→Programs→Accessories→Command Prompt to open up the command prompt).

Snow -m "Cash has been received" -p "apple125" original.txt final.txt

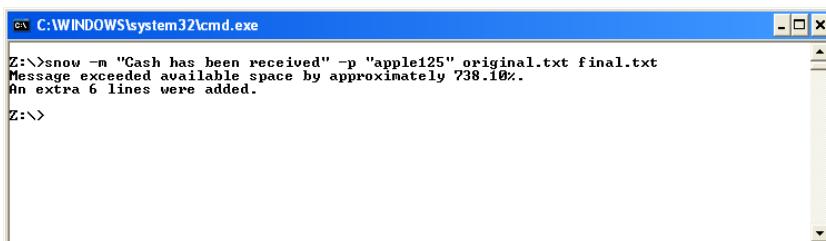
This is illustrated below:



```
C:\WINDOWS\system32\cmd.exe
Z:\>snow -m "Cash has been received" -p "apple125" original.txt final.txt
```

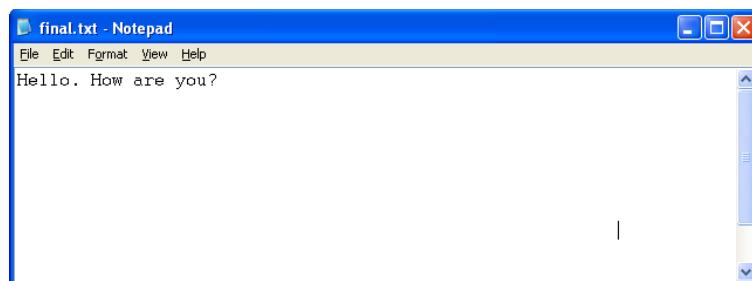
This will take the contents of the file *original.txt* and hide the text “Cash has been received” (with the password *apple125*) in it and then save this to a new file named *final.txt*

The following screen will be displayed:



```
C:\WINDOWS\system32\cmd.exe
Z:\>snow -m "Cash has been received" -p "apple125" original.txt final.txt
Message exceeded available space by approximately 738.10%.
An extra 6 lines were added.
Z:\>
```

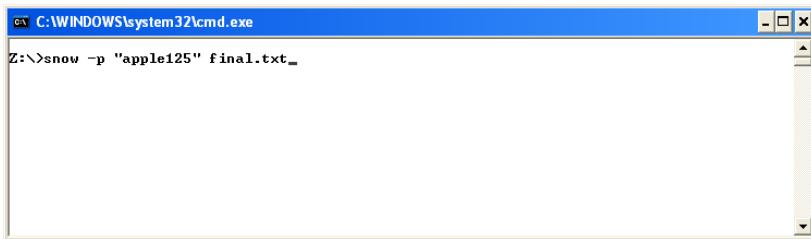
On opening the file *final.txt*, the hidden text will not be visible.



To recover the hidden information, run the following command from the command prompt

```
Snow -p "apple125" final.txt
```

This is illustrated below:



The following screen will be displayed:



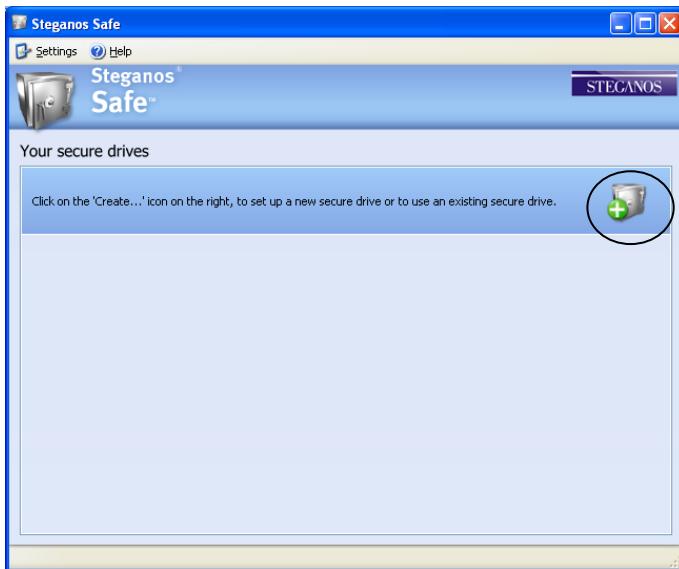
4.5 Using Steganos Security Suite

The trial version of Steganos Security Suite 2007 is provided in the CD accompanying this book. This software allows the creation of a “secret” safe i.e. a hidden drive within which data can be stored.

The main interface of the software is illustrated below:



Click on the “**Safe**” icon. The following screen will open up. Click on the icon on the right (marked with a circle).



The following screen will open up. Check the checkbox that reads “I want to create a new secure drive”, as illustrated below:



Click on “**Next**”.

The following screen will open up.



You need to enter a name for the secure drive as well as select a drive letter. This is illustrated in the next figure.



After entering the relevant information, click on “**Next**”. The following screen will open up:



At this stage you need to choose the location of the SLE file that will actually store the data of the secure drive. Note: The size of this file will be the same as the size of the secure drive. So if your secure drive is 10 GB, this SLE file will be 10 GB.

After selecting the location, click on “**Next**”. The following screen will open up:



Choose the size of your secure drive. The size will be limited by the size of the drive where the SLE file is being saved. After selecting the size, click on “Next”. The following screen will open up:



Enter your password and click on “Next”. The following screen will open up:



Click on “Finish”.

The following screen will open up:

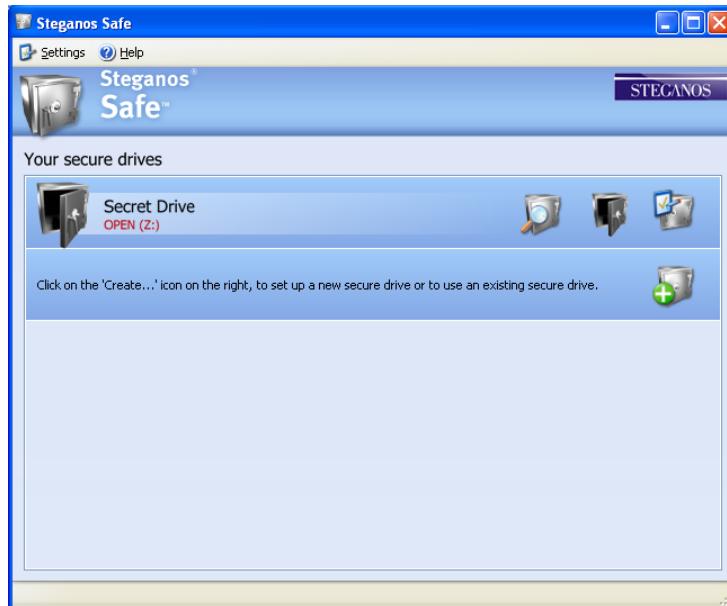


Click on “OK”.

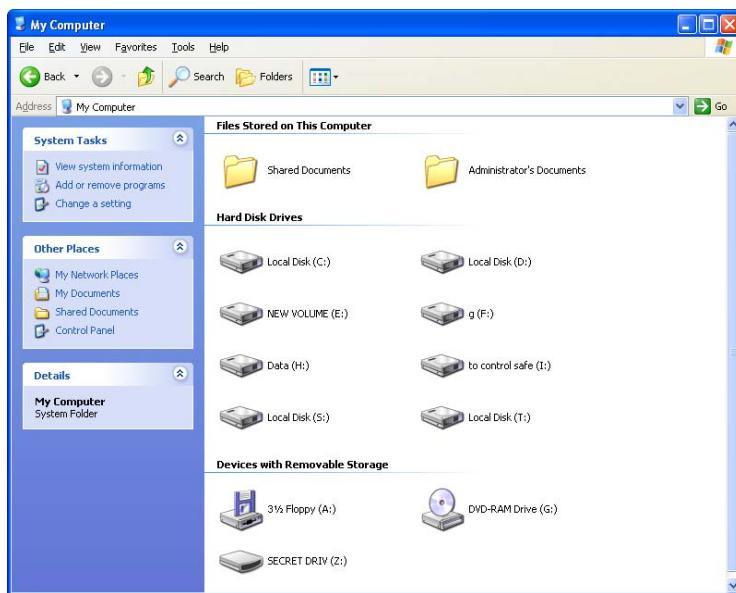
The following screen will open up:



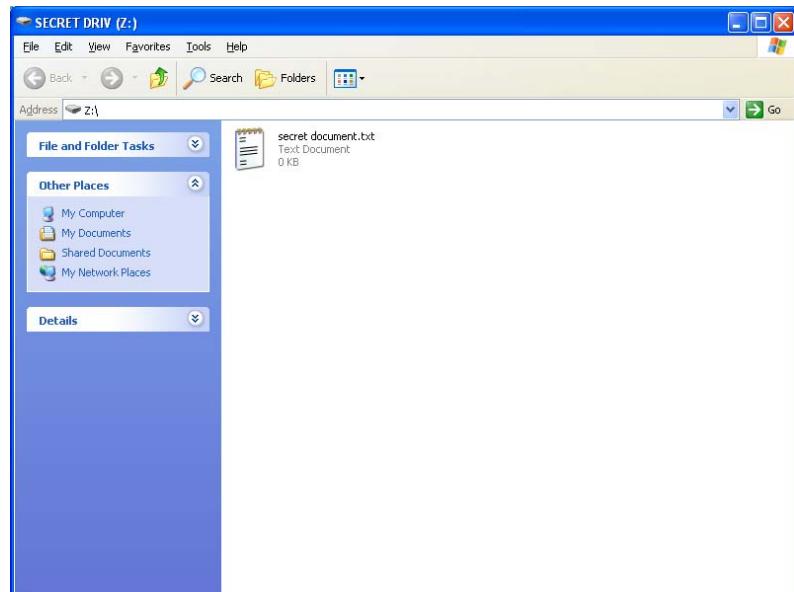
Choose a suitable option. The following screen will open up:



Double click on “My Computer” to go to the Windows Explorer to see the Z drive.



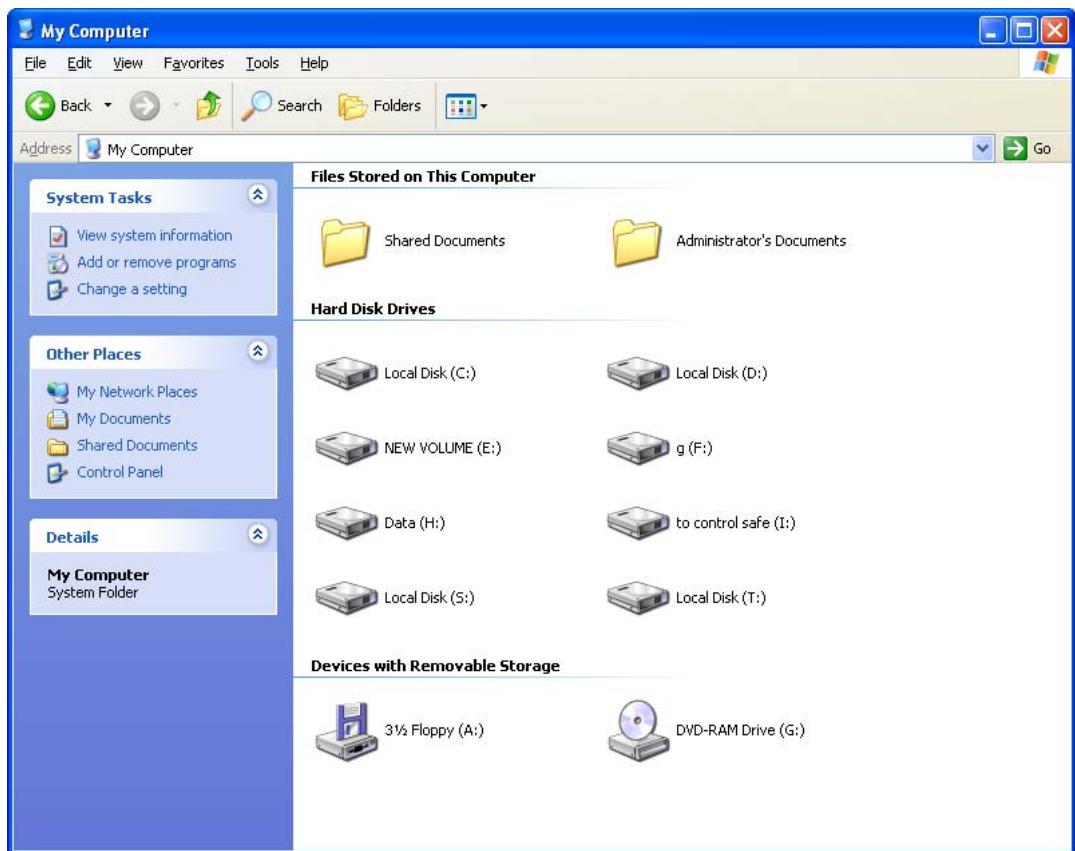
You can transfer files to the Z drive (illustrated below):



Once you close the safe, the following screen will be displayed:



The Z drive will not show in Windows Explorer or “My Computer”.



12. Investigating Intellectual Property crimes

1. Understanding Computer Software

Computer **software** is a general term that describes a collection of computer programs, procedures and documentation.

Computer **hardware**, on the other hand, consists of the physical devices that can store and execute computer software.

Illustration

Sanya downloads the OpenOffice software from the Internet. In effect what she downloads is an **executable** file. She double-clicks on the executable file and begins to **install** the software on her computer.

During the installation she specifies the part (drive and folder name etc) of the hard disk where the software files must be saved. During the installation the software also makes entries in system files (e.g. registry) maintained by the operating system (e.g. Windows XP).

Once the installation is complete, Sanya can **run the software**.

When she runs the software, relevant software files get loaded into **RAM** and are subsequently executed in the **CPU** (central processing unit).

When a computer programmer creates a software program, he usually follows the procedure outlined below:

- (1) Writes the **source code** using a high level programming language such as C, C++, Java etc.
- (2) Uses a **compiler** to **compile** the source code into the **object code**.
- (3) Links the object code with the relevant library files and creates an **executable**. This is done using a **linker**.
- (4) This executable can now be distributed to the end users.

Now let us discuss some of the important terms mentioned above:

Source code, simply put, is the listing of programmes, computer commands, design and layout etc. Let us understand this using some illustrations.

Illustration 1: Sanya has created a simple computer program. When a user double-clicks on the hello.exe file created by Sanya, the following small screen opens up:

Hello World

The hello.exe file created by Sanya is the executable file that she can give to others. The small screen that opens up is the output of the software program written by Sanya.

Sanya has created the executable file using the programming language called “C”. Using this programming language, she created the following lines of code:

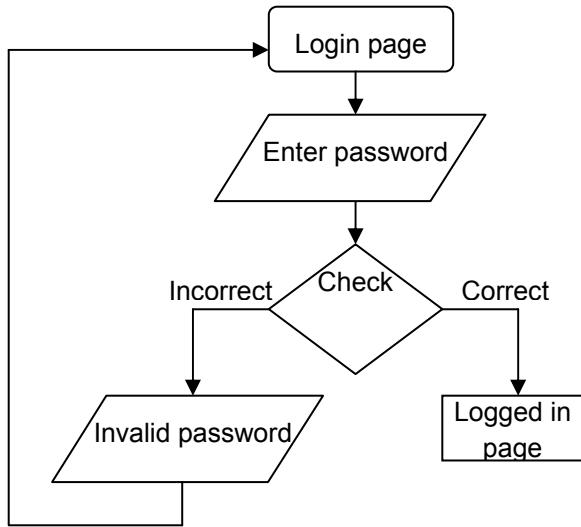
```
void main()
{
    printf("\n Hello World");
}
```

These lines of code are referred to as the source code.

Illustration 2: Noodle Ltd has created software for viewing and creating image files. The programmers who developed this program used the computer-programming language called Visual C++. Using the syntax of these languages, they wrote thousands of lines of code.

This code is then compiled into an executable file and given to end-users. All that the end user has to do is double-click on a file (called setup.exe) and the program gets installed on his computer. The lines of code are known as computer source code.

Illustration 3: Pooja is creating a simple website. A registered user of the website would have to enter the correct password to access the content of the website. She creates the following flowchart outlining the functioning of the authentication process of the website. This flowchart is source code.



A **compiler** processes a source code and produces **object code**. The object code contains code that can be directly executed by the CPU of a computer. A **decompiler** does the reverse of a compiler.

HELLO.OBJ	HELLO.C
00000000 80 09 00 07 48 45 4C 4C	4F 2E 43 8B 88 1F 00 00 ... HELLO.C...
00000010 00 1B 54 43 38 36 20 42	6F 72 6C 61 6E 64 20 54 ... TC86 Borland T
00000020 75 72 62 6F 20 43 2B 2B	20 33 2E 30 30 91 88 0F ... Turbo C++ 3.00...
00000030 00 00 E9 47 7E 6F 37 07	48 45 4C 4C 4F 2E 43 29 ... G~o7.HELLO.C)
00000040 88 06 00 00 E5 01 36 00	8C 88 06 00 00 E5 01 03 ...
00000050 00 89 88 05 00 00 E7 0D	00 7F 88 05 00 00 E7 0D ...
00000060 00 7F 88 0A 00 00 EE 01	00 00 03 00 0B 00 71 88q.
00000070 03 00 00 E9 8C 88 05 00	00 EA 01 09 7F 96 28 00 ... _TEXT_CODE_DA
00000080 00 05 5F 54 45 58 54 04	43 4F 44 45 05 5F 44 41 ... TA.DATA_BSS.BSS
00000090 54 41 04 44 41 54 41 04	5F 42 53 53 03 42 53 53 ... DGROUP...()
000000a0 06 44 47 52 4F 55 50 D1	98 07 00 28 0D 00 02 03 ... &...H...H...
000000b0 01 26 98 07 00 48 0E 00	04 05 01 02 98 07 00 48 ... _main_Z
000000c0 00 00 06 07 01 0B 9A 06	00 08 FF 02 FF 03 55 8C ... printf.q...
000000d0 0A 00 07 5F 70 72 69 6E	74 66 00 71 88 0B 00 00 ... #..K...
000000e0 E3 18 00 00 00 23 04 00	00 4B 88 04 00 00 E0 18 ... _main_M...
000000f0 7C 98 0C 00 00 01 05 5F	6D 61 69 68 00 00 00 5A ... a...U...
00000100 88 0B 00 00 E3 19 00 00	00 23 01 00 00 4D 88 05 ... P...Y)...V...
00000110 00 00 E1 19 18 61 A0 11	00 01 00 00 55 8B EC B8 ... Hello World...
00000120 00 00 50 E8 00 00 59 5D	C3 19 9C 0A 00 84 08 56 ... G~o7.HELLO.C...
00000130 01 C4 04 14 01 02 98 A0	12 00 02 00 00 0A 20 48 ...
00000140 65 6C 6C 6F 20 57 6F 72	6C 64 00 06 88 10 00 00 ...
00000150 E8 00 07 48 45 4C 4C 4F	2E 43 47 7E 6F 37 29 94 ...
00000160 0F 00 00 01 01 00 00 00	03 00 03 00 05 00 0B 00 ... E...t
00000170 45 8A 02 00 00 74	

A **library** is a collection of programs used to develop software. Most software programs use the libraries provided by the operating system. Simply put, a **linker** links object code files (and libraries) to generate an executable file. Computer software can be divided into two fundamental categories – **system software** and **application software**.

Application software uses the computer directly for performing user tasks. System software enables the application software to use the computer's capabilities.

Analogy

An oil company drills for oil on the sea bed. This oil is then processed and provided to the customer in the form of petrol for his car.

Here the petrol is like the application software – it helps the user to run his car. The oil company is like the system software – it enables the petrol to be taken to the user.

System software can be of various types such as:

- (1) operating systems which form the platform for all other software on a computer,
- (2) device drivers which allow computer programs to interact with hardware devices such as printers, scanners etc,
- (3) programming tools which help programmers to develop and test other programs,
- (4) compilers which compile the source code into the object code,

(5) linkers which link object code files (and libraries) to generate an executable file,

(6) utility software that helps manage and tune the computer hardware, operating system or application software.

Application software include

(1) word processors (e.g. Microsoft Word),

(2) spreadsheets (e.g. Microsoft Excel)

(3) presentation software (e.g. Microsoft Powerpoint)

(4) media players (e.g. Microsoft Windows Media Player)

(5) games (e.g. Need for Speed, Age of Empires)

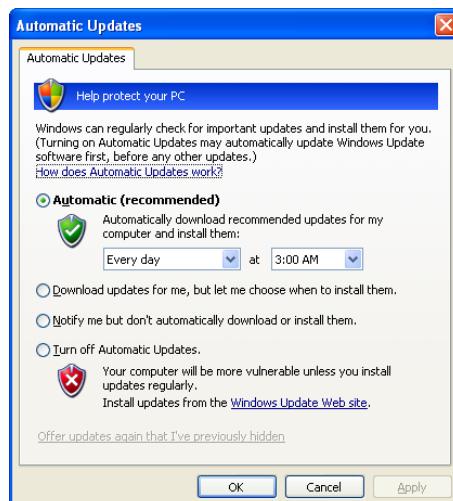
(6) forensic software (e.g. Winhex, X-Ways Forensics)

(7) encryption software (e.g. PGP)

(8) Internet browsers (e.g. Mozilla Firefox)

(9) FTP clients (e.g. FireFTP)

All computer software (whether system software or application software) is prone to bugs and vulnerabilities which are usually “fixed” through updates. **Updates** can be in various forms including bug-fixes, patches, plug-ins and new versions. Updates can be **automatic** wherein the installed software regularly connects to a particular website and downloads the new updates. The user is usually asked for permission before the updates are installed. Updates can also be **manual**, where the user must manually start the procedure for searching for, obtaining and installing the updates. The figure below illustrates the various options for obtaining updates for the Microsoft Windows XP operating system.



Some of the important terms used earlier are explained below using some simple illustrations.

Illustration 1: Sanya has developed the easyAV anti-virus software. Users can freely download the software from Sanya's website and install it on their computers. As new computer viruses and other malicious code are discovered all the time it is essential that the anti-virus software is constantly updated with the information about the latest viruses and the "cures" for them.

Once easyAV is installed on a computer, it regularly connects to Sanya's website to check for updates. New updates are automatically downloaded by the software and integrated with the existing software installation.

Illustration 2: Sameer has developed a new computer game called Rage of Vampires (ROV). Thousands of users around the world have downloaded the game and are regularly using it. Some users give a feedback to Sameer that they cannot open up the Mozilla Firefox browser if ROV is running on their computer.

Sameer researches on this and realizes that there is a bug in the ROV software that interferes with the Mozilla Firefox browser. He develops a "bug-fix" that users can download from his website. Once the "bug-fix" is downloaded it integrates with the ROV software and stops the interference with Firefox.

Illustration 3: Sameer has developed a new computer game called Rage of Vampires (ROV). Thousands of users around the world have downloaded the game and are regularly using it. During regular post release testing, Sameer realizes that the ROV software has a security vulnerability that can be exploited by malicious hackers. Sameer develops a "patch" software that users can download from his website. Once the "patch" is downloaded it integrates with the ROV software. The "patched" ROV software does not have the security vulnerability.

Illustration 4: Sameer has developed a new computer game called Rage of Vampires (ROV). At the time of release of ROV, the most popular operating system was FreeOS version 1. The ROV software was created to run smoothly on FreeOS version 1. However, a year later FreeOS version 2 has been released and the ROV software does not run smoothly on this.

Sameer studies the FreeOS version 2 operating system and develops a “patch” software that users can download from his website. Once the “patch” is downloaded it integrates with the ROV software. The “patched” ROV software runs smoothly on both versions of FreeOS.

Illustration 5: Sameer has developed a new computer game called Rage of Vampires (ROV). Some users (who use the SRTS speakers on their computer) give him a feedback that the audio quality of the game is not very good.

Sameer studies the device drivers of the SRTS speakers and develops a “plug-in” software that users can download from his website. Once the “plug-in” is downloaded it integrates with the ROV software and this improves the audio quality if the user is using the SRTS speakers. Users who do not have the SRTS speakers do not have to download this plug-in.

Illustration 6: Sanya uses Mozilla Firefox Internet browser to connect to her online share trading account. She is worried that someone may install a keylogger on her computer steal her password. She downloads the “key scrambler” anti-keylogger plug-in for Mozilla. Now even if a keylogger is installed on her computer, it cannot steal her password.

Illustration 7: Sameer has developed a new computer game called Rage of Vampires version 1 (ROV v1). Over a period of time he has issued many bug-fixes, updates and patches for the software. He now incorporates all the changes and releases a new version ROV version 2.

Software can be of various types including:

(1) Freeware

Freeware is computer software that is copyrighted, available for use free of charge for an unlimited time. Freeware is created and distributed by software developers who want to contribute something to the society but at the same time they want to control the future development of their software. They usually retain their rights over the source code.

Some types of freeware include:

Careware or Donateware in which the author requests the users to do something good for someone or to donate to a charity.

Cardware where the creator requests for a post card from every user. The Linux operating system started off as cardware.

Donationware in which the author requests for a donation e.g. Spybot – malicious code removal software.

(2) Shareware

This is also known as "try before you buy" software. These software usually come with full functionality for a limited period. After this trial period users must either buy the software or uninstall it from their computers.

This trial period could be in terms of number of days (e.g. 30 days after installation), number of times the programs is started up (e.g. 20 times).

(3) Demoware

Demoware is meant only for demonstrations. The demoware does not have any functional features, it only serves to demonstrate the features to potential users.

(4) Crippleware

Crippleware is software whose functions have been limited or "crippled" by the creator. This "crippling" is done so that the creator can charge a licence fee for the full functional version.

Crippleware can be used by potential users only for evaluation purposes. Because many features have been disabled in it, crippleware cannot be used in place of the fully functional version of the software.

Illustration: Sameer creates easyWord, a word processor software having most of the functions of Microsoft Word. easyWord is available for sale from Sameer's website.

In order to allow potential users to evaluate the software, Sameer also provides a "crippled" version of the software. In the crippled version, the "Save" button does not work.

This means that the user can create, edit, format a document but cannot save his work.

2. Computer Software & Copyright Law

According to section 2(ffc) of the Copyright Act, a computer program is a “set of instructions expressed in words, codes, schemes or in any other form, including a machine readable medium, capable of causing a computer to perform a particular task or achieve a particular results”.

The essential elements of a computer program are:

- (1) It is a set of instructions expressed in: words, codes, schemes or in any other form, including a machine readable medium.
- (2) capable of causing a computer to: perform a particular task or achieve a particular results.

Computer software is “computer program” within the meaning of the Copyright Act. Computer programs are included in the definition of literary work under the Copyright Act.

2.1 Meaning of Copyright

[This concept is explained using simple fictional illustrations involving Sanya, who has created easyPDF, a computer program for converting documents into PDF (Portable Document Format)]

According to section 14 of the Copyright Act, "copyright" means the exclusive right to do (or authorize the doing of) any of the following:

- (1) To reproduce a computer programme in any material form including the storing of it in any medium by electronic means,

Illustration 1: Sanya has the exclusive right to reproduce the easyPDF program on CD, DVD and other storage media.

Illustration 2: Sanya has the exclusive right to upload the easyPDF program onto her website.

- (2) To issue copies of the computer programme to the public

Illustration 1: Sanya has the exclusive right to provide the easyPDF program along with computer magazines so that the general public can use the software.

Illustration 2: Sanya has the exclusive right to upload the easyPDF program onto her website so that people around the world can download it.

- (3) To perform the computer programme in public, or communicate it to the public,

Illustration: Sanya has the exclusive right to give a public demonstration of the workings of the easyPDF program.

(4) To make any cinematograph film or sound recording in respect of the computer programme,

Illustration 1: Sanya has the exclusive right to make a promotional film depicting the working of the easyPDF program.

Illustration 2: Sanya has the exclusive right to make a promotional sound recording depicting the working of the easyPDF program.

(5) To make any **translation** of the computer programme

Illustration: Currently the easyPDF program has all the menu commands and help files in English. Sanya has the exclusive right to make a version of the easyPDF program that has the menu commands and help files in Hindi.

(6) To make any **adaptation** of the work

(7) To do, in relation to a translation or an adaptation of the computer programme, any of the acts specified above

(8) To sell, give on hire, offer for sale, or offer for hire, any copy of the computer programme.

Illustration 1: Sanya has the exclusive right to offer the easyPDF program for sale.

Illustration 2: Sanya has the exclusive right to act as an Application Service Provider for the easyPDF program e.g. a user will be charged a small fee for every document that he converts to PDF using the easyPDF program.

2.2 First owner of copyright

Section 17 of the Copyright Act is the relevant provision. To understand who the first owner of copyright is, let us take some simple illustrations:

Illustration 1: Sanya, a college student, has created easyPDF, a computer program for converting documents into PDF (Portable Document Format). Sanya will be the first owner of copyright in the easyPDF program.

Illustration 2: Pooja is a computer programmer employed with Noodle Software Ltd. Under her contract of employment with Noodle, the intellectual property in all computer programs created by her vests with Noodle. During the course of her employment, Pooja creates "Rage of Vampires", a computer game. The first owner of copyright in "Rage of Vampires" will be Noodle Software Ltd.

Illustration 3: Tanya is a freelance software consultant who advises several software companies. In her free time she creates easyNote, a personal accounting and finance software. Tanya will be the first owner of the copyright in easyNote.

Illustration 4: Sameer is a lawyer who is also proficient in computer programming. He is employed with N&P Law Firm. Under the terms of his employment with N&P Law Firm, the intellectual property of all legal opinions and drafting created by Sameer vests with the law firm.

Considering Sameer's proficiency in computer programming, his senior at N&P Law Firm requests him to make a "law firm management" software. Sameer creates this software on his holidays. Sameer will be the first owner of the copyright in the law firm management software.

2.3 Term of copyright

According to section 22 of the Copyright Act, copyright subsists in a computer program for 60 years from the beginning of the calendar year next following year in which the author dies.

Illustration 1: Ketaki creates a computer program in 2008. She dies on 12th March, 2010. The copyright in the computer program will subsist for 60 years from 1st January 2011.

Illustration 2: Ketaki and Rajan together create a computer program in 2008. Ketaki dies on 12th March, 2010 while Rajan dies on 13th July, 2014. The copyright in the computer program will subsist till 60 years from 1st January 2015.

2.4 Licences

According to section 30 of the Copyright Act, the following can grant interest in a copyright by way of licences:

- (1) the owner of the copyright in any existing work
- (2) the prospective owner of the copyright in any future work

The licence must be given in writing and signed by the above or their authorised agents. Let us consider some illustrations to understand this concept.

Illustration 1: Sanya has created a computer program. She can grant Sameer a licence to sell the program from his website.

Illustration 2: Sanya is working to create a computer program. She is currently testing the "beta" version of the program. She

can grant Sameer a licence to sell the final program from his website once it is ready. This licence will take effect only when the final program comes into existence.

Illustration 3: Sanya is working to create a computer program. She is currently testing the “beta” version of the program. She grants Rajan a licence to sell the final program from his website once it is ready.

The final program is ready on 12th March, 2008. But by then Rajan has passed away. In this case Rajan’s legal representatives are entitled to the benefit of the licence.

2.5 Infringement of Copyright

The copyright in a computer program is deemed to be infringed when any person without a license or in contravention of the conditions of a licence:

- (1) does anything, the exclusive right of which is conferred upon the owner of the copyright by the Copyright Act, or
- (2) commercially permits any place to be used for the communication of infringing work to the public.

The following are also deemed to be infringement:

- (1) distributing, selling or hiring out infringing copies,
- (2) exhibiting infringing copies in public,
- (3) importing infringing copies into India.

There are several acts that are not deemed to be infringement of copyright. These are explained using the following simple illustrations. In these illustrations, we use the fictional illustration of Sanya who has created the easyPDF software. Sameer has purchased a CD containing the easyPDF software.

Illustration 1: Sameer can make a backup copy of the easyPDF software on another CD so that in case the original CD gets damaged, he can reinstall from the CD ROM.

Illustration 2: The CD purchased by Sameer contains the easyPDF software in a compressed format. Sameer can decompress the software so that it can be installed on his computer.

Illustration 3: The easyPDF software is giving some errors when Sameer installs it on a computer running the proWord software. Sanya is unable to provide any information on why

this is happening. Sameer can decompile the easyPDF software to study its code and fix the error.

Illustration 4: Sameer can test the easyPDF software for security vulnerabilities.

Illustration 5: Sameer is using the easyPDF program on his personal laptop. He can also use a copy of the program on his personal desktop computer for non commercial purposes.

Punishment for copyright infringement:

Knowingly using the infringing copy of a computer program on a computer is punishable with:

- (1) imprisonment for a term between **7 days** and **3 years** and / or
- (2) fine between **Rs. 1 lakh** and **Rs. 2 lakh**

In case the infringement has not been made for commercial gain, the Court may impose **no imprisonment** and may impose a fine upto **Rs 50,000**.

The offence can be tried by a **magistrate** not below the rank of a Metropolitan Magistrate or a Judicial Magistrate First Class.

In case of offences by companies, persons in charge of the company are also liable unless they prove that the offence was committed:

- (1) without their **knowledge** or
- (2) despite their **due diligence** to prevent it.

Microsoft Corporation v Mr. Kiran & Another

C.S. (OS) 111/2003

Microsoft Corporation instituted a suit for permanent injunction restraining the infringement of copyrights etc. against Mr. Kiran.

Mr. Kiran was illegally loading Microsoft software on computers that his company was assembling and selling. The software loaded onto the machine was not accompanied by the original Media i.e.:

1. Compact Discs,
2. Certificate of Authenticity (COA),
3. End User License Agreements (EULAs),
4. User Instruction Manuals,
5. Registration Cards etc

that accompany the plaintiff's genuine software.

Points put forth by Microsoft

1. Microsoft Corporation's computer programs are "works" that were first published in the USA and are also registered in the USA. These programs have been created by Microsoft Corporation's employees for Microsoft.
2. Under the US Copyright Law, US Code Title 17, Section 201(b), the copyright in a work created by an employee belongs to the employer under the "Work made for Hire" doctrine.
3. The computer program, as well as the supplementary User Instructions and Manuals, are "original literary works" as contemplated under Section 2(o) and Section 13(1)(a) of the Copyright Act, 1957. Microsoft Corporation is the owner of the said copyrights.
4. The rights of authors of member countries of the Berne and Universal Copyright Conventions are protected under Indian Copyright law. India and the USA are signatories to both the Universal Copyright Convention as well as the Berne Convention.
5. Microsoft's works are created by authors of member countries and originate from and are first published in the said member countries. These works are, thus, protected in India under Section 40 of the Copyright Act, 1957 read with the International Copyright Order, 1999.
6. Microsoft suffers incalculable damage to its intellectual property rights and business on account of various forms of copyright piracy.
7. A brief description of common methods of copyright infringement employed in relation to computer software is:
 - a. reproducing the software and its packaging so that purchasers are deliberately misled into believing that the product they are buying is genuine software.
 - b. reproducing or "burning" the software onto a blank CD, where no attempt is made to represent that the copy is genuine.
 - c. reproducing a number of the programs on a single CD-ROM, known as a "compilation" CD.
8. Another form of piracy that is assuming great significance in the information age is that of Internet piracy. Internet piracy occurs when software is downloaded from the Internet or distributed via

the Internet without the permission of the copyright owner. Common Internet sites used for this infringing activity include online classified advertisements, Auction Houses, newsgroups, personal web sites and Bulletin Board Service (BBS) sites.

9. Mr. Kiran is indulging in the illegal activity of counterfeiting and piracy. Microsoft had earlier called Mr. Kiran for a settlement meeting which he ignored.
10. Microsoft had earlier obtained ex parte ad interim injunction restraining Mr. Kiran from manufacturing, selling, offering for sale, distributing, issuing to public, counterfeit / unlicensed versions of Microsoft software.
11. Microsoft has suffered damages under the following heads:
 - a. **Actual Damages** – Microsoft has suffered a heavy loss of revenue due to the unauthorized loading of pirated versions of the software free of cost, onto the computers of Mr. Kiran's consumers.
 - b. **Damages to Goodwill and Reputation** – The unauthorized loading of Microsoft software from pirated CDs has undermined Microsoft's reputation and goodwill.
 - c. **Exemplary Damages** - Such damages are awarded if there is a flagrant violation by the defendants of the plaintiff's rights, to set a deterrent example for others. Such violation can be inferred from, inter alia, nature of the infringing act, reasonable knowledge of a person skilled in the concerned trade and continuance of violation despite knowledge. Mr. Kiran's act leaves no doubt as to the flagrant violation of Microsoft, the plaintiff's, intellectual property rights.

Findings of the Court

1. The computer industry is a high investment industry not only in terms of money but also in terms of the valuable time, skill and effort which goes into the development of new and advanced computer programs and software, therefore, it becomes imperative that the illegal trade activities of traders like the defendants are restrained and the dangerous growth of the computer software piracy be stemmed. And since Microsoft is the world leader in this field, it tends to be the main target of such counterfeiting and piracy.

2. Various averments made by Microsoft have gone unrebutted as Mr. Kiran has not come forward with any defence.
3. Microsoft has been able to prove that Mr. Kiran has been infringing its copyright, as there is no licence granted by Microsoft to Mr. Kiran for this purpose.
4. Mr. Kiran has willfully, intentionally and flagrantly violated the copyrights and trade mark of Microsoft and has disregarded Microsoft's rights and caused "deliberate and calculated" infringement of copyrights and trademark.
5. Software piracy is a menace and needs to be put down with a heavy hand.

Conclusion

A decree for permanent injunction was passed in favour of Microsoft against Mr. Kiran restraining him from using or otherwise copying, selling, offering for sale, distributing, issuing to the public, counterfeit/unlicensed versions of Microsoft software, in any manner, amounting to infringement of Microsoft's copyrights in the said computer programs and related manuals.

A decree of damages was also passed in favour of Microsoft for Rs. 5 lakh.

3. Software Licenses

Licenses are far more prevalent in the “intangible” world as compared to the “real” world. Suppose you buy a car. Once you pay the price of the car to the dealer, you can do almost anything with the car. You can sell it, rent it, make modifications to it and even destroy it!

The situation is not the same when you “buy” software. In fact you hardly ever “buy” software. You buy a “license” to the software. This license sets the terms and conditions subject to which you can use (and sometimes distribute and modify) the software.

A software license usually consists of

1. **permissions** granted by the creator to the user,
2. **rights** granted by the creator to the user, and
3. **restrictions** placed by the creator,
4. limitations on the creator’s **liability**,
5. **warranties** and warranty disclaimers, and
6. **indemnity**,
7. **term** / duration of the license.

Violating the terms of the license infringes the legal rights of the creator of the software and can lead to **legal action**.

When a software is **mass produced** and sold, the license is usually of a **“take-it-or-leave-it”** type. The software vendor does not give the purchaser an opportunity to negotiate the terms of the license. The purchaser can either accept the license in total and purchase it or reject the license and not purchase it. In **customized software** that is usually specially developed for a particular customer, the terms of the license are negotiated between the creator and the user.

Software licenses can be of various types such as:

(1) **Time-based licenses** where the license expires after a particular time period (e.g. 1 year). The license has to be renewed after that (usually on payment of additional fees).

Illustration 1: AVG is a popular anti-virus software. Licenses can be purchased for 2 years at a time. During these two years all updates will be available to the user. On expiry of the 2 year period, the license expires and the user must uninstall the software. If the user wants to continue using the software, he must again pay fees and buy a license for a further 2 years.

Illustration 2: Winhex is a popular cyber forensics software. It can be purchased with a 1 year upgrade license. Suppose Sameer

purchases this license on 1st January 2008. Till 31st December 2008, he will be eligible to get all upgrades and new versions of Winhex for free. After 1 year this upgrade license will expire. Although Sameer can continue using Winhex, he will not get any further updates for free.

- (2) **User-based licenses** where the license fee depends upon the number of computers on which the software will be installed (e.g. in case of application software like a word processor). It could also depend upon the number of users who will connect simultaneously to a computer on which the software is installed (e.g. in case of database software or server operating systems)
- (3) **Feature-based licenses** where the license fee depends upon the features that are required by the user.

Illustration: Winhex is a popular cyber forensics software. Depending on the features that are required, users can purchase the personal license, professional license, specialist license, or forensic license.

Most software licenses also contain clauses relating to disclaimer of warranties, limitation of liability, privacy policy etc. In this book we will focus on software licenses from an intellectual property rights perspective only.

3.1 Freeware Licenses

Freeware is computer software that is: copyrighted, available for use free of charge and available for an unlimited time.

Freeware is created and distributed by software developers who want to contribute something to the society but at the same time they want to control the future development of their software. They usually retain their rights over the source code.

A freeware license is basically: personal, non-exclusive, non-transferable and limited.

Many freeware licenses restrict the use of the software for commercial or “non-personal” purposes. The license is non-exclusive as it does not confer any exclusive rights on a particular user. The license is non transferable and does not permit the licensee to transfer any rights to a third person.

The license is limited in the sense that it does not permit any alterations to the software (this is anyway not legally possible without the source code). The license may be further limited in terms of the purposes for

which it is permitted. This may be defined by the creator in a positive or negative fashion.

Illustration: Sanya has created easyPDF software and released it with a freeware license. The license states that the software cannot be used for commercial or military purposes. This is a limitation described in a negative fashion as it defines what cannot be done.

Terms of a freeware license usually include:

There are no prescribed standards for freeware licenses and software developers are free to choose and modify licenses as per their needs. This section discusses some of the clauses most commonly found in freeware licenses.

Although most of the clauses would also apply to web based code (such as Active Server Pages etc), this discussion primarily relates to non web-based application or system software.

(1) Describing what all is covered by the license

The freeware license usually covers and extends to the “content” of the software which includes all text, graphics, user interfaces, visual interfaces, trademarks, logos, and computer code

The license covers all aspects of the content including: design, structure, selection, coordination, "look and feel" and arrangement.

The freeware license itself is also covered by the license. The user does not have the right to change or modify the license in any way.

The license also extends to suggestions, ideas, enhancements, requests, feedback, recommendations, other information relating to the software and provided by anyone.

(2) Take-it-or-leave-it clause

The freeware license would contain a take-it-or-leave-it clause or statement. The usual wordings are:

By clicking the "I accept" button and/or using the software, you agree to these Terms of Use either for yourself or on behalf of your employer or another entity.

If you do not agree with the Terms of Use, you must press the "I do not accept" button below and you may not use the software.

(3) Restrictions and Prohibitions

This is one of the most important parts of the licence. It lays down what is restricted and / or prohibited. In many cases the creators of the software restrict its use for commercial purposes. The most common reason for this restriction is that the author has created two versions of the software – one for personal use (released as freeware) and one for commercial use (released commercially).

Commercial users may be given a limited license to test the freeware version for a limited period. After this they may be required to purchase the commercial license for continued usage. This concept is also discussed later under the section on shareware.

The meaning of commercial use can be interpreted differently and must be clarified in the license. Commercial use can mean either of the following: (i) use by a commercial organization such as a company. Under this interpretation, any usage by not-for-profit organizations (like Universities) would be permitted (even if the University was charging a fee for teaching the usage of the software) (ii) use for commercial purposes or endeavors. This would cover any commercial usage irrespective of the status of the user (whether an individual, a University, a company etc).

The license usually prohibits the following acts: modification of the software, adaptation of the software, translation of the software, preparing derivative works from the software, decompiling the software reverse engineering the software, disassembling the software.

Prohibitions in case of web based code include: copying, reproducing, republishing, uploading, posting, public display, encoding, translating, distributing, linking, mirroring and framing.

(4) Intellectual Property Ownership

The license must specify that the term "Intellectual Property Rights" covers all proprietary rights including but not restricted to rights existing globally under: copyright law, patent law, trade secret law, trademark law and unfair competition law.

(5) Trademarks

This clause lists the various trademarks owned by the software creator. In many countries the graphics, logos, designs, page headers, button icons, scripts and service names are also registered as trademarks, or trade dress.

This clause prohibits the unauthorized use of these trademarks and / or trade dress as part of domain names or in connection with any product or service.

(6) Jurisdiction

This clause specifies the city / country whose courts have exclusive jurisdiction over disputes involving the license.

3.2 Windows License

Considering the huge number of users worldwide who use the Microsoft Windows operating system, the Windows End-User License Agreement ("EULA") is discussed here.

This section discusses some of the terms of the EULA for Microsoft Windows XP Professional Edition. It may be noted that the EULA for most Microsoft products is similar.

(1) Basic information

The End-User License Agreement ("EULA") is a legal agreement between Microsoft Corporation and the end user. It extends to the Microsoft software accompanying the EULA as well as associated media, printed materials, "online" or electronic documentation, and Internet-based services (collectively known as "Software").

A user is bound by the terms of the EULA by installing, copying or otherwise using the Software. If a user does not agree to be bound by the EULA, he must not install copy or use the software.

The EULA applies to updates, supplements, add-on components, product support services, or Internet-based services components, of the Software obtained from Microsoft after the date of obtaining the initial copy of the Software.

To use Software identified as an upgrade, the user must first be licensed for the software identified by Microsoft as eligible for the upgrade. After upgrading, the user may no longer use the software that formed the basis for the upgrade eligibility.

(2) Grant of licence

Rights granted by the EULA are:

Installation and use

The user can install, use, access, display and run one copy of the Software on a single computer, such as a workstation, terminal or other device ("Workstation Computer"). The Software cannot be used by more than two (2) processors at any one time on any single Workstation Computer.

Mandatory Activation

The license rights granted under this EULA are limited to the first thirty (30) days after first installation of the Software unless the user activates the licensed copy through the Internet or telephone. Reactivation is needed if the computer hardware is altered.

Device Connections

The EULA permits a maximum of 10 computers or other electronic devices (each a "Device") to connect to the Workstation Computer to utilize one or more of the following services of the Software: File Services, Print Services, Internet Information Services, Internet Connection Sharing and telephony services.

Remote Desktop / Remote Assistance / NetMeeting

Remote Desktop access requires a separate Software license. As an exception, the single primary user of the Workstation Computer may access a Workstation Computer Session from any Device without acquiring an additional Software license for that Device.

Storage / Network Use

The EULA permits storage or installation of a copy of the Software on a storage device, such as a network server, used only to install or run the Software on other Workstation Computers over an internal network. An additional license is required for each separate Workstation Computer on or from which the Software is installed, used, accessed, displayed or run. A license for the Software may not be shared or used concurrently on different Workstation Computers.

(3) Reservations of rights and ownership

Microsoft reserves all rights not expressly granted in the EULA. The EULA stresses that the Software is protected by copyright and other intellectual property laws and treaties and that Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the Software. The EULA also expressly states that the Software is licensed, not sold.

(4) Reverse Engineering

The EULA prohibits reverse engineering, decompilation and disassembly of the software unless such activities are permitted by the law. Exception - Section 52(ab) of the Copyright Act permits this for specific purposes.

(5) Rental / commercial hosting

The EULA prohibits renting, leasing, lending or providing commercial hosting services with the Software.

(6) End user proof of license

A genuine Microsoft "Proof of License" label with a genuine copy of the software identifies a licensed copy of the Software. To be valid, the label must appear on Microsoft software packaging. If the label is received separately, it is invalid. The packaging should be kept as it has the label on it to prove that the user is licensed to use the Software.

(7) Software Transfer

The Software can be transferred to a different Workstation Computer. After the transfer, the Software must be completely removed from the former Workstation Computer.

The initial user of the Software may make a one-time permanent transfer of this EULA and Software to another end user, provided the initial user retains no copies of the Software.

This transfer must include the Software and the Proof of License label. The transfer may not be an indirect transfer, such as a consignment. Prior to the transfer, the end user receiving the Software must agree to all the EULA terms.

(8) Termination

Microsoft can terminate the EULA if the user fails to comply with the terms and conditions of the EULA. In such event, the user must destroy all copies of the Software and all of its component parts.

(9) Applicable Law

If the Software has been acquired in USA, the EULA is governed by the laws of the State of Washington.

If the Software has been acquired in Canada, the EULA is governed by the laws of the Province of Ontario, Canada.

If the Software has been acquired in the European Union, Iceland, Norway, or Switzerland, then local law applies.

If the Software has been acquired in any other country, then local law may apply.

3.3 Open Source Licenses

The Open Source Initiative (OSI) is a California (USA) based not for profit organization that spearheads the open source movement around the world.

To qualify as “open source”, the software must comply with several conditions. In order to understand these conditions, let us take a fictional illustration. Sanya has developed easyPDF - software for converting documents into PDF (portable document format). Sanya wants to release easyPDF as open source software. easyPDF must comply with the following conditions:

(1) Free Redistribution

The easyPDF license cannot restrict anyone from selling or giving away the easyPDF software as a component of an aggregate software distribution.

Illustration 1: Sameer advises small companies on using technology to streamline their business processes. He also sells software (including easyPDF) to such companies. Sanya cannot stop Sameer from selling easyPDF.

Illustration 2: Siddharth uses easyPDF along with some code developed by him to create easyWord, a word processing software. Sanya cannot stop Sameer from using the easyPDF software as part of easyWord.

The easyPDF license cannot provide for royalty or other fee for such sale or distribution.

Illustration3: In the previous illustrations, Sanya cannot charge Sameer or Siddharth any royalty or fee for selling or using easyPDF.

(2) Source Code

The easyPDF software program must include source code, and allow distribution in source code as well as compiled form.

Illustration 1: easyPDF is not distributed with the source code. However, when easyPDF is started up by a user, a message is flashed on the user's screen. This message contains details of the website from where the easyPDF source code can be downloaded for free. This is acceptable.

Illustration 2: easyPDF is not distributed with the source code. However, a CD containing the easyPDF source code can be obtained by sending the cost of postage and the cost of a blank CD to Sanya. This is acceptable.

The easyPDF source code must not be deliberately obfuscated. Obfuscated code (also called shrouded code) is source code that is very difficult to read and understand. Programs known as obfuscators can make source code very difficult to read and understand.

Let us take a **simple illustration of obfuscated code**. The following basic code can be put in a webpage:

```
<a href="http://www.sanyanagpal.com">Click here to visit Sanya Nagpal's website</a>
```

The webpage will display a link to sanyanagpal.com and will look something like this:

Click here to visit Sanya Nagpal's website

The obfuscated code will look like the illustration below:

```
<script  
language=JavaScript>m=%3Ca%20href%3D%22http%3A//www.sanyanagpal.com%2  
2%3EClick%20here%20to%20visit%20Sanya%20Nagpal%27s%20website%3C/a%3E'  
>;d=unescape(m);document.write(d);</script>
```

(3) Derived works

The easyPDF license must allow modifications and derived works. The license must also allow the modified or derived works to be distributed under the same terms as the easyPDF license.

(4) Integrity of the author's source code

The easyPDF license can restrict the source-code from being distributed in modified form under some conditions that are illustrated below.

Illustration 1: The easyPDF license allows others to include “patch files” along with the original easyPDF source code. The “patch files” can modify the easyPDF program at the time when it is compiled.

Illustration 2: The easyPDF license can state that the derived works must have a different name.

Illustration 3: Sanya has release easyPDF version 1. The license can state that the derived software must have a different version number.

(5) No Discrimination against Persons or Groups

The license must not discriminate against any person or group of persons.

Illustration: The easyPDF license cannot state that Pakistani citizens cannot use the program.

(6) No Discrimination against Fields of Endeavor

The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research.

Illustration: The easyPDF license cannot state that it cannot be used in commercial organisations or banks etc.

(7) Distribution of License

The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties.

Illustration: Sanya is distributing the easyPDF software from her website. Sameer copies the easyPDF source code and program and distributes it from his website. Pooja downloads easyPDF from Sameer's website. The rights attached to easyPDF now automatically lie with Pooja also.

(8) License Must Not Be Specific to a Product

The rights attached to the program must not depend on the program being part of a particular software distribution.

Illustration: Sanya is distributing the easyPDF software along with a group of other software that she has developed. Collectively this group is called the easySuite and distributed by Sanya as open source.

Sameer extracts the easyPDF program from easySuite. He then distributes easyPDF to Pooja.

Pooja will have the same rights as those granted by easySuite.

(9) License Must Not Restrict Other Software

The easyPDF license must not place restrictions on other software that are distributed along with it.

Illustration: The easyPDF license cannot state that all programs distributed on the same CD must be open source software.

(10) License Must Be Technology-Neutral

No provision of the license may be predicated on any individual technology or style of interface.

Illustration: The easyPDF license cannot be a click-wrap licence i.e. it cannot ask users to click on an "I Accept" button.

This is because "click-wrap" agreements are not possible in many cases such as FTP download or where the source code is run in a command line / non-GUI (Graphical User Interface) based environment.

3.4 GNU General Public License

Many popular software programs come with a licence similar to the one illustrated below:

This file is part of the easyPDF Software Suite.

easyPDF Software Suite is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License version 3 or any later version as published by the Free Software Foundation.

easyPDF Software Suite is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with easyPDF Software Suite.

If not, see <<http://www.gnu.org/licenses/>>.

GNU General Public License (GNU GPL) is one of the most popular licenses in contemporary software.

Essential features of GNU GPL version 3 are:

(1) It is a copyleft license for software and other kinds of works.

Copyleft is a general method for making a program or other work free, and requiring all modified and extended versions of the program to be free as well. Copyleft mandates that anyone who redistributes the software, with or without changes, must pass along the freedom to further copy and change it.

Usually, to copyleft a program, the programmer first states that the software is copyrighted. Then he adds distribution terms and conditions which are a legal instrument. These terms give everyone the rights to use, modify, and redistribute the program's code or derivatives only if the distribution terms are unchanged.

Copyleft is thus the opposite of copyright. Copyright takes away a user's freedom while copyleft guarantees the freedom.

(2) GNU GPL guarantees the freedom to share and change all versions of a program. This ensures that the software remains free software for all its users. GNU GPL covers free software. This does not imply that there can be no money charged for the software. It refers to freedom to do the following: to distribute copies of the software, to run the software for any purpose, to sell copies of the software, to access the source code, to modify the source code, to study how the software runs, to change and adapt the software and to use parts of the software for new free programs.

(3) The GNU GPL prohibits the registration of patents that can make the software "non-free". The following illustrations will clarify some of the conditions of the GNU GPL. The illustrations are based on a fictional situation where Sanya has developed easyPDF - a software for converting documents into PDF (portable document format). The easyPDF software and its source code have been released under GNU

GPL. Sanya holds the copyright over the source code as well as the software.

Illustration 1: Sanya can sell the easyPDF software and / or source code for any price that she deems suitable.

Illustration 2: Sanya can charge a fee for downloading the easyPDF software and / or source code from her website.

Illustration 3: Sameer pays a fee and downloads the easyPDF software from Sanya's website. Sameer can now distribute the software for free from his website, on CDs etc.

Pooja gets the software free from Sameer's website. Pooja is not required to inform Sanya about receiving the software. She is also not required to pay Sanya any fees.

Illustration 4: Sanya cannot ask Sameer to enter into a non-disclosure agreement in respect of the easyPDF software / source code.

Illustration 5: Sameer modifies the easyPDF source code. Sameer cannot ask Pooja to enter into a non-disclosure agreement in respect of the modified easyPDF software / source code.

Illustration 6: Noodle Ltd has requested Sanya to make some modifications to the easyPDF source code. Noodle Ltd and Sanya can enter into a non-disclosure agreement whereby Sanya cannot disclose these modifications till Noodle approves them.

Noodle can insist that Sanya cannot release the modified software / source code to anyone else without their permission.

Noodle has the right to distribute the software / source code to others without Sanya's permission.

Illustration 7: Sanya can write a copyright notice in her own name in the license. E.g. the easyPDF source code files can have the following notice: *Copyright © 2008 Sanya Nagpal*.

Illustration 8: Sanya can simultaneously release the easyPDF source code / software under the GNU GPL as well as under a commercial licence.

Illustration 9: Sameer wants to use the easyPDF source code along with the easyBook source code (created by Pooja) and combine them to create a new software program.

If the licences of easyPDF and easyBook allow the source codes to be combined then the two licences are said to be compatible. If not, the licences are incompatible.

Some licences may allow linking of the codes but not merging their code into one module.

The licences of two programs need not be compatible in case the programs are simply required to be installed in the same computer.

Illustration 10: Sanya cannot licence the easyPDF software / source code to Sameer for exclusive use. The GNU GPL license cannot be revoked.

Illustration 11: Sanya cannot force users of easyPDF software / source code to make their PDF documents open source. She has no rights over the documents created by others using easyPDF.

However, if the easyPDF program copies part of itself onto the output, then the output would also come under GNU GPL.

4. Computer Databases & the Law

According to section 43 of the Information Technology Act (IT Act), a "computer data base" means

a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network.

Computer database is a representation of information, knowledge, facts, concepts or instructions. This representation can be in text, image, audio, video. This representation must be such as being prepared in a formalized manner or has been prepared in a formalized manner or has been produced by a computer, computer system or computer network. Computer database is intended for use in a computer, computer system or computer network.

Illustration 1: Sameer has prepared an online database of all Hindi movies. This database is searchable by movie name, director name, lead actor etc.

Illustration 2: The Noodle Ltd website contains several password protected web-pages. The usernames and passwords of all authorized users are contained in a Microsoft Access database.

Illustration 3: Noodle Telecom Services Ltd creates a CD ROM containing the names and phone numbers of all their subscribers.

Illustration 4: Noodle School has an automated system for student administration. This system is powered by a database that contains detailed student information.

One table of this database is titled “basic_info” and contains the following categories of information:

Roll no.	Name	Address	Phone	Email

Another table is titled “student_marks” and contains the following categories of information:

Roll no.	Test 1	Test 2	Test 3	Final

When a student's report card is to be prepared, the system automatically takes the marks from the “student_marks” table and the name and contact information from the “basic_details”

table. It then collates the information and prepares the final report card.

Illustration 5: Noodle Law Firm has prepared a computerized database of all their client companies along with the relevant contact persons.

An interesting element of computer databases is that copyright can exist in two levels. Firstly, the information contained in the database may be the subject of copyright e.g. a list of computer vulnerabilities and the relevant security measures. Secondly, the actual representation of this information may be the subject of copyright protection e.g. the above mentioned information in a searchable online database. Let us take a simple illustration to see this protection at “two levels”.

Illustration: Sanya is a computer security professional. Based upon years of experience in this field, she prepares three large lists: (1) A list of vulnerabilities in major operating systems. (2) A list outlining the ways in which these vulnerabilities can be exploited. (3) A list outlining the security measures to plug these vulnerabilities.

She then enters this information into a Microsoft Access database. This database is searchable using Sanya’s website. Registered users of her website can enter the name of their operating system. The website then displays the list of vulnerabilities, relevant exploits and security measures.

The three lists that Sanya has prepared can be the subject of copyright protection. The online database containing the information in the lists can also be the subject of copyright protection.

Diljeet Titus case

130(2006)DLT330, 2006(32)PTC609(Del)

This case involved two counter suits filed by a group of legal professionals. Diljeet Titus (the plaintiff) is the proprietor of Titus and Co. His colleagues Alfred Adebare, Seema Jhingan, Alishan Naqvee and Dimpy Mohanty (hereinafter referred to as defendants) had left Titus and Co. While leaving Titus and Co, the defendants had taken with them computer data (from the computers of Titus and Co) relating to:

(1) proprietary drafts of precedents, agreements, forms, presentation, petitions, confidential documents, legal opinions, legal action plans, and

(2) computerized database containing client information, proprietary client list, proprietary potential client list and other related information.

Titus claimed to have copyright over the above.

The defendants claimed to be the owners of the copyright in what they had created. It was their contention that the creation was independent and was created by advising and counseling the clients.

The defendants sought a decree of declaration that they were the owners of the copyright in what they had created and sought a permanent injunction against Mr. Titus and his firm from using and parting with the same.

The question was whether there was exclusive right of any of the parties in what they had created or it was a joint right.

Background of the case

Just a couple of days before leaving Titus and Co, one of the defendants visited the Titus office (after office hours). He connected a CD-Writer to an office computer which was part of the office computer network. He then copied 7.2 GB of confidential data onto CDs and emailed some data to himself and other defendants. Additionally, the defendant took-

(1) proprietary legal drafts

(2) CDs (licensed in the name of Titus and Co.) of foreign judgments, precedents, conveyances and forms

(3) 3,000 visiting cards

Following a criminal complaint, the police raided the residence-cum-office of the defendant and seized hard disks from four computers found there. The confidential data referred to above was found in the said hard disks.

Points put forth by the Plaintiff

Mr. Titus put forth the following points:

(1) All the defendants were in full time employment of Mr. Titus.

(2) The billing to the clients was in the name of Mr. Titus.

(3) The defendants were paid performance linked remuneration and were under the discipline and regime of Mr. Titus which included maintaining daily time sheets and adhering to the disciplines of the plaintiff's law firm.

(4) There was no separate clientele of the defendants and the defendants provided professional services only to Mr. Titus and never independently represented any client of Mr. Titus.

- (5) The assignment of the work was done by Mr. Titus at his sole discretion.
- (6) The productivity of the defendants was determined by actual number of billable hours they had worked on a particular matter for a client of the plaintiff.
- (7) Under Mr. Titus' guidance and supervision the defendants and others developed extremely confidential electronic records, documents, data and information utilizing the computer system at Mr. Titus's office.

Points put forth by the Defendants

The Defendants claimed to be partners of Titus and Co. They stated that they had independently created most of the legal drafts and databases and as such were owners of the copyright in the same. The defendants put forth the following points:

- (1) They had a fee sharing agreement with Titus and Co.
- (2) They independently exercised professional skills and knowledge.
- (3) They had sole discretion to advise and serve clients without any supervision including that of Mr. Titus.
- (4) Mr. Titus' interaction on a daily basis with the clients was minimal and insignificant.
- (5) The time sheets were maintained only for billing purposes.
- (6) There was no fixed salary or remuneration for the defendants.

Findings of the Court

- (1) If there are certain aspects in common domain, it is open for all and sundry to utilize the same. It may not be disputed that there are books on conveyancing giving formats of agreements and checklists. These are available for use by all. What is, however, important is the treatment meted out to such standard format while applying it for assistance to any particular client. It is the expertise of a person or a firm in handling such matters which persuades a client to approach them in preference to others.
- (2) If everything was in common domain and one had to only punch information, there would be no occasion for clients to engage services of advocates for such purposes and pay them large fees. There is a utility, and that too of great importance, of how a particular format is applied to the needs of a client which gives importance to the whole exercise.
- (3) If an associate or an advocate whatever be the terminology by which it is called works for another advocate and his clients he certainly owes a duty and obligation not only to maintain the confidentiality between the client and his advocate but also not to surreptitiously take away what is

the final product of the effort put in to which he also may be a party. The report filed by the Investigating Officer in the criminal case thus show *prima facie* that there is complete copying by the defendants of the material of the plaintiff which has been taken away. Such an exercise has become easier because of the development of technology where most of such data is stored on computers and can be transmitted away were a person to misuse the trust and authority vested in him in being in control of utilization of such material.

(4) The information about clients and solicitors also to some extent is in public domain where it appears in printed directories and everyone can use the same. However, as an advocate or a law firm develops its work and relationship with other law firms or clients, the details about the particular persons in such law firms handling certain nature of work or as to which officer in a client's company is material for getting the work becomes of great importance. Such a list is of great importance to an advocate or a law firm. The mere fact that defendants would have done work for such clients while being associated with the plaintiff would not give them the right to reproduce the list and take it away. It may again be emphasized that it is possible that a part of this information is retained in the memory of the defendants and if that is utilized no grievance can be made in this behalf. This would, however, be different from a copy made of the list.

(5) The legal pronouncements also make it clear that the copyright exists not only in what is drafted and created but also in list of clients and addresses specially designed by an advocate or a law firm. The exposition in the commentary of David Bainbridge on Software Copyright Law leaves no manner of doubt where it is emphasized that copyright can exist at two levels including the level of the database itself as a form of work in its own right. This has been cited with approval in Berlington Hope Shopping Private Limited case where it has been further emphasized that customers' list and information consisting of mail order catalogues itself amounts to confidential information.

Conclusion

The Court concluded that Titus and Co was a sole proprietorship concern and not a partnership. It held that the defendants did not have a right over the subject matter of the suit.

5. Domain name disputes

5.1 What is a domain name?

Every computer on the Internet is assigned a unique address called an Internet Protocol Address (IP Address). A typical IP address looks like this: 67.19.217.53

The above IP address belongs to a web server on which the official website of Asian School of Cyber Laws (ASCL) is hosted. If you use an Internet browser and type in <http://67.19.217.53> in the address bar, you will reach the ASCL website.

However, it is very inconvenient to remember such numbers. It is much easier for humans to remember names (asianlaws.org is a domain name). This is why the domain name system (DNS) was developed.

Simply put, DNS is like a very large telephone directory that maps domain names with IP addresses. It is the DNS that enables you to type in <http://www.asianlaws.org> instead of <http://67.19.217.53> and still reach the ASCL website. Let us examine a simple domain name: *data64.com*

This domain can be split into two parts – “data64” and “com”. The two parts are separated by a “.” or dot. The “com” is referred to as the top level domain. Thus we can say that “data64” is a sub-domain on the top level domain “com”. The following generic top-level domains were first implemented in January 1985:

.com	for commercial organizations
.edu	for post-secondary educational establishments
.gov	for governments and their agencies in USA
.mil	for the US military
.net	originally for network infrastructures
.org	for others

Subsequently many other top level domains were added. These include:

.aero	for the air transport industry
.asia	for companies, organisations and individuals in the Asia Pacific region
.biz	for business use
.cat	for Catalan language/culture
.coop	for cooperatives
.info	for informational sites, but unrestricted

.int	for international organizations established by treaty
.jobs	for employment related sites
.mobi	for sites catering to mobile devices
.museum	for museums
.name	for families and individuals
.pro	for certain professions
.tel	for services involving connections between the telephone network and the Internet
.travel	for travel agents, airlines, hoteliers, tourism bureaus, etc.

In addition there are country top level domains such as “.in” for India and “.us” for USA.

Important facts about domain names:

- (1) Domain names are not case sensitive i.e. DATA64.COM is the same as data64.com or dAtA64.CoM
- (2) Domain names can only contain alphabets, numbers and hyphens.
- (3) You cannot legally own a domain name. Domain names are licensed to you by the relevant registries in return for a fee.
- (4) You can find out information about a domain name holder using a “whois search”. However, the results of a whois search are not of much evidentiary value as anyone can register a domain using a fake name and address.

Are domain names trademarks?

A domain name is not itself a trademark. A trademark is a right, granted under law, to use a mark in commerce to represent a product (or a business, in the case of a trade name). A domain name is a word or phrase registered in the domain name registration system.

A domain name may be a company’s expression of its trademark. The use of a trademark in a domain name, for instance, is the equivalent of using the trademark on a billboard, or in advertising.

For example, the trademark “data64” can be used in magazine advertising, or in the domain name, data64.com. The use of the domain name may be the way in which a company initially establishes its rights to a trademark.

Illustration: The use by Data64 LLC of the domain name data64.com was one way in which Data64 LLC established its right to the “data64” trademark.

Whether a word or phrase used in a domain name qualifies for trademark protection is determined under regular trademark law. Trademark law does not protect the use of generic words, such as “computer”.

Similarly, if a domain name is the same name by which the product or service is typically described, the law will consider it ‘generic’ and will not treat it as a trademark.

For instance, the domain name computers.com uses a word that is the generic term for a class of products and will most likely never receive protection as a trademark because the law does not allow monopolies over generic terms.

While trademark law may not protect the use of domain names, such as medicines.com, exclusive use of a domain name is guaranteed by the domain name registration system.

However, while no other website can use the domain medicines.com, there may be nothing to prevent them from using derivatives or copycats such as medicines123.com or medicinesindia.com

5.2 Domain Name Disputes

Domain name disputes often arise when “cyber-squatters” intentionally register domain names that include a trademarked word, company name, name brand of a product, or even names of film stars.

However, these disputes are not always between a person with a purely speculative reason for registering the domain name and a person with a legitimate reason to want the domain name. Sometimes both parties have a legitimate use and right to the domain name.

Illustration: In 1994 a journalist preparing an article on domain name policy realized that McDonalds.com was available. He registered the domain name.

The fast food chain McDonalds pressured Networks Solutions Inc (NSI) into taking action against the journalist. At that time, there was no formal dispute policy in place. A week after revoking the registration, NSI realized it had made a mistake and reversed its decision.

Finally McDonalds paid US \$3,500 for retaining the domain name.

Cyber squatting is the registration of a domain name by someone who lacks a legitimate claim with the intent to sell the name, prevent the trademark holder from gaining access to the name, or to divert traffic

In typo-squatting the squatter registers a variant of a famous trademark.

Illustration: While typing in google.com many people accidentally type googlw.com as the “e” and “w” keys on the keyboard are next to each other. Registering the domain googlw.com to intercept traffic meant for google.com would be typo-squatting.

5.3 Domain Name Disputes in India

India's top level domain is *.in* and the sunrise period for the *.in* domains was from 1st January, 2005 to 21st January, 2005. During this period owners of registered Indian trademarks or service marks were given an opportunity to apply for “.in” domains. The booking was opened to the public from 16th February, 2005.

INRegistry is the official “.in” registry. INRegistry is operated under the authority of NIXI (National Internet eXchange of India)

NIXI is a not-for-profit company registered under section 25 of the Indian Companies Act. NIXI has been set up to facilitate improved Internet services in India.

INRegistry has the following responsibilities:

- (1) maintaining the “in” top level domain
- (2) ensuring the operational stability, reliability, and security of “.in”
- (3) implementing Government of India policies

INRegistry took over its role from National Centre for Software Technology (NCST) and Centre for Development of Advanced Computing (C-DAC). End users cannot register “.in” domains from INRegistry. Registrations are handled by INRegistry accredited registrars. The following are the registrars for specific domains:

- (1) National Informatics Centre is the registrar for *gov.in* domains
- (2) ERNET is the registrar for *res.in* and *ac.in* domains
- (3) Ministry of Defence is the registrar for *mil.in* domains

.in domain name disputes are resolved in accordance with the .IN Dispute Resolution Policy (INDRP) and the INDRP Rules of Procedure.

The INDRP outlines the types of disputes that can be brought and the criteria that will be considered by the arbitrators.

The INDRP Rules of Procedure describe how to file a complaint, how to respond to a complaint, the fees, communications, and other procedures.

5.4 The .in Domain Name Dispute Resolution Policy

The “.in Domain Name Dispute Resolution Policy” (INDRP) sets out the terms and conditions to resolve a dispute between the Registrant and the

Complainant, arising out of the registration and use of a “.in” Internet Domain Name. Registrant is a holder of the .in Internet domain name. Complainant is the person who has complaint against the Registrant.

Illustration: Sameer has booked the domain name “noodle.in”. Noodle Ltd files a complaint against Sameer to get the “noodle.in” domain transferred to its own name. In this case, Sameer is the registrant while Noodle Ltd is the complainant.

A complaint can be filed with the .IN Registry on the following grounds:

- (1) the Registrant's domain name is identical or confusingly similar to a name, trademark or service mark in which the Complainant has rights,
- (2) the Registrant has no rights or legitimate interests in respect of the domain name,

Simply put, the following circumstances demonstrate the Registrant's rights to or legitimate interests in the domain name:

- (a) Before any notice to the Registrant of the dispute, the Registrant uses or prepares to use the domain in connection with a bona fide offering of goods or services.
 - (b) The Registrant (as an individual or organization) has been commonly known by the domain name, even if the Registrant has acquired no trademark or service mark rights.
 - (c) The Registrant is making a legitimate non-commercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.
- (3) The Registrant's domain name has been registered or is being used in bad faith. Simply put, the following circumstances are evidence of the registration and use of a domain name in bad faith:
 - (a) circumstances indicating that the Registrant has registered / acquired the domain name primarily for selling, renting, or otherwise transferring it to the Complainant or its competitor for a profit.
 - (b) the Registrant has registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name [provided that the Registrant has engaged in a pattern of such conduct]
 - (c) by using the domain name, the Registrant has intentionally attempted to attract Internet users to the Registrant's website or other on-line location.

The basic procedure for the dispute resolution is:

(4) The Complainant files the complaint with the .IN Registry and pays the relevant fees. The Complainant can ask for cancellation of the Registrant's domain name or transfer of the domain name registration to the Complainant.

(5) The .IN Registry appoints an Arbitrator out of the list of arbitrators maintained by it. The List of the Arbitrators is published online at www.registry.in

(6) The Arbitrator conducts the arbitration proceedings in accordance with the Arbitration & Conciliation Act 1996 and the IDRP and IDRP Policy and Rules. The Registrant is required to submit to the mandatory arbitration proceeding. The Registrant cannot transfer a domain name registration to another holder: (a) for 15 working days after conclusion of the proceeding (b) during a pending case unless the transferee agrees to be bound by the decision.

The Registry reserves the right to cancel any transfer of a domain name registration to another holder that is made in violation of this paragraph.

(7) The Arbitrator decides on the complaint. All decisions under this Policy are published in full over the Internet. Note: An Arbitration Panel can decide in exceptional cases to edit portions of its decision.

5.5 The INDRP Rules

The “.in Domain Name Dispute Resolution Policy Rules” (INDRP Rules) describe the following: how to file a complaint, how to respond to a complaint, the fees, communications and other procedures.

The complaint

An arbitration proceeding in respect of a domain name dispute can be initiated by submitting a complaint (in hard copy and electronic version) to:

.IN Registry
c/o NIXI (National Internet eXchange of India)
Corp. Office: 121-123, Ansal Tower, 38
Nehru Place, New Delhi 110019

The complaint must contain the following:

- (1) Name, postal addresses, e-mail addresses, telephone numbers and facsimile numbers of the complainant.
- (2) Contact information of the respondent.
- (3) The domain name which is the subject of the complaint.
- (4) The trademark(s) or service mark(s) on which the complaint is based.
- (5) The grounds on which the complaint is made.

The following must be specified:

- (a) The manner in which the domain name is identical (or confusingly similar) to the complainant's trademark or service mark.
 - (b) reasons why the respondent should be considered to have no rights or legitimate interests in the domain name,
 - (c) reasons why the domain name should be considered to have been registered and as being used in bad faith.
- (6) The remedies sought.
 - (7) Any other relevant legal proceedings.
 - (8) Relevant documents.
- (9) Cheque / draft (in favour of 'NATIONAL INTERNET EXCHANGE OF INDIA') for the relevant fees. The fees for adjudication is payable as per the following schedule:

.IN Registry's Administration Fee	Rs.5000
Arbitrator's Fee	Rs.25000
Personal hearing	Rs.5000 per hearing

Note: In case the Arbitrator calls for personal hearings, the fees for the same are to be shared by the parties equally.

If any party requests for personal hearing and that request is allowed by the Arbitrator, the fees for it is payable by the requesting party.

Notification of complaint

The procedure followed by the .IN Registry on receipt of the complaint is as under:

- (1) If the complaint is in accordance with the policy and rules, it will be forwarded to the respondent within 3 working days.
.IN Registry sends the complaint to all postal, facsimile and email addresses shown in the domain name's registration data through .IN Registry's WHOIS database at www.registry.in [see next page for an illustration of registration data]
- (2) If the complaint is not in accordance with the policy and rules, the deficiencies will be notified to the complainant within 3 working days. The complainant must correct the deficiencies in 5 working days.
- (3) The .IN Registry then appoints an arbitrator from the list of arbitrators.
- (4) The complaint and documents are forwarded to the respondent and the arbitrator for adjudicating (in accordance with the Arbitration and

Conciliation Act 1996, rules thereunder, and the Dispute Resolution Policy & rules).

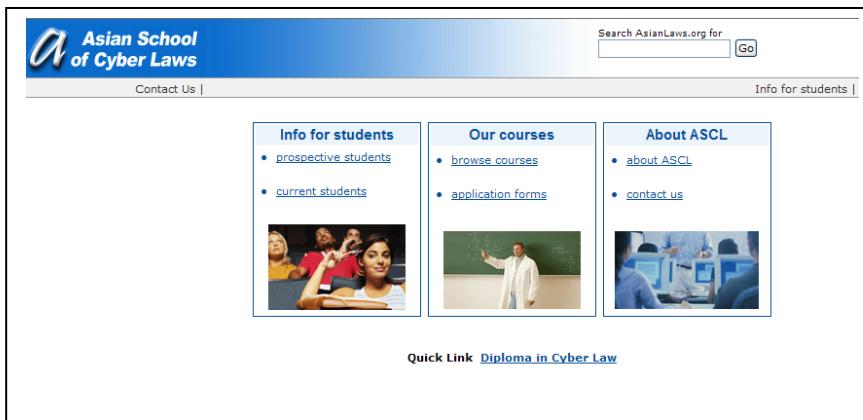
(5) Within 3 days from the receipt of the complaint the Arbitrator issues a notice to the Respondent. The date of commencement of the arbitration proceeding is the date on which the Arbitrator issues this notice to the respondent.

(6) The Arbitrator must pass a reasoned award (within 60 days) and put forward a copy of it immediately to the complainant, respondent and the .IN Registry.

6. Web related issues

6.1 Meta tags

Meta tags are codes contained within websites that provide a description of the website. Let us take the illustration of the Asian School of Cyber Laws (ASCL) website. When a student visits www.asianlaws.org, he sees the website illustrated below:



What the user does not see are the description and keywords meta tags as illustrated below:

```
<META content="education, training, consultancy, research, cyberlaws, cyber laws, cyberlaw, cyber law, cybercrime investigation, cyber crime investigation, cyber forensics" name=keywords>
```

```
<META content="Education, training, consultancy and research in Cyberlaws, cybercrime investigation and cyber forensics" name=description>
```

These tags are embedded in the source code of the website. They are put so that search engines (e.g. google.com, yahoo.com etc) can accurately identify what the website relates to.

As can be seen in the illustrations above:

- (1) The description tag contains a description of the web page.
- (2) The keywords tag contains relevant associated keywords.

When a user searches for “Asian School of Cyber Laws” in google.com, the first search result clearly contains the description of the ASCL website as per the description tag. This is illustrated below:

Google™ Advanced Search Preferences

Web Results 1 - 10 of about 1,100,000

Asian School of Cyber Laws
Education, training, consultancy and research in **Cyberlaws**, cybercrime investigation and **cyber forensics**.
www.asianlaws.org/ - 6k - Cached - Similar pages

[Diploma in Cyber Law](#) [Contact Us](#)
[Current students](#) [Our Courses](#)
[Prospective students](#) [About Us](#)

[More results from asianlaws.org »](#)

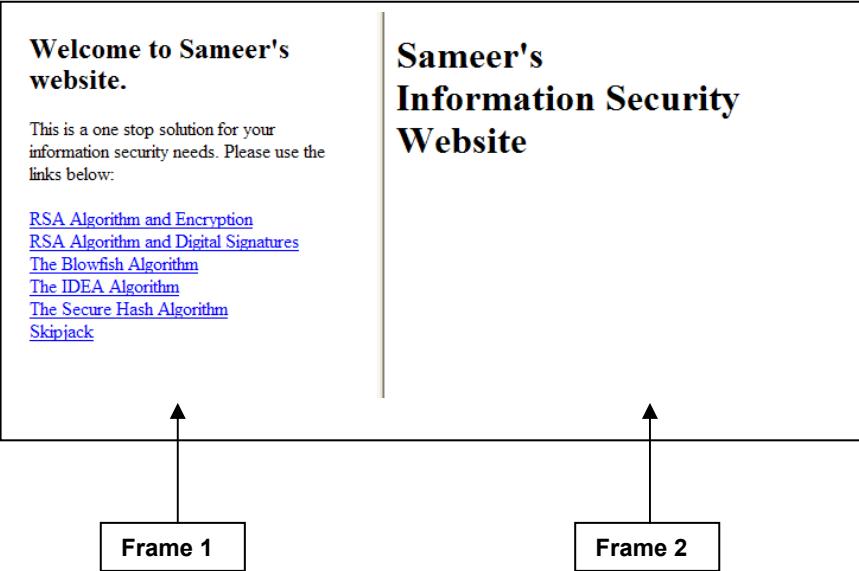
Trademark disputes can arise when someone's trademark is put by his rival in the meta tags of the rival website.

Illustration: Sameer sells a PDF creator software that rivals the PDF creator sold by Adobe. If Sameer writes the words “Adobe” in the meta tags of his website, then the search engines may mistakenly index Sameer’s website as being related to Adobe. Web users looking for Adobe software may get diverted to Sameer’s website.

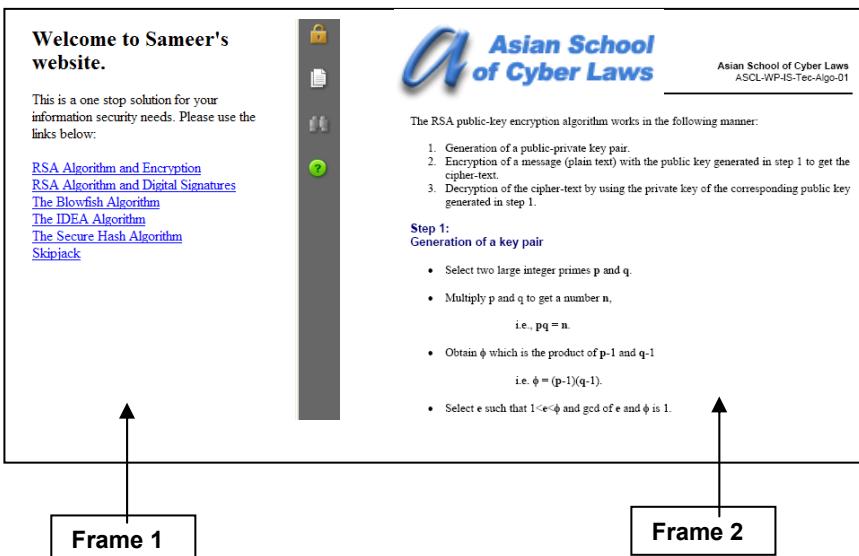
The act of putting meta tags of rival companies and brands in a website is also referred to as cyberstuffing.

6.2 Framing

A webpage can be divided into several frames. Each frame can display different content. Let us take a simple illustration. Sameer provides commercial consultancy in the field of information security. He puts up a website and one of the pages is illustrated below:



When a user clicks on the link “RSA Algorithm and Encryption” in Frame 1 above, a document from the Asian School of Cyber Laws (ASCL) website opens up in Frame 2. See the illustration in the next page:



To an ordinary user it may appear that the RSA Algorithm and Encryption document is a part of Sameer's website. In reality this document is being accessed from ASCL's website and being opened up in a frame on Sameer's website.

Clicking on the other links opens up different web pages in Frame 2 while the content in Frame 1 remains the same.

Such framing may give rise to a claim for **passing off** as an ordinary user may infer a business association between Sameer and ASCL. In reality, there is no business association between Sameer and ASCL. ASCL can claim that Sameer has indulged in misleading and deceptive conduct.

It is advisable to put a suitably worded disclaimer or acknowledgment which clearly informs the visitor about the relationship between the two sites (Sameer's and ASCL's in this case). For example Sameer could put the following disclaimer next to the link to ASCL's webpage.

This link leads to content on the website of Asian School of Cyber Laws (ASCL). The homepage of ASCL is at www.asianlaws.org

Sameer has no business or other association with ASCL and has provided this link purely for information.

6.3 Deep Hyperlinking

Simply, put hyperlink is a reference to a webpage or document on the Internet. Let us consider the **courses page** on the Asian School of Cyber Laws (ASCL) website.

This page is located at <http://www.asianlaws.org/courses/index.htm>

The screenshot shows a section titled "Our Courses" with two columns of course offerings. Each column features a small icon followed by a list of diploma programs.

Our Courses	
Diploma in Cyber Law	Diploma in Intellectual Property Law
Advanced Diploma in Cyber Laws	Diploma in Law relating to Corporate Mergers, Acquisitions & Reconstruction
ASCL Certified Cyber Crime Investigator	Diploma in Corporate Law
	Diploma in Business Laws
	Diploma in Securities & Investment Law
	Diploma in Patent Law
	Diploma in Infrastructure Law

The above webpage consists of several links to other web pages e.g. if a user clicks on the “Diploma in Cyber Law” link, he will be taken to the page containing details of the Diploma in Cyber Law course.

To a user the link appears as

Diploma in Cyber Law

In the source code of the website, the link appears as:

```
<a href=http://www.asianlaws.org/courses/dcl/index.htm>
```

Normally, no organisation or person objects if someone puts a hyperlink to their homepage. The objection comes when someone puts a link directly to an inner page or document.

For example, ASCL would not object if someone provides a link to the ASCL homepage (<http://www.asianlaws.org/index.htm>). However, if someone provides a link to a document “deep” in the ASCL website, then ASCL may have an objection.

Suppose Sameer puts a hyperlink in his website named “RSA Algorithm”. On clicking this link, the ASCL sponsored whitepaper on the topic opens up from:

http://www.asianlaws.org/infosec/library/algo/rsa_asym.pdf

This is called deep hyper-linking.

Deep hyper-linking may give rise to a claim for **passing off** as an ordinary user may infer a business association between Sameer and ASCL. In reality there is no business association between Sameer and ASCL. ASCL can claim that Sameer has indulged in misleading and deceptive conduct

It is advisable to put a suitably worded disclaimer or acknowledgment which clearly informs the visitor about the relationship between the two sites (Sameer’s and ASCL’s in this case). For example Sameer could put the following disclaimer next to the link to ASCL’s webpage.

This link leads to content on the website of Asian School of Cyber Laws (ASCL). The homepage of ASCL is at www.asianlaws.org

Sameer has no business or other association with ASCL and has provided this link purely for information.

7. Investigating IPR Crimes

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:

<i>File name</i>	<i>MD-5 hash value</i>
autimated-sheet.c	BFDF2A39169C6701C9AB28479BB1C256
buddy.c	4CA95ECF433D29C69566E6AAD9635494
calendar.c	38FB0AAF8D5C2942B942FCA237FBB33C
e-m-automation.c	680F17E9314F77715A431653E65F9020
tic-tac-toe.c	F32543DC2B10DA617A18B2C1884720B4

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.

Request for Service

RFS No. (Pl leave blank) IN-PNQ/03-08/085		Date 19 th March, 2008	
Client name and address SystNetSoft, Zimblia			
Client's authorised representative			
<i>Name</i> Manoj Kumar	<i>Email</i> mk@SystNetSoft.com	<i>Phone</i> 34221341	<i>Fax</i> 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.

<i>File name</i>	<i>MD-5 hash value</i>
autimated-sheet.c	BFDF2A39169C6701C9AB28479BB1C256
buddy.c	4CA95ECF433D29C69566E6AAD9635494
calendar.c	38FB0AAF8D5C2942B942FCA237FBB33C
e-m-automation.c	680F17E9314F77715A431653E65F9020
tic-tac-toe.c	F32543DC2B10DA617A18B2C1884720B4

For internal ASCL use only (Pl leave blank)

<i>Case recd on</i> 19 th March 2008	<i>Case recd by</i> Rohas Nagpal	<i>Referred by</i> Manoj Kumar
Tax Porn Financial	<u>Source Code</u>	Priority <u>1</u> 2 3 4 5 6 7 8 9 10

Chain of Custody Form

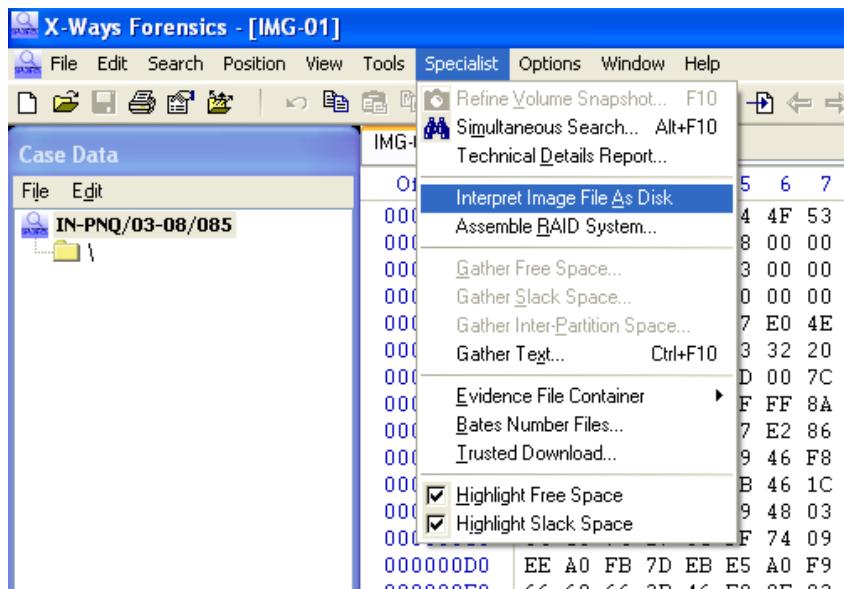
Lead Investigator:

Rohas Nagpal

1. Case Number: IN-PNQ/03-08/085	2. Evidence number: IMG-01		
3. Date and time of confiscation / recovery: 19 th March 2008 [1425 hours]			
4. Person from whom confiscated / recovered: Pooja			
5. Place of Confiscation / recovery: 128, Crescent Avenue, Zimblia			
6. Details of prior access / investigation: NIL			
7. Description of image file: Size: 507,490 KB MD-5 hash: 2D1D9725845E93FE1211C659D51108C6 SHA-1 hash: DCBF669CB5667558593146AD3FD43B8840FE6B38 Original media: iPod Shuffle 512 MB [Serial No. 5C644ZJCRS9]			
Chain of Custody			
Date & Time	Released by	Released to	Purpose of change of custody
20 th 2008 1430 hours	Rohas Nagpal	Manoj Kumar	Returned to client

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.



(3) I then recovered ?title9.mp3 using X-Ways Forensics.

(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:

<i>File name</i>	<i>MD-5 hash value</i>
autimated-sheet.c	BFDF2A39169C6701C9AB28479BB1C256
buddy.c	4CA95ECF433D29C69566E6AAD9635494
calendar.c	38FB0AAF8D5C2942B942FCA237FBB33C
e-m-automation.c	680F17E9314F77715A431653E65F9020
tic-tac-toe.c	F32543DC2B10DA617A18B2C1884720B4

(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.

13. Investigating Financial Crimes

Money is the most common motive behind all crime. The same is also true for cyber crime. Globally it is being observed that more and more cyber crimes are being committed for financial motives rather than for “revenge” or for “fun”.

With the tremendous increase in the use of internet and mobile banking, online share trading, dematerialization of shares and securities, this trend is likely to increase unabated. Financial crimes include cyber cheating, credit card frauds, money laundering, hacking into bank servers, computer manipulation, accounting scams etc.

Illustration 1: In April 2005, the Pune police arrested five employees of an MphasiS BPO for allegedly stealing almost Rs 2 crore from some Citibank customers. The accused had acquired the passwords to customer accounts and then transferred money to accounts opened under fictitious names.

Illustration 2: In March 2006, the Hyderabad police busted a counterfeit international credit card racket and arrested four people - Mohd Mohiuddin Khalid, Mirza Jawed Ali, Syed Muneeb Ahmed Irfan and Syed Ifteqharuddin Faheem. The 24 counterfeit credit cards recovered from the accused were allegedly manufactured in Taiwan, Indonesia and Malaysia.

Illustration 3: In August 2008, a software professional, S.V.N. Rajesh, was arrested by the Hyderabad police for allegedly misusing credit cards to purchase gold coins worth Rs. 20 lakh.

Rajesh was involved in marketing credit cards of different banks. During the course of his business he collected confidential information relating to more than a hundred high net worth individuals possessing premium category credit cards. He allegedly misused this information to place successful requests for change of address and add-on credit cards.

Interestingly, Rajesh never withdrew money from ATM centers as he feared that his photographs would be recorded by the bank cameras.

Illustration 4: In June 2008, the Hyderabad police arrested 8 youngsters involved in a Rs 10 lakh credit card fraud linked to an American Express call center.

The accused would first obtain the American Express international credit card details of foreigners, from some call

centre employees. Then they would use credit card information to make online payments for electricity, water and property tax bills for others. The people whose bills were paid for would be required to pay half the amount of the bill in cash to the accused.

Illustration 5: In January 2007, the U.S. Securities and Exchange commission filed a case against Aleksey Kamardin for allegedly manipulating share prices of penny-stocks by hacking into online share trading accounts of large investors. Aleksey would hack into these accounts and liquidate the holdings of the investors. He would then use the money in these accounts to pick up large quantities of penny stocks. When the price of these shares went up, he would then sell his own holdings of these shares. He is alleged to have made the equivalent of almost Rs 80 lakh by these fraudulent transactions.

A cyber crime investigator must understand the basics of finance in order to effectively investigate incidents of financial crime.

1. Basic Terms

You keep hearing that share prices are going up (or down!), the Sensex has crossed 20,000 points, it's a bull market, it's a bear market, stock prices are due for a correction etc – but what exactly does all this mean? Let us examine some of the relevant financial terms.

Equity shares

Equity shares are also called common shares and represent ownership of a company. As owners, equity shareholders normally have the right to elect directors and to vote on certain major corporate decisions. They are also entitled to share in any residual assets of the company if it is wound up.

It represents a share in the total equity capital of a company. Let us say that Noodle Ltd has raised Rs 100 from the public by way of equity share capital. That means members of the public have contributed this money to Noodle Ltd and in return they have received 10 shares of Rs 10 each (totaling Rs 100). If Noodle Ltd makes profits, these people (called shareholders) will receive benefits such as dividends, free shares (bonus shares) etc. If Noodle Ltd goes bankrupt, then the shareholders will lose their investment.

Equity shares are traded on stock exchanges (there are more than 6000 companies whose shares are traded on Bombay Stock Exchange). Equity share investments are **high risk – high return investments**. Risk depends upon factors such as the size, profitability and financial stability of the company, the capabilities of its management and its exposure to general economic downturns, foreign exchange risks and new competition.

Equity shareholders are the last in line (behind tax authorities, employees, creditors and preferred shareholders) to have claim on the assets of the company in the event of insolvency.

A **bonus issue** of shares implies that shares are given free of charge to the existing shareholders. In a **rights issue**, existing shareholders are given the right to purchase additional shares at a lower price.

The Sensex

"Sensex", which is the popular name for the Bombay Stock Exchange Sensitive Index, is the oldest stock market index currently in use in India.

It is a "**Market Capitalization-Weighted**" index of 30 stocks representing a sample of large, well-established and financially sound companies. The index is widely used to measure the performance of the Indian stock markets. BSE-SENSEX is considered to be the pulse of the Indian stock markets. Being the oldest index of the Indian Stock market, it provides data over a fairly long period of time (**since 1978-79**).

The objectives of the index are to measure market movements, describe the mood in the Indian Stock markets and act as a benchmark for mutual fund managers to compare the performance of their funds. SENSEX is calculated using a "**Market Capitalization-Weighted**" methodology wherein the level of index at any point of time reflects the total market value of 30 component stocks relative to a base period.

This market value (or market capitalization) of a company is determined by multiplying the price of its stock by the number of shares issued by the company.

Illustration: If Noodle Ltd has a total of 1 lakh equity shares and the current market price of each Noodle share is Rs 100, then the market value or market capitalization of Noodle will be $1 \text{ lakh} \times \text{Rs } 100$ i.e. Rs 1 crore. This also means that someone who wants to buy out 100% of Noodle's equity shares would need Rs 1 crore to do so.

The base period of SENSEX is 1978-79. The actual total market value of the stocks in the Index during the base period has been set equal to an indexed value of 100. This is often indicated by the notation 1978-79=100. The formula used to calculate the Index is fairly straightforward.

The calculation of SENSEX involves dividing the total market capitalization of 30 companies in the Index by a number called the Index Divisor. The Divisor is the only link to the original base period value of the SENSEX. It keeps the Index comparable over time and is the adjustment point for all Index maintenance adjustments.

During market hours, prices of the index scrips, at which latest trades are executed, are used by the trading system to calculate SENSEX every 15 seconds.

The criteria for selection and review of scrips for the BSE-SENSEX are:

- The scrip should figure in the top 100 companies listed by **market capitalization**.
- The scrip should have been **traded** on each and every trading day for the last one year subject to some exceptions.

- The scrip should be among the top 150 companies listed by average number of trades per day for the last one year.
- The scrip should be among the top 150 companies listed by average value of shares traded per day for the last one year.
- The average number of shares traded per day as a percentage of the total number of outstanding shares of the company should be greater than 0.05 % for the last one year.
- Scrip selection takes into account a **balanced representation** of the listed companies of BSE. The index companies should be leaders in their industry group.
- The scrip should have a **listing history** of at least six months on BSE.
- The company should preferably have a **continuous dividend paying record** and / or be promoted by **management having proven record**.

Illustration: The total market capitalization of the 30 scripts of the Sensex on the day the Sensex started was Rs 2 billion, when the Sensex value was 100. If, the total market capitalization today is Rs 250 billion, then the Sensex for today is calculated as follows:

$$\begin{aligned}
 &= \text{Old value} \times (\text{New capitalization} / \text{Old capitalization}) \\
 &= 100 \times (250 / 2) \\
 &= 12,500
 \end{aligned}$$

Balance sheet

Simply put, a balance sheet is an **accounting statement of a company's assets and liabilities**, provided for the benefit of shareholders and regulators. It gives a snapshot, at a specific point of time, of the assets that the company holds and how the assets have been financed.

The balance sheet of a company discloses the position of its assets and liabilities on a particular date. **Liabilities** represent things which the company owes to others e.g. bank loans, share capital etc. **Assets** are those things that the company has acquired by incurring those liabilities e.g. land, buildings, cars, machinery etc.

Illustration: Noodle Ltd has an equity capital of Rs 15 lakh and has taken a bank loan of Rs 10 lakh. It has invested Rs 14 lakh in buying a building, Rs 10 lakh in machinery and has a bank balance of Rs 1 lakh as on 1st April 2008. Its balance sheet as on 1st April 2008 would be as under:

Liabilities		Assets	
Equity share capital	15 lakh	Building	Rs 14 lakh
Bank Loan	10 lakh	Machinery	Rs 10 lakh
		Bank balance	Rs 1 lakh
Total	Rs 25 lakh	Total	Rs 25 lakh

As the name suggests, the total on both sides of the balance sheet would balance (i.e. be the same). You may wonder why equity capital is a liability for the company. The reason is simple. A company is a separate legal entity distinct from the share holders. The equity share capital represents the money invested by the equity share holders. In the event that the company is wound up, this capital is returnable to the shareholders (after paying off all the liabilities). That is why share capital is a liability.

A **current asset** is cash or an item of value expected to be converted into cash within one year or less. **Current liability** is money payable within the current accounting year or earlier to trade creditors etc.

Fixed assets are those that are used in current operation that would normally be of use for more than one year e.g. land, building etc. **Fixed liabilities** are obligations payable more than a year hence e.g. a ten year bank loan.

Intangible assets are those that cannot be touched or felt and whose true worth is almost impossible to determine e.g. goodwill, reputation, patents, trademarks, copyrights etc.

Bulls and bears

A **bull** is a market player who believes prices will rise and would, therefore, purchase a financial instrument with a view to selling it at a higher price. A **bull market** is a rising market with abundance of buyers and relatively few sellers.

A **bear** is a market operator who expects the market price of shares to decline. A bear would normally sell shares which he does not possess, in the hope of buying them back at a lower price, when the market price of the shares come down in the near future. A person can sell shares that he does not possess because he does not have to immediately “deliver” the shares sold by him. He is given a few days time for this. Bears can also use options and derivatives.

A **bear market** is a weak or falling market characterized by the dominance of sellers.

Blue Chip

The best rated shares with the highest status as investment based on return, yield, safety, marketability and liquidity are referred to as blue chips.

Circuit Breaker

This is a system applied by the Stock Exchange authorities to curb excessive speculation in the stock market. When the share price of a specific stock (or the index as a whole) rises or falls by more than a specified percentage, trading is then suspended for some time (or for the rest of the day) to let the market cool down.

Correction

This is a temporary reversal of trend in share prices. This could be a decrease following a consistent rise in share prices or an increase following a consistent fall in prices.

Insider Trading

An **insider** is a person who, because of his connections with a company, has access to unpublished price sensitive information in respect of securities of a company. This means that the information is not known to the public and is of such nature that it would affect the share price of the company.

Insider trading is the illegal act of buying or selling shares by or on behalf of an insider based upon such unpublished price sensitive information.

Junk Bond

A junk bond is a high yield bond issued by a low rated company. Investments in such bonds are very risky as there is a high probability that the company would default on its interest and principal repayment obligation. However the potential profits from such an investment are also high as the companies promise a very high rate of interest.

Earnings per share

Earnings per share (EPS) is an important financial ratio that helps to compare the profitability of various companies.

$$\text{EPS} = \frac{\text{Net Profit (after tax and preference share dividend)}}{\text{No. of shares}}$$

Illustration: The net profit of Noodle Ltd is Rs 5 lakh. Its share capital consists of 10,000 shares of Rs 10 each.

$$\text{EPS} = \frac{\text{Rs } 5,00,000}{10,000} = 50$$

Price to Earnings ratio

The price to earnings ratio (P/E ratio) is a ratio of the share price of a company to the earnings per share.

$$\text{P / E ratio} = \frac{\text{Market price per share}}{\text{Earnings per share}}$$

The P/E ratio indicates market expectations and is an important tool for gauging whether a share is overvalued or undervalued.

High P/E ratio indicates high growth potential and investor confidence. This is because a high P/E ratio indicates that the investors are ready to value the share at a higher multiple of its actual earnings as reflected by the EPS.

Illustration: Noodle Ltd manufactures mineral water. It has an authorized capital of Rs 2.8 crore and an issued capital of Rs 1.3 crore divided into equity shares of Rs 10. Its net profit for 2004-05 is Rs 26 lakh. The average P/E ratio of the mineral water industry is 42. Noodle shares are trading at Rs 52. Is the share overvalued or undervalued?

$$\text{No. of shares} = \frac{1,30,00,000}{10} = 13,00,000$$

$$\text{EPS} = \frac{\text{Net Profit}}{\text{No. of shares}} = \frac{26,00,000}{13,00,000} = 2$$

$$\text{P/E} = \frac{\text{Market price per share}}{\text{Earnings per share}} = \frac{52}{2} = 26$$

P/E of Noodle Ltd is below the industry average of 42. The Noodle shares are undervalued.

2. Shares

Every business organization needs funds for its growth strategies. This requirement can be short term or long term. The common avenues to raise short term funds are bank loans and public deposits.

Long terms funds can be raised through term loans from banks and financial institutions or through **issue of share capital**. Issue of capital can be through private placement of shares, public issue (i.e. raising funds from the public), rights issue, etc. In this section the various aspects related to shares are examined.

2.1 Types of shares

The two types of shares are Equity shares and Preference shares.

Preference share capital means that part of the share capital of the company which fulfils both the following requirements, namely:

1. it carries a preferential right to be paid a fixed dividend,
2. it carries a preferential right to be repaid in case of winding up or repayment of capital

Preference shares can be **cumulative or non-cumulative**. In case of cumulative preference shares if the dividend for a particular year is not paid (on account of the company making losses or insufficient profits), then the dividend is carried forward to subsequent years. In the subsequent years as and when the company makes sufficient profits, the pending dividend is required to be paid.

Illustration: Pooja holds one 10% cumulative Noodle Ltd. preference share having a face value of Rs 100. She is entitled to a dividend of Rs 10 each year.

In 2007, the company made losses and did not pay dividends to its preference shareholders. In 2008, it made a large profit. Pooja would be entitled to Rs 20 as dividend (Rs 10 for 2007 and Rs 10 for 2008).

In case of non-cumulative preference shares, the dividend is not carried forward.

Illustration: Pooja holds one 10% non-cumulative Noodle Ltd. preference share having a face value of Rs 100. She is entitled to a dividend of Rs 10 each year.

In 2007, the company made losses and did not pay dividends to its preference shareholders. In 2008, it made a large profit. Pooja would only be entitled to Rs 10 as dividend (for 2008).

Redeemable preference shares are those that are “bought back” or redeemed by the company after a fixed period. At the time of the issue it is decided whether the redemption will be at a premium or at a discount.

Illustration: Pooja holds one redeemable Noodle Ltd. preference share having a face value of Rs 100. It is redeemable at a discount of 10%. On redemption, Pooja would be given Rs 90 for the preference share.

Illustration: Pooja holds one redeemable Noodle Ltd. preference share having a face value of Rs 100. It is redeemable at a premium of 10%. On redemption, Pooja would be given Rs 110 for the preference share.

Irredeemable preference shares are not bought back or redeemed.

Equity shares are also called common shares and represent ownership of a company. As owners, equity shareholders normally have the right to elect directors, to vote on certain major corporate decisions and share the profits of the company in the form of dividends. They are also entitled to share in any residual assets of the company if it is wound up.

Illustration: Let us say that Noodle Ltd has raised Rs 100 from the public by way of equity share capital. That means members of the public have contributed this money to Noodle Ltd and in return they have received 10 shares of Rs 10 each (totaling Rs 100). If Noodle Ltd makes profits, these people (called shareholders) will receive benefits such as dividends, free shares (bonus shares) etc. If Noodle Ltd goes bankrupt, then the shareholders will lose their investment.

Equity shares are traded on stock exchanges (there are more than 6000 companies whose shares are traded on Bombay Stock Exchange). Equity share investments are **high risk – high return investments**.

Risk depends upon factors such as the size, profitability and financial stability of the company, the capabilities of its management, Government policies, the company’s exposure to general economic downturns, foreign exchange risks and new competition.

Equity shareholders are the last in line, behind tax authorities, employees (whose salaries etc may be due), creditors and preferred shareholders, to have claim on the assets of the company in the event of insolvency.

A **bonus issue** of shares implies that shares are given free of charge to the existing shareholders. In a **rights issue**, existing shareholders are given the right to purchase additional shares at a lower price.

2.2 Indian Capital & Stock Markets

The **Primary Market** is the place where the offerings of shares are made by Companies. This could be as an Initial Public Offering (IPO), a rights issue or a further issue of shares. A company makes these issues to raise share capital.

IPOs are offerings made by the Company for the first time. Such offer to the public can be at par or at a premium. The pricing of the issue depends upon the current status of the company and the company is allowed to fix a justifiable issue price.

Illustration: Noodle Ltd is a profit making company that has developed an international reputation. When it makes an IPO, it may price its shares (having a face value of Rs 10) at Rs 150. Here Rs 140 per share is the premium that Noodle Ltd is charging.

Illustration: Alpha Ltd is a new company. When it makes an IPO, it may price its shares (having a face value of Rs 10) at Rs 10. Here the shares are issued at par and there is no premium.

Rights issues are offerings of shares made to the existing shareholders.

Illustration: Noodle Ltd may offer its existing shareholders a 1:1 rights issue at Rs 100 per share. That means for every share held by a shareholder, he can purchase one additional at Rs 100. The rights price is usually lower than the current market price of the share. E.g. in this case the market price of Noodle Ltd shares may be Rs 140.

After an IPO, a rights issue or a further issue of shares by a company, the shares are traded on the secondary market. In other words investors can buy and sell shares on the secondary market or more precisely the stock exchanges.

The Bombay Stock Exchange (BSE) and the National Stock Exchange of India Ltd (NSE) are the two primary exchanges in India.

In addition, there are 22 Regional Stock Exchanges. However, the BSE and NSE have established themselves as the two leading exchanges and account for about 80 per cent of the equity volume traded in India.

Bombay Stock Exchange Limited is the oldest stock exchange in Asia with a rich heritage. Popularly known as "BSE", it was established as "The Native Share & Stock Brokers Association" in 1875. It is the first stock exchange in the country to obtain permanent recognition in 1956 from the Government of India under the Securities Contracts (Regulation) Act, 1956.

The Exchange's pivotal and pre-eminent role in the development of the Indian capital market is widely recognized and its index, SENSEX (Bombay Stock Exchange Sensitive Index), is tracked worldwide. Earlier an Association of Persons (AOP), the Exchange is now a demutualised and corporatised entity incorporated under the provisions of the Companies Act, 1956, pursuant to the BSE (Corporatisation and Demutualisation) Scheme, 2007 notified by the Securities and Exchange Board of India (SEBI).

The Exchange is professionally managed under the overall direction of the Board of Directors. The Board comprises of eminent professionals, representatives of brokers and the Managing Director of the Exchange.

In terms of organization structure, the Board formulates larger policy issues and exercises over-all control. The committees constituted by the Board are broad-based. The day-to-day operations of the Exchange are managed by the Managing Director and a management team of professionals.

The Exchange has a nation-wide reach with a presence in 417 cities and towns of India. The systems and processes of the Exchange are designed to safeguard market integrity and enhance transparency in operations.

The Exchange provides an efficient and transparent market for trading in equity, debt instruments and derivatives. The BSE's On Line Trading System (BOLT) is a proprietary system of the Exchange. The surveillance and clearing & settlement functions of the Exchange are ISO 9001:2000 certified.

The **National Stock Exchange of India Limited** has its genesis in the report of the High Powered Study Group on Establishment of New Stock Exchanges, which recommended promotion of a National Stock Exchange by financial institutions (FIs) to provide access to investors from all across the country on an equal footing.

Based on the recommendations, NSE was promoted by leading Financial Institutions at the behest of the Government of India and was incorporated in November 1992 as a tax-paying company unlike other stock exchanges in the country.

On its recognition as a stock exchange under the Securities Contracts (Regulation) Act, 1956 in April 1993, NSE commenced operations in the Wholesale Debt Market (WDM) segment in June 1994. The Capital Market (Equities) segment commenced operations in November 1994 and operations in Derivatives segment commenced in June 2000.

2.3 Initial Public Offering (IPO)

Initial Public Offering, in the context of this chapter, refers to the issue of shares by a company to the public for the first time and results in the listing of the company's shares on a recognised stock exchange.

Some of the advantages of an IPO are:

- (1) there is no liability to repay the money raised through the IPO except in case of buy back of shares or winding up of the company,
- (2) there is no liability to pay regular / fixed dividends,
- (3) once the company's shares are listed on a stock exchange, it becomes easier for the company to raise more capital in future,
- (4) it helps in building the reputation of the promoters and the company.

Some of the disadvantages of an IPO are:

- (1) the legal process is time consuming and expensive,
- (2) several intermediaries need to be involved in the process (e.g. merchant bankers, registrars, book running lead managers, underwriters etc),
- (3) the extensive transparency requirements and public disclosure of information may lead to lack of confidentiality,
- (4) once the company's shares are traded on the stock exchanges, there is the fear of a hostile takeover.

Book building process is a process by which a demand for the securities proposed to be issued by a company is elicited and built up. The company does not initially declare the exact price at which it would issue the securities. The exact price for the securities is assessed based on the price that investors are ready to pay and the quantum of securities that they are ready to purchase.

Illustration 1: Consider the red herring prospectus issued by HT Media Ltd for its 100% book building issue at a price of between Rs 445 to Rs 530 per equity share of face value Rs 10.

Book Building Process, with reference to the Issue, refers to the process of collection of Bids, on the basis of the Red Herring Prospectus within the Price Band. The Issue Price is fixed after the Bid Closing Date. The principal parties involved in the Book Building Process are the Company, the selling shareholders, SEBI registered intermediaries and the Registrar to the Issue.

Illustration 2: Assume that Noodle Ltd has offered 3000 equity shares at a price band of Rs. 20 to Rs. 24 per share and has received five bids as under:

Investor	Bid Quantity	Bid Price
A	500	24
B	1000	23
C	1500	22
D	2000	21
E	2500	20

The company would prefer the final price to be as close to Rs 24 as possible (so that it gets the maximum money). The next step is to calculate the highest price at (or above which) investors are ready to purchase 3000 shares. Consider the table below:

Investor	Bid Quantity	Bid Price	Cumulative Quantity
A	500	24	500
B	1000	23	1500
C	1500	22	3000
D	2000	21	5000
E	2500	20	7500

The highest price at which Noodle Ltd is able to issue the 3000 shares is the price at which the issue is subscribed, i.e., Rs. 22 in the above example.

The issuer, in consultation with the book running lead manager(s), will finalise the issue price at or below such cut-off price, i.e., at or below Rs. 22.

All bids at or above this issue price and cut-off bids are valid bids and are considered for allocation in the respective categories.

2.4 Rights issue

Rights Issue is when a listed company proposes to issue fresh securities to its existing shareholders as on a record date. The rights are normally offered in a particular ratio to the number of securities held prior to the issue. (E.g. 1:1 rights issue means one rights share for each share held by an existing shareholder).

This route is best suited for companies who would like to raise capital without diluting stake of its existing shareholders. Rights shares are usually issued at a discount to the market price.

Illustration: Noodle Ltd announces a 1:1 rights issue at Rs 100 per share. The market price of Noodle shares is Rs 150. Sameer owns 100 Noodle shares and hence is entitled to receive 100 additional shares at a discounted price of Rs 100.

One option available to Sameer is to exercise his rights and purchase the rights shares at the discounted price. Another option is for him to sell his entitlement. Pooja could buy the entitlement from Sameer at Rs 10 per share thereby paying Sameer Rs 1000. She could now buy the shares at Rs 100 from the company. Her total cost of acquisitions would be Rs 100 + Rs 10 i.e. Rs 110 per share.

2.5 Bonus issue

In case of bonus issues of shares, company issues fresh shares to existing shareholders as per the approved ratio, for instance one bonus share for every share held (1:1).

The existing shareholders are not required to pay any money for the bonus shares. The company “pays” for these additional shares out of its accumulated reserves. It is an accounting reclassification. A company’s reserves anyway belong to its shareholder. All that a bonus issue does is to issue shares against a part of those reserves and reclassify that portion of reserves as equity.

It is usually noticed that the share price of a company boosts up on announcement of a bonus issue. It is also noticed that the ex-bonus prices usually add-up to more than the pre-bonus price.

Illustration: Noodle Ltd shares are trading at Rs 100 on the stock exchange. The Earnings per share (EPS) of the company is 10 and its Price to Earnings ratio (P/E) is 10. The company announces a 1:1 bonus. The share price shoots up to Rs 120 on the announcement. After the bonus is issued, the ex-bonus price of the share becomes Rs 65.

Consider Sameer who initially held 100 Noodle shares. The value of his holding was Rs 10,000 (100 shares worth Rs 100 each). After receiving the bonus he now has 200 shares each valued at Rs 65. His total holding is now worth Rs 13,000 – an appreciation of 30%.

Post bonus the EPS would become 5 (total earnings have not changed but the number of shares have doubled so the EPS would become half). Post bonus P/E ratio of Noodle is $65 / 5 = 13$.

Some of the **advantages** of issuing Bonus Shares are that it increases the market price of the shares, creates confidence for the investors / shareholders in the company and improves the reputation of the company.

Some of the **disadvantages** are that shares are issued without any actual money coming in and the EPS of the company is reduced.

2.6 Sweat Equity

"Sweat equity shares" means equity shares issued by the company to employees or directors at a discount or for consideration other than cash for providing know-how or making available rights in the nature of intellectual property rights or value additions, by whatever name called.

In other words, sweat equity refers to equity shares given to the company's employees, on favorable terms, in recognition of their work.

It is used to refer to a **form of compensation** by businesses to their owners or employees. The term is sometimes used to describe the efforts put into a start-up company by the founders in exchange for ownership shares of the company. This concept, also called "**stock for services**" or sometimes "**equity compensation**" can also be seen when start-up companies use their shares of stock to entice service providers to provide necessary corporate services in exchange for a discount or for deferring service fees until a later date.

2.7 Employee Stock Options (ESOP)

Employee stock option means the option given to the whole-time Directors, Officers or employees of a company which gives such Directors, Officers or employees, the benefit or right to purchase or subscribe at a future date, the securities offered by the company at a predetermined price.

Employee Stock Option Scheme (ESOS) means a scheme under which a company grants employee stock option. An employee, other than one who is a promoter or part of the promoter group, shall be eligible to participate in ESOS of the company.

An "**employee**" means

- (1) a permanent employee of the company working in India or out of India; or
- (2) a director of the company, whether a whole time director or not; or
- (3) an employee of a subsidiary or holding company, in India or abroad.

A "**promoter**" means;

- (1) the person or persons who are in over-all control of the company;
- (2) person(s) instrumental in the formation of the company

(3) the person or persons named in the offer document as promoter(s).

A director or officer of the company, acting as such only in their professional capacity, will not be deemed to be a promoter. Where a promoter of a company is a body corporate, the promoters of that body corporate shall also be deemed to be promoters of the company.

Promoter group means an immediate relative of the promoter (i.e. spouse, parent, sibling or child).

Employee stock purchase scheme (ESPS) means a scheme under which the company offers shares to employees as part of a public issue or otherwise.

Share means equity shares and securities convertible into equity shares and shall include American Depository Receipts (ADRs), Global Depository Receipts (GDRs) or other depository receipts representing underlying equity shares or securities convertible into equity shares.

ESPS shares means shares arising out of grant of shares under ESPS.

2.8 Buy-back of shares

There are several reasons for which a company may decide to buy back shares issued by it. The top three reasons are:

(1) The company has **surplus funds** but does not have suitable projects to invest the funds in. Companies aim to maximize profits. For this they continuously seek to improve current projects, start new projects, expand into newer markets, acquire other companies etc. However there may be a situation wherein the company has a lot of surplus money but is unable to identify suitable avenues to invest that money. In such a situation it may consider using the surplus funds to buy back its shares from existing shareholders.

(2) The company may seek to **increase the market price of its shares**. Buying back shares would reduce the number of shares that are available in the market for trading. This decrease in supply of the shares may lead to an increase in the share price.

(3) Buy back of shares is a **defence to a hostile takeover**. The buyback would reduce the shares available in the open markets thereby making it difficult for a potential acquirer to buy the shares required to takeover the company.

2.9 Investing in shares

Share prices change every day because of supply and demand. If more people want to buy a stock (demand) than sell it (supply), then the price

moves up. If more people want to sell a stock (supply) than buy it (demand), then the price moves down.

The most important factor that affects the value of a company is its **profit**. Listed companies are required to report their earnings four times a year (once each quarter).

Equity analysts base their future value of a company on its **earnings projection**. If a company's results are better than expected, the price jumps up. If a company's results are worse than expected, then the price will fall.

However, it is not just earnings or profit statements that affect a share's price. **Market sentiment** in general or towards a particular company can be very difficult (if not impossible) to predict.

There are two major methods of analysis used by investors:

(1) Fundamental Analysis

Fundamental analysis is the analysis of a stock on the basis of core financial and economic analysis to predict the movement of stocks price. It looks at the actual company and tries to figure out what the company price is going to be like in the future.

(2) Technical Analysis

Technical analysis is the study of prices and volume, for forecasting of future stock price or financial price movements. It looks at the stocks chart, people's buying behavior etc. to try and figure out what the stock price is going to be like in the future.

Before investing in shares, an investor must understand the following concepts:

Dematerialization is the process by which an investor can get physical certificates converted into electronic form maintained in an account with a Depository. The investors can dematerialize only those share certificates that are already registered in their name and belong to the list of securities admitted for dematerialization at the depositories.

The organization responsible to maintain investor's securities in the electronic form is called the depository. The depository concept is similar to the Banking system with the exception that banks handle funds whereas a depository handles securities of the investors.

An investor wishing to utilize the services offered by a depository has to open an account with the depository through a Depository Participant.

Going Short implies selling shares that are not owned by the seller. Generally a trader will go short if he expects the price to decline. He

must “square off” the transaction by purchasing the shares within the allocated period.

Margin Trading is used by investors who do not have the full amount to pay for the shares purchased by them. They pay a small percentage of the transaction amount. They have to cover (square) the transaction before the close of the settlement cycle.

In case the price during the course of the settlement cycle moves in the favor of the investor he makes a profit and receives the payment from the exchange. In case the price movement is adverse, he makes a loss and will have to make the payment to the exchange.

Margins are collected to safeguard against any adverse price movement. Margins are quoted as a percentage of the value of the transaction.

Buying On Margin: Suppose you have Rs 1,00,000 with you in your Bank account. You can use this amount to buy 10 shares of Noodle Ltd. at Rs 10,000. In the normal course, you will pay for the shares on the settlement day to the exchange and receive 10 shares from the exchange which will get credited to your demat account. Alternatively you could use this money as margin and suppose the applicable margin rate is 25%.

You can now buy upto 40 shares of Noodle Ltd. at Rs 10,000 value Rs 4,00,000, the margin for which at 25% i.e. Rs 1,00,000. Now as you do not have the money to take delivery of 40 shares of Noodle Ltd. you have to cover (square) your purchase transaction by placing a sell order by end of the settlement cycle.

Now suppose the price of Noodle Ltd rises to Rs. 11,000 before end of the settlement cycle. In this case your profit is Rs 40,000 which is much higher than on the 10 shares if you had bought with the intent to take delivery.

The risk is that if the price falls during the settlement cycle, you will still be forced to cover (square) the transaction and the loss would be adjusted against your margin amount.

Selling On Margin: You do not have shares in your demat account and you want to sell as you expect the prices of share to go down. You can sell the shares and give the margin to your broker at the applicable rate.

As you do not have the shares to deliver you will have to cover (square) your sale transaction by placing a buy order before the end of the settlement cycle.

Just like buying on margin, in case the price moves in your favor (falls) you will make profit. In case price goes up, you will make loss and it will be adjusted against the margin amount.

There are various types of orders, which can be placed on the exchanges:

Limit Order: The order refers to a buy or sell order with a limit price. Suppose, you check the quote of Reliance Industries Ltd (RIL) as Rs. 251 (Ask). You place a buy order for RIL with a limit price of Rs 250. This puts a cap on your purchase price.

In this case as the current price is greater than your limit price, order will remain pending and will be executed as soon as the price falls to Rs. 250 or below. In case the actual price of RIL on the exchange was Rs 248, your order will be executed at the best price offered on the exchange, say Rs 249.

Thus you may get an execution below your limit price but in no case will exceed the limit buy price. Similarly, for a limit sell order in no case the execution price will be below the limit sell price.

Market Order: Generally, a market order is used by investors, who expect the price of share to move sharply and are yet keen on buying and selling the share regardless of price. Suppose, the last quote of RIL is Rs 251 and you place a market buy order.

The execution will be at the best offer price on the exchange, which could be above Rs 251 or below Rs 251. The risk is that the execution price could be substantially different from the last quote you saw.

Circuit Filters and Trading Bands: In order to check the volatility of shares, SEBI has come with a set of rules to determine the fixed price bands for different securities within which they can move in a day.

As per Government directives, all securities traded at or above Rs.10/- and below Rs.20/- have a daily price band of $\pm 25\%$. All securities traded below Rs. 10/- have a daily price band of $\pm 50\%$. Price band for all securities traded at or above Rs. 20/- has a daily price band of $\pm 8\%$.

The previous day's closing price is taken as the base price for calculating the price. As the closing price on BSE and NSE can be significantly different, this means that the circuit limit for a share on BSE and NSE can be different.

Badla financing: In common parlance the carry-forward system is known as 'Badla', which means something in return. Badla is the charge, which the investor pays for carrying forward his position. It is a hedge tool where an investor can take a position in a scrip without actually taking delivery of the stock. He can carry-forward his position on the payment of a small margin. In the case of short-selling the charge is termed as 'undha badla'.

3. Debt Instruments

3.1 Types of Debentures

A debenture is an instrument of debt executed by the company acknowledging its obligation to repay a sum at a specified rate and also carrying an interest.

A debenture is a popular method of raising loan capital. A debenture is like a certificate of loan evidencing the fact that the company is liable to pay a specified amount with interest and although the money raised by the debentures becomes a part of the company's capital structure, it does not become share capital.

The basic difference between the various types of debentures is in the manner of **redemption**. On reaching the date of maturity, the issuer repays the money borrowed from the investors. This is known as Redemption or Repayment of the debenture.

If the redemption proceeds are more than the face value of the bond/debentures, the debentures are said to be redeemed at a **premium**. If one gets less than the face value, then they are redeemed at a **discount** and if one gets the same as their face value, then they are redeemed at **par**.

The fundamental types of debentures are:

- (1) Non convertible debentures (NCD)
- (2) Partially convertible debentures (PCD)
- (3) Fully convertible debentures (FCD)

In case of NCDs, the total amount of the instrument is redeemed by the issuing company. In case of PCDs, part of the instrument is redeemed and part of it is converted into equity. In case of FCDs, the whole value of the instrument is converted into equity. The conversion price is stated when the debenture is issued.

The price of each equity share received by way of converting the face value of the convertible debenture is called the **conversion price**. The number of equity shares exchangeable per unit of the convertible debentures is called the **conversion ratio**.

The period of time after which the debenture is converted into equity is called the **conversion period**.

Illustration: On 1-1-2008 Noodle Ltd issues 6% fully convertible debentures having face value of Rs 100 each. Each debenture would be converted into 2 equity shares having face value of Rs 10 on 1-1-2007.

In this illustration the conversion price is Rs 50 while the conversion ratio is 2:1 or 2 shares for one debenture. The conversion period is 1 year. The “6%” signifies that prior to conversion the debenture-holders would be entitled to a 6% annual interest.

A **callable debenture** is a debenture in which the issuing company has the option of redeeming the debenture before the specified redemption date at a pre-determined price. Similarly, a **puttable debenture** is one where the debenture-holder has the option of getting it redeemed before maturity at a pre-determined price.

In the case of public issue of debentures, there would be a large number of debenture holders on the register of the company. As such it shall not be feasible to create a charge in favour of each of the debenture holders. A common methodology generally adopted is to create a **Debenture Trust Deed** conveying the property of the company.

The Debenture Trust Deed is an arrangement enabling the property to be held by a person or persons for the benefit of some other person known as beneficiary. The Trustees declare the Trust in favour of the debenture holders. The Trust Deed may grant the Trustees fixed charge over the freehold and leasehold property while a floating charge may be created over other assets. The Company must allow inspection of the Trust Deed and also provide a copy of the same to any member or debenture holder of the company on payment. Failure to provide the same would invite penalties by way of fine under the Act. Any provision contained in the Trust Deed, which exempts a Trustee from liability for breach of Trust, is void.

Registration of a charge for purpose of issue of debentures is mandatory. Prior to issuing a prospectus or a letter of offer to the public for subscription of its debentures, a company must appoint one or more **debenture trustees**. The main functions of the debenture trustees are to protect the interest of debenture-holders and to redress their grievances.

The company that issues debentures is required to create a **debenture redemption reserve** for the redemption of such debentures. Adequate amounts must be credited to this reserve every year until such debentures are redeemed.

Some of the other types of debentures are:

(1) Third party convertible debentures

These are debentures with attached share warrants. The attached share warrants are exchangeable for equity shares of some other company (within the same group). The warrant is to be exercised within a

stipulated time period. This helps a less profitable company to raise capital at a lower interest rate by attracting investors with the equity shares of a more profitable company in the same group.

(2) Guaranteed capital debentures

In these debentures, at the time of redemption, principal is paid in the form of equity shares of the company at the current market price. Additionally the interest payment is guaranteed by another company of the same group.

(3) Extendable debentures

Such debentures have pre-determined dates when the issuer or the investor can opt to either continue with the debenture or exercise put / call option. On such specified dates, there may be a provision for resetting the interest rate.

(4) Increasing rate debentures

Interest rate of such debentures increases with time. A debenture may be issued at 6% with the provision of a half percent increase per annum giving an 8.5% yield at the end of the 5th year.

(5) Split coupon debentures

Such debentures are issued at a discount to the face value and interest is accrued in the first few years and later paid. Such debentures are issued to manage cash outflows in a new project depending upon cash generation capacity.

3.2 Types of Bonds

According to section 2(5) of the Indian Stamp Act a "Bond" includes-

- (1) any instrument whereby a person obliges himself to pay money to another, on condition that the obligation shall be void if a specified act is performed, or is not performed, as the case may be;
- (2) any instrument attested by a witness and not payable to order or bearer, whereby a person obliges himself to pay money to another; and
- (3) any instrument so attested, whereby a person obliges himself to deliver grain or other agricultural produce to another.

The various types of bonds include:

Zero coupon or strip bonds

The cash flows of a normal bond consist of the regular interest or "coupon" payments, that take place over the term of the bond, and the principal repayment that occurs at maturity of the bond.

Illustration: For example, the cash flows of the Government of India 8% bond with a maturity date of June 1, 2023 are:

- (1) Rs.4 every 1st December and 1st June up to and including June 1, 2023, representing 4% of the Rs.100 par value; and
- (2) Rs.100 on 1st June 2023 - representing the repayment of the principal or par amount of the bond.

Taken individually, each of these payments is an obligation of the issuer, in this case, the Government of India.

The process of "**stripping**" a bond involves depositing bonds with a trustee and having the trustee separate the bond into its individual payment components. This allows the components to be registered and traded as individual securities. The interest payments are known as "**coupons**" and the final payment at maturity is known as the "**residual**" since it is what is left over after the coupons are stripped off.

Both coupons and residuals are known as "zero coupon" bonds or "zeros".

Once a bond has been stripped, a trustee directs the appropriate amount of the interest or maturity payment to the security holders. The holder of a zero coupon receives the par amount of the particular term of the zero coupon bond that she holds.

Illustration: An investor holding Rs.100,000 par amount of the December 1, 2001 coupon would receive Rs.100,000 on that date.

Conceptually, a zero coupon security is just like a Treasury Bill or "T-Bill". The investor pays something up front in exchange for a promise to receive Rs.100 on the maturity date.

Illustration: Take the earlier example of the coupons and residual generated by stripping the India 8% of 2023. If we start on December 1, 1996 the first two payments are identical to a 6 month and 1 year T-Bill. An investor would receive Rs.100 on June 1st and December 1st for each Rs.100 par amount she purchased of these terms of coupons.

What should an investor pay for the 1 year coupon? If the investor demands a 4% return over a one year period, she should pay something around Rs.96 for the Rs.100 maturity value.

Zero-Coupon Convertible Bond

This is a bond that is originally sold at a **discount** to its face value. It can be exchanged for **equity** shares of the issuer company at a later date.

These are debt instruments that include a call option on the issuing company's equity shares. The value of these securities reflects the underlying equity, based on the conversion premium--the difference between the price at which the bond may be converted to equity (which is set on the day of issuance), and the current stock price.

Because these instruments are structured as debt, they offer **protection** to the investors if the share price falls. Because the investors can gain from the increase in the value of the shares, the **interest rate** offered on these bonds is usually lower than for traditional debt instruments.

Liquid Yield Option Notes (LYONs) are a variety of these securities. These have both a conversion feature and a put option allowing the holder to sell the bonds back to the issuer.

Deep Discount Bonds

A bond that sells at a discount of 20% or more from face value is usually referred to as a deep discount bond.

Inflation Bonds

In 1997, the U.S. Treasury's first-ever offering of debt designed to protect investors from inflation was a huge hit. The government targeted it as a new investment vehicle for retirement. It is for investors who are worried about inflation eroding the value of their investment.

The earnings rate of Inflation Bonds issued by the US Government (called Treasury Inflation Protected Securities) combines two separate rates: (1) a fixed rate of return, which remains the same throughout the life of the bond, (2) a variable semiannual inflation rate based on changes in the Consumer Price Index for all Urban Consumers.

Disaster bonds

These bonds are issued by **insurance companies** to share their risk. These bonds link investor's returns to the size of the insurer's losses. Disaster bonds offer high returns if insurance claims are low, but in exchange, investors take on some of the insurers' risks.

There are two types of disaster bonds. They can either be linked to the fortunes of a specific insurer or to an index of the insurance market's overall claims performance. As with all investments, opting for a single-company bond carries a higher risk of loss than bonds that are diversified across the sector.

Easy exit Bonds

These bonds provide easy liquidity and exit routes to investors by way of redemption or buy-back facilities. Investors can get the benefits of ready encashment in case they need to withdraw money before maturity.

Pay-in-kind bonds

A pay-in-kind bond gives the issuer the option of paying interest either in additional securities or in cash.

Floating rate bonds

Floating-rate bonds (also called variable-rate bonds or floaters) are those whose interest is pegged to a benchmark (e.g. the Treasury Bill rate) and adjusted periodically. The most typical coupon formula ties the coupon rate to a certain benchmark (reference rate). Usually the formula looks like this:

$$\text{Coupon rate} = \text{reference rate} + \text{quoted margin}$$

Illustration: The most popular reference rate for floating-rate bonds is London interbank offer rate (LIBOR). So the coupon formula for an issue may be as follows:

$$\text{Coupon rate} = 3\text{-month LIBOR} + 2\%$$

Hence, if 3-month LIBOR for the relevant period is 6%, the interest rate for this period would be set as $6\% + 2\% = 8\%$.

The important features of many floaters are caps and floors. **Cap** is the maximum coupon rate that can be set for floaters.

Illustration: Coupon formula can be as 3-Month LIBOR + 2% with a cap of 7%. In that case, coupon will be set as 7% even if 3-Month LIBOR is greater than 5%.

Since the cap restricts the coupon from increasing, it is an unattractive feature for the investor. In contrast, there could be a minimum coupon rate specified for a floater. This rate is called a **floor**. A floater can have both a cap and a floor. This feature is referred to as **collar**.

Typically, the coupon formula for a floater is such that the coupon increases when the reference rate increases and decreases when reference rate decreases. However, some issues have coupon formulas where coupon rate moves in the direction opposite to the reference rate. Such issues are called **inverse floaters** (or reverse floaters).

Usually, the coupon rate for an inverse floater can not be negative, so it has a floor at zero. Unlike the other bondholders, buyer of a reverse floater benefits from falling interest rates.

A **dual index note** is a security whose coupon is tied to the spread between two market indices.

Secured Premium Notes

This instrument frees the issuing company from paying interest for the first few years. The attached share warrant makes the instrument attractive for the investors.

TISCO was the first Indian company which issued secured premium notes (SPN). These SPNs were issued to the existing shareholders on a rights basis. Each SPN was of the face value of Rs. 300. No interest became due during the first three years after allotment. Payment was made by the company in four equal annual installments of Rs. 150 each (Rs. 75 towards the original investment and Rs.75 towards interest and premium on redemption). This payment was made at the end of the 4th, 5th, 6th and 7th years.

Each warrant holder was entitled to be allotted 1 equity share of Rs 10 each at a premium of Rs 70 per share. The warrant was to be exercised in the period of one and half years from the date of allotment. This implies that the share could be purchased by a warrant holder at Rs 80 per share which was lower than the market price of the share.

Public Sector Undertaking Bonds (PSU Bonds)

These are medium or long term debt instruments issued by Public Sector Undertakings (PSUs). The term usually denotes bonds issued by the central PSUs (ie PSUs funded by and under the administrative control of the Government of India). Most of the PSU Bonds are sold on private placement basis to the targeted investors at market determined interest rates. Often investment bankers are roped in as arrangers to this issue. Most of the PSU Bonds are transferable. In case of **tax free bonds**, normally such bonds accompany post dated interest cheque / warrants.

Bonds of Public Financial Institutions

Apart from public sector undertakings, Public Financial Institutions (PFI) are also allowed to issue bonds through public issues targeted at retail investors and through private placements to large institutional investors. PFIs offer bonds with different features to meet the different needs of investors e.g. monthly return bonds, quarterly coupon bearing bonds, cumulative interest bonds etc.

Indexed bonds

Indexed bonds are a special kind of floating-rate bonds. For these bonds the par value is subject to change in accordance with some reference Index, and coupon payments are paid using this par value.

In fact, almost any index can be used for this purpose e.g. Sensex, NIFTY etc. The Government of Mexico used to issue bonds indexed to crude oil price, and the Russian government used to issue bonds tied to the price gold.

Foreign currency linked bonds

This type of bond is structured so that each payment is linked to changes in some foreign currency. There is a slight difference between this type

and bonds denominated in foreign currency, because in case of indexed bonds all payments are made in local currency though the amount is linked to foreign currency while in the case of bonds denominated in foreign currency transactions should also be made in this currency.

This type of bonds is very similar to indexed bonds, where foreign currency exchange rate is used as a reference index. These bonds are popular in countries with weak and unstable currencies.

Dual-currency bonds

This term is used for bonds with coupon payments in one currency and principal payment in another currency. For example, coupon payments can be in Japanese Yen and principal payment in US dollars.

This type of bond is usually used when the issuer places bonds on the foreign market (foreign bonds). In that case the issuer usually makes coupon payments in the currency of that market, and principal payment is its country of origin currency.

3.3 Credit Rating

Credit rating is a symbolic indicator of the current opinion on the relative capability of the corporate entity to timely service debts and obligations, with reference to the instrument rated.

The rating is based on an **objective analysis** of the information and clarifications obtained from the entity, as also other sources which are considered reliable by the rating agency.

The independence and professional approach of the agency ensure reliable, consistent and unbiased ratings. Ratings facilitate investors to factor credit risk in their investment decision.

Major credit rating agencies that exist in India are Credit Rating Information Services of India Limited (CRISIL), Investment Information and Credit Rating Agency (ICRA) and Credit Analysis & Research (CARE). The rating accorded by any rating agency is **instrument specific** and relates to debt instruments of any maturity, public deposits and preference shares.

International rating agencies like Moody's and S&P also **rate different countries**. The ratings of developing countries are used by foreign financial Institutions for making investments in a particular country.

The rating agency considers all **relevant factors** that have a bearing on the future cash generation of the issuers. These factors include:

- (1) industry characteristics,
- (2) competitive position of the issuer,
- (3) operational efficiency,

- (4) management quality,
- (5) commitment to new projects and other associate companies, and
- (6) funding policies of the issuer.

A detailed analysis of the past financial statements is made to assess the performance under the "real world" business dynamics. **Estimates of future earnings** under various sensitivity scenarios are drawn up and evaluated against the claims and obligations that require servicing over the tenure of the instrument being rated. Primarily, it is the relative comfort level of the issuers to service obligations that determines the rating. The **rating process** commences at the request of the prospective issuer and on receipt of information as may be available with such issuer. A team of analysts takes up the work of collection of data and information from the books and records of the concern and interacts with its executives. The team also relies on the in-house research and database and other secondary sources considered reliable by the rating agency.

On completion of the analysis, a **rating report** is submitted to the rating committee followed by presentation of key rating issues by the rating team. The ratings are assigned by the rating committee. The rating agency ensures strict confidentiality of the information collected from the issuers during the rating process.

The **rating symbols** indicated below are those awarded by ICRA. While all rating agencies in India follow a similar gradation for rating symbols, the prefix attached to each symbol would vary depending on the individual rating agency.

Long Term – including Debentures, Bonds, Preference Shares	LAAA	Highest Safety
	LAA	High Safety
	LA	Adequate Safety
	LBBB	Moderate Safety
	LBB	Inadequate Safety
	LB	Risk Prone
	LC	Substantial Risk
	LD	Default

Short Term – including Commercial Paper	A1 / A1+	Highest safety
	A2/ A2+	High safety
	A3/ A3+	Adequate safety
	A4/ A4+	Risk Prone
	A5	Default - Either already in default or

		expected to default
Medium Term – including Certificate of Deposit and Fixed Deposit Programmes	MAAA	Highest Safety
	MAA	High Safety
	MA	Adequate Safety
	MB	Inadequate Safety
	MC	High Risk
	MD	Default

The suffix of + or - may be used with the assessment symbol to indicate the comparative position of the borrower within the group covered by the symbol. Thus LAA+, MAA+, and A1+ are one notch above LAA, MAA, and A1 respectively.

4. Commodities

The origins of the Commodities Markets are traced to Chicago, USA in the mid 19th century. It evolved as farmers (sellers) and dealers (buyers) began to commit to future exchanges of grain for cash.

For instance, a corn farmer would agree with a cornflake manufacturer on a price to deliver to him one ton of corn on 6th November. The bargain suits both parties. The farmer knows how much he would be paid for his corn, and the cornflake manufacturer knows his costs in advance. The two parties may exchange a written contract to this effect. Some money representing a "guarantee" may also be paid.

The commodities that are traded in commodities markets are usually in a basic, raw, unprocessed state. Perishable commodities must have an adequate shelf life, because delivery on a futures contract is deferred. Moreover, the commodity's price must fluctuate enough to create uncertainty, which means both risk and potential profit.

Commodity includes all kinds of goods. **Forward Contracts (Regulation) Act, 1952** (FCRA) defines "**goods**" as "every kind of movable property other than actionable claims, money and securities".

In India, all goods and products of agricultural (including plantation), mineral and fossil origin are allowed for futures trading in the commodity exchanges recognized under the FCRA. These include precious (gold & silver) and non-precious metals; cereals and pulses; ginned and unginned cotton; oilseeds, oils and oilcakes; raw jute and jute goods; sugar and gur; potatoes and onions; coffee and tea; rubber and spices, etc.

As on 27th May, 2008, the official website of the Forward Markets Commission (<http://www.fmc.gov.in>), lists the following as the commodities exchanges in India:

- a. Rajdhani Oils and Oilseeds Exchange Ltd. , Delhi
- b. Ahmedabad Commodity Exchange Ltd
- c. Bhatinda Om & Oil Exchange Ltd., Bhatinda.
- d. Bikaner Commodity Exchange Ltd., Bikaner
- e. First Commodity Exchange of India Ltd, Kochi
- f. Haryana Commodities Ltd., Sirsa
- g. India Pepper & Spice Trade Association, Kochi
- h. Multi Commodity Exchange of India Ltd, Andheri, Mumbai
- i. National Board of Trade. Indore

- j. National Commodity & Derivatives Exchange Ltd.
- k. National Multi Commodity Exchange of India Limited, Ahmedabad
- l. Surendranagar Cotton oil & Oilseeds Association Ltd,
- m. The Bombay Commodity Exchange Ltd, Mumbai
- n. The Bullion Association Limited, Jaipur
- o. The Central India Commercial Exchange Ltd, Gwalior
- p. The Chamber Of Commerce, Hapur
- q. The Cotton Association of India, Mumbai
- r. The East India Jute & Hessian Exchange Ltd, Kolkata
- s. The Meerut Agro Commodities Exchange Co. Ltd., Meerut
- t. The Rajkot Commodity Exchange Ltd.
- u. The Spices and Oilseeds Exchange Ltd, Sangli
- v. Vijay Beopar Chamber Ltd., Muzaffarnagar

As on 27th May, 2008, the official website of the Forward Markets Commission (<http://www.fmc.gov.in>), lists the following amongst the commodities in which Futures Trading is being conducted in India:

Fibres and Manufacturers - Kapas, hessian, Indian cotton, staple fibre yarn, sacking, cotton bales, long staple cotton, medium staple cotton, silk, coffee, sugar, gram, mustardseed oilcake, PPTQ, cement and polyvinchloride etc.

Spices - Pepper, turmeric, cardamom, red chilly, jeera, rubber, cuminseed and arecanut etc.

Edible Oilseeds and Oil - RBD Pamolein, groundnut oil, sunflower oil, rapeseed / mustardseed, soy bean, copra, cotton seed, safflower, castor oil, coconut oil, copra cake, sesamum sunflower, seed, crude palm oil, vanaspati, linseed, middle east crude oil, refined sunflower oil etc.

Pulses - Masoor, urad, tur / arhar, moong, yellow peas, chana etc

Energy Products - Crude oil, Brent crude oil, furnace oil, and natural gas

Metals - Aluminium ingots, nickel, copper, zinc, lead, tin, gold, steel, silver and sponge iron.

5. Derivatives

Derivatives are financial instruments whose value is derived from the prices of one or more underlying assets. These underlying assets could be equity shares, foreign currencies, corn, wheat, silver etc.

Derivatives can also be defined as contracts between two parties to exchange payments linked to the prices of underlying assets. Derivative can also be defined as a financial instrument that does not constitute ownership, but a promise to convey ownership.

By their very nature, financial markets are marked by a very high degree of volatility. Through the use of derivative products, it is possible to partially or fully **transfer price risks** by locking-in asset prices. By locking-in asset prices, derivative products minimize the impact of fluctuations in asset prices on the profitability and cash flow situation of risk-averse investors.

The most common types of derivatives are: forwards, futures and options.

Forward contracts are contracts between two parties whereby one party agrees to sell to another party at some point in the future for a price agreed upon now. The amount of the sale as well as when it occurs is customizable to the contract.

Problems with this type of derivative include: the difficulty in finding someone to transact with, the contracts are non-transferable, and the contracts have a high probability of default.

Illustration

Pooja is a farmer who produces corn and Kellogg's is a cornflake manufacturer who regularly buys corn from farmers like Pooja. In 3 months Pooja will have 1000 kg of corn ready for sale. She is worried that the price of the corn will fall by then. Kellogg's on the other hand is worried that the price of corn will rise.

Pooja and Kellogg's can enter into a forward contract wherein they fix the price of the corn today. The actual delivery of the corn will be made by Pooja after 3 months but the price will be fixed today. Thereby both parties are minimizing their risks in case of an adverse price change.

Here Pooja is going short on corn while Kellogg's is going long on corn

The Chicago Board of Trade was set up in 1848 for the exchange trading of agricultural products such as wheat and corn. The exchange put in

place a mechanism that would play an important role in helping the agricultural community to plan for the future by enabling users of derivatives to lock-in the prices they will receive for their goods before they were even ready for harvesting.

A **futures contract** is an agreement between two parties to buy or sell an asset at a certain time in the future at a certain price.

The futures contracts are standardized and exchange traded.

To facilitate liquidity in the futures contracts, the exchange specifies certain standard features of the contract. It is a standardized contract with standard underlying instrument, a standard quantity and quality of the underlying instrument that can be delivered, (or which can be used for reference purposes in settlement) and a standard timing of such settlement.

Futures are like forwards but are transferable, standardized, and designed to reduce the probability and costs of a default.

While futures and forward contracts are both contracts to trade on a future date, key differences include:

- (1) Futures are always traded on an exchange, whereas forwards always trade directly between two parties.
- (2) Futures are highly standardized, whereas each forward is unique.
- (3) The price at which the contract is finally settled is different: Futures are settled at the settlement price fixed on the last trading date of the contract (i.e. at the end). Forwards are settled at the forward price agreed on the trade date (i.e. at the start).
- (4) The credit risk of futures is much lower than that of forwards: Traders are not subject to credit risk due to the role played by the clearing house.
- (5) In a forward there are no cash flows until delivery, whereas in futures there are margin requirements and periodic margin calls.

An **option** is a contract, which gives the buyer the right, but not the obligation to buy or sell an underlying security at a specific price on or before a specific date. ‘Option’, as the word suggests, is a choice given to the investor to either honour the contract; or ignore the contract.

6. Futures

A futures contract is a standardized contract, traded on a futures exchange, to buy or sell a certain underlying instrument at a certain date in the future, at a pre-set price.

The future date is called the **delivery date** or final settlement date. The pre-set price is called the **futures price**. The price of the underlying asset on the delivery date is called the **settlement price**. The futures price, normally, converges towards the settlement price on the delivery date.

Both parties of a "futures contract" must exercise the contract (buy or sell) on the settlement date. Futures contracts, or simply futures, are exchange traded derivatives. The exchange acts as counterparty on all contracts, sets margin requirements, etc.

Futures contracts ensure their liquidity by being highly standardized, usually by specifying:

- (1) The **underlying asset**. This can be anything from a barrel of crude oil to a short term interest rate.
- (2) The **type of settlement**, either cash settlement or physical settlement.
- (3) The **amount** and **units** of the underlying asset per contract. This can be the notional amount of bonds, a fixed number of barrels of oil, units of foreign currency, the notional amount of the deposit over which the short term interest rate is traded, etc.
- (4) The **currency** in which the futures contract is quoted.
- (5) The **grade** of the deliverable. In the case of bonds, this specifies which bonds can be delivered. In the case of physical commodities, this specifies not only the quality of the underlying goods but also the manner and location of delivery. For example, the New York Mercantile Exchange Light Sweet Crude Oil contract specifies the acceptable sulphur content and API specific gravity, as well as the location where delivery must be made.
- (6) The **delivery month**.
- (7) The **last trading date**.

The price of a futures contract constantly fluctuates. This renders the owner liable to adverse changes in value thereby creating a credit risk to the exchange (who acts as counterparty). To minimize this risk, the exchange demands that contract owners post a form of collateral commonly known as **margin**.

Initial margin is paid by both buyer and seller. It represents the loss on that contract, as determined by historical price changes. This is the loss that is not likely to be exceeded on a usual day's trading.

Because a series of adverse price changes may exhaust the initial margin, a further margin, usually called **variation** or **maintenance margin**, is required by the exchange.

Settlement is the act of consummating the contract, and can be done in one of two ways, as specified per type of futures contract:

(1) Physical delivery - the specified amount of the underlying asset is delivered by the seller of the contract to the exchange. The exchange then delivers it to the buyers of the contract. Physical delivery is common with commodities and bonds.

(2) Cash settlement - a cash payment is made based on the underlying reference rate, such as a short term interest rate index, or the closing value of a stock market index.

Single Stock Futures

Single stock futures are futures contracts with individual stocks as the underlying asset. It is an agreement to buy or sell a specified quantity of underlying equity share for a future date at a price agreed upon between the buyer and seller. The contracts have standardized specifications like market lot, expiry day, unit of price quotation, tick size, and method of settlement.

According to L C Gupta Committee Report on Derivatives, a minimum contract value should be Rs. 2 lakh. This value of Rs. 2 lakh was divided by the market value of individual stock to arrive at the **initial market lot** for it. The profits and losses in single stock futures depend upon the difference between the price at which the position is opened and the price at which it is closed.

Illustration: Pooja has a long position of one November Noodle Ltd Futures @ 500. If she squares up her position by selling November Noodle Ltd Futures @ 550, the profit would be Rs. 50 per share. In case, she squares up her position by selling November Noodle Ltd futures @ 400, the loss would be Rs. 100 per share.

Stock futures offer **high leverage**. This means that one can take large position with less capital.

Illustration: Pooja has Rs 1 lakh at her disposal. By paying the entire Rs 1 lakh as an initial 20% margin, she can take a position of Rs 5 lakh.

Futures may look over-priced or under-priced compared to the spot or current price and can offer opportunities to **arbitrage** or earn risk-less profit.

Illustration: Noodle shares are currently trading at Rs 100 per share. The 3 month futures contract is valued at Rs 110. Pooja can buy one Noodle share at Rs 100 today and sell one futures contract at Rs 110. She is assured a risk free profit of Rs 10 after 3 months.

Single stock futures can be an effective **risk management tool**.

Illustration: Pooja has a long position in Noodle shares in the cash segment. She can minimize market risk or price risk of Noodle stock by taking a short position in an appropriate futures contract.

6.1 Index Futures

In case of Index futures, the underlying asset is a stock market index e.g. Bombay Stock Exchange sensitive index (Sensex).

Contract Specification for Sensex® Futures contracts

Security Symbol	BSX
Underlying	SENSEX®
Contract Multiplier	50
Contract Period	1, 2, 3 months
Tick size	0.1 index points
Price Quotation	SENSEX points
Trading Hours	9:55 a.m. to 3:30 p.m.
Last Trading / Expiration Day	Last Thursday of the contract month. If it is a holiday, the immediately preceding business day. Note: Business day is a day during which the underlying stock market is open for trading.
Final Settlement	Cash Settlement. On the last trading day, the closing value of the underlying index would be the final settlement price of the expiring futures contract.

The **contract multiplier** is the minimum number of the underlying - index that a participant has to trade (50 in this case) e.g. if contracted price of futures is 20,000 then the notional value of the contract will be $20,000 \times 50$ i.e. Rs 10 lakh.

The **tick size** is the minimum difference between two buy or two sell quotes. As discussed above, each index point is Rs 50. An index point of 0.1 equals Rs 5. Hence tick size for trading in Sensex futures is 0.1 index point or Rs 5.

The month in which a contract expires is called the **contract month** e.g. a contract expiring in March 2008 will be termed as a March 2008 contract.

6.2 Cost of carry model

The cost-of-carry model is where the price of the contract is defined as:

$$\text{Futures price} = \text{Spot price} + \text{Holding costs or carry costs}$$

In the following cases there would be chances for arbitrage or risk free profits:

$$\text{Futures price} < \text{Spot price} + \text{Holding costs or carry costs}$$

$$\text{Futures price} > \text{Spot price} + \text{Holding costs or carry costs}$$

Illustration: Noodle shares are quoted at Rs 100 per share and the 3 months futures of Noodle is Rs 107.

Pooja can purchase one Noodle share at Rs 100 in spot by borrowing money at the rate of 12% annum (i.e. 1% per month) for 3 months. She can sell the Noodle futures for 3 months at Rs 107.

After 3 months her profit would be [Rs 107-Rs 100] i.e. Rs 7. However she would have paid Rs 3 as interest (cost of carrying). Her actual profit would be Rs 4.

In this case the spot price is Rs 100, the futures price is Rs 107 and the cost of carrying is Rs 3.

6.3 Important Terms

Long position is an outstanding or unsettled buy position in a futures contract.

Illustration: Pooja buys 10 contracts of Noodle Ltd futures. She is long on 10 contracts on Noodle.

Short position is an outstanding or unsettled sell position in a futures contract.

Illustration: Pooja sells 8 contracts of Noodle Ltd futures. She is short on 8 contracts on Noodle.

Open position is a long or short position that is outstanding / unsettled in various futures contracts.

Illustration: Pooja sells 8 contracts of Noodle Ltd futures. She is short on 8 contracts on Noodle. She also buys 10 contracts of Poodle Ltd. She is long on 10 contracts on Poodle. This is an open position.

Naked position implies a long or short position in any futures contract without having any cash position in the underlying asset.

Illustration: Sameer sells 8 contracts of Noodle Ltd futures. He does not have any Noodle shares. This is a naked position. Sameer sells 10 contracts of Poodle Ltd futures. He has 1000 shares of Poodle. This is not a naked position.

Calendar position implies a position in one futures contract hedged by an opposite position in another futures contract for a different maturity. The underlying asset is the same in both the contracts.

Illustration: Sameer sells 8 contracts of Noodle Ltd March 2008 futures. He also buys 8 contracts of Noodle Ltd April 2008 futures. This is a calendar spread.

Opening a position implies increasing an open position by either buying or selling a futures contract.

Illustration: Sameer is short on Noodle futures. He now sells 8 contracts of Noodle Ltd March 2008 futures. He is opening his position.

Sameer is long on Poodle futures. He now also buys 10 contracts of Poodle Ltd April 2008 futures. He is opening his position.

Closing a position implies reducing an open position by either buying or selling a futures contract.

Illustration: Sameer is short on Noodle futures. He now buys contracts of Noodle Ltd March 2008 futures. He is closing his position.

Sameer is long on Poodle futures. He now also sells contracts of Poodle Ltd April 2008 futures. He is closing his position.

Position calculations refer to calculation of brokers positions by the exchange.

Illustration: Sameer is a broker and has 2 clients, Siddharth and Rahul.

On 1st January, Rahul buys 20 Noodle futures and sells 6 of them. Rahul's open position is now long on 14 contracts.

On the same day Siddharth sells 30 Noodle futures and buys 12 of them. Siddharth's open position is now short on 18 contracts.

The open position of Sameer will be 14 long and 18 short contracts.

Beta measures the sensitivity of a scrip / portfolio vis-à-vis index movement. Beta of a scrip is index specific i.e. beta of a scrip vis-à-vis Sensex will be different from its beta vis-à-vis Nifty. Beta is calculated

on the basis of historic data and is used to estimate the future price movement of a scrip or portfolio vis-à-vis an index.

Illustration: Noodle Ltd shares have a beta of 3. This means that if the stock index falls by 10%, the Noodle share price will fall by 30%. This also means that if the stock index rises by 10%, the Noodle share price will rise by 30%.

7. Hedging

Index futures are used for risk management or hedging. Let us understand this through a simple illustration.

Illustration: Pooja has a portfolio of 3 scrips with a beta of 0.75, 1.20 and 1.50 respectively. The weight-ages of these scrips are 25%, 50% and 25% respectively.

The beta of this portfolio would be:

$$\begin{aligned} &= [0.75 \times 0.25] + [1.20 \times 0.50] + [1.50 \times 0.25] \\ &= 0.1875 + 0.6 + 0.375 \\ &= 1.1625 \end{aligned}$$

Pooja's portfolio is worth Rs 5 lakh and as discussed above it has a beta of 1.1625 vis-à-vis the Nifty.

Nifty futures are trading at 2900 and the contract multiplier is 100. A Nifty futures contract will be 2900×100 i.e. Rs 2.90 lakh.

Pooja expects the market to fall during the next few weeks. She has the following choices:

(1) Sell the portfolio today and buy it again after the prices fall. There would be a lot of inconvenience as well as brokerage and other costs to be incurred.

(2) She can sell Nifty futures as per the following formula:
Portfolio value * beta of the portfolio

Value of the index futures contract

$$= 5 \text{ lakh} * 1.1625 = 2 \text{ lakh}$$

Pooja goes short on 2 Nifty futures contracts at 2900 [at a value of $2 \times 2900 \times 100$ i.e. Rs 5.8 lakh]. In ten days, the Nifty falls by 10% i.e. falls by 290 points to 2610. Since the beta of her portfolio is 1.1625, the portfolio will fall by 11.625%. The position will be:

Loss on cash position: 11.625% of 5 lakh i.e. 58,125

Profit on futures position: 10% of 5.80 lakh i.e. 58,000.

Long hedge is a transaction where a position in the cash market is hedged by going long in the futures market.

Illustration: Pooja is expecting a gift from her uncle after 2 months. She wants to invest these funds in the stock market but is concerned that the market would rise in the next few weeks.

This risk can be hedged by buying index futures today. When she receives the gift she can invest the money in securities of her choice and the corresponding futures position can be unwound.

Now suppose that the stock prices rise during the intermediate period. Pooja can make a profit from the index futures. This profit can totally or partially offset the loss that she would incur by having to buy securities at a higher rate.

Short hedge is a transaction where a position in the cash market is hedged by going short in the futures market.

Illustration: Pooja may need to liquidate her portfolio in 3 months in case her overseas college admissions come through. She is concerned that the market would fall in the next few weeks.

This risk can be hedged by selling index futures today. When her admissions come through, she can liquidate the portfolio and the corresponding futures position can be unwound.

Now suppose that the stock prices fall during the intermediate period. Pooja can make a profit from the index futures. This profit can totally or partially offset the loss that she would incur on having to sell her portfolio at a lower rate.

Cross hedge is a hedge where futures of a closely associated asset are used to hedge an asset for which no futures are available.

Illustration: Suppose there are no futures available for crude oil. Crude oil users and traders use natural gas futures to hedge their risks. The prices of crude oil and natural gas usually move in a similar pattern.

8. Options

An option is a contract, which gives the buyer the right, but not the obligation to buy or sell an underlying security at a specific price on or before a specific date. ‘Option’, as the word suggests, is a choice given to the investor to either honour the contract; or ignore the contract.

Option contracts restrict the downside risk while allowing the profits to run unlimited. Apart from risk containment, options can be used for speculation and investors can create a wide range of potential profit scenarios.

8.1 Call Option

A Call Option is an option to buy a stock at a specific price on or before a certain date. When you buy a Call option, the price you pay for it, called the **option premium**, secures your right to buy that certain stock at a specified price called the **strike price**. If you decide not to use the option to buy the stock, and you are not obligated to, your only cost is the option premium.

Illustration: Pooja purchases

1 HiTech Computer (HITECH) AUG 150 Call --Premium 8

This contract allows Pooja to buy 100 shares of HITECH at Rs 150 per share at any time between the current date and the end of next August. For this privilege, Pooja pays a fee of Rs 800 (Rs eight a share for 100 shares).

The buyer of a call has purchased the right to buy and for that she pays a premium. If the stock rises above Rs 158 (150+8) Pooja will break even and she will start making a profit. Suppose the stock does not rise and instead falls she will choose not to exercise the option and forego the premium of Rs 8 and thus limiting her loss to Rs 8.

CALL OPTION BUYER	CALL OPTION WRITER (Seller)
<ul style="list-style-type: none">- Pays premium- Right to exercise and buy the shares- Profits from rising prices- Limited losses,- Potentially unlimited gain	<ul style="list-style-type: none">- Receives premium- Obligation to sell shares if exercised- Profits from falling / neutral prices- Potentially unlimited losses,- Limited gain

8.2 Put Option

Put Options are options to sell a stock at a specific price on or before a certain date. In this way, Put options are like insurance policies.

If you buy a new car, and then buy auto insurance on the car, you pay a premium and are, hence, protected if the asset is damaged in an accident. If this happens, you can use your policy to regain the insured value of the car. In this way, the put option gains in value as the value of the underlying instrument decreases. If all goes well and the insurance is not needed, the insurance company keeps your premium in return for taking on the risk.

With a Put Option, you can "insure" a stock by fixing a selling price. If something happens which causes the stock price to fall, and thus, "damages" your asset, you can exercise your option and sell it at its "insured" price level. If the price of your stock goes up, and there is no "damage," then you do not need to use the insurance, and, once again, your only cost is the premium.

Technically, an option is a contract between two parties. The buyer receives a privilege for which he pays a premium. The seller accepts an obligation for which he receives a fee.

PUT OPTION BUYER	PUT OPTION WRITER (Seller)
<ul style="list-style-type: none"> - Pays premium - Right to exercise and sell shares - Profits from falling prices - Limited losses, - Potentially unlimited gain 	<ul style="list-style-type: none"> - Receives premium - Obligation to buy shares if exercised - Profits from rising / neutral prices - Potentially unlimited losses, - Limited gain

Illustration: Pooja purchases

1 HiTech Computer (HITECH) AUG 150 Put --Premium 8

This contract allows Pooja to sell 100 shares of HITECH at Rs 150 per share at any time between the current date and the end of next August. For this privilege, Pooja pays a fee of Rs 800 (Rs eight a share for 100 shares).

The buyer of a put has purchased the right to sell and for that he pays a premium.

If the stock falls below Rs 142 (150-8) Pooja will break even and he will start making a profit. Suppose the stock rises he will choose not to exercise the option and forego the premium of Rs 8 and thus limiting his loss to Rs 8.

Settlement of options is based on the expiry date. There are two basic styles of options: European and American.

European options give the holder the right, but not the obligation, to buy or sell the underlying instrument only on the expiry date. This means that the option cannot be exercised early. Settlement is based on a particular strike price at expiration. Currently, in India only index options are European in nature.

American options give the holder the right, but not the obligation, to buy or sell the underlying instrument on or before the expiry date. This means that the option can be exercised early. Settlement is based on a particular strike price at expiration.

Illustration: The share price of Oxyrich is Rs 100 on 1 May. Priyanka Chopra expects the price to touch Rs 150 by July. If she buys 1 share and the price actually goes up she makes Rs 50 profit. However she needs to invest Rs 100. Plus there is a risk that if the share price falls to Rs 20 she would lose Rs 80.

Illustration: The share price of Oxyrich is Rs 100 on 1 May. Priyanka Chopra expects the price to touch Rs 150 by July. She buys a 3 month **option to buy** Oxyrich shares at Rs 100 by paying a premium of Rs 10.

If the share price falls to Rs 20, she can choose not to exercise her option. She loses only Rs 10 and not Rs 80. If the share price rises to Rs 150 she can exercise her option and make a profit of Rs 40.

Illustration: The share price of Oxyrich is Rs 100 on 1 May. Priyanka Chopra expects the price to fall to Rs 70 by July. She buys a 3 month **option to sell** Oxyrich shares at Rs 100 (premium of Rs 10).

If the share price rises to Rs 150, she can choose not to exercise her option. If the share price falls to Rs 70 she can exercise her option and make a profit of Rs 20.

9. Swaps

A swap is a derivative, where two counterparties exchange one stream of cash flows against another stream.

Swaps are over-the-counter (OTC) derivatives. This means that they are negotiated outside exchanges. They cannot be bought and sold like securities or futures contracts, but are all unique.

A **currency swap** is a foreign exchange agreement between two parties to exchange a given amount of one currency for another and, after a specified period of time, to give back the original amounts swapped.

Currency swaps can be negotiated for a variety of maturities up to at least 10 years. A swap is considered to be a foreign exchange transaction (short leg) plus an obligation to close the swap (far leg) being a forward contract.

Currency swaps are often combined with interest rate swaps. For example, one company would seek to swap a cash flow for their fixed rate debt denominated in US dollars for a floating-rate debt denominated in Euro. This is especially common in Europe where companies "shop" for the cheapest debt regardless of its denomination and then seek to exchange it for the debt in desired currency.

10. Arbitrage

Arbitrage is the practice of taking advantage of a state of imbalance between two or more markets. A combination of matching deals are struck that capitalize upon the imbalance, the profit being the difference between the market prices.

A person who engages in arbitrage is called an **arbitrageur**. The term is mainly applied to trading in financial instruments, such as bonds, stocks, derivatives and currencies.

If the market prices do not allow for profitable arbitrage, the prices are said to constitute an **arbitrage equilibrium** or arbitrage free market.

Illustration: Suppose that the exchange rates (after taking out the fees for making the exchange) in London are £5 = \$10 = Rs 500 and the exchange rates in India are Rs 500 = £6 = \$10. Converting \$10 to £6 in India and converting that £6 into \$12 in London, for a profit of \$2, would be arbitrage.

In reality, this "triangle arbitrage" is so simple that it almost never occurs. But more complicated foreign exchange arbitrages are common.

Illustration: One example of arbitrage involves the Bombay Stock Exchange (BSE) and the National Stock Exchange (NSE). When the price of a stock on BSE and its corresponding futures contract on the NSE are out of sync, one can buy the less expensive one and sell the more expensive.

Because the differences between the prices are likely to be small (and not to last very long), this can only be done profitably with computers examining a large number of prices and automatically exercising a trade when the prices are far enough out of balance.

Illustration: If you can buy items at one price at a factory outlet and sell them for a higher price on an internet auction website such as eBay, you can capitalize upon the imbalance between those two markets for those items.

Economists use the term "**global labour arbitrage**" to refer to the tendency of manufacturing jobs to flow towards whichever country has the lowest wages per unit output at present and has reached the minimum requisite level of political and economic development to support industrialization. At present, many such jobs are flowing towards China and India.

11. Hedging

In finance, a hedge is an investment that is taken out specifically to reduce or cancel out the risk in another investment. Hedging is a strategy designed to minimize exposure to an unwanted business risk, while still allowing the business to profit from an investment activity.

Illustration: Pooja owns a shop selling shirts. She has natural risks such as the risk of competition, of poor or unpopular products, and so on. However, the risk of her inventory of shirts being destroyed by fire can be hedged via a fire insurance contract. In this she pays a premium to an insurance company. In case her goods are destroyed by fire, the insurance company will compensate her for the loss.

A very popular type of hedge is "pairs trade" hedge which involves trading on a pair of related securities.

Illustration: Pooja believes that the stock price of NOODLE LTD will rise over the next month, based on her information about consumer preferences for computer hardware. She wants to buy NOODLE LTD shares to profit from their expected price increase. But NOODLE LTD is part of the highly volatile computer hardware industry.

Pooja wants to hedge out the risk by short selling an equal value of the shares of NOODLE LTD's direct competitor, POODLE LTD.

On the first day Pooja's portfolio is:

Long 1000 shares of NOODLE LTD at Rs.1 each (total value Rs 1000)

Short 500 shares of POODLE LTD at Rs.2 each (total value Rs 1000)

On the second day, a favorable news story about the computer hardware industry is published and the value of all computer hardware stock goes up. NOODLE LTD, however, because it is a stronger company, goes up by 10%, while POODLE LTD goes up by just 5%:

On the second day Pooja's portfolio is:

Long 1000 shares of NOODLE LTD at Rs.1.10 each — Rs.100 profit

Short 500 shares of POODLE LTD at Rs.2.10 each — Rs.50 loss

(In a short position, the investor loses money when the price goes up)

The trader might regret the hedge on day two, since it's reduced the profits on the NOODLE LTD position. But on the third day an unfavorable news story is published about the health effects of computer hardware, and all computer hardware stocks crash - 50% is wiped off the value of the computer hardware industry in the course of a few hours. Nevertheless, since NOODLE LTD is the better company it suffers less than POODLE LTD:

Value of long position:

Day 1 — Rs.1000

Day 2 — Rs.1100

Day 3 — Rs.550

Value of short position:

Day 1 — Rs.1000

Day 2 — Rs.1050

Day 3 — Rs.525

Without the hedge, the trader would have lost Rs.450. But the hedge - the short sale of POODLE LTD - gives a profit of Rs.475, for a net profit of Rs.25 during a dramatic market collapse.

12. Related Concepts

12.1 Equity Linked Note

An Equity-Linked Note (ELN) is a debt instrument. The final payout is based on the return of the underlying equity. The underlying equity may be a single stock, basket of stocks, or an equity index. Usually the investor is guaranteed to receive 100% of the original amount invested at maturity.

Illustration 1: Sanya purchases a 100 rupee equity-linked note in which the underlying is the Noodle equity share. The participation rate is 100%. During the period of the note, the Noodle share price doubles. On maturity, Sanya will receive Rs 200.

Illustration 2: Samirah purchases a 100 rupee equity-linked note in which the underlying is the Poodle equity share. The participation rate is 80%. During the period of the note, the Poodle share price doubles. On maturity, Samirah will receive Rs 160 (i.e. 80% of Rs 200).

Illustration 3: Pooja purchases a 100 rupee equity-linked note in which the underlying is the Moodle equity share. The participation rate is 80%. During the period of the note, the Moodle share price reduces by 50%. On maturity, Pooja will receive Rs 100.

12.2 Catastrophic Bonds

Catastrophe bonds enable an insurer or reinsurer to access funds if a severe disaster produces large-scale damage. Cat bonds typically cover narrowly defined risks on an excess-of-loss basis. They are issued in the form of debt with high coupons.

How do cat bonds work?

Consider an insurer or reinsurer, SafeCompany, that would like to cover part of its exposure against catastrophic losses. In order to do so, it creates a new company, BigCat, whose only purpose is to cover SafeCompany and not any other company. In that sense, BigCat is a single purpose reinsurer (also called "special purpose vehicle, SPV").

When the reinsurance contract is signed, the sponsor (SafeCompany) pays premiums to BigCat. On the other side, investors place their funds with the SPV BigCat; these funds constitute the initial principal for the bond to be issued by BigCat. Reinsurance premiums collected from

SafeCompany will be used to provide the investors with a high enough interest rate to compensate for a possible loss should a disaster occur.

What happens next? If the losses exceed a pre-specified trigger, then the interest on the bond, the principal, or both, are forgiven depending on the specifications of the issued catastrophe bond. These funds are then provided to SafeCompany to help cover its claims from the event.

In addition to the interest rate on the cat bond, there are other components for the investor to consider:

(1) The protection of the principal

The principal of a catastrophe bond often consists of different tranches, some of which might or might not be protected. A protected tranche guarantees that the investor will receive the principal from this tranche when the bond matures. For this tranche, if a covered event occurs, the SPV stops paying interest and can extend the maturity of the loan for several years. An unprotected tranche has both principal and interest at risk should a covered event occur.

(2) The nature of the trigger

The nature of the trigger varies from one bond to another. The trigger can be indemnity-based, meaning that the transaction is based on the actual losses of the sponsor. This eliminates the basis risk for the sponsor, but also reduces the transparency of the transaction for the investors.

The trigger can also be based on industry losses using a predetermined industry index of losses. The trigger can also be determined by a **parametric index**, such as an earthquake of magnitude 7 or greater on the Richter scale occurring in the San Francisco Bay area or a Category 4 hurricane in Florida. A parametric trigger provides transparency for the investors, but sponsors may have significant basis risk.

Illustration 1: Vivendi Universal (Universal Studios) issued in 2002 a \$175 million bond, Studio Re, to cover its production studios against an earthquake in Southern California.

Illustration 2: Walt Disney also issued a bond to cover its large park in Japan.

Illustration 3: The first European corporate bond was issued in 2003 by EDF, the French electrical company; this \$230 million bond, Pylon, covers the company against windstorm in France.

Illustration 4: In 2006, another corporate sponsor went with coverage by cat bond: Dominion Resources, an energy producer,

obtained protection for oil-drilling assets located off the coasts of Louisiana and Texas by issuing a \$50 million bond, Drewcat.

Illustration 5: The first bond that insured against terrorism was issued in Europe in August 2003.

Illustration 6: The world governing body of football (soccer), the International Federation of Association Football, which organized the 2006 World Cup in Germany, developed a \$262 million bond to protect its investment. Under very specific conditions, the catastrophic bond covered losses resulting from both natural and terrorist extreme events that would have resulted in the cancellation of the World Cup final game without the possibility of it being re-scheduled to 2007.

Illustration 7: The government of Mexico, which through its FONDEN facility sponsored the \$160 million CAT-Mex transaction in May 2006, was the first government to issue a cat bond.

Source:

<http://www.palgravejournals.com/gpp/journal/v33/n1/full/2510159a.html>

12.3 Weather derivatives

Weather derivatives are financial instruments that can be used to reduce risk associated with adverse or unexpected weather conditions. The difference from other derivatives is that the underlying asset (rain/temperature/snow) has no direct value to price the weather derivative.

Farmers can use weather derivatives to hedge against poor harvests caused by drought or frost; theme parks may want to insure against rainy weekends during peak summer seasons; and gas and power companies may use heating degree days (HDD) or cooling degree days (CDD) contracts to smooth earnings.

Heating degree days are one of the most common types of weather derivative. Typical terms for an HDD contract could be: for the November to March period, for each day where the temperature falls below 18 degrees Celsius keep a cumulative count of the difference between 18 degrees and the average daily temperature.

Payout is a set amount depending upon the days that the actual temperature differs from the defined temperature.

The first weather derivative deal was in July 1996 when Aquila Energy structured a dual-commodity hedge for Consolidated Edison Co. The

transaction involved ConEd's purchase of electric power from Aquila for the month of August. The price of the power was agreed to, but a weather clause was embedded into the contract. This clause stipulated that Aquila would pay ConEd a rebate if August turned out to be cooler than expected.

The measurement of this was referenced to Cooling Degree Days measured at New York City's Central Park weather station. If total CDDs were from 0 to 10% below the expected 320, the company received no discount to the power price, but if total CDDs were 11 to 20% below normal, Con Ed would receive a \$16,000 discount. Other discounted levels were worked in for even greater departures from normal.

The Chicago Mercantile Exchange introduced the first exchange-traded weather futures contracts (and corresponding options), in 1999. The CME currently trades weather derivative contracts for 18 cities in the United States, nine in Europe, six in Canada and two in Japan. Most of these contracts track cooling degree days or heating degree days, but recent additions track frost days in the Netherlands and monthly/seasonal snowfall in Boston and New York.

Chicago Mercantile Exchange (CME) Weather products quantify weather in terms of how much temperatures, frost or snowfall deviate from the monthly or seasonal average in a particular city.

The variations are geared to specific indexes, with a dollar amount attached to each index point. Quantifying weather in this way makes it a tradable commodity comparable to trading the varying values of stock indexes, currencies, interest rates and agricultural commodities.

For example, summer weather is measured in terms of temperatures that exceed a base of 65 degrees Fahrenheit (18 degrees Celsius in Europe) and referenced to a Cooling Degree Day (CDD) Index.

Winter weather is measured in terms of how much temperatures are below 65 degrees and referenced to a Heating Degree Day (HDD) Index. Frost and snowfall are similarly geared to CME Frost and CME Snowfall Indexes.

(Source: http://www.cme.com/files/weather_factcard.pdf)

Investment bank UBS has developed a Global Warming Index (UBS-GWI) to be the benchmark for measuring weather market performance.

12.4 The Nicholas Leeson Derivatives Fraud

The man behind the widely-reported debacle involving Barings Bank was Nicholas Leeson. He had an established track record of being a savvy operator in the derivatives market and was the darling of the top management at the Barings Bank headquarters in London.

As head of derivatives trading, Leeson was responsible for both the trading and clearing functions of Barings Futures Singapore (BFS), a subsidiary of London-based Barings Plc.

Leeson engaged himself in proprietary trading on the Japanese stock exchange index Nikkei 225. He operated simultaneously on the Singapore Exchange – Derivatives Trading Ltd., (SGX – DT) (erstwhile Singapore International Monetary Exchange, SIMEX), Singapore and Osaka Securities Exchange (OSE), Japan in Nikkei 225 futures and options.

A major part of Leeson's trading strategy involved the sale of options on the Nikkei 225 index futures contracts. He sold a large number of option straddles (a strategy that involves simultaneous sale of both call and put options) on Nikkei 225 index futures.

Without going into the intricacies, it may be understood that straddle results in a loss, if the market moves in either direction (up or down) drastically. His strategy amounted to a bet that the Japanese stock market would neither fall nor rise substantially.

But events took an unexpected and dramatic turn. The news of a killer earthquake in Kobe sent the Japanese stock markets tumbling. The futures on the Nikkei 225 started declining and Leeson's straddle position started incurring losses.

Desperate to make some profit from his straddles, he started supporting the index by building up extraordinarily huge long positions in Nikkei 225 futures on both exchanges - SGX – DT and OSE.

However, the Barings management was made to understand that Leeson was trying to arbitrage between the SGX-DT and OSE with the Nikkei 225 index futures.

When OSE authorities warned Leeson about his huge long positions on the exchange in Nikkei 225 futures, the trader claimed that he had built up exactly the opposite positions in the Nikkei 225 on SGX - DT. He wanted to suggest that if his positions in the Nikkei 225 at the OSE suffered losses, they would be made up by the profits by his position in the SGX - DT.

A similar impression was given to SGX - DT authorities, when they inquired about Leeson's positions. While Leeson misled both exchanges

with wrong information, neither exchange bothered to cross-check the trader's positions on the other exchanges because they were competing for the same business.

Both exchanges were more concerned about protecting their financial integrity and in doing so, allowed the continuation of the exceptionally large positions of Leeson after securing adequate margins.

The market crashed drastically. Consequently, Barings registered losses on Leeson's futures and straddle positions. But, we must note that the flames of the Leeson disaster did not singe the financial integrity of either market. This was because the markets were protected with proper margins.

A single operator can't move the market: Leeson was trying to drive up prices by buying index futures on the Nikkei 225 but could not succeed as the market was gripped by pessimism emanating from the devastating Kobe earthquake.

It is understood that he had sent fictitious reports about his trading activities to the Barings' headquarters in London. Had the top management been aware of the real situation, the disaster could probably have been avoided. Therefore, scrupulous monitoring of the position limits is as important as setting them. The top management's job of monitoring the positions of each dealer in the dealing room may be facilitated by bifurcating the front and back office operations.

Different people should be in charge of front and back-office operations so that any exposure by dealers, over and above the limits set, can be detected immediately. It means having proper checks and balances at various levels to ensure that everyone in the organisation has the disciplinary approach and works within set limits. In fact, trading systems should be capable enough to automatically disallow traders any increase in exposures as soon as they touch pre-determined limits.

Another conclusion is that exchanges should compete professionally. Both the competing exchanges, SGX – DT and OSE, were unconcerned about checking Barings' position at the other exchange. The point to be noted is that exchanges can compete, but at the same time, must co-operate and share information. It could also help in deterring efforts at price manipulation.

Another conclusion is that big institutions are as prone to incurring losses in the derivatives market as is any other individual. Therefore, irrespective of the entity, margins should be collected by the clearing corporation/ house and/ or exchange on time. Only timely collection of margins can protect the financial integrity of the market.

Clearly, the failure of Barings was not a 'derivatives' failure' but a failure of management. After the investigations were through in the Barings case, the Board of Banking Supervision's report also placed responsibility on poor operational controls at Barings rather than the use of derivatives.

An important lesson from the entire episode is that we all need a disciplinary and self-regulatory approach. The moment we go against this fundamental rule, this leveraged market is capable of threatening our very existence.

Source: Bombay Stock Exchange.

13. Carbon Credits

The United Nations Framework Convention on Climate Change (UNFCCC) was formed with two basic objectives:

1. to consider measures to reduce global warming and
2. to cope with whatever temperature increases are inevitable.

The Kyoto Protocol strengthens the UNFCCC by *committing some countries to individual, legally-binding targets to limit or reduce their greenhouse gas emissions.*

It was adopted in Kyoto, Japan, on 11th December 1997. The detailed rules for the implementation of the Kyoto Protocol were finalized with the adoption of the Marrakesh Accords.

175 countries have ratified the Kyoto Protocol. Of these some countries and the European Community (**Annex I Parties**) are required to reduce greenhouse gas emissions below levels specified for each of them in Annex B of the Protocol.

These countries are: Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, European Community, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Monaco, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russian Federation, Slovakia, Slovenia, Spain, Sweden, Switzerland, Ukraine, United Kingdom of Great Britain and Northern Ireland, United States of America.

The commitment period is 2008 to 2012.

The Kyoto Protocol focuses on reduction in the level of the following gasses: carbon dioxide, methane, nitrous oxide, hydrofluorocarbons, perfluorocarbons, sulphur hexafluoride.

The Kyoto Protocol defines **three mechanisms**:

- (1) Clean development mechanism
- (2) Joint Implementation
- (3) International Emission Trading / Carbon Trading

These mechanisms enable countries to harness cost-effective opportunities to reduce emissions or to remove carbon from the atmosphere in other countries.

Clean development mechanism

The clean development mechanism (CDM) provides for Annex I Parties to implement project activities that reduce emissions in non-Annex I Parties, in return for certified emission reductions (CERs).

The CERs generated by these project activities can be used by Annex I Parties to help meet their **emissions targets** under the Kyoto Protocol.

These project activities also assist the non-Annex I Parties in achieving **sustainable development** and in contributing to the ultimate objective of the Convention.

CDM focuses on **activities that reduce emissions** e.g. a rural electrification project using solar panels or the installation of more energy efficient boilers.

Annex I Parties are refrained from using CERs generated through nuclear facilities to meet their emission targets.

Joint Implementation

An Annex I Party can implement the following projects in the territory of another Annex I Party:

- (1) an emission-reducing project or
- (2) a project that enhances removals by sinks

Simply put, a **carbon sink** (e.g. forests, oceans etc) can absorb carbon dioxide from the atmosphere. The UNFCCC defines “sink” as “any process, activity or mechanism which removes a greenhouse gas, an aerosol or a precursor of a greenhouse gas from the atmosphere”.

It can count the resulting emission reduction units (ERUs) towards meeting its own Kyoto target.

International Emission Trading / Carbon Trading

Annex I Parties can acquire **units** from other Annex I Parties and use them towards meeting their emissions targets under the Kyoto Protocol.

Only Annex I Parties to the Kyoto Protocol with emission limitation and reduction commitments inscribed in Annex B to the Kyoto Protocol can participate in such trading. Such Parties can transfer units when they do not require them for compliance with their own emission targets.

Transfers and acquisitions of these units are tracked and recorded through the **registry systems** under the Kyoto Protocol.

ICE ECX Carbon Financial Instruments Futures

Under the European Union Emissions Trading Scheme (EU ETS), each **emission allowance** is an entitlement to emit one ton of carbon dioxide equivalent gas.

The EU ETS regulates the carbon dioxide emissions from installations across the European Union and includes power generation, mineral oil refineries, offshore installations, and other heavy industrial sectors.

Member countries are required to prepare a **National Allocation Plan** setting out:

- (1) total quantity of emission allowances to be allocated to all installations
- (2) how those emissions allowances will be distributed to each installation which holds a permit to emit carbon dioxide.

Installations emitting below the capped level can trade the excess emission allowances.

Each installation is required to surrender emission allowances equivalent to its total emissions in the calendar year. Failure to do so results in excess emissions penalty.

Emission allowances are held in dematerialized form in a series of National Registries.

The ICE Futures ECX Carbon Financial Instruments Futures Contracts (ICE ECX CFI Futures) are designed to facilitate the trading, risk management, hedging and physical delivery of emission allowances.

Contract Specifications

Unit of Trading	One lot of 1000 Emission Allowances, each Emission Allowance being an entitlement to emit one tonne of carbon dioxide equivalent gas.
Minimum trading size	1 lot.
Quotation	Euro (€) and Euro cent (c) per metric tonne.
Tick size	€0.01 per tonne (i.e. €10.00 per lot).
Minimum / maximum price fluctuation	€0.01 / no maximum limit.
Contract/delivery months	Contracts are listed on a monthly expiry cycle from September 2006 to March 2008. Additionally 6 December contracts will be listed from December 2007 to December 2012.
Expiry day	Last Monday of the contract month. Where this falls on a Non-Business Day, or there is a Non-Business Day in the 4 days immediately following the last Monday, the last day of trading shall be the penultimate Monday of the delivery month.
Trading system	Trading occurs on the ICE Futures electronic trading platform known as the ICE Platform which

	is accessible via Web ICE or through an ICE Futures conformed Independent Software Vendor.
Trading hours	07:00 hours to 17:00 hours UK local time.
Settlement prices	Trade weighted average during the daily closing period or Quoted Settlement Prices at the Exchange's discretion.
Delivery	<p>The contracts are physically deliverable by the transfer of Emission Allowances from the Person Holding Account of the Selling Clearing Member at a Registry to the Person Holding Account of LCHC at a Registry, and from the Person Holding Account of LCHC at that Registry to the Person Holding Account of the Buying Clearing Member at a Registry.</p> <p>Delivery is between Clearing Members and LCHC during a Delivery Period. The Delivery Period is the period beginning at 19:00 hours on the business day following the last trading day and ending at 19:30 hours on the third business day following that last trading day.</p> <p>There are provisions for delayed and failed delivery within the Contract Rules.</p>
Clearing and Contract Security	LCHC acts as central counterparty to all trades and guarantees the financial performance of the ICE Futures contracts registered in the name of its Members.
Margin	Variation and initial margin are charged in the usual manner by LCHC.

14. Depository Receipts

14.1 American Depository Receipts

An American Depository Receipt (ADR) is how the stock of most foreign companies trades in United States stock markets.

Each ADR is issued by a U.S. depository bank and represents one or more shares of a foreign stock or a fraction of a share. If investors own an ADR they have the right to obtain the foreign stock it represents, but U.S. investors usually find it more convenient to own the ADR. The price of an ADR is often close to the price of the foreign stock in its home market, adjusted for the ratio of ADRs to foreign company shares.

Depository banks have numerous responsibilities to the holders of ADRs and to the non-U.S. companies the ADRs represent. The largest depository bank is The Bank of New York. Individual shares of a foreign corporation represented by an ADR are called American Depository Shares (ADS).

It can be summarized that ADRs are negotiable receipts, issued to investors by an authorized depository, normally a US bank or depository, in lieu of shares of the foreign company which are actually held by the depository. The depository receives dividends directly from the Indian company in rupees and issues dividend cheques to ADR holders in dollars.

The benefits of an ADR include:

- (1) ADRs can be listed and traded in a US-based stock exchange and they help the Indian company to be known in the highly liquid US stock exchanges.
- (2) ADRs also help the US-based and other foreign investors to have the twin benefit of having a shareholding in a high growth Indian company and the convenience of trading in a highly liquid and well-known stock market.
- (3) Indian companies are prohibited by law from listing rupee-denominated shares directly in foreign stock markets. Therefore, they issue such shares to a depository which has an office within India. These shares remain in India with a custodian. Against the underlying shares, the depository issues dollar-denominated receipts to foreign investors.
- (4) Foreign investors can then sell these receipts in the foreign stock exchanges. They can also sell the receipts back to the depository and get the delivery of the underlying rupee-denominated shares which can then be sold in the Indian markets. This is generally done if Foreign

Institutional Investors with a presence in both India and the US see an arbitrage opportunity arising out of a difference in prices on the US and Indian exchanges.

14.2 ADRs v/s GDRs

ADRs are listed on an American stock exchange. The issue process is governed by American laws and Securities and Exchange Commission (SEC), the market regulator, monitors the issue. GDRs or global depository receipts are listed in a stock exchange other than an American stock exchange e.g. Luxembourg or London.

A listing in America involves adhering to very stringent disclosure and accounting norms. The accounts of the company have to be represented according to US Generally Accepted Accounting Principles (GAAP).

US GAAP requires representing a combined balance sheet of all group companies, and not just the company which is going for the issue. Typically, a good company can expect its reported profits according to Indian accounting rules to be eroded by 20-30 per cent under US GAAP.

Against this, the disclosure requirements for GDR issues are widely thought to be less stringent.

An ADR listing allows American retail investors to partake in the offering and leads to wider interest and better valuations of a company's stock, thus enhancing shareholder value. Also, the Indian company can acquire US companies against issue of shares.

The GDR market is mainly an institutional market with lower liquidity.

15. Investigating Financial Crimes

15.1 Income Tax Raid case

Gurubhai Batliwala 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.

Request for Service

RFS No. IN-PNQ/03-08/084	Date 19 th 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 19 th March 2008	Case recd by Rohas Nagpal	Referred by Manoj Kumar	
<input checked="" type="checkbox"/> Tax	Porn	Financial	Cyber
_____		Priority 1 2 <u>3</u> 4 5 6 7 8 9 10	

Chain of Custody Form

Lead Investigator:
Rohas Nagpal

1. Case Number: IN-PNQ/03-08/084	2. Evidence number: HDD-01		
3. Date and time of confiscation / recovery: 19 th March 2008 [1425 hours]			
4. Person from whom confiscated / recovered: Gurubhai Batliwala			
5. Place of Confiscation / recovery: 128, Crescent Avenue, Zimblia			
6. Details of prior access / investigation: NIL			
7. Description of hard disk:			
Model no: SV4002H Manufacturer: Samsung Serial no: 0439J1BT731517 Dimensions: 10cm*14.5 cm*2.5 cm	Capacity: 40GB Jumper: Master Interface: IDE LBA Add. Sec.: 78,242,976		
8. Unusual marks, if any: None			
Chain of Custody			
Date & Time	Released by	Released to	Purpose of change of custody
20 th Mar 2008 1005 hours	Rohas Nagpal	Parag Singh	Creation of image Computation of hash value
20 th Mar 2008 1245 hours	Parag Singh	Rohas Nagpal	For returning to client
20 th 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:

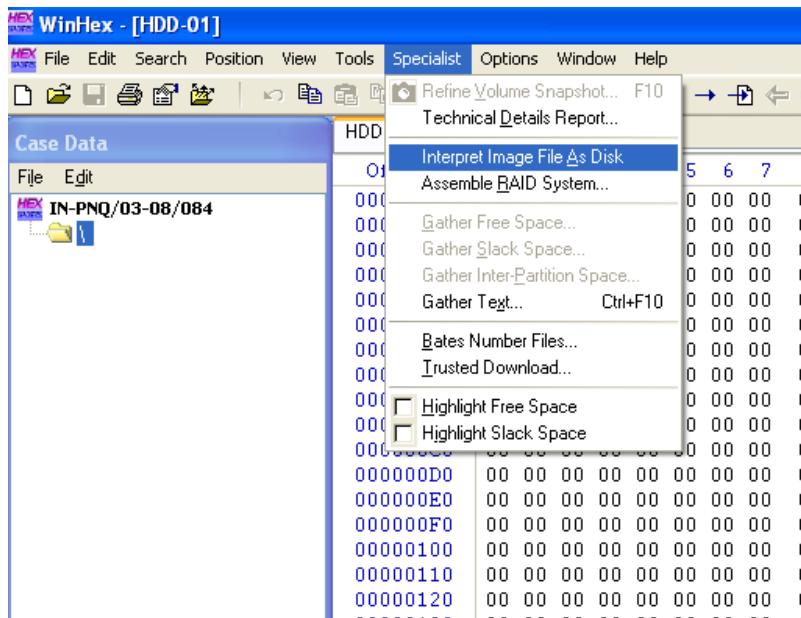
DFF0AC234C03F75E9EC13DFF77C48911

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:

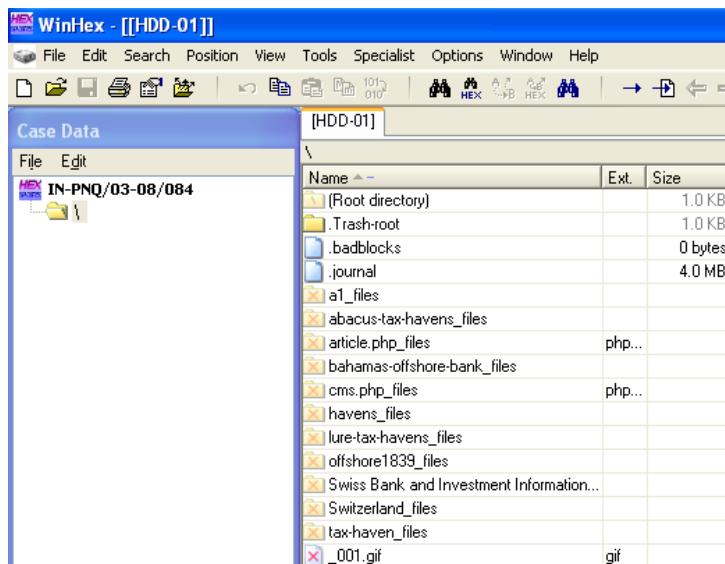
DFF0AC234C03F75E9EC13DFF77C48911

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).

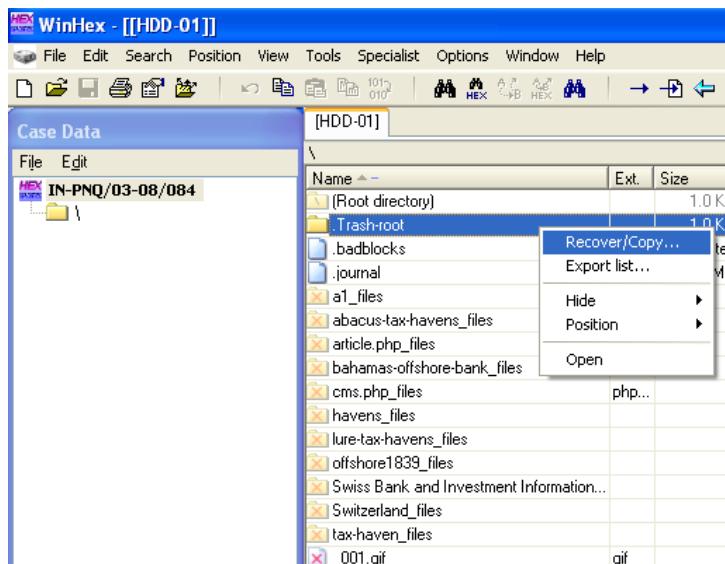


- (2) I then viewed the contents of the image file in the Directory Browser of Winhex (illustrated below).



(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.

(4) The **.Trash-root** folder contains 336 files and 21 directories.



(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:

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

(8) The file ‘**details2.txt**’ contains details of transactions as under:

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

15.2 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 Bxxxxxxxxxxxxxxxxxxxxxx77.

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/cci/case_8/18022006.htm

Request for Service

RFS No. (Pl leave blank) IN-PNQ/02-06/086	Date 18 th Feb, 2006		
Client name and address Manoj Kumar, 24/2 Zimblia Drive			
Client's authorised representative			
Name Manoj Kumar	Email mk@gmail.com	Phone 34221341	Fax 3423412

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)			
Case recd on 18 th February 2006	Case recd by Rohas Nagpal	Referred by Manoj Kumar	
Tax _____	Porn _____	Financial _____	Cyber _____
		Priority 1 2 3 <u>4</u> 5 6 7 8 9 10	

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
A:12-B:34-C:56-D:98-E:40-F:62-G:78

(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.

15.3 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 19 th March, 2008		
Client name and address Fly-in Florist Inc, Zimblia			
Client's authorised representative			
Name Manoj Kumar	Email mk@flyinflorist.in	Phone 34221341	Fax 3423412

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)			
Case recd on 19 th March 2008	Case recd by Rohas Nagpal	Referred by Manoj Kumar	
Tax _____ _____	Porn Financial _____	Cyber	Priority 1 2 3 4 5 6 <u>7</u> 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:

The screenshot shows a web page for 'The FlyinFlorist'. At the top left is the logo 'the flyinflorist' with a stylized flower icon. To its right is the tagline 'Fresh, Fast and Fabulous – The FlyinFlorist'. On the left side of the main content area, there is a vertical sidebar with a list of navigation links:

- Home
- Take order
- View Sales Reports
- View customer Details
- View Delivery Reports

Below this sidebar is a large vertical image of a floral arrangement.

The main content area is divided into two sections:

Enter Customer Information

Name: Rohas Nagpal

Address: 6th Floor, Pride Senate, Senapati Bapat Road, Pune

Phone Number: +91-20-65206029

E-Mail: rn@asianlaws.org

Enter Payment Information

Bank Name: NFS Bank

Credit Card no: ASDF132207ZB1 CVV no: 123

Expiry Date: November 2010

(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:

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

Rohas Nagpal	TFF-TU-996-2007	91-20-65206029	6th Floor, Pride Senate	3-March-2008
--------------	-----------------	----------------	-------------------------	--------------

(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:

Name	Bill No.	Product ID	Quantity	Amount
Rohas Nagpal	TFF-TU-977-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-978-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-979-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-981-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-982-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-983-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-984-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-986-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-987-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-988-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-989-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-991-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-992-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-993-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-994-2007	TU-01	10	1000
Rohas Nagpal	TFF-TU-996-2007	TU-01	10	1000

(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:

Name	Product ID	Quantity	Amount	Bill No.	Merchant
Rohas Nagpal	TU-01	10	1000	TFF-TU-977-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-978-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-979-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-980-2007	FLYINGFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-981-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-982-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-983-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-984-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-985-2007	FLYINGFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-986-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-987-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-988-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-989-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-990-2007	FLYINGFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-991-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-992-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-993-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-994-2007	FLYINFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-995-2007	FLYINGFLORIST
Rohas Nagpal	TU-01	10	1000	TFF-TU-996-2007	FLYINFLORIST

(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.

14. Investigating Digital Signature crimes

1. Introduction

The basic concepts relating to digital signatures have been discussed in Chapter 11. This chapter discusses the concept of digital signature certificates and then analyzes a case study.

Simply put, a digital signature certificate contains a public key as “certified” by a Certifying Authority (CA).

Let us take a simple illustration. Rohas Nagpal wants to digitally sign emails and electronic contracts. The first step he would take is to generate a private-public key pair. Once he has done that, he can use his private key to sign contracts etc. Anyone can use Mr. Nagpal’s public key to verify his signature. That’s where the problem begins.

How can anyone be sure which is Mr. Nagpal’s public key? What if Mr. Nagpal denies that a particular public key is actually his? To solve this problem digital signature certificates are used.

Mr. Nagpal would apply to a licenced CA for a digital signature certificate. As part of the application process he would submit identification documents (such as passport, PAN card etc). He would also send his public key to the CA. The CA would then “certify” the public key as belonging to Mr. Nagpal and issue a digital signature certificate that contains Mr. Nagpal’s public key along with information identifying him.

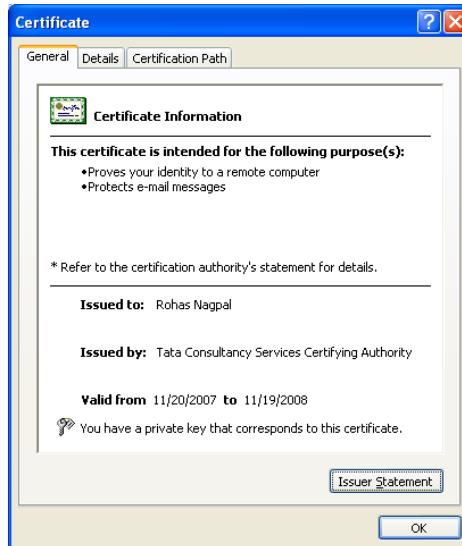
Let us now discuss the contents of a digital signature certificate in detail. For the purposes of this discussion we will discuss the digital signature certificate issued to Mr. Rohas Nagpal by the TCS CA.

To view digital signature certificates stored by default on your computer, you can open up the Microsoft Internet Explorer program and click on Tools → Internet Options → Content → Certificates option.

To make this section easy to understand, the language used is in the first person. References to “I”, “me” etc refer to “Rohas Nagpal”, the author of this book.

Let us discuss my digital signature certificate (DSC) in detail. I have been issued a DSC by TCS CA which is licenced by the Controller of Certifying Authorities of India. The DSC has been imported into my personal computer that also has the Microsoft Internet Explorer program installed.

To view my DSC, I first open up the Microsoft Internet Explorer program and click on Tools → Internet Options → Content → Certificates option.



The first view of the DSC displays the **Certificate Information** which contains the following basic information: (1) Purposes for which the certificate is intended (2) Person to whom it is issued (3) Issuer of the certificate (4) Validity period of the certificate.

As can be seen from figure 1, the certificate is intended to do the following: (1) Prove my identity to another computer (2) Protect email messages.

The certificate is issued to me by Tata Consultancy Services Certifying Authority (TCS CA) and is valid from 20th November 2007 to 19th November 2008.

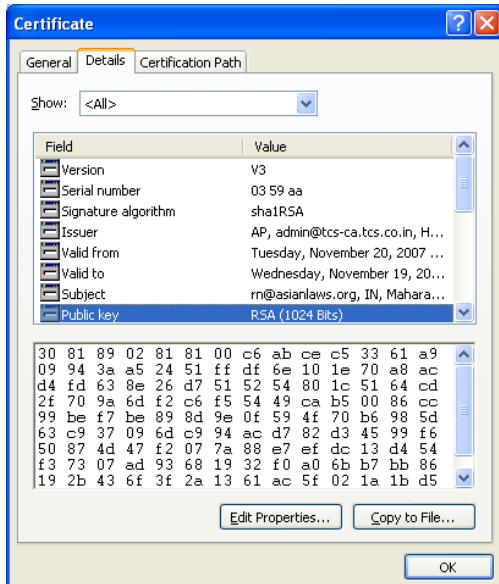
It can be noticed that the DSC states that “You have a private key that corresponds to this certificate”. This is because the DSC is on my personal computer and my private key is also on this computer. If you were to download my DSC onto your computer, then this statement would not show up as your computer does not have my private key.

Clicking on the “Issuer Statement” button on the DSC opens up the Relying Party Agreement from the TCS website.

The Relying Party Agreement is an agreement between TCS CA and the person relying on a DSC (or verifying a DSC). The agreement must be read along with the TCS-CA trust network

certification practice statement (CPS) posted at the TCS-CA web site (<https://www.tcs-ca.tcs.co.in>) as amended from time to time.

Clicking on the **Details** tab, displays the certificate details.



The following are some of the details of the certificate:

(1) Version: This is stated as V3. This signifies that the DSC is based on the X509 version 3 technology standards.

(2) Serial number: The serial number is a positive integer assigned by the CA to each DSC issued by it. This number is unique for each DSC issued by the CA.

Note: “03 59 aa” is a hexadecimal number that corresponds to the decimal number 50696362

(3) Signature Algorithm: This field identifies the mathematical algorithm used by the CA to sign the certificate [sha1RSA is this case]. *sha1* stands for Secure Hash Algorithm 1 while *RSA* stands for Rivest Shamir Adleman.

(4) Issuer: This field identifies the CA who has issued this DSC. The table below summarizes the information as contained in the DSC and the brief explanation of what that information stands for.

Information on DSC	Explanation
S = AP	State = Andhra Pradesh
E = admin@tcs-ca.tcs.co.in	Email = admin@tcs-ca.tcs.co.in
L = Hyderabad	Location = Hyderabad
CN = Tata Consultancy Services Certifying Authority	Common Name = Tata Consultancy Services Certifying Authority
OU = TCS CA	Organizational-unit = TCS CA,
O = India PKI	Organization = India PKI
C = IN	Country = India

- (1) Valid From: This indicates that the DSC is valid from 11:31:07 AM on Tuesday, November 20, 2007.
- (2) Valid To: This indicates that the DSC is valid till 11:31:07 AM on November 19, 2008.
- (3) Subject: The subject field identifies the person to whom this DSC has been issued by the CA – Rohas Nagpal in this case. The table below summarizes the information as contained in the DSC and the brief explanation of what that information stands for.

Information on DSC	Explanation
E = rn@asianlaws.org	Email = rn@asianlaws.org
C = IN	Country = India
S = Maharashtra	State = Maharashtra
L = Pune	Location = Pune
O = Tata Consultancy Services - Certifying Authority	Organisation = Tata Consultancy Services - Certifying Authority
OU = Class 3 Certificate	Organization Unit = Class 3 Certificate ³¹
OU = Individual - Others	Organization Unit = Individual - Others ³²
OU = TCS-CA - Registration Authority	Organization Unit = TCS-CA - Registration Authority
CN = Rohas Nagpal	Common Name= Rohas Nagpal

³¹ Class-3 Certificates are legally recognized digital signatures as per the IT Act, 2000.

³² The basic options are Company user, Government user and Individual user. Under Individual user the options are Banking, Government and Others.

(1) Public Key: This field specifies my public key (see below), the algorithm used by me to generate the key (RSA) and the key size (1024 bits).

```
30 81 89 02 81 81 00 c6 ab ce c5 33 61 a9 09 94 3a a5 24 51 ff df 6e 10 1e 70 a8 ac d4 fd 63  
8e 26 d7 51 52 54 80 1c 51 64 cd 2f 70 9a 6d f2 c6 f5 54 49 ca b5 00 86 cc 99 be f7 be 89 8d  
9e 0f 59 4f 70 b6 98 5d 63 c9 37 09 6d c9 94 ac d7 82 d3 45 99 f6 50 87 4d 47 f2 07 7a 88 e7  
ef dc 13 d4 54 f3 73 07 ad 93 68 19 32 f0 a0 6b b7 bb 86 19 2b 43 6f 3f 2a 13 61 ac 5f 02 1a  
1b d5 52 e5 70 24 16 fa 5d 83 79 02 03 01 00 01
```

(2) CRL Distribution Points: A certificate revocation list (CRL) is a list of serial numbers of those digital signature certificates which should not be relied upon because they: (1) have been revoked, or (2) are no longer valid. This field indicates the URL from where the relevant Certification Revocation List can be downloaded, which in this case is-
http://www.tcs-ca.tcs.co.in/crl_2785.crl

Clicking on the **Certification Path** tab, displays the certification path. This shows that my digital signature certificate has been issued by TCS CA. It also shows that the TCS CA digital signature certificate has been issued by the Controller of Certifying Authorities.

2. Case study

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.

Request for Service

RFS No. (Pl leave blank) IN-PNQ/01-08/086	Date 5 th January, 2008		
Client name and address Manoj Kumar, Data64 LLC			
Client's authorised representative			
Name Manoj Kumar	Email mk@data64.com	Phone 34221341	Fax 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 19 th March 2008	Case recd by Rohas Nagpal	Referred by Manoj Kumar	
Tax	Porn	Financial	Cyber
		Priority <u> 1 2 3 4 5 6 7 8 9 10 </u>	

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.

[日本語](#) | [Slovenščina](#) | [Dansk](#) | [Русский](#) | [Română](#) | [Türkçe](#) | [Nederlands](#) | [Ελληνικά](#) | [Français](#) | [Svenska](#) | [Português](#) |
[Italiano](#) | [繁體中文](#) | [简体中文](#) | [Magyar](#) | [Deutsch](#) | [Česky](#) | [Polski](#) | [Español](#)



Virustotal 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. [More information...](#)

File **taxdetails.doc.exe** received on **02.13.2008 06:56:31 (CET)**

Current status: **finished**

Result: **30/32 (93.75%)**

[Compact](#)

[Print results](#)

Antivirus	Version	Last Update	Result
AhnLab-V3	2008.2.13.11	2008.02.13 -	
AntiVir	7.6.0.65	2008.02.12	BDS/Ciadoor.13.1
Authentium	4.93.8	2008.02.13	W32/Ciadoor.DC@bd
Avast	4.7.1098.0	2008.02.12	Win32:Pakes-EL
AVG	7.5.0.516	2008.02.12	BackDoor.Ciadoor.3.BS
BitDefender	7.2	2008.02.13	Trojan.Keylogger.88
CAT-QuickHeal	None	2008.02.12	W32.Brontok.Q
ClamAV	0.92	2008.02.12	Trojan.Ciadoor.13.H
DrWeb	4.44.0.09170	2008.02.12	Trojan.KeyLogger.88

Screenshot of the TotalVirus.com scan results

Details of the TotalVirus.com scan results

Antivirus	Version	Last Update	Result
AhnLab-V3	2008.2.13.11	2008.02.13	-
AntiVir	7.6.0.65	2008.02.12	BDS/Ciadoor.13.1
Authentium	4.93.8	2008.02.13	W32/Ciadoor.DC@bd
Avast	4.7.1098.0	2008.02.12	Win32:Pakes-EL
AVG	7.5.0.516	2008.02.12	BackDoor.Ciadoor.3.BS
BitDefender	7.2	2008.02.13	Trojan.Keylogger.88
CAT-QuickHeal	None	2008.02.12	W32.Brontok.Q
ClamAV	0.92	2008.02.12	Trojan.Ciadoor.13.H
DrWeb	4.44.0.09170	2008.02.12	Trojan.KeyLogger.88
eSafe	7.0.15.0	2008.02.11	suspicious Trojan/Worm
eTrust-Vet	31.3.5532	2008.02.12	Win32/Ciadoor.J
Ewido	4.0	2008.02.12	Backdoor.Ciadoor.13
FileAdvisor	1	2008.02.13	-
Fortinet	3.14.0.0	2008.02.13	W32/Ciadoor.13!tr.bdr
F-Prot	4.4.2.54	2008.02.12	W32/VB-EMU:VB-Dropper-based!Maximus
F-Secure	6.70.13260.0	2008.02.13	W32/Ciadoor.R
Ikarus	T3.1.1.20	2008.02.13	IM-Worm.Win32.Sumom.C
Kaspersky	7.0.0.125	2008.02.13	Backdoor.Win32.Ciadoor.13
McAfee	5228	2008.02.12	BackDoor-ASB
Microsoft	1.3204	2008.02.12	VirTool:Win32/VB.L
NOD32v2	2870	2008.02.12	Win32/Ciadoor.13
Norman	5.80.02	2008.02.12	W32/Ciadoor.R
Panda	9.0.0.4	2008.02.13	Bck/Ciadoor.X
Prevx1	V2	2008.02.13	Heuristic: Suspicious File With Covert Attributes
Rising	20.29.22.00	2008.01.30	Backdoor.CiaDoor.13
Sophos	4.26.0	2008.02.13	Troj/Ciadoor-K
Sunbelt	2.2.907.0	2008.02.13	VIPRE.Suspicious
Symantec	10	2008.02.13	Backdoor.Ciadoor

TheHacker	6.2.9.218	2008.02.12	W32/Behav-Heuristic-066
VBA32	3.12.6.0	2008.02.11	OScope.Backdoor.VB
VirusBuster	4.3.26:9	2008.02.12	Backdoor.Ciadoor.DA
Webwasher-Gateway	6.6.2	2008.02.13	Trojan.Backdoor.Ciadoor.13.1

(3) The file taxdetails.doc.exe described as under is stored in the CD ROM accompanying this investigation report.

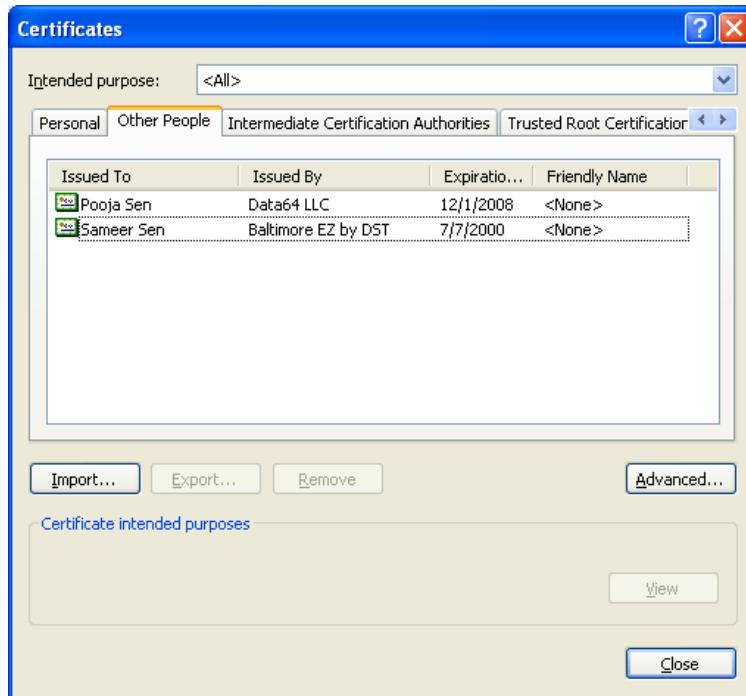
File size: 125692 bytes
MD5: 9f0247316edd0d885efe1116fde5f56f
SHA1: 3466bee9e491e718a080264ac07386c958655aa4

(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 Sen. This certificate was stored in the "Other People" tab of the certificate store on Pradeep's computer. 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.



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

(9) I then examined the certificate in detail.

(10) The subject of the certificate was

E = ps@data64.com

CN = Pooja Sen

OU = Finance

O = Data64 LLC

L = Pune

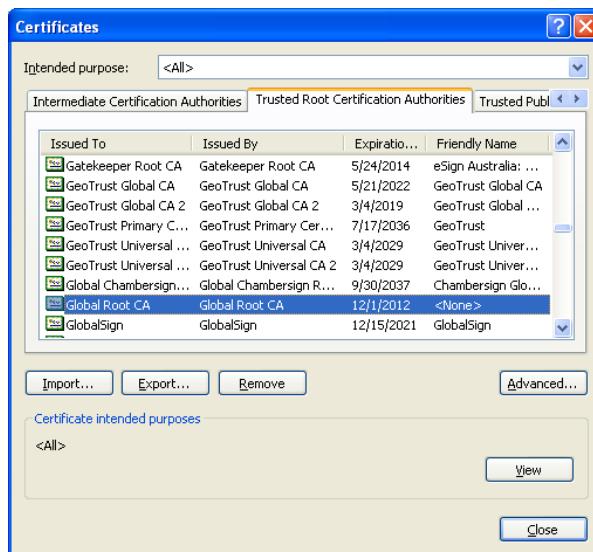
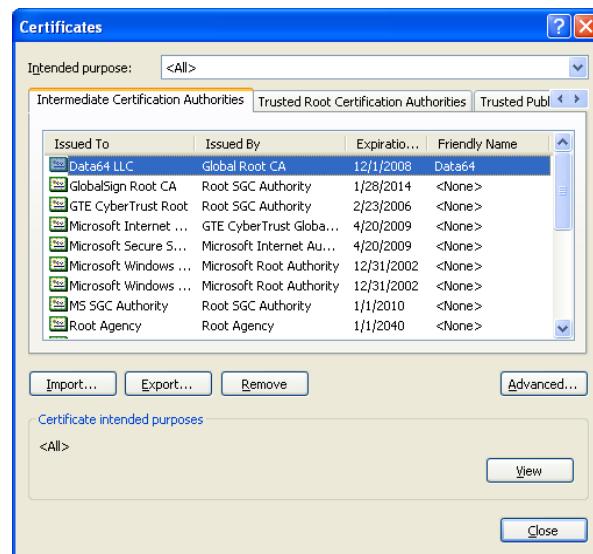
S = Maharashtra

C = IN

(11) The certification path of this certificate is illustrated below:



- (12) 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.
- (13) 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:



- (14) The IT department of Data64 stated that they had never applied to Global Root CA for a digital signature certificate.

(15) 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

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

(17) 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:

The screenshot shows a web-based tracking report from ReadNotify. At the top, there are buttons for Refresh, Display, and Close. Below that, the title 'ReadNotify email tracking history' is displayed. The main content area has a table with the following data:

To	info@globalroot-ca.com
From	info@data64.in
Subject	Information request
Sent on	13-Feb-08 at 13:19:34pm 'Asia/Calcutta' time
1st Open	13-Feb-08 at 13:33:18pm +05:30
Tracking Details	
Opened	
Opened	13-Feb-08 at 13:33:18pm (UTC +05:30) - 13mins44secs after sending
Location	Mumbai, Maharashtra, India (86% likelihood)
Opened on	ABT3-MH-dynamic-052.31.169.122.airtelbroadband.in (122.169.31.52:2357)
Language	of recipient's PC: en-us (English/United States), en;q=0.5 (English)
Browser	used by recipient: Moz5.0 (Win; U; Windows NT 5.1; en-US; rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12
Accepts	Files browser can open: */png,*/*;q=0.5
Referrer	http://mail.google.com/mail/?ui=2&view=bsp&ver=ymdfwq781tpu
Summary - as at 13-Feb-08 at 13:33:38pm (UTC +05:30)	- 14mins4secs after sending
Total	Opened 1 time by 1 reader

(18) 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.

(19) 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.

(20) 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.

(21) 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.

(22) 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:
- (d) Global Root CA certificate got installed in the Trusted Root Certification Authorities section of his certificate store.
- (e) Fake Data64 LLC certificate got installed in the Intermediate Certification Authorities section of his certificate store.
- (f) 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.
- (g) Siddharth Kumar then sent a spoofed email to Pradeep, asking him to download the taxdetails.doc file from <https://finance.data64.com>
- (h) 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.

15. Legal issues

This chapter provides an overview of the relevant legal aspects. For a detailed discussion on the legal aspects, refer to the *Commentary on the Information Technology Act, 2000* authored by Rohas Nagpal and published by Asian School of Cyber Laws.

The section numbers mentioned in this chapter refer to the *Information Technology Act, 2000* unless otherwise specified.

The format followed in this chapter is as follows:

First the relevant section of the Information Technology Act is quoted. This is formatted in a different font of a larger size and is in bold print.

If relevant, then some comments are provided. These comments are made by the author and do not form part of the section being quoted.

Finally, where relevant, a summary is provided. This contains the following details:

- (1) Acts penalized by the section
- (2) The punishment for violating the section
- (3) The punishment for an attempt to violate the section
- (4) The punishment for abetting a violation of the section
- (5) Whether the offence is cognizable i.e. whether the police can arrest without a warrant.
- (6) Whether the offence is bailable i.e. bail is granted as a right to the accused.
- (7) Whether the offence is compoundable i.e. it can be condoned by payment of money.
- (8) The authorities legally empowered to investigate the offence.
- (9) The court where the case must be filed.
- (10) The court to which the first appeal may be made.
- (11) Points for prosecution of a case under this section.
- (12) Points for defence of a case under this section.

Section 65. Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation. - For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

SUMMARY:

Acts penalized	(1) knowingly or intentionally concealing, destroying or altering computer source code (2) knowingly or intentionally causing another to conceal, destroy or alter computer source code
Punishment	Imprisonment upto 3 years and / or fine upto Rs 2 lakh
Punishment for attempt	Imprisonment upto 18 months and / or fine upto Rs 2 lakh
Punishment for abetment	Imprisonment upto 3 years and / or fine upto Rs 2 lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act

Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	<ul style="list-style-type: none"> (1) Accused has concealed or destroyed or altered computer source code or caused another to do so (2) Accused did such act(s) with knowledge and / or intention (3) Accused does not have the legal rights with respect to the source code to do such act(s)
Points for defence	<ul style="list-style-type: none"> (1) Acts committed by the accused did not result in the source code being concealed, destroyed or altered (2) The acts of the accused were not done with knowledge or intention (3) Accused had the legal rights with respect to the source code to do such act(s)

Section 66. Computer related offences

If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Explanation – For the purposes of this section, -

- (a) the word “dishonestly” shall have the meaning assigned to it in section 24 of the Indian Penal Code;**
- (b) the word “fraudulently” shall have the meaning assigned to it in section 25 of the Indian Penal Code.**

COMMENTS:

The acts referred to in section 43 of the *Information Technology Act* are:

- (a) accessing or securing access to a computer, computer system, computer network or computer resource without the permission of the owner or person in-charge;
- (b) downloading, copying or extracting any data, computer data base or information from a computer, computer system or computer network or removable storage medium without the permission of the owner or person in-charge;
- (c) introducing or caused to be introduced any computer contaminant or computer virus into any computer, computer system or computer network without the permission of the owner or person in-charge;
- (d) damaging or causing to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network without the permission of the owner or person in-charge;
- (e) disrupting or causing disruption of any computer, computer system or computer network;
- (f) denying or causing the denial of access to any person authorised to access any computer, computer system or computer network by any means without the permission of the owner or person in-charge;
- (g) providing any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder without the permission of the owner or person in-charge;

(h) charging the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network without the permission of the owner or person in-charge;

(i) destroying, deleting or altering any information residing in a computer resource or diminishing its value or utility or affecting it injuriously by any means without the permission of the owner or person in-charge;

(j) stealing, concealing, destroying or altering or causing any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage without the permission of the owner or person in-charge;

Section 24 of *Indian Penal Code* states-

Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly".

Section 25 of *Indian Penal Code* states-

A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

Another relevant provision is Section 23 of *Indian Penal Code* which defines some of the words discussed above, as under:

"Wrongful gain" is gain by unlawful means of property to which the person gaining is not legally entitled.

"Wrongful loss".--"Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled.

Gaining wrongfully, losing wrongfully.--A person is said to gain wrongfully when such person retains wrongfully, as well as when such person acquires wrongfully. A person is said to lose wrongfully when such person is wrongfully kept out of any property, as well as when such person is wrongfully deprived of property.

SUMMARY:

Acts penalized	(1) dishonestly or fraudulently accessing or securing access to a computer, computer system, computer network or computer resource without the permission of the owner or person in-charge; (2) dishonestly or fraudulently downloading, copying or extracting any data, computer data
-----------------------	---

	<p>base or information from a computer, computer system or computer network or removable storage medium without the permission of the owner or person in-charge;</p> <p>(3) dishonestly or fraudulently introducing or caused to be introduced any computer contaminant or computer virus into any computer, computer system or computer network without the permission of the owner or person in-charge;</p> <p>(4) dishonestly or fraudulently damaging or causing to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network without the permission of the owner or person in-charge;</p> <p>(5) dishonestly or fraudulently disrupting or causing disruption of any computer, computer system or computer network;</p> <p>(6) dishonestly or fraudulently denying or causing the denial of access to any person authorised to access any computer, computer system or computer network by any means without the permission of the owner or person in-charge;</p> <p>(7) dishonestly or fraudulently providing any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder without the permission of the owner or person in-charge;</p> <p>(8) dishonestly or fraudulently charging the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network without the permission of the owner or person in-charge;</p> <p>(9) dishonestly or fraudulently destroying, deleting or altering any information residing in a computer resource or diminishing its value or utility or affecting it injuriously by any means without the permission of the owner or person in-charge;</p> <p>(10) dishonestly or fraudulently stealing,</p>
--	--

	concealing, destroying or altering or causing any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage without the permission of the owner or person in-charge;
Punishment	Imprisonment upto 3 years and / or fine upto Rs 5 lakh
Punishment for attempt	Imprisonment upto 18 months and / or fine upto Rs 5 lakh
Punishment for abetment	Imprisonment upto 3 years and / or fine upto Rs 5 lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused committed one or more act prohibited by this section (2) The accused committed these acts dishonestly and / or fraudulently or has the relevant (3) The accused committed these acts without the permission of the owner or person in-charge
Points for defence	(1) The accused acted with the permission of the owner or person in-charge (2) The accused was the owner or person in-charge (3) The accused did not have the relevant intention or knowledge (4) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise

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

Any person who sends, by means of a computer resource or a communication device, -

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation. – For the purposes of this section, terms “electronic mail” and “electronic mail message” means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

SUMMARY:

Acts penalized	<p>(1) sending grossly offensive or menacing information by email, sms, mms etc</p> <p>(2) sending false information by email, sms, mms etc for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will</p> <p>(3) sending email, sms, mms etc for the purpose of causing annoyance or inconvenience</p> <p>(4) sending email, sms, mms etc to deceive or to mislead the addressee or recipient about the origin of such messages</p>
-----------------------	---

Punishment	Imprisonment upto 3 years and fine
Punishment for attempt	Imprisonment upto 18 months and fine
Punishment for abetment	Imprisonment upto 3 years and fine
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused sent grossly offensive or menacing information by email, sms, mms etc (2) The accused sent false information by email, sms, mms etc for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will (3) The accused sent email, sms, mms etc for the purpose of causing annoyance or inconvenience (4) The accused sent email, sms, mms etc to deceive or to mislead the addressee or recipient about the origin of such messages
Points for defence	(1) The nature of the information was such that it would generally not be considered grossly offensive or menacing (2) The accused had reason to believe that the information was true and did not send it for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will (3) The accused did not send the information for the purpose of causing annoyance or inconvenience

	<p>(4) The accused did not have reason to believe that the addressee or recipient would be deceived or misled about the origin of such messages</p> <p>(5) The accused did not have the relevant intention or knowledge</p> <p>(6) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise</p>
--	--

Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

SUMMARY:

Acts penalized	(1) dishonestly receiving any stolen computer resource or communication device knowing or having reason to believe the same to be stolen (2) dishonestly retaining any stolen computer resource or communication device knowing or having reason to believe the same to be stolen
Punishment	Imprisonment upto 3 years and / or fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 18 months and / or fine upto Rs 1 lakh
Punishment for abetment	Imprisonment upto 3 years and / or fine upto Rs 1 lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused dishonestly received / retained stolen computer resource or communication device

	(2) The accused knew or having reason to believe the same to be stolen
Points for defence	<p>(1) The accused did not have reason to believe that the computer resource or communication device was stolen</p> <p>(2) The accused received / retained the computer resource or communication device for the purpose of handing it over to the police or the rightful owner</p> <p>(3) The accused received / retained the computer resource or communication device for the purpose of tracing the rightful owner</p> <p>(4) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise to ascertain that the said were stolen</p>

Section 66C. Punishment for identity theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

SUMMARY:

Acts penalized	(1) fraudulently making use of the electronic signature, password or any other unique identification feature of any other person (2) dishonestly making use of the electronic signature, password or any other unique identification feature of any other person
Punishment	Imprisonment upto 3 years and fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 18 months and fine upto Rs 1 lakh
Punishment for abetment	Imprisonment upto 3 years and fine upto Rs 1 lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused made use of the electronic signature, password etc of any other person (2) The accused did this act fraudulently and / or dishonestly

	(3) The accused did not have any permission or legal right to use the said electronic signature, password etc
Points for defence	<p>(1) The accused did not have reason to believe that the electronic signature, password etc belonged to some other person</p> <p>(2) The accused had permission, express or implied, to use the said electronic signature, password etc</p> <p>(3) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise</p>

Section 66D. Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

COMMENTS:

The term “cheating” is defined in section 415 of the *Indian Penal Code*, which states:

Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".

Explanation,--A dishonest concealment of facts is a deception within the meaning of this section.

Illustrations

- (a) A, by falsely pretending to be in the Civil Service, intentionally deceives Z, and thus dishonestly induces Z to let him have on credit goods for which he does not mean to pay, A cheats.
- (b) A, by pulling a counterfeit mark on an article, intentionally deceives Z into a belief that this article was made by a certain celebrated manufacturer, and thus dishonestly induces Z to buy and pay for the article. A cheats.
- (c) A, by exhibiting to Z a false sample of an article, intentionally deceives Z into believing that the article corresponds with the sample, and thereby, dishonestly induces Z to buy and pay for the article. A cheats.
- (d) A, by tendering in payment for an article a bill on a house with which A keeps no money, and by which A expects that the bill will be dishonored, intentionally deceives Z, and thereby dishonestly induces Z to deliver the article, intending not to pay for it. A cheats.

- (e) A, by pledging as diamonds article which he knows are not diamonds, intentionally deceives Z, and thereby dishonestly induces Z to lend money. A cheats.
- (f) A intentionally deceives Z into a belief that A means to repay any money that Z may lead to him and thereby dishonestly induces Z to lend him money. A not intending to repay it. A cheats.
- (g) A intentionally deceives Z into a belief that A means to deliver to Z a certain quantity of indigo plant which he does not intend to deliver, and thereby dishonestly induces Z to advance money upon the faith of such delivery. A cheats; but if A, at the time of obtaining the money, intends to deliver the indigo plant, and afterwards breaks his contract and does not deliver it, he does not cheat, but is liable only to a civil action for breach of contract.
- (h) A intentionally deceives Z into a belief that A has performed A's part of a contract made with Z, which he has not performed, and thereby dishonestly induces Z to pay money. A cheats.
- (i) A sells and conveys an estate to B. A, knowing that in consequence of such sale he has no right to the property, sells or mortgages the same to Z, without disclosing the fact of the previous sale and conveyance to B, and receives the purchase or mortgage money for Z. A cheats.

The term "cheating by personation" is defined in section 416 of the *Indian Penal Code*, which states:

A person is said to "cheat by personation" if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is.

Explanation.--The offence is committed whether the individual personated is a real or imaginary person.

Illustration

- (a) A cheats by pretending to be a certain rich banker of the same name. A cheats by personation.
- (b) A cheats by pretending to be B, a person who is deceased. A cheats by personation.

SUMMARY:

Acts penalized	(1) Cheating by personation using a computer resource (2) Cheating by personation using a cell phone or other communication device
Punishment	Imprisonment upto 3 years and fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 18 months and fine upto Rs 1 lakh
Punishment for abetment	Imprisonment upto 3 years and fine upto Rs 1 lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused cheated someone (2) The said cheating was done by personation using a computer / communication device
Points for defence	(1) The accused did not have the relevant intention or knowledge (2) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise

Section 66E. Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Explanation – For the purposes of this section –

- (a) “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;
- (b) “capture”, with respect to an image, means to videotape, photograph, film or record by any means;
- (c) “private area” means the naked or undergarment clad genitals, public area, buttocks or female breast;
- (d) “publishes” means reproduction in the printed or electronic form and making it available for public;
- (e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that –
 - (i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
 - (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

SUMMARY:

Acts penalized	(1) Intentionally capturing, publishing or transmitting the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person (2) Intentionally capturing, publishing or transmitting the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person
Punishment	Imprisonment upto 3 years and / or fine upto Rs 2- lakh

Punishment for attempt	Imprisonment upto 18 months and / or fine upto Rs 2 lakh
Punishment for abetment	Imprisonment upto 3 years and / or fine upto Rs 2 lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused intentionally or knowingly captured, published or transmitted the image of a private area of any person (2) The accused did so without the consent of the victim (3) The accused did so under circumstances violating the privacy of the victim
Points for defence	(1) The accused had obtained the consent of the victim, either expressly or impliedly (2) The circumstances were such that they did not violate the privacy of the victim (3) The accused did not have the relevant intention or knowledge (4) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise

Section 66F. Punishment for cyber terrorism

(1) Whoever, -

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by -

- (i) denying or cause the denial of access to any person authorised to access computer resource; or**
- (ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or**
- (iii) introducing or causing to introduce any computer contaminant,**

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

COMMENTS:

Section 55 of the *Indian Penal Code* is titled “Commutation of sentence of imprisonment for life” and states-

In every case in which sentence of imprisonment for life shall have been passed, the appropriate Government may, without the consent of the offender, commute the punishment for imprisonment of either description for a term not exceeding fourteen years.

SUMMARY:

Acts penalized	<p>(1) Doing the following with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people:</p> <ul style="list-style-type: none">(i) causing denial of access to computer resource;(ii) attempting to unauthorizedly penetrate or access a computer resource; or(iii) introducing any computer contaminant, <p>(2) Acts in (1) above are penalized if by means of such conduct, the accused causes or is likely to cause the following:</p> <ul style="list-style-type: none">(i) death or injuries to persons, or(ii) damage to property, or(iii) destruction of property, or(iv) disruption of supplies or services essential to the life of the community, or(v) adverse affect to the critical information infrastructure specified under section 70. <p>(3) Unauthorizedly and knowingly / intentionally penetrating or accessing a computer resource and obtaining access to:</p> <ul style="list-style-type: none">(i) information that is restricted for reasons of the security of the State or foreign relations;(ii) restricted information, with reasons to believe that such information may be used to cause or likely to cause injury to: (a) the interests of the sovereignty and integrity of India (b) the security of the State (c) friendly relations with foreign States (d) public order, decency or morality,
-----------------------	---

	(iii) restricted information, with reasons to believe that such information may be used: (a) in relation to contempt of court (b) defamation (c) incitement to an offence (d) to the advantage of any foreign nation, group of individuals or otherwise.
Punishment	Imprisonment upto life imprisonment
Punishment for attempt	Imprisonment upto 10 years
Punishment for abetment	Imprisonment upto life imprisonment
Whether cognizable?	Yes
Whether bailable?	No
Whether compoundable?	No.
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Court of Session
First appeal lies to	High Court
Points for prosecution	(1) The accused either had no authorization, or exceeded the authorization granted to him (2) The accused committed one or more of the acts penalized by this section
Points for defence	(1) The accused had authorization, whether express or implied (2) The accused did not have the relevant intention or knowledge (3) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise

Section 67. Punishment for publishing or transmitting obscene material in electronic form

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

SUMMARY:

Acts penalized	(1) Publishing or transmitting obscene electronic material (2) Causing to be published or transmitted obscene electronic material
Punishment	On first conviction: Imprisonment of either description upto 3 years and fine upto Rs 5 lakh On subsequent conviction: Imprisonment of either description upto 5 years and fine upto Rs 10 lakh
Punishment for attempt	Imprisonment upto 18 months and / or fine upto Rs 5 lakh
Punishment for abetment	Imprisonment upto 3 years and / or fine upto Rs 5 lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	On first conviction: Yes However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman On subsequent conviction: No

Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused published or transmitted obscene electronic material (2) The accused caused obscene electronic material to be published or transmitted
Points for defence	(1) The electronic material was of such nature that it would not be considered obscene by the intended recipient (2) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise (3) The electronic material was for the public good (e.g. in the interest of science, literature, art, learning etc) (4) The electronic material was kept or used for bona fide heritage or religious purposes.

Section 67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

SUMMARY:

Acts penalized	(1) Publishing or transmitting electronic material containing sexually explicit act or conduct (2) Causing to be published or transmitted electronic material containing sexually explicit act or conduct
Punishment	On first conviction: Imprisonment of either description upto 5 years and fine upto Rs 10 lakh On subsequent conviction: Imprisonment of either description upto 7 years and fine upto Rs 10 lakh
Punishment for attempt	Imprisonment upto 30 months and / or fine upto Rs 10 lakh
Punishment for abetment	Imprisonment upto 5 years and / or fine upto Rs 10 lakh
Whether cognizable?	Yes
Whether bailable?	No
Whether compoundable?	No
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session

Points for prosecution	(1) The accused published or transmitted electronic material containing sexually explicit act or conduct (2) The accused caused such material to be published or transmitted
Points for defence	(1) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise (2) The electronic material was for the public good (e.g. in the interest of science, literature, art, learning etc) (3) The electronic material was kept or used for bona fide heritage or religious purposes.

Section 67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form

Whoever, -

- (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or
- (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
- (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
- (d) facilitates abusing children online; or
- (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form –

- (i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or
- (ii) which is kept or used for *bona fide* heritage or religious purposes.

Explanation – For the purposes of this section, “children” means a person who has not completed the age of 18 years.

SUMMARY:

Acts penalized	(1) Publishing or transmitting electronic material which depicts children engaged in sexually explicit act or conduct (2) Causing to be published or transmitted electronic material which depicts children engaged in sexually explicit act or conduct (3) Creating text or digital images depicting children in obscene or indecent or sexually explicit manner (4) Collecting, seeking, browsing, downloading, advertising, promoting, exchanging or distributing electronic material depicting children in obscene or indecent or sexually explicit manner (5) Cultivating, enticing or inducing children to online relationship with one or more children for sexually explicit act (6) Cultivating, enticing or inducing children to online relationship with one or more children in a manner that may offend a reasonable adult (7) Facilitating abusing children online (8) Recording in any electronic form abuse pertaining to sexually explicit act with children
Punishment	On first conviction: Imprisonment of either description upto 5 years and fine upto Rs 10 lakh On subsequent conviction: Imprisonment of either description upto 7 years and fine upto Rs 10 lakh
Punishment for attempt	Imprisonment upto 30 months and / or fine upto Rs 10 lakh
Punishment for abetment	Imprisonment upto 5 years and / or fine upto Rs 10 lakh
Whether cognizable?	Yes
Whether bailable?	No
Whether compoundable?	No
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section

	28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	The accused committed one or more of the acts penalized by this section
Points for defence	<ul style="list-style-type: none"> (1) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise (2) The electronic material was for the public good (e.g. in the interest of science, literature, art, learning etc) (3) The electronic material was kept or used for bona fide heritage or religious purposes (4) The person(s) depicted in the electronic material were above 18 years of age

Section 67C. Preservation and retention of information by intermediaries

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

SUMMARY:

Acts penalized	(1) Intentionally or knowingly failing to preserve and retain information specified by the Central Government (2) Intentionally or knowingly failing to preserve and retain such information for such duration and in such manner and format as prescribed.
Punishment	Imprisonment upto 3 years and fine
Punishment for attempt	Imprisonment upto 18 months and fine
Punishment for abetment	Imprisonment upto 3 years and fine
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The intermediary intentionally or knowingly failed to preserve and retain information specified by the Central Government (2) The intermediary intentionally or knowingly failed to preserve and retain such information for

	such duration and in such manner and format as prescribed.
Points for defence	<ul style="list-style-type: none"> (1) The said information was destroyed for reasons beyond the control of the intermediary e.g. a virus attack, hard-disk failure etc (2) Prescribed information was never available to the intermediary. (3) The failure to retain / preserve the information was on account of mistake or reasons beyond the control of the intermediary (4) There was no knowledge or intention behind the failure to retain / preserve the information

Section 68. Power of the Controller to give directions

- (1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.**
- (2) Any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or with both.**

SUMMARY:

Acts penalized	Intentionally or knowingly failing to comply with the order of the Controller
Punishment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 1 year and / or fine upto Rs 1 lakh
Punishment for abetment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Whether cognizable?	No
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The Controller directed a Certifying Authority or its employee to take specified measures or cease carrying on specified measures

	<p>(2) The order was issued to ensure compliance with the provisions of the Information Technology Act and allied rules or regulations.</p> <p>(3) The Certifying Authority or its employee knowingly and intentionally failed to comply with the order of the Controller</p>
Points for defence	<p>(1) The non-compliance was for reasons beyond the control of the certifying authority or its employee</p> <p>(2) The non-compliance was on account of mistake or reasons beyond the control of the certifying authority or its employee</p> <p>(3) There was no knowledge or intention behind the non-compliance</p> <p>(4) The order of the Controller was not issued to ensure compliance with the provisions of the Information Technology Act and allied rules or regulations</p> <p>(5) Complying with the order would have resulted in violation of the law for the time being in force</p>

Section 69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource

- (1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.
- (2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.
- (3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to –
- (a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or
 - (b) intercept, monitor, or decrypt the information, as the case may be; or
 - (c) provide information stored in computer resource.
- (4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

SUMMARY:

Acts penalized	(1) Not providing access to the relevant computer resource (2) Not providing assistance to intercept, monitor, or decrypt the relevant information (3) Not providing assistance to provide relevant information
Punishment	Imprisonment upto 7 years and fine
Punishment for attempt	Imprisonment upto 3.5 years and fine
Punishment for abetment	Imprisonment upto 7 years and fine
Whether cognizable?	Yes
Whether bailable?	No
Whether compoundable?	No
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused did not extend all facilities and technical assistance to provide access to the relevant computer resource (2) The accused did not extend all facilities and technical assistance to intercept, monitor, or decrypt the information (3) The accused did not extend all facilities and technical assistance to provide information stored in the relevant computer resource
Points for defence	(1) The order was not issued by the authorized agency or official (2) The reasons for the order were not recorded (3) The prescribed procedures and safeguards were not carried out by the authorized agency or official (4) The accused did not have the technical capabilities to comply with the order (5) The accused was unable to comply with the order due to reasons outside its control

Section 69A. Power to issue directions for blocking public access of any information through any computer resource

- (1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.
- (2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.
- (3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

SUMMARY:

Acts penalized	Not blocking for access, by the public, specified information
Punishment	Imprisonment upto 7 years and fine
Punishment for attempt	Imprisonment upto 3.5 years and fine
Punishment for abetment	Imprisonment upto 7 years and fine
Whether cognizable?	Yes
Whether bailable?	No
Whether compoundable?	No
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class

First appeal lies to	Court of Session
Points for prosecution	<p>(1) The accused did not block for access by the public any information generated, transmitted, received, stored or hosted in any computer resource</p> <p>(2) The accused did not cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource</p>
Points for defence	<p>(1) The order was not issued by the authorized agency or official</p> <p>(2) The reasons for the order were not recorded</p> <p>(3) The prescribed procedures and safeguards were not carried out by the authorized agency or official</p> <p>(4) The accused did not have the technical capabilities to comply with the order</p> <p>(5) The accused was unable to comply with the order due to reasons outside its control</p>

Section 69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security

(1) The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The intermediary or any person in-charge or the computer resource shall, when called upon by the agency which has been authorised under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation. – For the purposes of this section, -

- (i) “computer contaminant” shall have the meaning assigned to it in section 43;
- (ii) “traffic data” means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service and any other information.

SUMMARY:

Acts penalized	(1) Not providing technical assistance to the authorized agency (2) Not extending all relevant facilities to the authorized agency
Punishment	Imprisonment upto 3 years and fine
Punishment for attempt	Imprisonment upto 18 months and fine
Punishment for abetment	Imprisonment upto 3 years and fine
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused did not provide technical assistance to the authorized agency (2) The accused did not extend all relevant facilities to the authorized agency
Points for defence	(1) The order was not issued by the authorized agency or official (2) The prescribed procedures and safeguards were not carried out by the authorized agency or official (3) The accused did not have the technical capabilities to comply with the order (4) The accused was unable to comply with the order due to reasons outside its control

Section 70. Protected system

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation. – For the purposes of this section, “Critical Information Infrastructure” means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety;

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (1)

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system.

SUMMARY:

Acts penalized	(1) Securing access to a protected system (2) Attempting to secure access to a protected system
Punishment	Imprisonment upto 10 years and fine
Punishment for attempt	Imprisonment upto 10 years and fine
Punishment for abetment	Imprisonment upto 10 years and fine
Whether cognizable?	Yes
Whether bailable?	No
Whether compoundable?	No
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Court of Session
First appeal lies to	High Court

Points for prosecution	(1) The accused secured access to a protected system (2) The accused attempted to secure access to a protected system
Points for defence	(1) The accused was authorised to access the protected system (2) The accused did not have the relevant intention or knowledge (3) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise

Section 70B. Indian Computer Emergency Response Team to serve as national agency for incident response

- (1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the Government to be called the Indian Computer Emergency Response Team.
- (2) The Central Government shall provide the agency referred to in sub-section (1) with a Director-General and such other officers and employees as may be prescribed.
- (3) The salary and allowances and terms and conditions of the Director-General and other officers and employees shall be such as may be prescribed.
- (4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security,-
 - (a) collection, analysis and dissemination of information on cyber incidents;
 - (b) forecast and alerts of cyber security incidents;
 - (c) emergency measures for handling cyber security incidents;
 - (d) coordination of cyber incidents response activities;
 - (e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
 - (f) such other functions relating to cyber security as may be prescribed.
- (5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.
- (6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person.
- (7) Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.
- (8) No court shall take cognizance of any offence under this section, except on a complaint made by an officer authorised in this behalf by the agency referred to in sub-section (1).

SUMMARY:

Acts penalized	(1) The accused did not provide the information called for by the Indian Computer Emergency Response Team (2) The accused did not comply with a direction of Indian Computer Emergency Response Team
Punishment	Imprisonment upto 1 year and / or fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 6 months and / or fine upto Rs 1 lakh
Punishment for abetment	Imprisonment upto 1 year and / or fine upto Rs 1 lakh
Whether cognizable?	No
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused did not provide the information called for by the Indian Computer Emergency Response Team (2) The accused did not comply with a direction of Indian Computer Emergency Response Team
Points for defence	(1) The accused did not have the technical capabilities to provide the information (2) The accused did not have the technical capabilities to comply with the direction (3) The accused was unable to comply with the direction due to reasons outside its control (4) The accused was unable to comply with the direction due to reasons outside its control

Section 71. Penalty for misrepresentation

Whoever makes any misrepresentation, to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a terms which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

SUMMARY:

Acts penalized	(1) Misrepresentation to the Controller for obtaining any licence (2) Suppression of any material fact from the Controller for obtaining any licence (3) Misrepresentation to the Certifying Authority for obtaining any Electronic Signature Certificate (4) Suppression of any material fact from the Certifying Authority for obtaining any Electronic Signature Certificate
Punishment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 1 year and / or fine upto Rs 1 lakh
Punishment for abetment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Whether cognizable?	No
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused made a misrepresentation to the

	<p>Controller for obtaining any licence</p> <p>(2) The accused suppressed a material fact from the Controller for obtaining any licence</p> <p>(3) The accused made a misrepresentation to the Certifying Authority for obtaining any Electronic Signature Certificate</p> <p>(4) The accused suppressed a material fact from the Certifying Authority for obtaining any Electronic Signature Certificate</p>
Points for defence	<p>(1) The act was a result of a mistake or negligence and was not done with knowledge or intention</p> <p>(2) The alleged misrepresentation or suppression was due to incorrect information provided to the accused by others</p> <p>(3) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise</p>

Section 72. Penalty for breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

SUMMARY:

Acts penalized	(1) Disclosure of records without consent (2) Person who discloses records must have obtained the same in pursuance of powers conferred under the Information Technology Act or allied rules, regulations etc
Punishment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 1 year and / or fine upto Rs 1 lakh
Punishment for abetment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Whether cognizable?	No
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session

Points for prosecution	(1) The accused disclosed records without consent (2) The accused had obtained the records in pursuance of powers conferred under the Information Technology Act or allied rules, regulations etc
Points for defence	(1) The accused had not obtained the records in pursuance of powers conferred under the Information Technology Act or allied rules, regulations etc (2) The disclosure was a result of a mistake or negligence and was not done with knowledge or intention (3) The disclosure was committed accidentally or by mistake as the accused did not have the relevant technical expertise (4) The accused had obtained consent for the disclosure (5) The accused was acting in the discharge of his duties under the law

Section 72A. Punishment for disclosure of information in breach of lawful contract

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

SUMMARY:

Acts penalized	(1) Disclosure of personal information about some other person (2) The disclosure must either be without consent or in breach of contract (3) There must be intention to cause wrongful loss or wrongful gain or knowledge that wrongful loss or wrongful gain may be caused
Punishment	Imprisonment upto 3 years and / or fine upto Rs 5 lakh
Punishment for attempt	Imprisonment upto 18 months and / or fine upto Rs 5 lakh
Punishment for abetment	Imprisonment upto 3 years and / or fine upto Rs 5 lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section

	28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	<p>(1) The accused disclosed personal information about some other person</p> <p>(2) The accused made the disclosure either without consent or in breach of contract</p> <p>(3) The accused had the intention to cause wrongful loss or wrongful gain or knowledge that wrongful loss or wrongful gain may be caused</p>
Points for defence	<p>(1) The act was a result of a mistake or negligence and was not done with knowledge or intention</p> <p>(2) The disclosure was committed accidentally or by mistake as the accused did not have the relevant technical expertise</p> <p>(3) The accused had obtained consent for the disclosure</p> <p>(4) The accused was acting in the discharge of his duties under the law</p> <p>(5) The accused did not breach the terms of any contract</p>

Section 73. Penalty for publishing Electronic Signature Certificate false in certain particulars

(1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that-

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended,

unless such publication is for the purposes of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of subsection (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

SUMMARY:

Acts penalized	(1) Publishing an Electronic Signature Certificate with the knowledge that the Certifying Authority listed in it has not issued it (2) Publishing an Electronic Signature Certificate with the knowledge that the subscriber listed in it has not accepted it (3) Publishing an Electronic Signature Certificate with the knowledge that the certificate has been revoked or suspended
Punishment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 1 year and / or fine upto Rs 1 lakh
Punishment for abetment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Whether cognizable?	No
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime

	affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused published an Electronic Signature Certificate with the knowledge that the Certifying Authority listed in it has not issued it (2) The accused published an Electronic Signature Certificate with the knowledge that the subscriber listed in it has not accepted it (3) The accused published an Electronic Signature Certificate with the knowledge that the certificate has been revoked or suspended
Points for defence	(1) The act was a result of a mistake or negligence and was not done with knowledge or intention (2) The disclosure was committed accidentally or by mistake as the accused did not have the relevant technical expertise (3) The publication was for the purposes of verifying a digital signature created prior to such suspension or revocation. (4) The accused was acting in the discharge of his duties under the law

Section 74. Publication for fraudulent purpose

Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

SUMMARY:

Acts penalized	Knowingly creating, publishing or making available an Electronic Signature Certificate for any fraudulent or unlawful purpose
Punishment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 1 year and / or fine upto Rs 1 lakh
Punishment for abetment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Whether cognizable?	No
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused knowingly created, published or made available an Electronic Signature Certificate for any fraudulent purpose (2) The accused knowingly created, published or made available an Electronic Signature Certificate for any unlawful purpose

Points for defence	<p>(1) The act was a result of a mistake or negligence and was not done with knowledge or intention</p> <p>(2) The disclosure was committed accidentally or by mistake as the accused did not have the relevant technical expertise</p> <p>(3) The act was not for any fraudulent purpose</p> <p>(4) The act was not for any unlawful purpose</p>
---------------------------	---

Section 77A. Compounding of offences

A court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided, under this Act:

Provided that the court shall not compound such offence where the accused is, by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind:

Provided further that the court shall not compound any offence where such offence affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

(2) The person accused of an offence under this Act may file an application for compounding in the court in which offence is pending for trial and the provisions of sections 265B and 265C of the Code of Criminal Procedure, 1973 shall apply.

COMMENTS:

A ready-reference guide of offences under the Information Technology Act and whether they are compoundable or not is provided below:

Offence	Punishment	Compoundable
Section 65. Tampering with computer source documents	Imprisonment upto 3 years and / or fine upto Rs 2 lakh	Compoundable
Section 66. Computer related offences	Imprisonment upto 3 years and / or fine upto Rs 5 lakh	Compoundable
Section 66A. Punishment for sending offensive messages through communication service, etc	Imprisonment upto 3 years and fine	Compoundable
Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device	Imprisonment upto 3 years and / or fine upto Rs 1 lakh	Compoundable
Section 66C. Punishment for identity theft	Imprisonment of either description upto 3 years and / or fine upto Rs 1 lakh	Compoundable

Section 66D. Punishment for cheating by personation by using computer resource	Imprisonment of either description upto 3 years and / or fine upto Rs 1 lakh	Compoundable
Section 66E. Punishment for violation of privacy	Imprisonment upto 3 years and / or fine upto Rs 2 lakh	Compoundable
Section 66F. Punishment for cyber terrorism	Imprisonment extend to imprisonment for life	Not Compoundable
Section 67. Punishment for publishing or transmitting obscene material in electronic form	On first conviction: Imprisonment upto 3 years and / or fine upto Rs 5 lakh	Compoundable
	On subsequent conviction: Imprisonment upto 5 years and / or fine upto Rs 10 lakh	Not Compoundable
Section 67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form	On first conviction: Imprisonment of either description upto 5 years and / or fine upto Rs 10 lakh	Not Compoundable
	On subsequent conviction: Imprisonment of either description upto 7 years and / or fine upto Rs 10 lakh	Not Compoundable
Section 67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form	On first conviction: Imprisonment of either description upto 5 years and / or fine upto Rs 10 lakh	Not Compoundable
	On subsequent conviction: Imprisonment of either description upto 7 years and / or fine upto Rs 10 lakh	Not Compoundable
Section 67C. Preservation and retention of information by intermediaries	Imprisonment upto 3 years and fine	Compoundable
Section 68. Power of the Controller to give directions	Imprisonment upto 2 years and / or fine upto Rs 1 lakh	Compoundable

Section 69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource	Imprisonment upto 7 years and fine	Not Compoundable
Section 69A. Power to issue directions for blocking public access of any information through any computer resource	Imprisonment upto 7 years and fine	Not Compoundable
Section 69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security	Imprisonment upto 3 years and fine	Compoundable
Section 70. Protected system	Imprisonment of either description upto 10 years and fine	Not Compoundable
Section 70B. Indian Computer Emergency Response Team to serve as national agency for incident response	Imprisonment upto 1 year and / or fine upto Rs 1 lakh	Compoundable
Section 71. Penalty for misrepresentation	Imprisonment upto 2 years and / or fine upto Rs 1 lakh	Compoundable
Section 72. Breach of confidentiality and privacy	Imprisonment upto 2 years and / or fine upto Rs 1 lakh	Compoundable
Section 72A. Punishment for disclosure of information in breach of lawful contract	Imprisonment upto 3 years and / or fine upto Rs 5 lakh	Compoundable
Section 73. Penalty for publishing Electronic Signature Certificate false in certain particulars	Imprisonment upto 2 years and / or fine upto Rs 1 lakh	Compoundable

Section 74. Publication for fraudulent purpose	Imprisonment upto 2 years and / or fine upto Rs 1 lakh	Compoundable
---	--	--------------

Section 265B of the *Code of Criminal Procedure* is titled “Application for plea bargaining” and states:

- (1) A person accused of an offence may file an application for plea bargaining in the Court in which such offence is pending for trial.
- (2) The application under sub-section (1) shall contain a brief description of the case relating to which the application is filed including the offence to which the case relates and shall be accompanied by an affidavit sworn by the accused stating therein that he has voluntarily preferred, after understanding the nature and extent of punishment provided under the law for the offence, the plea bargaining in his case and that he has not previously been convicted by a Court in a case in which he had been charged with the same offence.
- (3) After receiving the application under sub-section (1), the Court shall issue notice to the Public Prosecutor or the complainant of the case, as the case may be, and to the accused to appear on the date fixed for the case.
- (4) When the Public Prosecutor or the complainant of the case, as the case may be, and the accused appear on the date fixed under sub-section (3), the Court shall examine the accused in camera, where the other party in the case shall not be present, to satisfy itself that the accused has filed the application voluntarily and where--
 - (a) the Court is satisfied that the application has been filed by the accused voluntarily, it shall provide time to the Public Prosecutor or the complainant of the case, as the case may be, and the accused to work out a mutually satisfactory disposition of the case which may include giving to the victim by the accused the compensation and other expenses during the case and thereafter fix the date for further hearing of the case;
 - (b) the Court finds that the application has been filed involuntarily by the accused or he has previously been convicted by a Court in a case in which he had been charged with the same offence, it shall proceed further in accordance with the provisions of this Code from the stage such application has been filed under sub-section (1).

Section 265C of the *Code of Criminal Procedure* is titled “Guidelines for mutually satisfactory disposition” and states:

In working out a mutually satisfactory disposition under clause (a) of sub-section (4) of section 265B, the Court shall follow the following procedure, namely:

(a) in a case instituted on a police report, the Court shall issue notice to the Public Prosecutor, the police officer who has investigated the case, the accused and the victim of the case to participate in the meeting to work out a satisfactory disposition of the case:

Provided that throughout such process of working out a satisfactory disposition of the case, it shall be the duty of the Court to ensure that the entire process is completed voluntarily by the parties participating in the meeting:

Provided further that the accused may, if he so desires, participate in such meeting with his pleader, if any, engaged in the case;

(b) in a case instituted otherwise than on police report, the Court shall issue notice to the accused and the victim of the case to participate in a meeting to work out a satisfactory disposition of the case:

Provided that it shall be the duty of the Court to ensure, throughout such process of working out a satisfactory disposition of the case, that it is completed voluntarily by the parties participating in the meeting:

Provided further that if the victim of the case or the accused, as the case may be, so desires, he may participate in such meeting with his pleader engaged in the case.

Section 77B. Offences with three years imprisonment to be bailable

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

COMMENTS:

A *ready-reference guide* of offences under the Information Technology Act and whether they are cognizable / bailable or not is provided below:

Offence	Punishment	Cognizable / Bailable
Section 65. Tampering with computer source documents	Imprisonment upto 3 years and / or fine upto Rs 2 lakh	Cognizable Bailable
Section 66. Computer related offences	Imprisonment upto 3 years and / or fine upto Rs 5 lakh	Cognizable Bailable
Section 66A. Punishment for sending offensive messages through communication service, etc	Imprisonment upto 3 years and fine	Cognizable Bailable
Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device	Imprisonment upto 3 years and / or fine upto Rs 1 lakh	Cognizable Bailable
Section 66C. Punishment for identity theft	Imprisonment of either description upto 3 years and / or fine upto Rs 1 lakh	Cognizable Bailable
Section 66D. Punishment for cheating by personation by using computer resource	Imprisonment of either description upto 3 years and / or fine upto Rs 1 lakh	Cognizable Bailable
Section 66E. Punishment for violation of privacy	Imprisonment upto 3 years and / or fine upto Rs 2 lakh	Cognizable Bailable

Section 66F. Punishment for cyber terrorism	Imprisonment extend to imprisonment for life	Cognizable Non-bailable
Section 67. Punishment for publishing or transmitting obscene material in electronic form	On first conviction: Imprisonment upto 3 years and / or fine upto Rs 5 lakh	Cognizable Bailable
	On subsequent conviction: Imprisonment upto 5 years and / or fine upto Rs 10 lakh	Cognizable Non-bailable
Section 67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form	On first conviction: Imprisonment of either description upto 5 years and / or fine upto Rs 10 lakh	Cognizable Non-bailable
	On subsequent conviction: Imprisonment of either description upto 7 years and / or fine upto Rs 10 lakh	Cognizable Non-bailable
Section 67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form	On first conviction: Imprisonment of either description upto 5 years and / or fine upto Rs 10 lakh	Cognizable Non-bailable
	On subsequent conviction: Imprisonment of either description upto 7 years and / or fine upto Rs 10 lakh	Cognizable Non-bailable
Section 67C. Preservation and retention of information by intermediaries	Imprisonment upto 3 years and fine	Cognizable Bailable
Section 68. Power of the Controller to give directions	Imprisonment upto 2 years and / or fine upto Rs 1 lakh	Non-cognizable Bailable
Section 69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource	Imprisonment upto 7 years and fine	Cognizable Non-bailable

Section 69A. Power to issue directions for blocking public access of any information through any computer resource	Imprisonment upto 7 years and fine	Cognizable Non-bailable
Section 69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security	Imprisonment upto 3 years and fine	Cognizable Bailable
Section 70. Protected system	Imprisonment of either description upto 10 years and fine	Cognizable Non-bailable
Section 70B. Indian Computer Emergency Response Team to serve as national agency for incident response	Imprisonment upto 1 year and / or fine upto Rs 1 lakh	Non-cognizable Bailable
Section 71. Penalty for misrepresentation	Imprisonment upto 2 years and / or fine upto Rs 1 lakh	Non-cognizable Bailable
Section 72. Breach of confidentiality and privacy	Imprisonment upto 2 years and / or fine upto Rs 1 lakh	Non-cognizable Bailable
Section 72A. Punishment for disclosure of information in breach of lawful contract	Imprisonment upto 3 years and / or fine upto Rs 5 lakh	Cognizable Bailable
Section 73. Penalty for publishing Electronic Signature Certificate false in certain particulars	Imprisonment upto 2 years and / or fine upto Rs 1 lakh	Non-cognizable Bailable
Section 74. Publication for fraudulent purpose	Imprisonment upto 2 years and / or fine upto Rs 1 lakh	Non-cognizable Bailable

Some relevant provisions of the *Code of Criminal Procedure* are quoted below for reference:

Section 436 - In what cases bail to be taken

(1) When any person other than a person accused of a non-bailable offence is arrested or detained without warrant by an officer in charge of a police station, or appears or is brought before a Court, and is prepared at any time while in the custody of such officer or at any stage of the proceeding before such Court to give bail, such person shall be released on bail:

Provided that such officer or Court, if he or it thinks fit, may, and shall, if such person is indigent and is unable to furnish surety, instead of taking bail from such person, discharge him on his executing a bond without sureties for his appearance as hereinafter provided:

Provided further that nothing in this section shall be deemed to affect the provisions of sub-section (3) of section 1161 or section 446A.

Explanation.-- Where a person is unable to give bail within a week of the date of his arrest, it shall be a sufficient ground for the officer or the Court to presume that he is an indigent person for the purposes of this proviso.

(2) Notwithstanding anything contained in sub-section (1), where a person has failed to comply with the conditions of the bail-bond as regards the time and place of attendance, the Court may refuse to release him on bail, when on a subsequent occasion in the same case he appears before the Court or is brought in custody and any such refusal shall be without prejudice to the powers of the Court to call upon any person bound by such bond to pay the penalty thereof under section 446.

Section 436A - Maximum period for which an undertrial prisoner can be detained

Where a person has, during the period of investigation, inquiry or trial under this Code of an offence under any law (not being an offence for which the punishment of death has been specified as one of the punishments under that law) undergone detention for a period extending up to one-half of the maximum period of imprisonment specified for that offence under that law, he shall be released by the Court on his personal bond with or without sureties:

Provided that the Court may, after hearing the Public Prosecutor and for reasons to be recorded by it in writing, order the continued detention of such person for a period longer than one-half of the said period or release him on bail instead of the personal bond with or without sureties:

Provided further that no such person shall in any case be detained during the period of investigation inquiry or trial for more than the maximum period of imprisonment provided for the said offence under that law.

Explanation.--In computing the period of detention under this section for granting bail the period of detention passed due to delay in proceeding caused by the accused shall be excluded.

Section 437 - When bail may be taken in case of non-bailable offence

(1) When any person accused of, or suspected of, the commission of any non-bailable offence is arrested or detained without warrant by an officer in charge of a police station or appears or is brought before a Court other than the High Court or Court of Session, he may be released on bail, but-

- (i) such person shall not be so released if there appear reasonable grounds for believing that he has been guilty of an offence punishable with death or imprisonment for life;
- (ii) such person shall not be so released if such offence is a cognizable offence and he had been previously convicted of an offence punishable with death, imprisonment for life or imprisonment for seven years or more, or he had been previously convicted on two or more occasions of a cognizable offence punishable with imprisonment for three years or more but not less than seven years:

Provided that the Court may direct that a person referred to in clause (i) or clause (ii) be released on bail if such person is under the age of sixteen years or is a woman or is sick or infirm:

Provided further that the Court may also direct "that a person referred to in clause (ii) be released on bail if it is satisfied that it is just and proper so to do for any other special reason:

Provided also that the mere fact that an accused person may be required for being identified by witnesses during investigation shall not be sufficient ground for refusing to grant bail if he is otherwise entitled to be released on bail and gives an undertaking

that shall comply with such directions as may be given by the Court.

Provided also that no person shall, if the offence alleged to have been committed by him is punishable with death, imprisonment for life, or imprisonment for seven years or more be released on bail by the Court under this sub-section without giving an opportunity of hearing to the Public Prosecutor.

(2) If it appears to such officer or Court at any stage of the investigation, inquiry or trial as the case may be, that there are not reasonable grounds for believing that the accused has committed a non-bailable offence, but that there are sufficient grounds for further inquiry into his guilt, the accused shall, subject to the provisions of section 446A and pending such inquiry, be released on bail], or, at the discretion of such officer or Court on the execution by him of a bond without sureties for his appearance as hereinafter provided.

(3) When a person accused or suspected of the commission of an offence punishable with imprisonment which may extend to seven years or more or of an offence under Chapter VI, Chapter XVI or Chapter XVII of the Indian Penal Code (45 of 1860) or abetment of, or conspiracy or attempt to commit, any such offence, is released on bail under sub-section (1) the Court shall impose the conditions,--

- (a) that such person shall attend in accordance with the conditions of the bond executed under this Chapter,
- (b) that such person shall not commit an offence similar to the offence of which he is accused, or suspected, of the commission of which he is suspected, and
- (c) that such person shall not directly or indirectly make any inducement, threat or promise to any person acquainted with the facts of the case so as to dissuade him from disclosing such facts to the Court or to any police officer or tamper with the evidence.

and may also impose, in the interests of justice, such other conditions as it considers necessary.]

(4) An officer or a Court releasing any person on bail under sub-section (1), or sub-section (2), shall record in writing his or its reasons or special reasons for so doing.

(5) Any Court which has released a person on bail under sub-section (1), or sub-section (2), may, if it considers it necessary so

to do, direct that such person be arrested and commit him to custody.

(6) If, in any case triable by a Magistrate, the trial of a person accused of any non-bailable offence is not concluded within a period of sixty days from the first date fixed for taking evidence in the case, such person shall, if he is in custody during the whole of the said period, be released on bail to the satisfaction of the Magistrate, unless for reasons to be recorded in writing, the Magistrate otherwise directs.

(7) If, at any time after the conclusion of the trial of a person accused of a non-bailable offence and before judgment is delivered the Court is of opinion that there are reasonable grounds for believing that the accused is not guilty of any such offence, it shall release the accused, if he is in custody, on the execution by him of a bond without sureties for his appearance to hear judgment delivered.

Section 438 - Direction for grant of bail to person apprehending arrest

(1) Where any person has reason to believe that he may be arrested on accusation of having committed a non-bailable offence, he may apply to the High Court or the Court of Session for a direction under this section that in the event of such arrest he shall be released on bail; and that Court may, after taking into consideration, inter alia, the following factors, namely:--

- (i) the nature and gravity of the accusation;
- (ii) the antecedents of the applicant including the fact as to whether he has previously undergone imprisonment on conviction by a Court in respect of any cognizable offence;
- (iii) the possibility of the applicant to flee from justice; and.
- (iv) where the accusation has been made with the object of injuring or humiliating the applicant by having him so arrested, either reject the application forthwith or issue an interim order for the grant of anticipatory bail:

Provided that, where the High Court or, as the case may be, the Court of Session, has not passed any interim order under this subsection or has rejected the application for grant of anticipatory bail, it shall be open to an officer in-charge of a police station to arrest, without warrant the applicant on the basis of the accusation apprehended in such application.

(1A) Where the Court grants an interim order under sub-section (1), it shall forthwith cause a notice being not less than seven days notice, together with a copy of such order to be served on the Public Prosecutor and the Superintendent of Police, with a view to give the Public Prosecutor a reasonable opportunity of being heard when the application shall be finally heard by the Court,

(1B) The presence of the applicant seeking anticipatory bail shall be obligatory at the time of final hearing of the application and passing of final order by the Court, if on an application made to it by the Public Prosecutor, the Court considers such presence necessary in the interest of justice.

(2) When the High Court or the Court of Session makes a direction under subsection (1), it may include such conditions in such directions in the light of the facts of the particular case, as it may thinks fit, including-

(i) a condition that the person shall make himself available for interrogation by a police officer as and when required;

(ii) a condition that the person shall not, directly or indirectly, make any inducement, threat or promise to any person acquainted with the facts of the case so as to dissuade him from disclosing such facts to the Court or to any police officer;

(iii) a condition that the person shall not leave India without the previous permission of the Court;

(iv) such other condition as may be imposed under sub-section (3) of section 437, as if the bail were granted under that section.

(3) If such person is thereafter arrested without warrant by an officer in charge of a police station on such accusation, and is prepared either at the time of arrest or at any time while in the custody of such officer to give bail, he shall be released on bail, and if a Magistrate taking cognizance of such offence decides that a warrant should issue in the first instance against that person, he shall issue a bailable warrant in conformity with the direction of the Court under sub-section (1).

Section 439 - Special powers of High Court or Court of Session regarding bail

(1) A High Court or Court of Session may direct-

- (a) that any person accused of an offence and in custody be released on bail, and if the offence is of the nature specified in sub-section (3) of section 437, may impose any condition which it considers necessary for the purposes mentioned in that sub-section;
- (b) that any condition imposed by a Magistrate when releasing any person on bail be set aside or modified:

Provided that the High Court or the Court of Session shall, before granting bail to a person who is accused of an offence which is triable exclusively by the Court of Session or which, though not so triable, is punishable with imprisonment for life, give notice of the application for bail to the Public Prosecutor unless it is, for reasons to be recorded in writing, of opinion that it is not practicable to give such notice.

(2) A High Court or Court of Session may direct that any person who has been released on bail under this Chapter be arrested and commit him to custody.

Section 440 - Amount of bond and reduction thereof

- (1) The amount of every bond executed under this chapter shall be fixed with due regard to the circumstances of the case and shall not be excessive.
- (2) The High Court or Court of Session may direct that the bail required by a police officer or Magistrate be reduced.

Section 441 - Bond of accused and sureties

- (1) Before any person is released on bail or released on his own bond, a bond for such sum of money as the police officer or Court, as the case may be, thinks sufficient shall be executed by such person, and, when he is released on bail, by one or more sufficient sureties conditioned that such person shall attend at the time and place mentioned in the bond, and shall continue so to attend until otherwise directed by the police officer or Court, as the case may be.
- (2) Where any condition is imposed for the release of any person on bail, the bond shall also contain that condition.
- (3) If the case so requires, the bond shall also bind the person released on bail to appear when called upon at the High Court, Court of Session or other Court to answer the charge.

(4) For the purpose of determining whether the sureties are fit or sufficient, the Court may accept affidavits in proof of the facts contained therein relating to the sufficiency or fitness of the sureties, or, if it considers necessary, may either hold an inquiry itself or cause an inquiry to be made by a Magistrate subordinate to the Court, as to such sufficiency or fitness.

Section 442 - Discharge from custody

(1) As soon as the bond has been executed, the person for whose appearance it has been executed shall be released; and when he is in jail the Court admitting him to bail shall issue an order of release to the officer in charge of the jail, and such officer on receipt of the orders shall release him.

(2) Nothing in this section, section 436 or section 437 shall be deemed to require the release of any person liable to be detained for some matter other than that in respect of which the bond was executed.

Section 443 - Power to order sufficient bail when that first taken is insufficient

If, through mistake, fraud, or otherwise, insufficient sureties have been accepted, or if they afterwards become insufficient, the Court may issue a warrant of arrest directing that the person released on bail be brought before it and may order him to find sufficient sureties, and on his failing so to do, may commit him to jail.

Section 78. Power to investigate offence

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act.

COMMENTS:

According to section 2(h) of the *Code of Criminal Procedure*, "investigation" includes all the proceedings under this Code for the collection of evidence conducted by a police officer or by any person (other than a Magistrate) who is authorised by a Magistrate in this behalf.

Section 28 of the *Information Technology Act* empowers the following to investigate any contravention of the Act and allied rules and regulations: (1) the Controller (2) any officer authorised by the Controller.

Additionally, section 78 of the *Information Technology Act* empowers a police officer not below the rank of Inspector to investigate offence under the Act. Offences are defined under Chapter XI of the Act.

Additionally, rule 4(i) of the *Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003* authorize the Adjudicating Officer, may get a matter or report investigated from an officer in the Office of Controller or CERT-IND or from the concerned Deputy Superintendent of Police [Inspector], to ascertain more facts and whether *prima facie* there is a case for adjudicating on the matter or not.

Additionally, section 80 of the *Information Technology Act* provides a special power to police officers not below the rank of a Inspector of Police and to other Government officers authorised by the Central Government. Such authorised persons can enter and search any public place. Public places include cyber cafes, hotels, shops etc accessible to the public.

Additionally, they can arrest without warrant any person found in such a public place who is reasonably suspected of:

- (1) having committed an offence under the Act,
- (2) committing an offence under the Act,
- (3) being about to commit any offence under the Act.

The steps most commonly followed in the investigation and trial of a criminal case are outlined as under (Note: CrPC stands for *Code of Criminal Procedure, 1973*):

1. The complainant approaches the local police station to file a complaint.
2. The police listen to the facts disclosed by the complainant. If the facts disclose a non-cognizable offence then the police make an entry in a special register for non-cognizable complaints. This register is regularly submitted to the local magistrate. A non-cognizable case is one in which the police cannot arrest a person without a warrant.
3. If the facts disclose a cognizable offence then an FIR (First Information Report) is lodged. The FIR is numbered, dated and a copy is given to the complainant. A copy is also submitted to the local Court. A cognizable case is one in which the police can arrest a person without a warrant e.g. cyber terrorism is punishable with life imprisonment and is a cognizable offence.
4. The police then begin the investigation. They may visit the scene of the crime, question witnesses and suspects etc.
5. A person being questioned by the police is legally bound to give true answers. Exception: A person is not legally bound to answer a question if the answer can incriminate him. This exception is provided by section 161 of CrPC. The right against self incrimination is vested by the Constitution of India.
6. The police can write down the statements made by the witnesses, suspects etc. The person making the statement is not required to sign it. Note: A person can voluntarily make a statement or confession to a Court.
7. The police cannot threaten a person into making any statement.
8. The police can search any house, office etc and seize evidence. They do not need a search warrant for this.
9. If some evidence is to be collected from abroad, the Court can make an order which is then forwarded by the Central Government to the suitable authority in the relevant countries.
10. The police can arrest and confine a suspect. The freedom of an arrested person is restricted by the police. The police are empowered to use force if a person attempts to evade arrest. An arrested person must be informed about the grounds for his arrest.
11. The police can search the arrested person and recover evidence.
12. The arrested person must be produced before a Court within 24 hours of his arrest. The Court can then do one of the following:
 - (a) release the arrested person on bail,

- (b) send the arrested person into the custody of the police so that the police can carry out their investigation (police custody),
- (c) send the arrested person to jail (judicial / magisterial custody).

It is a common misconception that Courts are closed on weekends and public holidays and a person will have to wait till a Monday to be produced before a Court. There is always at least one criminal court functioning on every holiday and weekend.

13. After completing the investigation, the police are required to submit their report and relevant documents to the Court.

14. After studying the investigation report, the Court can dismiss the complaint if there are insufficient grounds against the accused persons.

15. If there are sufficient grounds to proceed against the accused, the Court can take cognizance of the case and frame charges against the accused.

16. If the accused person pleads guilty to the charges then the court can convict him under the relevant law and impose sufficient imprisonment term and / or fine.

17. If the accused person does not plead guilty to the charges, the trial takes place. The prosecution and the defence argue the case, examine witnesses and place evidence before the court.

18. If scientific reports are provided as evidence, then the Court can call the scientific expert to Court to examine him e.g. the director, deputy director or assistant director of a Central or State Cyber Forensic Laboratory is usually summoned to court in cases involving cyber crime and digital evidence.

19. After hearing the arguments, the Court gives the judgment. If the accused is found guilty then the court can convict him under the relevant law and impose sufficient imprisonment term and / or fine. The convicted person can appeal to a higher court against this judgment.

20. If the accused is found not guilty, then the court can acquit him. The Court can also order the complainant to pay compensation if the case appears to be frivolous.

21. Once a person has been tried by a Court, he cannot be prosecuted again for the same offence or for another offence based on the same facts. It does not matter whether the person was convicted or acquitted.

Cyber Crime Investigation

Cyber Crime Investigation is the collecting, analyzing and investigation of digital evidence and cyber trails.

This digital evidence and cyber trail may be found in computer hard disks, cell phones, CDs, DVDs, floppies, computer networks, the Internet etc.

Digital evidence and cyber trails can be hidden in pictures (steganography), encrypted files, password protected files, deleted files, formatted hard disks, deleted emails, chat transcripts etc.

Given below are some of the cases that cyber crime investigators are called in to solve. All these cases involve recovery and analysis of digital evidence and cyber trails (1) Divorce cases (2) Murder cases (3) Organized crime, Terrorist operations, Extortion (4) Defamation, Pornography (5) Online banking / share trading / credit card fraud (6) Smuggling, Tax evasion, Money laundering (7) Virus attacks, Cyber sabotage, Source code theft (8) Phishing attacks, Email hijacking, Denial of service (9) Counterfeit currency, stamp papers, postage stamps etc

The actual process of the investigation of any computer related crime begins with an external examination of the premises. Normally, for this part of the investigation, the rules and regulations of investigation and forensics related to traditional crimes also apply to some extent.

This part of the investigation basically assists the computer forensics expert in adjudging the strengths and vulnerabilities of the network. It also helps him in deciding the steps to be taken to investigate the crime and also the peculiarities of the incident.

A cyber crime investigator also has to decide whether it is prudent to confiscate computer resources from the suspect's premises or to complete the investigation at the scene.

Confiscating and carrying out the investigation off-site would involve proper packaging and transporting of the computers and accessories, reassembling them at the laboratory and then recreating the network or configuration.

This can be a complex and sensitive issue and hence the cyber crime investigator must decide based on the volume of evidence, technical and infrastructural issues and time available.

Cyber Forensics is a wide term that encompasses computer forensics (gathering evidence from computer media seized at the crime scene) and network forensics (gathering digital evidence that is distributed across networks).

Digital evidence is the foundation of any case involving computers. Searching, examining, collecting, and preserving digital evidence has to be done in such a manner that the court can rely upon the evidence to

deliver its judgment. Any errors in gathering, developing, or presenting digital evidence can adversely affect the trial.

As per the definition provided by the Computer Emergency Response Team of the Asian School of Cyber Laws (ASCL-CERT):

Cyber Forensics is the discovery, analysis, and reconstruction of evidence extracted from and / or contained in a computer, computer system, computer network, computer media or computer peripheral.

Discovery implies recovery of something previously unknown or unrecognized. Analysis is the detailed examination of something made in order to understand its nature or determine its essential characteristics. Reconstruct means to construct again, to rebuild, and to form again or anew. Evidence refers to all documents including electronic records produced for the inspection of the Court. Extract means to take out or derive.

Broadly speaking, Cyber Forensics involves: (1) finding and decrypting password protected information, encrypted information and steganography content (2) tracing the source of e-mail (3) tracking software piracy (4) recovering deleted data (5) matching information to computers that created them (6) remotely monitoring computers and (7) preserving digital evidence for presentation in court.

Some of the basic techniques that are used for cyber crime investigation are: (1) whois search (2) IP tracing from ISP (3) analyzing a web server log (4) analyzing email headers (5) tracking an email account (6) recovering deleted evidence (7) cracking passwords (8) handling encrypted information (9) handling steganography information (10) handling hidden data (11) using keyloggers for investigation.

Section 80. Power of police officer and other officers to enter, search, etc

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 any police officer, not below the rank of a Inspector, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

Explanation.- For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

COMMENTS:

The provisions of Chapter 5 of the *Code of Criminal Procedure* are relevant for arrest of persons. Some of the sections are:

Section 45 - Protection of members of the Armed Forces from arrest

(1) Notwithstanding anything contained in sections 41 to 44 (both inclusive), no member of the Armed Forces of the Union shall be arrested for anything done or purported to be done by him in the discharge of his official duties except after obtaining the consent of the Central Government.

Section 46 - Arrest how made

- (1) In making an arrest the police officer or other person making the same shall actually touch or confine the body of the person to be arrested, unless there be a submission to the custody by word or action.
- (2) If such person forcibly resists the endeavour to arrest him, or attempts to evade the arrest, such police officer or other person may use all means necessary to effect the arrest.
- (3) Nothing in this section gives a right to cause the death of a person who is not accused of an offence punishable with death or with imprisonment for life.
- (4) Save in exceptional circumstances, no women shall be arrested after sunset and before sunrise, and where such exceptional circumstances exist, the woman police officer shall, by making a written report, obtain the prior permission of the Judicial Magistrate of the first class within whose local jurisdiction the offence is committed or the arrest is to be made.

Section 47 - Search of place entered by person sought to be arrested

- (1) If any person acting under a warrant of arrest, or any police officer having authority to arrest, has reason to believe that the person to be arrested has entered into, or is within, any place, any person residing in, or being in charge of, such place shall, on demand of such person acting as aforesaid or such police officer, allow him such free ingress thereto, and afford all reasonable facilities for a search therein.
- (2) If ingress to such place cannot be obtained under sub-section (1), it shall be lawful in any case for a person acting under a warrant and in any case in which a warrant may issue, but cannot be obtained without affording the person to be arrested an opportunity of escape, for a police officer to enter such place and search therein, and in order to effect an entrance into such place, to break open any outer or inner door or window of any house or place, whether that of the person to be arrested or of any other person, if after notification of his authority and purposes, and demand of admittance duly made, he cannot otherwise obtain admittance:

Provided that, if any such place is an apartment in the actual occupancy of a female (not being the person to be arrested) who, according to custom, does not appear in public, such person or

police officer shall, before entering such apartment, give notice to such female that she is at liberty to withdraw and shall afford her every reasonable facility for withdrawing, and may then break open the apartment and enter it.

(3) Any police officer or other person authorised to make an arrest may break open any outer or inner door or window of any house or place in order to liberate himself or any other person who, having lawfully entered for the purpose of making an arrest, is detained therein.

Section 49 - No unnecessary restraint

The person arrested shall not be subjected to more restraint than is necessary to prevent his escape.

Section 50 - Person arrested to be informed of grounds of arrest and of right to bail

(1) Every police officer or other person arresting any person without warrant shall forthwith communicate to him full particulars of the offence for which he is arrested or other grounds for such arrest.

(2) Where a police officer arrests without warrant any person other than a person accused of a non-bailable offence, he shall inform the person arrested that he is entitled to be released on bail and that he may arrange for sureties on his behalf.

Section 51 - Search of arrested persons

(1) Whenever a person is arrested by a police officer under a warrant which does not provide for the taking of bail, or under a warrant which provides for the taking of bail but the person arrested cannot furnish bail, and whenever a person is arrested without warrant, or by a private person under a warrant, and cannot legally be admitted to bail, or is unable to furnish bail.

The officer making the arrests or, when the arrest is made by a private person, the police officer to whom he makes over the person arrested, may search such person, and place in safe custody all articles, other than necessary wearing-apparel, found upon him and where any article is seized from the arrested person, a receipt showing the articles taken in possession by the police officer shall be given to such person.

(2) Whenever it is necessary to cause a female to be searched, the search shall be made by another female with strict regard to decency.

Section 52 - Power to seize offensive weapons

The officer or other person making any arrest under this Code may take from the person arrested any offensive weapons which he has about his person, and shall deliver all weapons so taken to the Court or officer before which or whom the officer or person making the arrest is required by this Code to produce the person arrested.

Section 53 - Examination of accused by medical practitioner at the request of police officer

(1) When a person is arrested on a charge of committing an offence of such a nature and alleged to have been committed under such circumstances that there are reasonable grounds for believing that an examination of his person will afford evidence as to the commission of an offence, it shall be lawful for a registered medical practitioner, acting at the request of a police officer not below the rank of sub-inspector, and for any person acting in good faith in his aid and under his direction, to make such an examination of the person arrested as is reasonable necessary in order to ascertain the facts which may afford such evidence, and to use such force as is reasonably necessary for that purpose.

(2) Whenever the person of a female is to be examined under this section, the examination shall be made only by, or under the supervision of, a female registered medical practitioner.

Explanation.-

In this section and in sections 53A and 54,--

(a) "examination" shall include the examination of blood, blood stains, semen, swabs in case of sexual offences, sputum and sweat, hair samples and finger nail clippings by the use of modern and scientific techniques including DNA profiling and such other tests which the registered medical practitioner thinks necessary in a particular case;

(b) "registered medical practitioner" means a medical practitioner who possess any medical qualification as defined in clause (h) of

section 2 of the Indian Medical Council Act, 1956(102 of 1956) and whose name has been entered in a State Medical Register.]

Section 54 - Examination of arrested person by medical officer

(1) When a person who is arrested, whether on a charge or otherwise, alleges, at the time when he is produced before a Magistrate or at any time during the period of his detention in custody that the examination of his body will afford evidence which will disprove the commission by him of any offence or which will establish the commission by any other person of any offence against his body, the Magistrate shall, if requested by the arrested person so to do direct the examination of the body of such person by a registered medical practitioner unless the Magistrate considers that the request is made for the purpose of vexation or delay or for defeating the ends of justice.

Where an examination is made under sub-section (1), a copy of the report of such examination shall be furnished by the registered medical practitioner to the arrested person or the person nominated by such arrested person.

(2) The medical officer or a registered medical practitioner so examining the arrested person shall prepare the record of such examination, mentioning therein any injuries or marks of violence upon the person arrested, and the approximate time when such injuries or marks may have been inflicted.

(3) Where an examination is made under sub-section (1), a copy of the report of such examination shall be furnished by the medical officer or registered medical practitioner, as the case may be, to the arrested person or the person nominated by such arrested person.

Section 54A - Identification of person arrested

Where a person is arrested on a charge of committing an offence and his identification by any other person or persons is considered necessary for the purpose of investigation of such offence, the Court, having jurisdiction, may on the request of the officer in charge of a police station, direct the person so arrested to subject himself to identification by any person or persons in such manner as the Court may deem fit."

Section 56 - Person arrested to be taken before Magistrate or officer in charge of police station

A police officer making an arrest without warrant shall, without unnecessary delay and subject to the provisions herein contained as to bail, take or send the person arrested before a Magistrate having jurisdiction in the case, or before the officer in charge of a police station.

Section 57 - Person arrested not to be detained more than twenty-four hours

No police officer shall detain in custody a person arrested without warrant for a longer period than under all the circumstances of the case is reasonable, and such period shall not, in the absence of a special order of a Magistrate under section 167, exceed twenty-four hours exclusive of the time necessary for the journey from the place of arrest to the Magistrate's Court.

Section 58 - Police to report apprehensions

Officers in charge of police stations shall report to the District Magistrate, or, if he so directs, to the Sub-divisional Magistrate, the cases of all persons arrested without warrant, within the limits of their respective stations, whether such persons have been admitted to bail or otherwise.

Section 59 - Discharge of person apprehended

No person who has been arrested by a police officer shall be discharged except on his own bond, or on bail, or under the special order of a Magistrate.

Section 60 - Powers, on escape, to pursue and re-take

(1) If a person in lawful custody escapes or is rescued, the person from whose custody he escaped or was rescued may immediately pursue and arrest him in any place in India.

(2) The provisions of section 47 shall apply to arrests under sub-section (1) although the person making any such arrest is not acting under a warrant and is not a police officer having authority to arrest.

Section 94 - Search of place suspected to contain stolen property, forged documents, etc

(1) If a District Magistrate, Sub-divisional Magistrate or Magistrate of the first class, upon information and after such inquiry as he thinks necessary, has reason to believe that any place is used for the deposit or sale of stolen property, or for the deposit, sale or production of any objectionable article to which this section applies, or that any such objectionable article is deposited in any place, he may by warrant authorise any police officer above the rank of a constable--

- (a) to enter, with such assistance as may be required, such place,
- (b) to search the same in the manner specified in the warrant,
- (c) to take possession of any property or article therein found which he reasonably suspects to be stolen property or objectionable article to which this section applies,
- (d) to convey such property or article before a Magistrate, or to guard the same on the spot until the offender is taken before a Magistrate, or otherwise to dispose of it in some place of safety,
- (e) to take into custody and carry before a Magistrate every person found in such place who appears to have been privy to the deposit, sale or production of any such property or article knowing or having reasonable cause to suspect it to be stolen property or, as the case may be, objectionable article to which this section applies.

(2) The objectionable articles to which this section applies are—

- (a) counterfeit coin;
- (b) pieces of metal made in contravention of the Metal Tokens Act, 1889 (1 of 1889), or brought into India in contravention of any notification for the time being in force under section 11 of the Customs Act, 1962 (52 of 1962);
- (c) counterfeit currency note; counterfeit stamps;
- (d) forged documents;
- (e) false seals;
- (f) obscene objects referred to in section 292 of the Indian Penal Code (45 of 1860);
- (g) instruments or materials used for the production of any of the articles mentioned in clauses (a) to (f).

16. Sample documentation

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.
- (4) 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.
- (5) 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.
- (6) The images are authenticated using MD5 and / or SHA1 hash function. 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.
- (7) The **findings** of the analysis and investigation are properly documented and relevant **reports** are submitted to the client.

Request for Service

RFS No.	Date		
Client name and address			
Client's authorised representative			
Name	Email	Phone	Fax
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)			
Case recd on	Case recd by	Referred by	
Tax _____	Financial Cyber	Priority 1 2 3 4 5 6 7 8 9 10	

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: _____ Capacity: _____ Manufacturer: _____ Jumper: _____ Serial no: _____ Interface: _____ Dimensions: _____ LBA Add. Sec.: _____			
8. Unusual marks, if any:			
Chain of Custody			
Date & Time	Released by	Released to	Purpose of change of custody

Computer Evidence Assessment Checklist

Activity	Date
<p>The “request for service” was obtained from the client.</p> <p>Details of the case were obtained from the client.</p> <p>The cyber crime investigator met with the client and discussed the investigative avenues and potential evidence being sought in the investigation.</p> <p>Computers and other devices were received from the client.</p> <p>The evidence was marked and photographed.</p> <p>Chain of custody was properly documented.</p> <p>BIOS information documented.</p> <p>Image files created and mathematically authenticated.</p>	

Computer Evidence Analysis Checklist

Activity	Date
<p>An ASCL computer was prepared with Windows® XP and forensic and investigation software programs.</p> <p>The image files from the evidence devices were copied onto the ASCL computer and examined.</p> <p>Deleted files were recovered.</p> <p>File data was recorded.</p> <p>Keyword text searches were conducted and hits were reviewed.</p> <p>Graphics files were opened and viewed.</p> <p>Data files opened and viewed.</p> <p>Passwords for password protected files were recovered.</p> <p>Encryption keys were recovered.</p> <p>Unallocated and slack space was searched.</p> <p>Relevant files (of evidentiary / investigative value) were copied onto a CD ROM</p>	

Computer Evidence Analysis Report

Case Background

Many employees of the India office of Data64 Ltd, a global software development company, were receiving phone calls from banks for non payment of credit card bills. 225 employees informed the Human Resources (HR) department of Data64 that they had never applied for the credit cards in question.

Kavita Kher, the HR department chief suspected that someone within the company had fraudulently applied for the credit cards in the names of the various employees. The prime suspect was a desktop support engineer Priyanka Chopra.

Priyanka had been allotted a laptop computer by Data64. Additionally, she had recently been gifted an iPod Shuffle ® by the company. Both these were taken into custody by the company and were handed over to the Computer Investigation department of Asian School of Cyber Laws (ASCL) for analysis.

Objective

To determine if the laptop computer and iPod contain any evidence to show that Priyanka was involved in the credit card fraud affecting the employees of Data64.

Evidence device 1: Toshiba ® Laptop Model no – A48756876

Evidence device 2: iPod Shuffle ® 512 MB Model no – M9724ZP/A

The analysis of the laptop computer and iPod resulted in the recovery of 506 files of evidentiary / investigative value. These included:

- (1) 467 scanned images of documents (such as salary slips, driving licences, electricity and telephone bills) pertaining to the employees in whose names credit cards had been fraudulently issued.
- (2) 3 password protected Microsoft ® Excel ® files which contained details of credit card transactions purportedly made by Priyanka Chopra using credit cards issued in the names of various Data 64 Ltd employees.
- (3) 14 email messages exchanged between Priyanka Chopra and Daisy Irani of the HR department of Data64 Ltd.

- (4) 6 PDF files containing airline e-tickets. These tickets had been booked online using some of the credit cards issued in the names of the employees of Data64 Ltd.
- (5) 13 MDI files containing airline e-tickets. These tickets had been booked online using some of the credit cards issued in the names of the employees of Data64 Ltd.
- (6) 3 encrypted files which could not be accessed.

The 506 files mentioned above have been copied onto 3 CD ROMs. One CD ROM has been archived at ASCL. Two CD ROMs have been handed over to the client with the final report.

Cyber Forensic Analysis Report

Report of Cyber Forensic Analysis of hard disk described as under:

Model No.: K5UFHYG

Capacity: 160 GB

Serial no: 45V7GQW34545Q

which contains the image of the IIS server

(Intranet IP address: 10.110.11.179)

Report no.: Zimblia/072006/02 dt. 23rd July, 2006

Introduction

On 10th July 2006, Mr. Prakash Singh of Zimblia Softech Ltd. requested Mr. Rohit of Asian School of Cyber Laws (hereinafter ASCL) to conduct a detailed investigation of the log files (previously retrieved by ASCL) and the image of the computer hard disk of the IIS Server described above.

Mr. Prakash Singh has declared that he is the person legally entitled to hand over the said computer hard disk and the said log files for the said cyber forensic analysis. The said hard disk is owned by Zimblia Softech Ltd., a company registered under the Companies Act, 1956 and having its office at Zimblia Softech Ltd., Park Street, Zimblia. The said company has authorised Mr. Prakash Singh to hand over the said computer hard disk and the said log files to ASCL for the said cyber forensic analysis.

Background of the issue

Note: The information below forming the background of the issue, is as provided by Mr. Prakash Singh. The said information has not been verified or cross checked by ASCL or its employees.

According to Mr. Prakash Singh,

1. The company, Zimblia Softech Ltd., suspects that an unauthorised person had obtained access

into their IIS Server and had altered the database entries.

2. All relevant server logs from the said IIS Server had been deleted.
3. The said IIS Server had been in use for about a week after the suspected incident, before it was isolated.
4. Authorised officials of Zimblia Softech Ltd. suspect that the said unauthorised access and alteration were carried out by Mr. Siddharth R. Sharma.
5. Mr. Sharma is an ex-employee of Zimblia Softech Ltd.
6. Authorised officials of Zimblia Softech Ltd. therefore have requested ASCL to conduct a cyber forensic analysis of the above mentioned IIS Server hard disk to analyse the retrieved log files and any other relevant information obtained from the said hard disk.

Details of the Cyber Forensic Analysis carried out by ASCL

1. The entire cyber forensic analysis was carried out by Mr. R Nagpal of ASCL.
2. The computers and other devices and relevant software used for the cyber forensic analysis are regularly used to store and process information. Throughout the material part of the said cyber forensic analysis, the said hard disk and the said IIS Server were operating properly.
3. The objective of the investigation was to analyze the log files and the entire IIS Server hard disk to detect if any attempts were made to obtain unauthorized access to the said IIS Server.
4. The following IP address has been recovered from the retrieved log file (ex060528): **51.178.152.78.** After analyzing the said IP address and related information recovered from the said log file, it can be concluded that the said

IP address was used to successfully access the said IIS Server (intranet IP address 10.110.11.179) using the method known as SQL Injection.

5. The email address reflected in the said log file is: sidsharma@hotmail.com

After analyzing the said log file it was concluded that the code running on the said IIS Server was manipulated to enable information to be sent out to the said email address. After conducting an intensive analysis of the IIS Server hard-disk, it was found that the said email address belongs to Mr. Siddharth R. Sharma.

6. After a complete and thorough analysis of all the investigative findings, we conclude that unauthorised access was gained to the said IIS Server (intranet IP address 10.110.11.179) on 28th May 2006, between 19.44.47 hours and 21.20.04 hours, from the MTNL public IP address 51.178.152.78, by using SQL Injections.
7. The logs display that the **humanresourcedepartment**, **hr.employeemaster**, **processmaster** and **hr.departmentmaster** fields, among others, of the IIS Server database were accessed. (Please find enclosed a print-out of the said log file.)

2. FIR

First Information Report (FIR) is a **written document** prepared by the police when they receive information about the commission of a cognizable offence. It is a report of information that reaches the police first in point of time and that is why it is called the First Information Report.

A **cognizable offence** is one in which the police may arrest a person without warrant. They are authorised to start investigation into a cognizable case on their own and do not require any orders from the court to do so.

A **non-cognizable offence** is an offence in which a police officer has no authority to arrest without warrant. The police cannot investigate such an offence without the court's permission.

In simple terms, an FIR is a complaint lodged with the police by the victim of a cognizable offence or by someone on his/her behalf.

An FIR is a very important document as it sets the process of criminal justice in motion. It is only after the FIR is registered in the police station that the police takes up investigation of the case. Anyone who knows about the commission of a cognizable offence can file an FIR.

Section 154 of the Code of Criminal Procedure (CrPC) contains the legal provisions in relation to an FIR. According to the section, if information relating to the commission of a cognizable offence is given orally to a police officer, then it is reduced to writing under his direction and then read over to the informant(s).

Such information is required to be signed by the person giving it. A copy of the information is to be given free of cost to the informant.

If the police refuse to record the FIR, the informant can send the information to the relevant Superintendent of Police. The Superintendent has the option of investigating the case himself or directing an investigation to be made by any police officer subordinate to him.

Instead of lodging an FIR, a complainant can directly file a criminal complaint in the court. The court can then order the police to investigate the complaint and based on the police report, the court can try the case. Alternatively, the court can directly begin the case if the court is of the opinion that police investigation is not required.

2.1 Sample FIR

FIRST INFORMATION REPORT (Under Section 154 Cr.P.C.)

1. District: Zimblia **P.S.:** Green Lawns **Year:** 2009 **FIR No.** 1234
Date: 23rd March

2. (i) Act Information Technology Act, 2000 **Sections** 66
(ii) Act _____ **Sections** _____
(iii) Act _____ **Sections** _____
(iv) Other Acts & Sections _____

3. (a) Occurrence of offence:

Date from 23rd March 2009 Date to 23rd March 2009
Time from 1045 hrs Time to 1115 hrs

(b) Information received at P.S.:
Date 23rd March 2009 Time 1245hrs

(c) General Diary Reference: Entry No. 23 Time 1245 hrs

4. Type of Information: Written /Oral

5. Place of Occurrence:

(a) Direction and distance from P.S. _____
Beat No. _____
(b) Address 36th Floor, Centrino Towers, Main Street, Green Lawns Enclave, Zimblia
(c) In case, outside the limit of this Police Station, then
Name of P.S. _____ District _____

6. Complainant / Informant:

(a) Name Pooja Malhotra
(b) Father's/Husband's Name Sameer Malhotra
(c) Date/Year of Birth 6th November, 1972 **(d) Nationality** Indian

(e) Passport No. A12345678 **Date of Issue** 20th October 2001 **Place of Issue** Zimblia

(f) Occupation Director, Centrino Technologies Ltd

(g) Address 36th Floor, Centrino Towers, Main Street, Green Lawns Enclave, Zimblia

7. Details of known/suspected/unknown accused with full particulars:

(Attach separate sheet, if necessary)

(1) _____

(2) _____

(3) _____

8. Reasons for delay in reporting by the complainant / informant

Not applicable

9. Particulars of properties stolen (Attach separate sheet, if necessary)

Not applicable

10. Total value of property stolen Not applicable

11. Inquest Report / U.D. case No., if any

12. First Information contents (Attach separate sheet, if required):

Centrino Technologies Ltd is a company involved in the business of software development, computer training and allied works. The company relies heavily on Internet, computers, computer systems, computer network and electronic information. The company has a dedicated Research & Development facility that develops the source codes and various programmes thereby developing various software. The company is also involved in promoting, trading in and licensing these software.

On 23rd March 2009 at around 1045 hrs the computer network at Centrino crashed and nearly all the information on the computers was effectively destroyed, altered and/or deleted. Due to the disruption so caused, the computers had to be shut down resulting in stoppage of the

business of the company. It is suspected that the company's networks have been deliberately attacked by malicious code sent electronically by unidentified persons.

13. Action taken: Since the above information reveals commission of offence(s) u/s as mentioned at Item No. 2. :

- (1) Registered the case and took up the investigation or
- (2) Directed (Name of I.O.) _____ Rank _____ No. _____ to take up the Investigation or
- (3) Refused investigation due to _____ or
- (4) Transferred to P.S. _____ District _____ on point of jurisdiction.

F.I.R. read over to the complainant / informant, admitted to be correctly recorded and a copy given to the complainant /informant, free of cost.

R.O.A.C.
Police Station

Signature of Officer in charge,

Name Karan Saxena

Rank Asst. Commissioner of
Police No. 12345

14. Signature / Thumb impression of the complainant / informant.

15. Date and time of despatch to the court 23rd March 2009 at 1530 hrs

Physical features, deformities and other details of the suspect/accused: (If known / seen)

Sl. No.	Sex	Date/Year of Birth	Build	Height (cms.)	Complexion	Identification Mark(s)
1	2	3	4	5	6	7

Deformities/ Peculiarities	Teeth	Hair	Eyes	Habit(s)	Dress Habit(s)
8	9	10	11	12	13

LANGUAGE/ DIALECT	PLACE OF				
	Burn Mark	Leucoderma	Mole	Scar	Tattoo
14	15	16	17	18	19

These fields will be entered only if complainant/informant gives any one or more particulars about the suspect/accused.

2.2 Sample criminal complaint

IN THE COURT OF JUDICIAL MAGISTRATE FIRST CLASS
(COURT NO. 4) ZIMBLIA, AT ZIMBLIA

Regular Criminal Complaint No. / 2009

Amit Singh,

S/o Deepak Singh aged about 40 years

Occupation-business Complainant

Residing at 2, Deccan, Zimblia

Vs.

1. Sameer Sen
Chairman and Managing Director,
Hi Tech Ltd,
1, MG Road,
Zimblia

2. Hi Tech Ltd,
A company registered under the a
Companies Act, 1956
and having Regd. Office at,
1, MG Road,
Zimblia

Accused

Complaint u/s 67 of the
Information Technology Act, 2000

The complainant above named submits as follows:

1. That the complainant is a resident of the above mentioned address.
2. That the complainant is a web development consultant and regularly views websites on the Internet for educational and information purposes.
3. That accused number 2 owns, runs, and maintains the website <http://www.porn.com> (details as per annexure I).

4. That the accused number 1 is the Chairman and Managing Director of the accused number 2 (details as per annexure II).
5. That it came to the notice of the complainant that pornographic and obscene photographs are available on the above mentioned website.
6. That on the 27th day of March, 2009, the complainant viewed the above mentioned website, from a computer at his residence, in order to verify whether the above mentioned website disseminates pornographic and obscene materials.
7. On investigation, the complainant found that the website contains obscene and pornographic photographs (as per annexure III). The website states that it is "Dedicated to the beautiful girls of Zimblia".
8. The actions of the accused number 1 and 2 fall under the scope of section 67 of the Information Technology Act, 2000.
9. That the cause of action for this complaint arose on 27th March, 2009 and hence the complaint filed today is well within limitation.
10. That the offence has been committed within the local limits of the jurisdiction of this court and hence this Hon'ble Court has jurisdiction to try and decided this complaint.
11. That the necessary court fees have been paid herewith.
12. That the complainant therefore prays that the accused be charged with and tried for the offences punishable under section 67 of the Information Technology Act, 2000 and punished according to law.

Zimblia

Date: 27th March, 2009

Advocate for the complainant

Complainant

VERIFICATION

I, Amit Singh, S/o Deepak Singh aged about 40 years, Occupation-business, residing at Deccan, Zimblia, the above named complainant swear on solemn affirmation that the information contained in paragraphs 1 to 12 above is true to the best of my knowledge and belief.

Complainant

3. Property Search & Seizure Form

Section 51 of the Code of Criminal Procedure empowers the police to search an arrested person. The police can place in safe custody all articles (other than necessary wearing-apparel), found upon the arrested person. In case any article is seized from the arrested person, a receipt showing the articles taken in possession by the police officer shall be given to such person.

The section stipulates that whenever it is necessary to cause a female to be searched, the search shall be made by another female with strict regard to decency.

Section 102 of the Code of Criminal Procedure empowers the police to seize any property which may be alleged or suspected to have been stolen, or which may be found under circumstances, which create suspicion of the commission of any offence.

Section 165 of the Code of Criminal Procedure empowers a police officer to search any place within his jurisdiction. Such a search is permitted if the police officer has reasonable grounds for believing that something necessary for the purposes of his investigation may be found and must be obtained without undue delay.

Sample Property Search & Seizure Form

PROPERTY SEARCH & SEIZURE FORM

(Search/Production/Recovery u/s 51/102/165 Cr.P.C..... etc.)

1. District: Zimblia **P.S.:** Green Lawns **Year:** 2009 **FIR No.** 1234
Date: 23rd March

2. Act & sections Section 66 of the Information Technology Act, 2000

3. Nature of property seized: Stolen / Unclaimed / Unlawful possession
Involved Intestate.

4. Property seized/ recovered:

- (a) **Date** 24th March 2009
- (b) **Time** 1100 hrs
- (c) **Place** 14 Alex Street, Zimblia
- (d) **Description of the place** Residence of accused no. 1 and 2

5. Person from whom seized /recovered :

Name Siddharth Kapoor **Father's/Husband's name** Prathmesh Kapoor

Sex Male **Age** 21 years **Occupation** Student

Address 14 Alex Street, Zimblia

Professional receiver of stolen property. Yes / No

6. Witnesses:

(i) **Name** Savita Kulkerni

Father's/Husband's name Gokul Kulkerni

Age 43 years **Occupation** IT Professional

Address 123, Sim Lim, Zimblia

(ii) **Name** Abhijeet Narayan

Father's/Husband's name Venkat Narayan

Age 29 years **Occupation** IT Professional

Address 411, Sim Lim, Zimblia

7. Action taken/recommended for disposal of perishable property
Not applicable

8. Action taken/recommended for keeping of valuable property
Deposited with computer storage room at the Zimblia District Court

9. Identification required. Yes/No

10. Details of properties seized/ recovered (Use appropriate prescribed form(s) and attach).

(1) Toshiba ® Laptop Model no – A48756876 having serial number 95535353BF

(2) Toshiba ® Laptop Model no – A48756876 having serial number 95535354BF

(Attach separate sheet, if required)

11. Circumstances/grounds for seizure

The above laptop computers are suspected to have been used to plan and commit offence by the accused in Case no. 1234 registered with the Green Lawns police station.

12. The above mentioned properties were seized in accordance with the provisions of law in the presence of the above said witnesses/* and a copy of the seizure form was given to the person/ the occupant of the place from whom seized.

13. The following properties were packed and/or sealed and the signature of the above said witnesses obtained thereon or on the body of the property.

Sl. No.	Property	Indicate whether signature obtained on the packet or on the body of the property
1	2	3

Signature of the person from whom seized
(if present)

Signature of Investigating officer

Name Karan Saxena

Rank Asst. Comm. of Police No. 12345

Place Zimblia

Date 24th March 2009

Witness-1

Signature

Witness-2

Signature

* In case the property is seized from such a place that no receipt is required to be given to anybody, this portion of the sentence should be struck off.

Details of Counterfeit Currency recovered/seized:

District _____ P.S. _____ Year_____ FIR No. _____
Date _____

Sl. No.	Number of pieces	Series	Serial Number	Type of currency	Denomination	Visible counterfeiting mark(s)
1	2	3	4	5	6	7

Signature of Investigating officer

Name _____

Rank _____ No. _____

Witness-1

Signature

Witness-2

Signature

Details of Narcotic drugs recovered/seized:

District _____ P.S. _____ Year _____ FIR No. _____
Date _____

Sl. No.	Name of drug	No. of packets	Weight (kg./gms.)	Description of the packing and marking, if any	Method of concealment	Estimated value (Rs.)
1	2	3	4	5	6	7

Whether the notice under Section 50 of NDPS Act served on the person? Yes/No

Whether the Laboratory analysis form filled on the spot? Yes/No

Signature of Investigating officer

Name _____

Rank _____ No. _____

Witness-1

Signature

Signature of Magistrate (when present) /
Gazetted Officer

Witness-2

Name _____

Court _____

Signature

4. Final Form / Report

The final form / report discussed here refers to the report of the police officer on completion of investigation. Section 173 of the Code of Criminal Procedure provides the legal provisions relating to this form / report.

This section stipulates that on completion of investigation, the officer in charge of the police station is required to submit to the relevant court a report stating the following:

1. The names of the parties;
2. The nature of the information;
3. The names of the persons who appear to be acquainted with the circumstances of the case;
4. Whether any offence appears to have been committed and, if so, by whom;
5. Whether the accused has been arrested;
6. Whether he has been released on his bond and, if so, whether with or without sureties;
7. Whether he has been forwarded in custody under section 170.

Where there is sufficient evidence for prosecution, the police officer is required to forward to the Magistrate along with the report-

1. All documents on which the prosecution proposes to rely other than those already sent to the Magistrate during investigation;
2. The statements recorded under section 161 of all the persons whom the prosecution proposes to examine as its witness.

The police officer investigating the case may provide copies of the documents referred above to the accused.

Sample Property Final Form / Report

FINAL FORM/ REPORT (Under Section 173 Cr.P.C.)

IN THE COURT OF JUDICIAL MAGISTRATE FIRST CLASS,
ZIMBLIA AT ZIMBLIA

1. District Zimblia P.S. Green Lawns Year 2009 FIR No 1234
Date 23rd March 2009

2. Final Report / Charge Sheet No 1234 **3. Date 23rd April**
2009

4. (i) Act Information Technology Act, 2000 **Sections 66**
(ii) Act _____ **Sections _____**
(iii) Act _____ **Sections _____**
(iv) Other Acts & Sections _____

5. Type of Final Form/Report: Charge Sheet / Not charge sheeted for want of evidence / FR True, Undetected / FR True, Untraced / FR True, offence abated / FR Unoccurred. (tick applicable portion).

6. If FR Unoccurred: False/Mistake of Fact/Mistake of law/Non cognisable /Civil nature. (tick applicable portion).

7. If Charge sheet: Original / Supplementary.
(tick applicable portion).

8. Name of I.O. Karan Saxena Rank Asst. Commissioner of Police
No. 12345 (at the time of charge sheet)

9. (a) Name of complainant / informant Pooja Malhotra
(b) Father's / Husband's name Sameer Malhotra

10. Details of Properties/Articles/Documents recovered/seized during investigation and relied upon (separate list can be attached, if necessary).

Sl. No.	Property description	Estimated value (Rs.)	P.S. Property Register No.	From whom/ where recovered or seized	Disposal
1	2	3	4	5	6

11. Particulars of accused persons charge-sheeted: (Use separate sheet for each accused)

Sl. No. 1

- (i) Name Siddharth Kapoor Whether verified _____
- (ii) Father's/Husband's name Prathmesh Kapoor
- (iii) Date/ Year of birth 10th Jan 1988
- (iv) Sex Male
- (v) Nationality Indian
- (vi) Passport No. B12345678 Date of Issue 14th February 2007
Place of Issue Zimblia
- (vii) Religion Hindu
- (viii) Whether SC/ST/OBC No
- (ix) Occupation Student
- (x) Address 14 Alex Street, Zimblia Whether verified _____
- (xi) Provisional criminal No. 4567
- (xii) Regular criminal No. (if known) _____
- (xiii) Date of arrest 30th March 2009
- (xiv) Date of release on bail 4th April 2009 (xv) Date on which forwarded to court _____
- (xvi) Under Acts & Sections section 66 of the Information Technology Act, 2000

(xvii) Details of bailers / sureties:

Name Prathmesh Kapoor Father's/Husband's name Sankalp Kapoor

Occupation Business Address 14 Alex Street, Zimblia

(xviii) Previous convictions with case references

(xix) Status of the accused:

Forwarded / Bailed by police Bailed by court Judicial custody /

Absconding / Proclaimed offender

(tick applicable portion).

Sl. No. 2

(i) Name Priyanka Kapoor Whether verified _____

(ii) Father's/Husband's name Prathmesh Kapoor

(iii) Date/ Year of birth 16th Jan 1987

(iv) Sex Female

(v) Nationality Indian

(vi) Passport No. B12345679 **Date of Issue** 14th February 2007

Place of Issue Zimblia

(vii) Religion Hindu

(viii) Whether SC/ST/OBC No

(ix) Occupation Student

(x) Address 14 Alex Street, Zimblia Whether verified _____

(xi) Provisional criminal No. 4568

(xii) Regular criminal No. (if known) _____

(xiii) Date of arrest 30th March 2009

(xiv) Date of release on bail 4th April 2009

(xv) Date on which forwarded to court _____

(xvi) Under Acts & Sections section 66 of the Information Technology Act, 2000

(xvii) Details of bailers / sureties:

Name Prathmesh Kapoor Father's/Husband's name Sankalp Kapoor

Occupation Business Address 14 Alex Street, Zimblia

(xviii) Previous convictions with case references

(xix) Status of the accused:

Forwarded / Bailed by police / Bailed by court / Judicial custody /
Absconding / Proclaimed offender
(tick applicable portion).

12. Particulars of accused persons - not charge sheeted (suspect) :
(Use separate sheet for each suspect)

Sl. No. ____

(i) Name _____ Whether verified _____

(ii) Father's/Husband's name _____

(iii) Date/ Year of birth _____

(iv) Sex _____

(v) Nationality _____

(vi) Passport No. _____ **Date of Issue** _____

Place of Issue _____

(vii) Religion _____

(viii) Whether SC/ST/OBC _____

(ix) Occupation _____

(x) Address _____ Whether verified _____

(xi) Provisional criminal No. _____

(xii) Suspicion approved: Yes/No

(xiii) Status of the accused (suspect):

Bailed by police/Bailed by court/ Judicial custody/Not arrested
(tick applicable portion).

(xiv) Under Acts & Sections

(xv) Any special remarks including reasons for not charge sheeting

13. Particulars of witnesses to be examined:

Sl. No.	Name	Father's / Husband's name	Date / Year of birth	Occupation	Address	Type of evidence to be tendered
1	2	3	4	5	6	7
1	Pravin Kale	Sudhir Kale	1971	Manager, Tetra Internet Services Ltd	12, Sun City, Zimblia	Details of IP addresses
2	Sudhir Sen	Shubro Sen	1976	Cyber Crime Investigator	44, Sim Lim, Zimblia	Forensic report of laptop seized from the accused

14. If FR is false, indicate action taken or proposed to be taken u/s 182/211 I.P.C _____

15. Result of Laboratory analysis

16. Brief facts of the case (Add separate sheet, if necessary)

Centrino Technologies Ltd (the complainant) is a company involved in the business of software development, computer training and allied works. The complainant relies heavily on Internet, computers, computer systems, computer network and electronic information. The company has a dedicated Research & Development facility that develops the information source codes and various programmes thereby developing various software. The complainant is also involved in promoting, trading in and licensing these software.

The complainant has invested substantially, both in computer hardware and software to provide standard quality. Furthermore the complainant has to also hire and/or take help of experts for development of various programmes, source codes and software for which the complainant has to bear heavy expenses.

On 23rd March 2009 at around 1045 hrs the computer network at Centrino crashed and nearly all the information on the computers was effectively destroyed, altered and/or deleted. Due to the disruption so caused, the computers had to be shut down resulting in stoppage of the business of the company.

The Complainant lost nearly all files thereby losing the important information present in 15 of its computers. All these 15 computers had the major information including the source codes and programmes of various software, all of which were damaged and / or destroyed. The Complainant lost large amounts of software apart from incurring problems on day-to-day basis. The loss of software and Intellectual Property included the following code lines:

ABC Project = 81000 lines of code.

DEF Project = 159000 lines of code.

The incident also resulted in delay in development of most of the software on account of information loss. Thus the Complainant suffered heavy damages and losses on account of the loss of information, source codes, programmes, registry, delay in software development and damage to computer/s, computer system and computer network and irreparable damage to the software.

The detailed examination of the entire incident revealed that the incident of loss of information, source codes and programmes, damage to computers, computer system and the computer network occurred on account of a virus being introduced in the computer / computer system /computer network.

The detailed forensic examination of the computer network led to the conclusion that the virus that caused the damage was sent to two of the company's email accounts as under.

Date	Sender	Receiver	Attachment
23 rd March 2009	Sameer Sen <s_sen@hitech.com>	a.singh@centrino.com	Imp.doc
23 rd March 2009	Sameer Sen <s_sen@hitech.com>	k.varun@ centrino.com	Vimp.doc

The IP address of the computers from which the emails were sent was ascertained by analyzing the headers of the two emails. A whois search

revealed that the IP addresses were registered in the name of Tetra Internet Services Ltd.

Tetra Internet Services Ltd disclosed that at the relevant time periods, the said IP addresses had been allotted to its customer Siddharth Kapoor. When the residence of Siddharth Kapoor was searched, two laptops were recovered. One of these laptops belonged to Siddharth Kapoor and the other belonged to his sister Priyanka Kapoor. A detailed forensic examination of the laptop computers revealed that the said laptops had been used to create the “belinga” virus and subsequently to email the virus to Centrino.

Siddharth Kapoor and Priyanka Kapoor were subsequently arrested and the Hon’ble Court granted six days police custody. During the custody, the accused confessed to having created the “belinga” virus and subsequently emailing it to Centrino. They had done so on account of a professional rivalry that they had with some of the Directors of Centrino.

17. Refer Notice served: Yes No

Date _____

(Acknowledgement to be placed)

18. Despatched on _____

19. No. of enclosures _____

20. List of enclosures: As annexed

- (1) Printouts of the emails (along with detailed headers) which contained the virus as attachments.
- (2) Details of the IP address provided by Pravin Kale Manager, Tetra Internet Services Ltd.
- (3) Forensic report of laptop seized from the accused provided by Sudhir Sen.
- (4) CD containing source code of the virus as recovered from the laptops seized from the accused.

Forwarded by
Officer in charge

Name Pavan Jain

Rank Deputy Comm. of Police
No. 12345

Signature of Investigating Officer
submitting Final report / Charge sheet

Name Karan Saxena

Rank Asst. Comm. of Police
No. 12345

5. Adjudication Proceedings

The chief responsibility of Adjudicating Officers (AO) under the Information Technology Act is to adjudicate on cases under section 43, 44 and 45 of the IT Act e.g. unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, computer manipulations etc.

The Secretary of Department of Information Technology in each state and Union Territory is the Adjudicating Officer for that state or Union Territory.

Chapter 9 of the IT Act and the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 contain the relevant provisions.

The outline of the procedure is as under:

- (1) The complaint to the AO must be made on plain paper along with the fee payable. The fee is calculated on the basis of damages claimed by way of compensation.
- (2) The AO then issues a notice fixing a date and time for further proceedings to all the necessary parties. On that date, the AO explains the allegations to the respondent.
- (3) If the respondent pleads guilty, the AO can impose suitable penalty.
- (4) Otherwise, based on the complaint, investigation report, submissions, etc the AO can either dismiss the matter or hear the matter.
- (5) The AO can get the matter investigated by an officer in the Office of Controller or CERT-IND or by the concerned Deputy Superintendent of Police [or Inspector].
- (6) The AO can impose penalty after considering the – (a) amount of gain of unfair advantage, wherever quantifiable, made as a result of the default; (b) the amount of loss caused to any person as a result of the default; (c) the repetitive nature of the default.
- (7) The AO must attempt to decide the matter within 6 months and must promote on-line settlement of disputes.
- (8) If the matter involves violation of Chapter 11 of the IT Act, then the AO can transfer the case to a Magistrate.
- (9) When an adjudication is pending before an AO, the same matter cannot be pursued before any court, Tribunal etc.
- (10) If a complaint appears to be frivolous then the AO can fine and penalize the complainant.

(11) Certifying Authorities, the Controller and other officers / agencies established under the Act and other government agencies like CERT-IND are required to promptly assist the AO.

The list of Adjudicating Officers and their contact information can be obtained from: <http://cca.gov.in/adju-offlist.jsp>

Sample Complaint to the Adjudicating Officer

**COMPLAINT TO ADJUDICATING OFFICER
UNDER INFORMATION TECHNOLOGY ACT - 2000**

I

1. Name of the Complainant	Pooja Sharma
2. E-mail address	ps@asianlaws.org
3. Telephone No.	9112345677
4. Address for correspondence	12, Senapati Bapat Road, Pune
5. Digital Signature Certificate, if any	N.A

II

1. Name of the Respondent	Sameer Sen
2. E-mail address	sameer_sen@internomoda.com
3. Telephone No.	917658756
4. Address for correspondence	173/5, Sadashiv Peth, Pune
5. Digital Signature Certificate, if any	N.A

III

Damages claimed:	Rs 500,000
Fee deposited:	Rs 13,000
Demand Draft No.123456 dated 5 th January 2008 drawn on Noodle Bank, Pune	

IV

Complaint under Section/Rule/Direction/Order etc	Section 43 of the IT Act
---	--------------------------

V

Time of Contravention:	5 pm on 1 st January 2008
-------------------------------	--------------------------------------

VI

Place of Contravention:	Pune
--------------------------------	------

VII

Cause of action:	The complainant alleges that the respondent has introduced computer viruses into her computer and thereby damaged computer source code and other important data.
-------------------------	--

VIII

Brief facts of the case:	<p>1. The Complainant is a freelance software programmer.</p> <p>2. The Respondent is also a freelance software programmer.</p> <p>3. On 1st January 2008 at around 5 pm, the complainant received an email from sameer_sen@internomoda.com</p> <p>4. In the past the respondent has sent many emails to the complainant from this email address.</p> <p>5. The said email contained an attachment purporting to be the outline of a new software program that the respondent wanted the complainant to design.</p> <p>6. As soon as the complainant downloaded and executed the attachment, her computer stopped functioning. When she restarted her computer she realized that all data on her computer had been destroyed.</p> <p>7. The loss of software and Intellectual Property included the following code lines:</p> <p>ABC Project = 8100 lines of code.</p>
---------------------------------	---

	<p>DEF Project = 1590 lines of code.</p> <p>8. The Complainant suffered heavy damages and losses on account of the loss of information, source codes, programmes, and damage to computer.</p> <p>9. A detailed examination of the entire incident revealed that the incident of loss of information, source codes and programmes, damage to computer etc occurred on account of a virus being introduced into the computer.</p> <p>10. The Complainant reviewed the computer security in the wake of the above incident and further upgraded the virus detection software. The Complainant also took help of experts to detect the original file that was carrying the virus.</p> <p>11. The Complainant suspected some foul play on the part of the Respondent and wanted to verify and ascertain the same.</p> <p>12. The upgradation of the virus detection software and the observations of the experts led to the detection of the Respondent as the originator/sender of the virus.</p> <p>13. The virus that caused the above mentioned damages and wrongful losses to the Complainant, was sent by the Respondent as an email attachment mentioned in para 5.</p>
--	---

(Signature of the Complainant)

17. Guidelines for Real World Investigations

1. Social networking sites related cases

Social networking sites like Orkut and Facebook are very popular nowadays. Users of such sites can search for and interact with people who share the same hobbies and interests. The profiles of such users are usually publicly viewable.

Scenario 1:

A **fake profile of a woman is created** on a social networking site. 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 “loose character” who wants to have sexual relations with anyone. Other 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.

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

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 67 of the <i>Information Technology Act</i> and section 509 of <i>Indian Penal Code</i>	Sections 66A and 67 of the <i>Information Technology Act</i> and section 509 of <i>Indian Penal Code</i>

Scenario 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.

Usual motives: Desire to cause racial hatred and communal discord and disharmony.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 153A & 153B of <i>Indian Penal Code</i>	Section 66A of the <i>Information Technology Act</i> and sections 153A & 153B of <i>Indian Penal Code</i>

Scenario 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).

Usual motives: Hatred (e.g. a school student who has failed may victimize his teachers).

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 500 of <i>Indian Penal Code</i>	Section 66A of the <i>Information Technology Act</i> and section 500 of <i>Indian Penal Code</i>

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 website officials is required to obtain the IP addresses used to create and update the offensive profile,

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.

Scenario 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.

Usual motives: Corporate espionage or a perverse pleasure in being able to destroy valuable information belonging to strangers etc.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the <i>Information Technology Act</i>	Sections 43, 66, 66A and 66C of <i>the Information Technology Act</i>

Scenario 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.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the <i>Information Technology Act</i>	Sections 43, 66, 66A & 66C of the <i>Information Technology Act</i>

Scenario 3:

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

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43, 66 and 67 of the <i>Information Technology Act</i>	Section 43, 66, 66A and 67 of the <i>Information Technology Act</i> Additionally, depending upon the content, sections 66C and 67B of the <i>Information Technology Act</i> may also apply

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

In credit card fraud cases, the victim's credit card information is stolen and misused for making online purchases (e.g. airline tickets, software, subscription to pornographic websites etc).

Modus Operandi 1: The suspect would install keyloggers in public computers (such as cyber cafes, airport lounges etc) or the computer 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.

Modus Operandi 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.

Usual motives: Illegal financial gain

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the <i>Information Technology Act</i> and section 420 of <i>Indian Penal Code</i>	Sections 43, 66, 66C, 66D of the <i>Information Technology Act</i> and section 420 of <i>Indian Penal Code</i>

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. This has led to a large number of online share trading frauds.

Scenario 1:

The victim's account passwords are stolen and his accounts are misused for making fraudulent bank transfers.

Usual motives: Illegal financial gain

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the <i>Information Technology Act</i> and section 420 of <i>Indian Penal Code</i>	Sections 43, 66, 66C & 66D of the <i>Information Technology Act</i> and section 420 of <i>Indian Penal Code</i>

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.

Usual motives: Revenge, jealousy, hatred.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the <i>Information Technology Act</i> and section 426 of <i>Indian Penal Code</i>	Sections 43, 66, 66C & 66D of the <i>Information Technology Act</i> and section 426 of <i>Indian Penal Code</i>

Modus Operandi:

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

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.

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.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
<i>Information Technology Act</i> usually does not apply. Applicable laws are usually the <i>Income Tax Act</i> and the <i>Prevention of Money Laundering Act</i> .	<i>Information Technology Act</i> usually does not apply. Applicable laws are usually the <i>Income Tax Act</i> and the <i>Prevention of Money Laundering Act</i> .

Scenario 2:

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

Applicable law

Before 27 October, 2009	After 27 October, 2009
<i>Information Technology Act</i> usually does not apply. Applicable laws are usually the <i>Income Tax Act</i> and the <i>Prevention of Money Laundering Act</i> .	<i>Information Technology Act</i> usually does not apply. Applicable laws are usually the <i>Income Tax Act</i> and the <i>Prevention of Money Laundering Act</i> .

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 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 organizations that get original software developed for their use.

Scenario 1:

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

Modus Operandi: 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.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43, 65 & 66 of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>	Sections 43, 65, 66 & 66B of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>

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.

Modus Operandi: 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.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43, 65 & 66 of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>	Sections 43, 65, 66 & 66B of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>

Investigation Guidelines:

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.

7. Theft of Confidential Information

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

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).

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 & 66 of the <i>Information Technology Act</i> and section 426 of <i>Indian Penal Code</i>	Sections 43, 66 & 66B of the <i>Information Technology Act</i> and section 426 of <i>Indian Penal Code</i>

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.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 & 66 of the <i>Information Technology Act</i> and section 384 of <i>Indian Penal Code</i>	Sections 43, 66 & 66B of the <i>Information Technology Act</i> and section 384 of <i>Indian Penal Code</i>

Scenario 3:

A disgruntled employee steals the information and mass mails it to the victim's rivals and also posts it to numerous websites and newsgroups.

Usual motives: Revenge.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the <i>Information Technology Act</i> and section 426 of <i>Indian Penal Code</i>	Sections 43, 66, 66B of the <i>Information Technology Act</i> and section 426 of <i>Indian Penal Code</i>

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.

Scenario 1:

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

Modus Operandi: 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.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 43 & 66 of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>	Section 43 & 66 of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>

Scenario 2:

The software pirate sells the pirated software through electronic downloads through websites, bulletin boards, newsgroups, spam etc.

Modus Operandi: 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.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 43 & 66 of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>	Section 43 & 66 of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>

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 that music is not “property”. There is a huge business in music piracy. Thousands of unscrupulous businessmen sell pirated music at throw away prices.

Scenario 1:

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

Modus Operandi: 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.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 43 & 66 of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>	Section 43 & 66 of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>

Scenario 2:

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

Modus Operandi: 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.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 43 & 66 of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>	Section 43 & 66 of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>

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 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.

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.

Usual motive: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 420 of <i>Indian Penal Code</i>	Sections 66A and 66D of the <i>Information Technology Act</i> and section 420 of <i>Indian Penal Code</i>

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.

Scenario:

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.

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 The suspect can target Noodle customers using a domain name like 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.

Usual motive: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 43 & 66 of the <i>Information Technology Act</i> and sections 419, 420 & 468 of <i>Indian Penal Code</i>	Sections 66, 66A & 66D of the <i>Information Technology Act</i> and sections 419, 420 & 468 of <i>Indian Penal Code</i>

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 be 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).

Scenario:

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

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.

Usual motive: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 67 of the <i>Information Technology Act</i>	Section 67 of the <i>Information Technology Act</i> and depending upon the content, sections 67A and 67B may also apply

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 sale of narcotic 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.

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 only 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 modes of communication for gathering people for the illegal “drug” party.

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.

Usual motive: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
<i>Information Technology Act</i> usually does not apply. Depending upon the illegal items being transacted in, the following may apply: <i>Narcotic Drugs and Psychotropic Substances Act, Arms Act, Indian Penal Code, Wildlife related laws etc</i>	<i>Information Technology Act</i> usually does not apply. Depending upon the illegal items being transacted in, the following may apply: <i>Narcotic Drugs and Psychotropic Substances Act, Arms Act, Indian Penal Code, Wildlife related laws etc</i>

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.

Scenario:

The suspects carry laptops wherein information relating to their activities is 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 almost impossible.

Terrorists 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.

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.

Usual motives: Keeping terrorism related information confidential, securing communication amongst terrorist group members.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Apart from conventional terrorism laws, section 69 of the <i>Information Technology Act</i> may apply	Apart from conventional terrorism laws, section 69 of the <i>Information Technology Act</i> may apply

Investigation Guidelines:

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.

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 organization.

Modus Operandi: A 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.

Usual motives: Thrill and a perverse pleasure in destroying data belonging to strangers.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 & 66 of the <i>Information Technology Act</i> and section 426 of <i>Indian Penal Code</i>	Sections 43, 66 & 66A of the <i>Information Technology Act</i> and section 426 of <i>Indian Penal Code</i>

Scenario 2:

The virus targets a particular organization. This type of a virus is not known to anti-virus companies as it is a new virus created specifically to target a particular organization.

Modus Operandi: A 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 go undetected by the victim company’s anti-virus software and hence would be able to cause a lot of damage. Anti-virus companies may never get to know about the existence of the virus.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 & 66 of the <i>Information Technology Act</i> and section 426 of <i>Indian Penal Code</i>	Sections 43, 66 & 66A of the <i>Information Technology Act</i> and section 426 of <i>Indian Penal Code</i>

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.

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. the Independence day of the country).

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.

Usual motives: Thrill or a perverse pleasure in inciting communal disharmony.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 & 66 of the <i>Information Technology Act</i> and in some cases sections 67 and 70 may also apply	Sections 43 & 66 of the <i>Information Technology Act</i> and in some cases sections 66F, 67 and 70 may also apply

Investigation Guidelines:

The first step is to analyze 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).

18. Annexures

1. Case study on footprinting

This case study features a website that is conducting the Mega Model Hunt competition. This website allows registered users to upload their photos onto the website for secure storage.

Your mission is to:

- (1) Manipulate the voting system. Officially, the voting system allows each registered user to vote once only.
- (2) Download the photos that Natalya Fyodorovna Simonova has uploaded to this website.
- (3) Ascertain more information about the website.

The website is located at:

<http://www.data64.org/commonfiles/cases/footprinting/>

2. Solution to Case study on footprinting

Objective

- (1) To manipulate the voting system and cast multiple votes for one or more of the finalists.
- (2) Download the photos that one of the registered models - Natalya Fyodorovna Simonova has uploaded to this website.
- (3) Ascertain more information about the website.

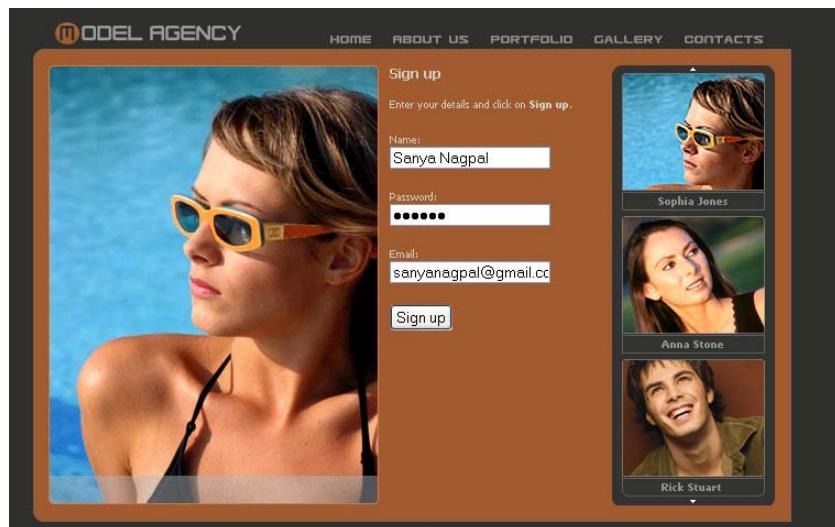
Step-by-step solution

- (1) The first step is to visit:

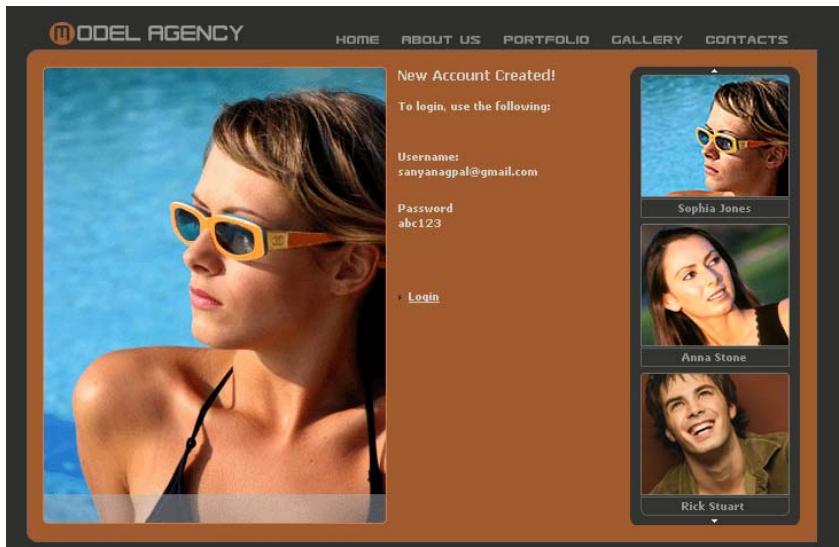
<http://www.data64.org/commonfiles/cases/footprinting/index.php>
and click on **Sign up**.

- (2) <http://www.data64.org/commonfiles/cases/footprinting/signup.php>
page opens up.

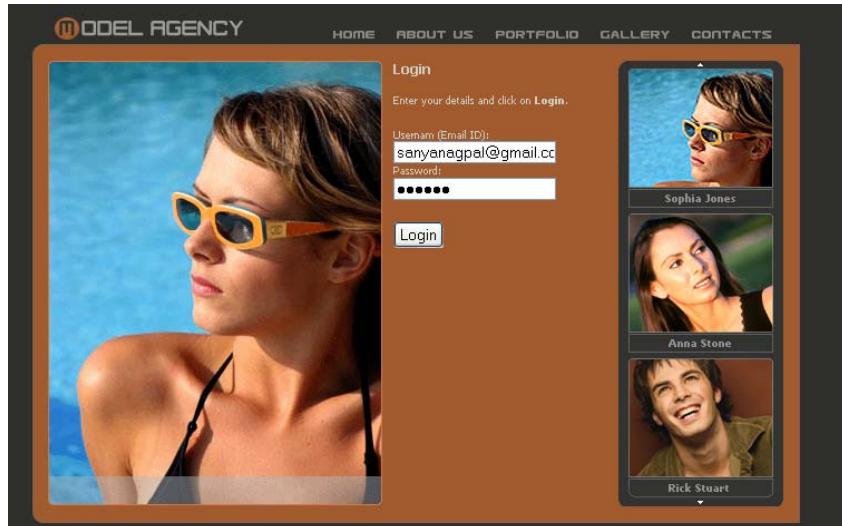
- (3) We enter a name, password and email address and click on **Signup**.
This is illustrated below:



- (4) <http://www.data64.org/commonfiles/cases/footprinting/signup1.php>
opens up and displays the following information.



(5) We then click on the **Login** link at the bottom of this page. The <http://www.data64.org/commonfiles/cases/footprinting/login.php> page opens up. We enter the email id and password for the account just created by us and click on **Login**, as illustrated below:

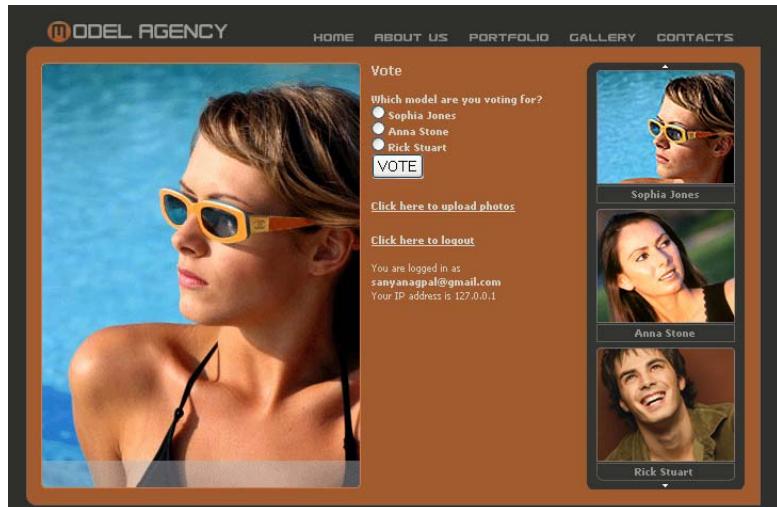


(6) <http://www.data64.org/commonfiles/cases/footprinting/login1.php> page opens up, which is illustrated below:

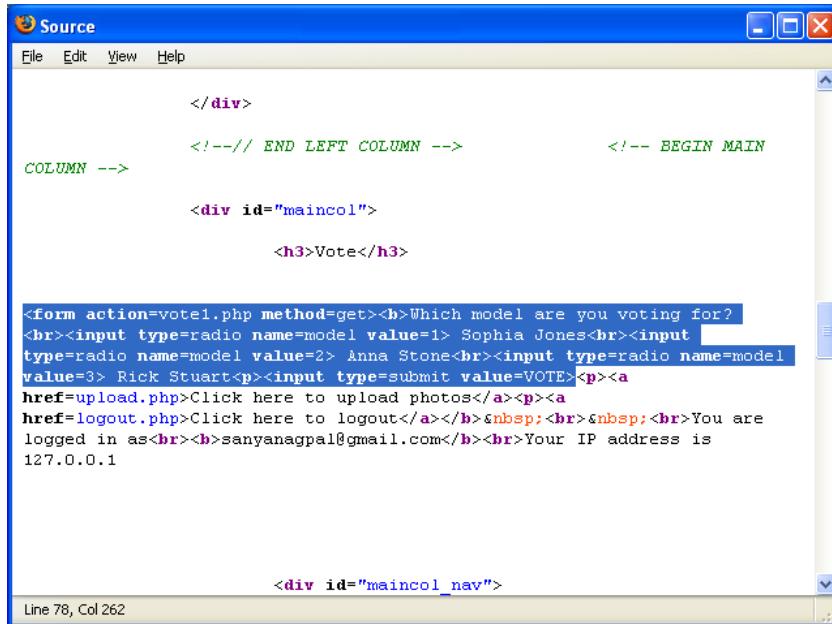


This page gives us the following options: (a) Vote (b) Upload photos and (c) Logout

(7) Click on **Vote**. The following page opens up:
<http://www.data64.org/commonfiles/cases/footprinting/vote.php>



(8) This page contains a form with radio buttons and options to vote for a model. We view the source of this page (In Firefox click on View → Page Source and in Internet Explorer click on View → Source). The source is displayed below:



The screenshot shows a Windows Notepad window titled "Source". The content of the window is the source code for a PHP voting script. The code includes HTML structure, PHP logic, and user input fields. A blue selection bar highlights the "value=1" attribute of the first radio button, which corresponds to the name "Sophia Jones". The code also includes links for file uploads and logouts, and displays the user's IP address.

```
</div>
<!--// END LEFT COLUMN -->           <!-- BEGIN MAIN
COLUMN -->

<div id="maincol">
    <h3>Vote</h3>

    <form action="vote1.php" method="get"><b>Which model are you voting for?</b>
        <br><input type="radio" name="model" value="1" /> Sophia Jones<br><input type="radio" name="model" value="2" /> Anna Stone<br><input type="radio" name="model" value="3" /> Rick Stuart<p><input type="submit" value="VOTE"><p><a href="upload.php">Click here to upload photos</a><p><a href="logout.php">Click here to logout</a><b>&ampnbsp&ampnbsp&nbsp;</b><br>You are
logged in as<br><b>sanyanagpal@gmail.com</b><br>Your IP address is
127.0.0.1

<div id="maincol_nav">

```

(9) As we can see, the form submits the model's code number (**1** for *Sophia Jones*, **2** for *Anna Stone* and **3** for *Rick Stuart*) to the `vote1.php` page using the **GET** method.

(10) To cast our vote, we select *Sophia Jones* and click on **VOTE** in the <http://www.data64.org/commonfiles/cases/footprinting/vote.php> page.

(11) The following page opens up:

<http://www.data64.org/commonfiles/cases/footprinting/vote1.php?model=1>

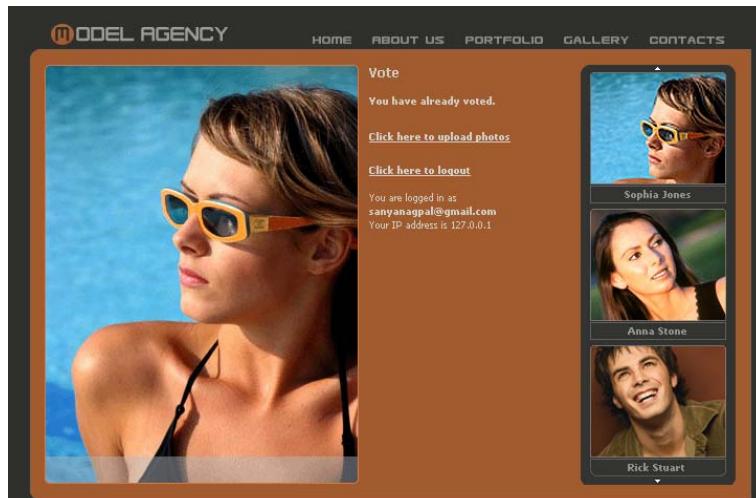
(12) The **?model=1** at the end of the url above denotes that the vote has been cast for *Sophia Jones*. In case we had voted for *Anna Stone*, the URL would have ended with **?model=2** and in case we had voted for *Rick Stuart*, the URL would have ended with **?model=3**

- (13) www.data64.org/commonfiles/cases/footprinting/vote1.php?model=1
page is illustrated below:



- (14) This page shows us the numbers of votes that the models have received so far. We click on the photographs of any one of the models on the right, to try to vote again.

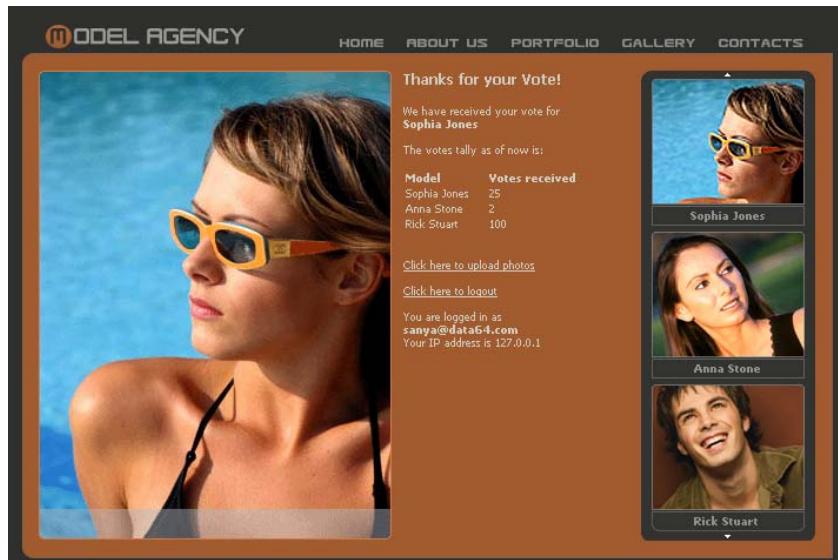
- (15) <http://www.data64.org/commonfiles/cases/footprinting/vote.php>
opens up and displays “**You have already voted**”, as illustrated below:



(16) We then type in the following URL in the address bar of our browser:

<http://www.data64.org/commonfiles/cases/footprinting/vote1.php?model=1>

(17) The following page opens up:



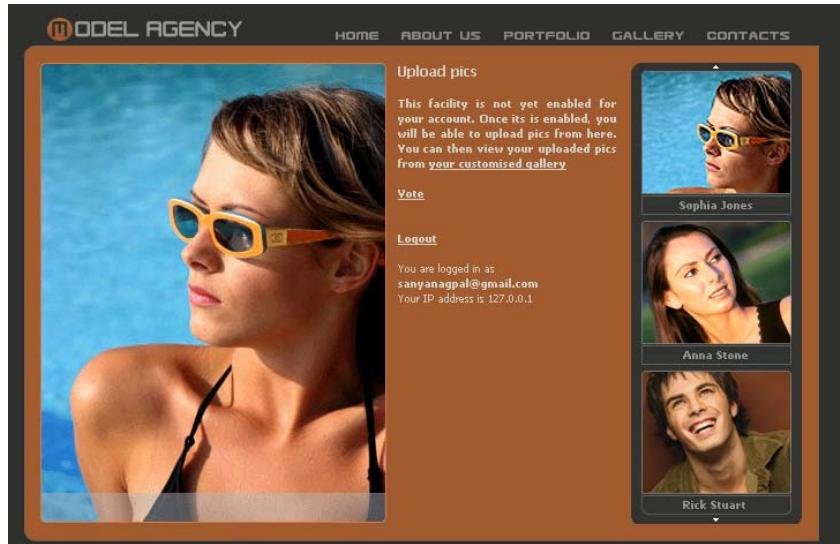
(18) As we can see, we have been able to manipulate the system and cast another vote for Sophia Jones.

(19) There is a defect in the programming logic of the website. The vote.php page checks whether the logged in user has voted or not. If yes, it displays "**You have already voted**". If no, it open up the form to select the model and vote. But the vote1.php does not do any such validation. It simply reads the URL and gets the model code number. It then updates the site database to increase the model's vote count.

(20) We have succeeded in manipulating the voting system and have completed the first objective of the case study. Now we need to find the photos uploaded by Natalia.

(21) We go to the
<http://www.data64.org/commonfiles/cases/footprinting/vote.php> page
and click on the "**Click here to upload photos**" link.

(22) <http://www.data64.org/commonfiles/cases/footprinting/upload.php> opens up. This is illustrated below:



(23) We click on the “**your customised gallery**” link and are taken to the following page:

<http://www.data64.org/commonfiles/cases/model/lapgaNaynaS11>

(24) Looking at this link, we can conclude that for every registered user, a folder is created on the website so that the user can upload photos to that folder. In our case, the folder is called “**lapgaNaynaS11**”.

(25) To get a better idea of the naming convention being used to create these folders, we create a few more accounts on the website with different names. The details of the various users and their folder names are as under:

Name	Email id	Password	Folder name
Sanya Nagpal	sanyanagpal@gmail.com	xyz888	lapgaNaynaS11
abc	sanya@data64.com	Pqr999	cba3
Apple	sn@data64.com	ttuuu	elppA5

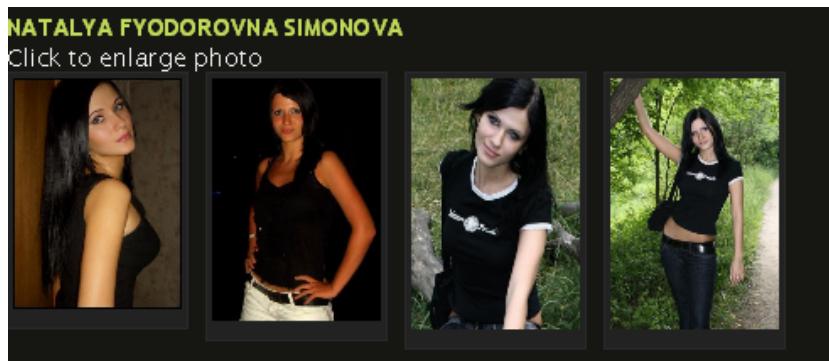
(26) We can conclude that the folder is generated by reversing the name of the user and then appending a number to the end. This number signifies the number of characters in the name of the user.

(27) Using this algorithm, we can that the folder name for Natalya Fyodorovna Simonova will be **avonomiSanvorodoyFaylataN25**

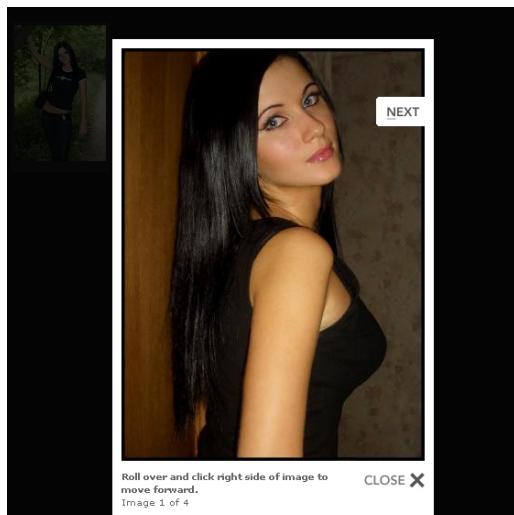
(28) We now enter the following URL in our browser:

<http://www.data64.org/commonfiles/cases/model/avonomiSanvorodoyFaylataN25>

(29) The following page opens up: .



(30) Clicking on one of the photos, enlarges it as illustrated below:



(31) We have now succeeded in the second objective of the case study.

(32) For ascertaining more information about the website we conduct a whois search for data64.org using the Data64 IP / DNS tools located at <http://www.data64.info/tool.php>

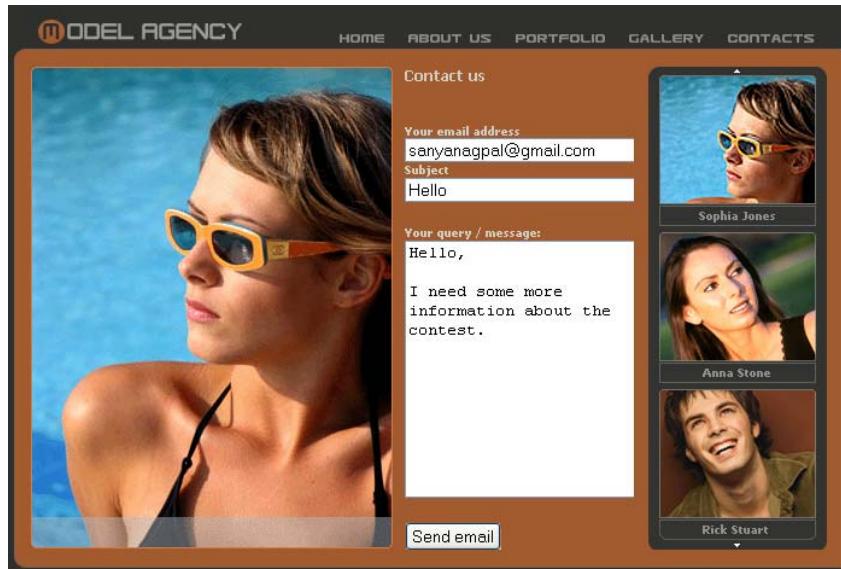
Host Information		Host Connectivity	
<input type="checkbox"/> Resolve Host / Reverse Lookup		<input type="checkbox"/> Ping - count: 4	
<input type="checkbox"/> Get Country [?]		<input type="checkbox"/> Traceroute	
<input type="checkbox"/> Whois (IP) <input type="text" value="whois.arin.net"/> [?]		<input type="checkbox"/> Tracepath [?]	
<input checked="" type="checkbox"/> Whois (Domain) <input type="text" value="whois-servers.net"/> [?]			
<input type="checkbox"/> NS Lookup			
<input type="checkbox"/> Dig ANY <input type="button" value="▼"/> [?]			
Host: <input type="text" value="data64.org"/>		<input type="button" value="Get Info"/>	

(33) We also use the netcraft add-on for Firefox to ascertain that the website is running on a server with Linux operating system and the web server is Apache/2.2.11 (Unix) PHP/4.4.9 mod_ssl/2.2.11 OpenSSL/0.9.8c mod_fastcgi/2.4.6

The screenshot shows a Firefox browser window with the following details:

- Page Content:** A website for a "Mega Model Hunt" competition. It features three models: Sophia Jones (wearing sunglasses), Anna Stone (smiling), and Rick Stuart (smiling). A sidebar on the left contains text about the competition and voting instructions.
- Netcraft Add-on:** An open menu in the bottom right corner displays the following information:
 - Host: www.data64.org
 - Copy to Clipboard
 - netcraft (selected)
 - whois.sc
 - full site report
 - robtex.com - Host
 - ip2country.cc
 - whoishostingthis.com
- Firefox Status Bar:** Shows the IP address 75.119.212.143 and the time 1:42 PM.

(34) To ascertain more about the email system in use, we visit:
<http://www.data64.org/commonfiles/cases/footprinting/contacts.php>
page and send a message as illustrated below:



The screenshot shows a contact form on a website titled "MODEL AGENCY". The form includes fields for "Your email address" (sanyanagpal@gmail.com), "Subject" (Hello), and "Your query / message" (Hello, I need some more information about the contest.). To the right, there is a sidebar displaying three model profiles: Sophia Jones (a woman in sunglasses), Anna Stone (a woman in a black top), and Rick Stuart (a man smiling). A "Send email" button is located at the bottom left of the form area.

(35) The automated response that we get shows that the actual email address used by the site is models.data64@gmail.com

3. International case studies

3.1 Man charged for targeting fiancé's bank account

John Bradley Egan, a 42 year old US citizen was indicted on charges of bank fraud, computer fraud, and aggravated identity theft in connection with an alleged scheme to obtain money from his fiancé's bank account. [Note: An indictment contains allegations that a defendant has committed a crime. Every defendant is presumed innocent until and unless proven guilty beyond a reasonable doubt.]

According to the indictment, Egan and his fiancé, "L.C." started dating sometime in 2005 and became engaged to be married. Throughout the relationship, L.C. and Egan lived in separate residences. L.C. owned a condominium in North Salt Lake City, which was in her name alone, and Egan lived in Bountiful. Eventually, Egan allegedly convinced L.C. to sell her condominium and move to Tampa, Fla., where they would get married and live.

Egan also convinced L.C. to use some of the proceeds of the sale of her condominium for a down payment on a house for which he would pay the mortgage. L.C.'s condominium was sold in June 2006 and she received a check for more than \$113,000 for the net proceeds. L.C. deposited the check into an account held in her name at America First Credit Union on June 5, 2006, according to the indictment. She also deposited \$900 from the sale of furniture and other belongings into an account she shared with Egan. After making the deposits, L.C. and her daughter flew to Tampa. Egan said he would drive to Florida with his son on June 8, 2006 to meet them.

The indictment alleges the pair spoke by telephone on June 6 and 7, 2006. On June 8, 2006, Egan told L.C. that he was in a hotel with his son and would be leaving for Florida in the morning. On June 9, 2006, L.C. attempted to return a call from Egan but was unable to reach him. She never heard from him again.

According to the indictment, six bank transfers totaling \$59,400 were made on the credit union's online banking website using L.C.'s account and her personal identification number on June 9, 2006. The money was transferred from her personal account into the account she shared with Egan. The indictment alleges L.C. did not make or authorize anyone else to make the transfers nor did she authorize anyone else to use her PIN to access her account.

On the same day, six transfers totalling \$50,500 were made from L.C.’s personal account to an account Egan shared with his mother. Again, the transfers were not authorized by L.C.

Shortly after the money was transferred, Egan arrived at the credit union in Centerville, Utah, and withdrew \$60,372 in cash from the account he and L.C. shared. He then went to a branch of the credit union in downtown Salt Lake City and withdrew \$50,000 in cash from the account he shared with his mother.

The credit union has reimbursed L.C. for the \$109,000 in fraudulent withdrawals, but has not recovered the money from Egan.

According to a complaint filed in the case, Egan’s mother discovered on June 21, 2006, that her and her husband’s passports were missing from a safe in their home. She later discovered social security cards were missing as well. There was probable cause to believe Egan had traveled to Mexico. He was later intercepted by Cuban authorities when a boat he was sailing from Mexico had mechanical trouble. Cuban authorities determined he was traveling on a false passport and took him into custody. The State Department facilitated his return from Cuba to Florida.

The potential maximum penalty for bank fraud is 30 years in prison and a \$1 million fine. Computer fraud carries a potential penalty of up to five years in prison and a fine of \$250,000. The minimum penalty for aggravated identity theft is two years in prison. The indictment also seeks forfeiture of the boat Egan was discovered on and \$109,900.

Source: Computer Crime & Intellectual Property Section, United States Department of Justice.

3.2 Trojans used for infecting thousands of computers for fraud

A 19-year-old Wyoming, USA based man was charged with using modified peer-to-peer software to infect computers and create “botnets” – armies of compromised computers numbering from 5,000 to 15,000 machines – that he exploited to obtain credit card and banking information.

Jason Michael Milmont agreed to plead guilty to a federal felony charge of unauthorized access to a computer to further a fraud. The case against Milmont relates to his development of the Nugache Worm, which he developed to infect computers running the Windows operating system and is the first time a person has been prosecuted for using peer-to-peer software as a delivery mechanism for malicious computer code.

Milmont modified Limewire peer-to-peer software to work as “trojan” software that carried a hidden payload and then posted his modified version of Limewire on the Internet for victims to download.

Milmont also used instant messaging spam to surreptitiously download infected files to victims’ computers. After victims downloaded the software, Milmont gained control of their computers, allowing him to obtain credit card and banking information from the compromised computers. He also used the compromised computers to carry out an Internet attack on an online business in Southern California, USA. Because the users of those compromised computers were unaware that their computers had been turned into “zombies,” they continued to use their computers to engage in online banking and purchases.

Once he pleads guilty to the charge, Milmont will face a statutory maximum sentence of five years in federal prison and a fine of \$250,000. Milmont has agreed to pay restitution in the amount of \$73,866.

Source: Computer Crime & Intellectual Property Section, United States Department of Justice.

3.3 Russian computer hackers sentenced to 3 years in prison

Vasiliy Gorshkov, a 27-year-old Russian was sentenced to serve 36 months in prison for his convictions at trial on 20 counts of conspiracy, various computer crimes, and fraud committed against Speakeasy Network of Seattle, Washington; Nara Bank of Los Angeles, California; Central National Bank of Waco, Texas; and the online credit card payment company PayPal of Palo Alto, California.

Gorshkov also was ordered to pay restitution of nearly \$700,000 for the losses he caused to Speakeasy and PayPal.

According to evidence presented at trial and other court records: Gorshkov was one of two men from Chelyabinsk, Russia, who were persuaded to travel to the United States as part of an FBI undercover operation. The operation arose out of a nationwide FBI investigation into Russian computer intrusions that were directed at Internet Service Providers, e-commerce sites, and online banks in the United States.

The hackers used their unauthorized access to the victims’ computers to steal credit card information and other personal financial information, and then often tried to extort money from the victims with threats to expose the sensitive data to the public or damage the victims’ computers. The hackers also defrauded PayPal through a scheme in which stolen credit cards were used to generate cash and to pay for computer parts purchased from vendors in the United States.

The FBI's undercover operation was established to entice persons responsible for these crimes to come to U.S. territory. As part of the operation, the FBI created a start-up computer security company named "Invita" in Seattle, Washington. Posing as Invita personnel, the FBI communicated with Gorshkov and the other man, Alexey Ivanov, by e-mail and telephone during the summer and fall of 2000. The men agreed to a face-to-face meeting in Seattle. As a prelude to their trip to the United States, the FBI arranged a computer network for the two men to hack into and demonstrate their hacking skills. The men successfully broke into the test network.

Gorshkov and Ivanov arrived in Seattle, Washington, on November 10, 2000, and a meeting was held at the office of Invita. Unbeknownst to the Russian men, the participants in the meeting were undercover FBI agents and the meeting was recorded on audio and video tape. During the meeting, Gorshkov discussed their hacking prowess and took responsibility for various hacking incidents and activities. Gorshkov shrugged off any concern about the FBI, explaining that the FBI could not get them in Russia. When asked about their access to credit cards, Gorshkov declined to talk about it while they were in the United States and added that "this kind of question is better discussed in Russia."

A few days after the two men were arrested, the FBI obtained access via the Internet to two of the men's computers in Russia. The FBI copied voluminous data from the accounts of Gorshkov and Ivanov and examined the data pursuant to a search warrant issued by a United States Magistrate Judge. Gorshkov's pretrial challenge to the FBI's copying and search of the Russian data was denied by the Judge.

The data copied from the Russian computers provided a wealth of evidence of the men's computer hacking and fraud. They had large databases of credit card information that was stolen from Internet Service Providers like Lightrealm of Kirkland, Washington. More than 50,000 credit cards were found on the two Russian computers. The Russian computers also contained stolen bank account and other personal financial information of customers of online banking at Nara Bank and Central National Bank - Waco.

The data from the Russian computers revealed that the conspirators had gained unauthorized control over numerous computers - including computers of a school district in St. Clair County, Michigan - and then used those compromised computers to commit a massive fraud involving PayPal and the online auction company e-Bay.

The fraud scheme consisted of using computer programs to establish thousands of anonymous e-mail accounts at e-mail web sites like

Hotmail, Yahoo!, and MyOwnEmail. Gorshkov's programs then created associated accounts at PayPal with random identities and stolen credit cards. Additional computer programs allowed the conspirators to control and manipulate e-Bay auctions so that they could act as both seller and winning bidder in the same auction and then effectively pay themselves with stolen credit cards.

Source: Computer Crime & Intellectual Property Section, United States Department of Justice.

3.4 Indian hackers indicted for online brokerage intrusion scheme

Three Indians were indicted on charges of conspiracy, fraud and aggravated identity theft stemming from a high-tech, international fraud scheme designed to hijack online brokerage accounts for profit. [Note: An indictment contains allegations that a defendant has committed a crime. Every defendant is presumed innocent until and unless proven guilty beyond a reasonable doubt.]

The indictment charges Jaisankar Marimuthu, 32, a resident of Chennai, India, and Chockalingam Ramanathan, 33, a resident of Chennai, India, each with one count of conspiracy, eight counts of computer fraud, six counts of wire fraud, two counts of securities fraud, and six counts of aggravated identity theft as part of this "hack, pump and dump" scheme. The indictment also charges Thirugnanam Ramanathan, 34, a native of India and resident of Malaysia, with one count of conspiracy, two counts of computer fraud, and two counts of aggravated identity theft.

As part of this ongoing investigation, at least 60 customers and nine brokerage firms in the United States and elsewhere have been identified as victims, with one of the brokerage firms reporting more than \$2 million in losses. This case marks the first time that individuals have been arrested overseas in connection with an online brokerage intrusion scheme perpetrated in the United States. In a related action, the SEC filed a civil complaint against all three defendants in federal court in Nebraska today.

According to the indictment, between July and November 2006, the defendants, operating primarily from Thailand and India, used their personal online brokerage accounts to purchase shares of several thinly-traded stocks. They then hacked into online brokerage accounts of others using stolen usernames and passwords or established new brokerage accounts using stolen identities. Using these accounts, the defendants made scores of unauthorized purchases of the same stocks to drive up the market price. Once the share prices were artificially inflated, the defendants sold their own shares for a substantial profit.

In one of many examples alleged in the indictment, Marimuthu placed orders on Aug. 28, 2006, through his personal online brokerage account, to purchase 32,000 shares of stock in a company at prices from \$2 to \$3.20 per share. Chockalingam also placed an order through his personal online brokerage account to purchase 450 shares of the same stock for \$3.20 per share.

The same day, the defendants gained unauthorized access to the online brokerage account of an unsuspecting investor. According to the indictment, the defendants used this account to illegally acquire 26,000 shares of the same stock at prices from \$2.84 to \$3.40 per share, causing the stock's trading volume to rise to more than nine times its 15-day average.

Marimuthu then placed an order to sell 1,500 shares of the same stock from his personal online brokerage account at five dollars per share. This was one of at least 22 sell orders for this stock placed in Marimuthu's personal online brokerage accounts between August 28, 2006, and the morning of August 29, 2006. These transactions allegedly resulted in the sale of 30,700 shares of this stock, yielding a substantial profit for the defendants over the course of just a few hours. The defendants used this type of scheme with various stocks between July and November, 2006.

Marimuthu was arrested on Dec. 20, 2006, by the Hong Kong Police on charges of computer fraud, money laundering, and possession of equipment to make a false instrument. These Hong Kong charges concern crimes similar to those charged in the U.S. indictment. Thirugnanam Ramanathan was arrested by authorities in Hong Kong on Jan. 26, 2007, pursuant to a U.S. provisional arrest warrant. Chockalingam Ramanathan is at large. The government will seek the extradition of the arrested defendants to face charges in Nebraska.

The conspiracy and computer fraud charges in this case each carry a maximum sentence of five years in prison. Wire fraud and securities fraud carry maximum sentences of 20 and 15 years respectively. Each count of aggravated identity theft adds two years in prison.

Source: Computer Crime & Intellectual Property Section, United States Department of Justice.

3.5 E-Gold indicted for Money Laundering and Illegal Money Transmitting

E-Gold, Ltd., (E-Gold) an Internet-based digital currency business, and its three principal directors and owners, pleaded guilty to criminal

charges relating to money laundering and the operation of an illegal money transmitting business.

E Gold's digital currency, "E Gold," functioned as an alternative payment system and was purportedly backed by stored physical gold. Persons seeking to use the E Gold payment system were only required to provide a valid email address to open an E Gold account – no other contact information was verified. Once an individual opened an E Gold account, he/she could fund the account using any number of exchangers, which converted national currency into E Gold. Once open and funded, account holders could access their accounts through the Internet and conduct anonymous transactions with other parties anywhere in the world.

E Gold has been a highly favored method of payment by operators of investment scams, credit card and identity fraud, and sellers of online child pornography. The indictment alleges that the defendants conducted funds transfers on behalf of their customers, knowing that the funds involved were the proceeds of unlawful activity; namely child exploitation, credit card fraud, and wire (investment) fraud; and thereby violated federal money laundering statutes. The defendants operated the E Gold operation without a license in any US state and without registering with the federal government. They thereby violated federal and state money transmitting laws at various times from 1999 through December 2005.

E-Gold and its corporate affiliate Gold & Silver Reserve Inc. each pleaded guilty to conspiracy to engage in money laundering and conspiracy to operate an unlicensed money transmitting business. The principal director of E-Gold and CEO of Gold & Silver Reserve Inc. (Gold & Silver Reserve), Dr. Douglas Jackson, 51, of Melbourne, Fla., pleaded guilty to conspiracy to engage in money laundering and operating an unlicensed money transmitting business. E-Gold's other two senior directors, Barry Downey, 48, of Baltimore, and Reid Jackson, 45, of Melbourne each pleaded guilty to felony violations of District of Columbia law relating to operating a money transmitting business without a license.

At sentencing, E-Gold and Gold & Silver Reserve face a maximum fine of \$3.7 million. Douglas Jackson faces a maximum prison sentence of 20 years and a fine of \$500,000 on the conspiracy to engage in money laundering charge, and a sentence of five years and a fine of \$250,000 on the operation of an unlicensed money transmitting business charge.

Downey and Reid Jackson each face a maximum of five years in prison and a fine of \$25,000. Additionally, as part of the plea, E-Gold and Gold

& Silver Reserve have agreed to forfeiture in the amount of \$1.75 million in the form of a money judgment for which they are joint and severally liable.

Source: Computer Crime & Intellectual Property Section, United States Department of Justice.

3.6 One man convicted for counterfeiting Citibank ATM cards

Kenneth J. Flury, a 41-year-old American was sentenced to 32 months in prison, to be followed by 3 years of supervised release on account of being convicted for bank fraud and conspiracy. Flury was also ordered to pay restitution to CitiBank in the amount of \$300,748.64, and a \$200 special assessment to the Crime Victim's Fund.

Flury had obtained stolen CitiBank debit card account numbers, PINs and personal identifier information of true account holders and fraudulently encoded this information onto blank ATM cards.

After encoding blank cards with the stolen account information, he used the counterfeit ATM to obtain cash advances to withdraw cash and obtain cash advances totaling over \$384,000 from ATM machines over a 3 week period.

After he fraudulently obtained the funds, he transferred approximately \$167,000 of the fraud proceeds via Western Union money transfers to the individuals supplying the stolen CitiBank account information located in Europe and Asia. Law enforcement officers seized approximately \$157,080 in cash from Flury on May 5, 2004, and also intercepted an additional \$32,345 Flury had attempted to transfer via Western Union to Russia on or about May 4, 2004.

Kenneth Flury was also one of 19 defendants indicted by a federal grand jury in New Jersey in October 2004, as a result of the "Shadowcrew" investigation, a long term on-line undercover investigation conducted by the U.S. Secret Service targeting domestic and international subjects engaged in identity theft, credit card fraud and production of false identification documents.

Source: Computer Crime & Intellectual Property Section, United States Department of Justice.

3.7 Elaborate phishing scam mastermind jailed for 7 years

Michael Dolan, a 24-year-old US citizen was sentenced to 84 months of imprisonment, followed by three years of supervised release for his

participation in an elaborate internet “phishing” scheme that targeted and victimized America Online subscribers.

From approximately 2002 through 2006, Dolan conspired with others to obtain names, credit card numbers, bank account numbers, Social Security account numbers, and other private personal and financial information through an internet “spamming” and “phishing” scheme that targeted AOL subscribers. “Phishing” is the act of sending fraudulent email in an attempt to scam individuals into surrendering private information that will be used for identity theft.

The scheme involved the use of software to collect AOL account names from chat rooms and to “spam” those accounts with counterfeit emails, including emails purporting to convey electronic greeting cards from Hallmark.com. Through this scheme, an AOL subscriber who attempted to open one of the purported greeting cards would unwittingly download a software trojan that would prevent the subscriber from accessing AOL without first entering information including the subscriber’s name, credit card number, bank account number, and Social Security account number.

The subscriber’s information would then be used by Dolan and others to order products online and to produce counterfeit debit cards, which were used at ATM machines and retail outlets such as gas stations.

In May 2004, Dolan was sentenced to two years of probation after pleading guilty in Eastern District of New York to one misdemeanor count of accessing a protected computer without authorization. In April 2006, the court revoked Dolan’s probation and sentenced him to 9 months of imprisonment after ruling that Dolan had violated the conditions of his probation by failing to report to his probation officer and by making numerous trips out of Connecticut without permission, including at least one trip overseas.

In addition, while incarcerated after being charged for his participation in this phishing scheme, Dolan induced his girlfriend to perjure herself before a federal grand jury, attempted to bribe a co-defendant to exonerate him falsely, and threatened to kill someone he believed to be a Government informant.

Source: Computer Crime & Intellectual Property Section, United States Department of Justice.

3.8 Romanian admits role in international phishing scheme

Ovidiu-Ionut Nicola-Roman, a 22-year-old resident of Craiova, Romania, pleaded guilty to one count of conspiracy to commit fraud in connection with access devices.

Nicola-Roman and six other Romanian citizens were charged in connection with an Internet “phishing” scheme. A phishing scheme uses the Internet to target large numbers of unwary individuals, using fraud and deceit to obtain private personal and financial information such as names, addresses, bank account numbers, credit card numbers and Social Security numbers. Phishing schemes often work by sending out large numbers of counterfeit email messages, which are made to appear as if they originated from legitimate banks, financial institutions or other companies.

The investigation leading to the Indictment stemmed from a complaint concerning a fraudulent e-mail message made to appear as if it originated from Connecticut-based People’s Bank. In fact, the email message directed victims to a computer in Minnesota that had been compromised, or “hacked,” and used to host a counterfeit People’s Bank Internet site. During the course of the investigation, it was determined that the individuals had engaged in similar phishing schemes against many other financial institutions and companies, including Citibank, Capital One, JPMorgan Chase & Co., Comerica Bank, Wells Fargo & Co., eBay and PayPal.

In pleading guilty, Nicola-Roman admitted that he participated in this phishing scheme, that he accessed email accounts containing stolen credit card information, and that the stolen credit card numbers were used to obtain money unlawfully.

According to information provided to the Government by just one of the victim banks, the scheme resulted in losses of approximately \$150,000.

Nicola-Roman faces a maximum term of imprisonment of five years and a fine of up to \$250,000.

Nicola-Roman was located in Bulgaria and arrested on an Interpol warrant on June 6, 2007. He was extradited to the United States on Nov. 8, 2007.

Source: Computer Crime & Intellectual Property Section, United States Department of Justice.

3.9 Teacher charged for hacking protected system

Tina Kafka, a teacher of the Explorer Elementary Charter School was charged with one count of intentionally causing damage to a protected computer.

According to the indictment, Ms. Kafka was employed as a teacher by Explorer Elementary Charter School (“Explorer”) for the 2006-2007 school year. Beginning in December 2006 and continuing to November

2007, Ms. Kafka gained unauthorized access to the electronic mail accounts of at least 16 Explorer employees and read their email messages. In addition, Ms. Kafka attempted to forward an email from one of the illegally accessed accounts to a local newspaper reporter. As a result of the intrusion, Explorer incurred a loss in excess of \$5000.

She has been charged with intentionally causing damage to a protected computer and faces a maximum penalty of 10 years' imprisonment and \$250,000 fine per count.

[Note: An indictment contains allegations that a defendant has committed a crime. Every defendant is presumed innocent until and unless proven guilty beyond a reasonable doubt.]

Source: Computer Crime & Intellectual Property Section, United States Department of Justice.

3.10 Hacker controlling 7000 botnets convicted

Gregory King, a 21-year-old American was sentenced to two years in federal prison and ordered to pay over \$69,000 in restitution after he pleaded guilty to two counts of transmitting code to cause damage to a protected computer.

Online, King was known as Silenz, Silenz420, sZ, GregK, and Gregk707. This case is the product of an extensive investigation by the FBI, whose agents analyzed Internet logs, executed search warrants, performed forensic analysis of King's computers, and took his confession.

King admitted to using a "botnet" to conduct distributed denial of service attacks (DDOS attacks) against two different business Web sites: Killanet and Castlecops. A botnet is a network of malware-infected, zombie computers (bots) that can be used to conduct DDOS attacks, send spam, and commit fraud over the Internet. Bots are also used to infect other computers and thus propagate the botnet. The owners of the infected computers do not know that their computers have been infected with "botware," but their computers can nonetheless be secretly directed by the "bot herder," the person in control of the botnet. In a DDOS attack, a bot herder directs the bots to flood a victim computer with information and thereby disable the target computer.

King admitted to controlling about 7,000 bots and using them to DDOS attack Killanet and Castlecops. Killanet is an interactive forum where members could share advice on graphic design, web design, photography, and gaming and was DDOS attacked in 2004, 2005, and 2006. Castlecops is an Internet security community specializing in anti-

phishing, malware analysis, and combating spam and was DDOS attacked in 2007.

On October 1, 2007, FBI agents went to King's residence to arrest him. After agents knocked on the front door, King exited the back door, hid a laptop computer in the backyard, and then returned to answer the front door. Pursuant to a search warrant, the laptop was seized and searched. It contained, among other things, botnet software and references to King's various Internet monikers.

Source: Computer Crime & Intellectual Property Section, United States Department of Justice.

3.11 Brazilian charged with conspiracy to infect 100,000 computers

Leni de Abreu Neto, a 35-year-old Brazilian man was charged for his role in a conspiracy to sell a network of computers infected with malicious software. The indictment alleges that more than 100,000 computers worldwide were damaged. If convicted, Neto faces a maximum penalty of five years in prison and up to three years of supervised release. Neto also faces the greater of a \$250,000 fine or the gross amount of any pecuniary gain or the gross amount of any pecuniary loss suffered by the victims.

[Note: An indictment is merely an allegation. Defendants are presumed innocent until and unless proven guilty in a court of law.]

According to the indictment, Neto participated in a conspiracy along with others, including an unindicted co-conspirator, Nordin Nasiri, 19, of Sneek, Netherlands, to use, maintain, lease and sell an illegal botnet. As defined in the indictment, a botnet is a network of computers that have been infected by malicious software, commonly referred to as "bot code."

Bot code is typically designed to permit an operator or controller to instruct infected computers to perform various functions, without the authorization and knowledge of their owners, such as launching denial of service attacks to disable targeted computer systems or sending spam e-mail. Installation of bot code is typically accomplished by "hacking" computers with particular security vulnerabilities. Bot code typically contains commands for infected computers to search local networks or the Internet for other computers to infect, thereby increasing the botnet's size and power. The indictment alleges that prior to May 2008, Nasiri was responsible for creating a botnet consisting of more than 100,000 computers worldwide, and that Neto used the botnet and paid for the servers on which the botnet was hosted.

According to the indictment, between May and July 2008, Neto agreed initially with Nasiri to broker a deal to lease the botnet to a third party. The indictment alleges Neto expected the botnet to be used to send spam through the infected computers. Subsequently, Neto agreed with Nasiri to broker the sale of the botnet and underlying bot code to the third party for 25,000 euros.

Neto was apprehended by Dutch authorities on July 29, 2008, in the Netherlands and is currently in confinement in the Netherlands pending resolution of extradition proceedings.

Nasiri was also apprehended by Dutch authorities and is being prosecuted by Dutch authorities in the Netherlands.

Source: Computer Crime & Intellectual Property Section, United States Department of Justice.

3.12 "Botmaster" sentenced to 5 years in prison

Jeanson James Ancheta, a 21-year-old well-known member of the "botmaster underground" was sentenced to nearly 5 years in prison for profiting from his use of "botnets" - armies of compromised computers - that he used to launch destructive attacks, to send huge quantities of spam across the Internet and to receive surreptitious installations of adware.

Ancheta pleaded guilty to causing damage to computers used by the federal government in national defense, and accessing protected computers without authorization to commit fraud. When he pleaded guilty, Ancheta admitted using computer servers he controlled to transmit malicious code over the Internet to scan for and exploit vulnerable computers. Ancheta caused thousands of compromised computers to be directed to an Internet Relay Chat channel, where they were instructed to scan for other computers vulnerable to similar infection, and to remain "zombies" vulnerable to further unauthorized accesses.

Ancheta further admitted that, in more than 30 separate transactions, he earned approximately \$3,000 by selling access to his botnets. The botnets were sold to other computer users, who used the machines to launch distributed denial of service (DDOS) attacks and to send unsolicited commercial email, or spam. Ancheta acknowledged specifically discussing with the purchasers the nature and extent of the DDOS attacks or proxy spamming they were interested in conducting. Ancheta suggested the number of bots or proxies they would need to accomplish the specified acts, tested the botnets with them to ensure that

the DDOS attacks or proxy spamming were successfully carried out, and advised them on how to properly maintain, update and strengthen their purchased armies.

In relation to the computer fraud scheme, Ancheta admitted generating for himself and an unindicted co-conspirator more than \$107,000 in advertising affiliate proceeds by downloading adware to more than 400,000 infected computers that he controlled. By varying the download times and rates of the adware installations, as well as by redirecting the compromised computers between various servers equipped to install different types of modified adware, Ancheta avoided detection by the advertising affiliate companies who paid him for every install. Ancheta further admitted using the advertising affiliate proceeds he earned to pay for, among other things, the multiple servers he used to conduct his illegal activity.

Following the prison term, Ancheta will serve three years on supervised release. During that time, his access to computers and the Internet will be limited, and he will be required to pay approximately \$15,000 in restitution to the Weapons Division of the United States Naval Air Warfare Center in China Lake and the Defense Information Systems Agency, whose national defense networks were intentionally damaged by Ancheta's malicious code. The proceeds of Ancheta's illegal activity - including more than \$60,000 in cash, a BMW automobile and computer equipment - have been forfeited to the government.

4. Hardware devices

Modern computers began with the Difference Engine, a machine made by **Charles Babbage** in 1822 to perform differential equations. It was powered by steam and was the size of a train engine. The machine had a stored program and it could automatically perform calculations and print the results.

Later, Babbage was inspired to begin work on the first general-purpose computer, which he called the **Analytical Engine**.

Babbage's assistant, Augusta Ada King (daughter of English poet Lord Byron), was instrumental in the machine's design. Her fine understanding of the machine allowed her to create the instruction routines to be fed into the computer, making her the first female computer programmer.

Later, in the 1980s, the U.S. Defence Department named a programming language **ADA** in her honour. Babbage's steam-powered engine, although ultimately never constructed, outlined the basic elements of a modern general-purpose computer and was a breakthrough concept.

A modern computer typically consists of the following:

1. a central processing unit (CPU) which is the brain of the computer and performs the processing,
2. a motherboard to which the essential devices are connected,
3. data storage devices such as hard disks,
4. a monitor or screen,
5. keyboard and mouse,
6. power unit,
7. cooling fan.

Most computers would also contain floppy drives, CD and DVD readers and writers, USB drives etc.

A computer may be **standalone** or it may be connected to a **network** through wires or a wireless connection. Additional components include modems, printers, scanners, external data storage devices etc.

The idea of the **Internet** was born out of a fear of nuclear attack in the early 1960s. The US Government wanted to build a communications network that could continue to operate even when a major "node" or "hub" was destroyed. When a direct route of communication was not available, the system would redirect the communication traffic around the network via alternate routes.

Before the connecting of two computers together, the only way to get data from one computer to another was to copy the information onto some type of portable medium such as a floppy disk, walk over to the other computer, and upload the information from the disk.

But if the two computers could be “networked” together, one could simply send the information to the other computer through a wire. Engineers developed a way in which computers could “talk” to each other using packets of information.

As each computer was added to the Internet, it would be assigned a specific number similar to a telephone number. Today this is called an IP address, which stands for Internet Protocol address. Information from one computer could be sent to another computer by inputting that computer’s IP address.

The information would be separated into several “packets” and each **packet of information** would be able to find the destination computer by that computer’s Internet number. In this manner, all kinds of information could be shared among the various computers connected to the Internet, the “network of networks”.

The Internet became a medium of communication that is now almost limitless in its applications. People devised ways to send messages back and forth between computers - hence the development of **electronic mail** (better known as e-mail).

The Internet allowed people to share funny stories and interesting articles. Engineers could create new software and send that software to people all over the world to use. People could connect to virtual “bulletin boards” to get information about a particular community. Corporations could provide information to individual consumers.

The Internet actually embodies all forms of communication: one-to-one, one-to-many, and finally, many-to-many.

The last significant development of the Internet was the graphical interface, which is referred to as the “**World Wide Web**”. For a long time, the Internet was only open to those users who could memorize several specialized commands. But the graphical interface opened up the Internet for “less-technical” people.

Instead of typing an exact address for every website, a user can use an **Internet browser** such as Internet Explorer or Mozilla Firefox, to simply click on a “hyperlink” which immediately connects to a particular website. Websites present their information in graphical form and users can navigate through the Internet using **hyperlinks**.

A cyber crime investigator has to examine various hardware devices including data storage devices in computer systems and various miscellaneous electronic devices like a credit card skimmer or a copier.

It becomes important to be aware of these devices and their functions to truly assess their importance in cyber crime investigation. In order to do this, it becomes imperative that we first obtain an overview of these devices and how these devices fit into the overall scheme of things during an investigation. A good understanding of these concepts is also useful while making and defending an investigation report in any cyber crime investigation.

4.1 Computer Hardware components

Typically, desktop computers, regardless of brand or type, have three pieces of hardware:

- (1) The chassis containing the CPU (central processing unit) is the box that contains the electronic chips and wires that make up the computer's "engine",
- (2) The keyboard, on which directions or commands are typed, and the mouse
- (3) The monitor, a television-like screen.

These three components are the essential hardware, the physical equipment or machinery of a computer system.

4.2 Central Processing Unit (CPU)

The Central Processing Unit or microprocessor is the main computer chip. The CPU executes instructions. The major CPU manufacturers are Intel, AMD and Cyrix.

Since a CPU generates enormous quantities of heat while processing, it is necessary to dissipate this heat to the surroundings to prevent damage. This is usually done by using a heat sink and a fan attached to the CPU.

Evidentiary value: The CPU does not store any information. Therefore, the evidentiary value is limited to the component itself. The CPU itself may be stolen or counterfeited.

4.3 RAM

RAM stands for **Random Access Memory**. The requirement for RAM in a computer is to provide quick access to data. RAM is a medium of storage which is faster than any other form of storage such as a hard disk.

A program or data which the CPU is processing, resides temporarily in the RAM. When the CPU wants to process information, it can quickly access that information without having to go through other information stored in the hard disk. This saves time and makes computing operations faster.

However, RAM is temporary memory and information stored on RAM exists as long as the RAM has power. Once power is switched off, the information stored in the RAM vanishes. Therefore, once the CPU has processed data stored in the RAM, the data needs to be saved to a more permanent storage medium such as a hard disk before power is switched off.

The best analogy to explain the relationship between memory and disk storage is to think of a small office with a desk and a file cabinet.

In this popular analogy, the file cabinet represents the system's hard disk, where both programs and data are stored for long-term safekeeping.

The desktop represents the system's main memory, which allows the person working at the desk (acting as the processor) direct access to any files placed on it. To work on a particular file, it first must be retrieved from the cabinet and placed on the desktop.

If the desktop is large enough, you may be able to have several files open on it at one time; likewise, if your system has more memory, you can run more or larger programs.

Adding hard disk space to a system is like putting a bigger file cabinet in the office; more files can be permanently stored.

Adding more memory to a system is like getting a bigger desk; you can work on more programs and data at the same time.

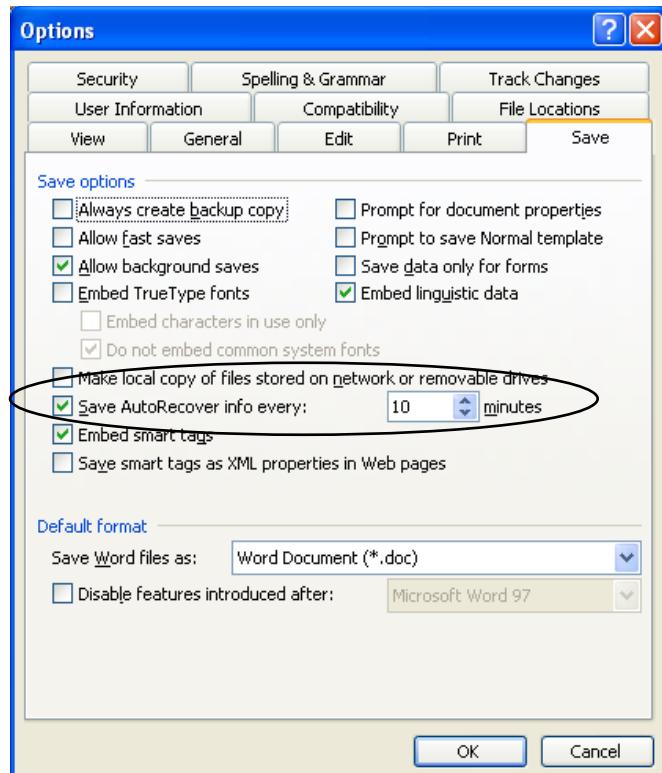
One difference between this analogy and the way things really work in a computer is that when a file is loaded into memory, it is a copy of the file that is actually loaded; the original still resides on the hard disk.

Note that because of the temporary nature of memory, any files that have been changed after being loaded into memory must then be saved back to the hard disk before the system is powered off and the memory subsequently cleared. If the changed file is not saved, then the original copy of the file on the hard disk will remain unaltered. This is like saying that any changes made to any files left on the desktop will be discarded when the office is closed, although the original files themselves will still be present in the cabinet. *[Source: computerbooksonline.com]*

Memory temporarily stores programs when they are running, along with the data being used by those programs. RAM chips are termed volatile storage because when one turns off a computer or an electrical failure

occurs, whatever is stored in RAM is lost unless it was saved to the hard drive.

Because of the volatile nature of RAM it is advisable to save work frequently. Some software applications such as Microsoft Word can do timed backups automatically as illustrated below:



For Microsoft Word auto saving feature, go to the Tools → Options → Save tab and then select the “Save AutoRecover info every” check box. The interval in minutes must be entered in the “minutes” box. The more frequently the files are saved, the more information is recovered if there is a power failure or similar problem.

Launching a computer program brings files into RAM, and as long as they are running, computer programs reside in RAM.

The CPU executes programmed instructions in RAM, and also stores results in RAM. RAM stores your keystrokes when you use a word processor (like MS-Word or Adobe Acrobat), and also stores numbers

used in calculations. Telling a program to save your data instructs the program to store RAM contents on your hard drive as a file.

The **hibernate** feature in Windows operating systems saves everything in memory onto the hard disk and then turns off the computer. When the computer is restarted, the desktop is restored exactly as it was left.

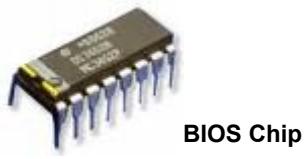
There can be a host of RAM types like: SD (Synchronous Dynamic) RAM, DDR SD (Double Data Rate Synchronous Dynamic) RAM, RD (Rambus Dynamic) RAM etc.

These are compatible with various motherboard and CPU architectures. However, they all perform the same function as described above.

Evidentiary Value: The RAM stores data when the computer is powered on. In such instances, the RAM may hold crucial information like passwords, which may be lost if the computer is powered down. A cyber crime investigator can clone the contents of the RAM using forensic software like Winhex and store it for future analysis.

4.4 ROM BIOS Chip

A ROM BIOS Chip stores data that is non – volatile unlike the RAM chip. Data held in a ROM BIOS Chip does not get lost when power is switched off. As the name suggests, data in a ROM (Read only Memory) BIOS chip can only be read and cannot usually be altered.



BIOS stands for Basic Input Output System, a small set of programs stored in the ROM chip essential for booting a computer.

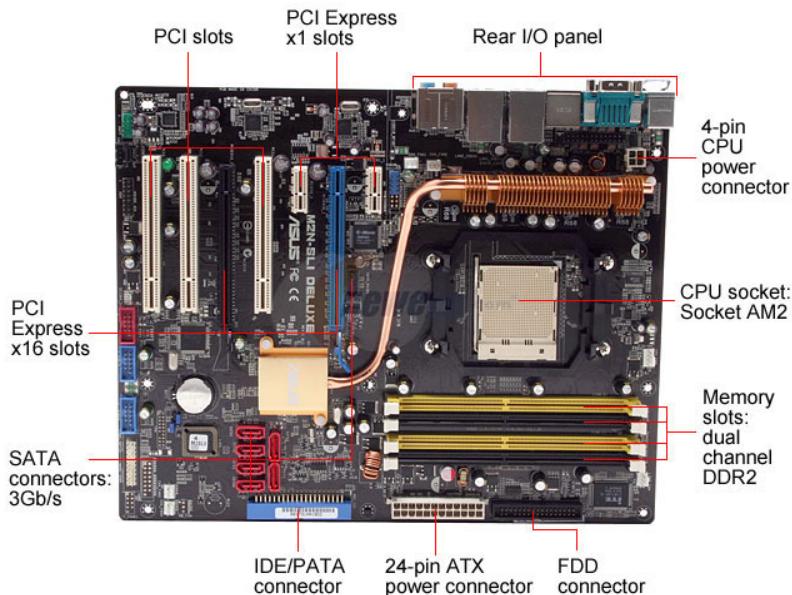
A ROM BIOS chip contains information that helps the computer boot and stores the system configuration.

Evidentiary Value: The ROM BIOS chip contains important information regarding the system configuration. It is also important for time and date stamps.

4.5 Motherboard or Mainboard

The Motherboard or mainboard is a printed circuit board on which all computer peripherals and components are attached and interconnected. It is one of the most essential pieces of hardware components on a computer system.

Motherboards can be of various shapes and sizes. Some of these form factors can be specific to a manufacturer.



Evidentiary Value

The motherboard does not store any information. The component itself is of evidentiary value as it can be the target of theft.

4.6 Ports, Buses, Interfaces

A **port** is an outlet that serves to connect a computer and other devices. Ports can be physical as well as virtual. There are a host of different physical ports which connect various devices and peripherals to a computer system, e.g. printer port, mouse port, port for keyboard and so on. Recent additions include USB and Firewire ports. We will discuss virtual ports later in this book.

A **serial port** sends and receives one bit of data at a time while a **parallel port** sends and receives multiple bits of data simultaneously or in parallel.

A **BUS** (Bidirectional Universal Switch) is a subsystem or method of data transmission between certain points inside a computer or between computer components. A bus must have the capability to transfer data as well as control the flow of data between an origin and a destination. It

must also include or define ports through which physical interfacing of two or more devices is possible. Thus, a bus may transfer data between the CPU and the printer using ports.

USB (Universal Serial Bus) is a standard developed for connecting devices to a computer while the computer is still running. Devices connected to a computer through a USB typically do not require the computer to reboot, which is known as hot plugging.

USB is a very popular standard connection method to connect devices (such as mouse, printers, keyboards, digital cameras, data storage devices etc) to a computer using a **USB port**.

FireWire is a brand name promoted by Apple Inc., for the serial bus standard IEEE 1394 developed for high speed data communication between devices. Although used for data storage devices, it is the preferred technology for use in industrial systems and professional audio systems. FireWire has the same hot plugging capabilities as USB.

IEEE (Institute of Electrical and Electronics Engineers) is a non - profit body established for advancement of technology. It develops standards on technology through consensus.

The standardization of technology is ultimately beneficial to end users as it serves to eliminate compatibility issues between devices manufactured by different vendors.

SCSI (Small Computer Systems Interface) pronounced “scuzzy” is a standard for data transfer between a computer and peripheral devices connected to it. Standardized in 1986, SCSI can be used to connect almost any peripheral device to a computer system. However, it is most widely used to connect hard disk drives and tape drives.

IDE (Integrated Drive Electronics) is another standardized interface for connecting hard disk drives and optical drives. Also known as **ATA** (Advanced Technology Attachment), this interface is found in most motherboards by virtue of which four devices, usually hard disks and CD/DVD drives, can be connected.

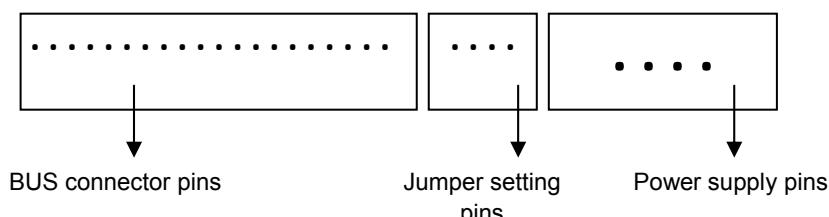
On the motherboard, usually two IDE connectors are found, IDE 1 and IDE 2 or primary IDE and secondary IDE. Each connector can support 2 devices, e.g., a hard disk and an optical drive or two hard disks. When two devices are connected to the same IDE connector on the motherboard, one device is called a master and the other a slave. A master device is recognized by the BIOS first when the computer is booting and the slave device later.

The terms master and slave are misleading. When these two terms are used, the inference is that one drive (the master drive) dictates when the other drive (the slave drive) will perform an instructed operation.

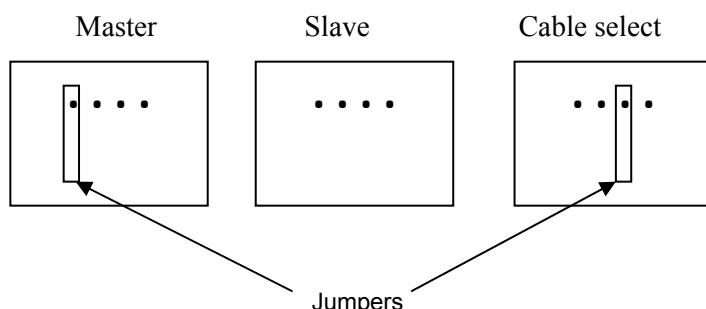
In reality, whichever drive receives an instruction from the operating system first, completes that operation irrespective of whether it is a master drive or a slave drive.

Whether a drive will be master or slave depends on the jumper setting of that drive. A jumper is a small metal connector usually encased in plastic used to complete or bypass an electrical circuit.

The figure below is a representation of the connector pins viewable on a IDE hard disk:



The following diagrams illustrate various jumper settings (these may vary based on the manufacturer of the hard disk).



The IDE/ATA interface is now slowly being phased out by a newer interface known as **SATA** (Serial Advanced Technology Attachment) which can transmit data at much higher speeds than the IDE interface.

Expansion Slots are connectors in the motherboard used to connect peripheral devices to the CPU. Expansion cards are usually connected to these expansion slots providing enhancements to a computer system.

For example, a multimedia card used for providing enhanced graphics and sound, a network interface card used for computer networking or a

modem card used to connect the computer system to the Internet, are all expansion cards connected to the CPU through expansion slots in the motherboard. These cards interface with the motherboard using another common standard known as **PCI** (Peripheral Component Interconnect).

4.7 Data Storage Devices

Hard disk drive is a primary storage device in a computer system holding non-volatile data. It is a sealed unit containing round metal plates with magnetic surfaces on which data is stored magnetically. These metal plates are commonly referred to as platters.

Data on the platters are read and modified by **read-write heads** positioned above and below the platters as they are made to spin at very high speeds by a small motor placed inside the hard disk drive. Usually quoted in Gigabytes (10^9 bytes), the storage capacity of a hard disk drive has been increasing by leaps and bounds with time. Today hard disks can store Terabytes (10^{12} bytes) of data.

The smallest unit of storage in a hard disk is known as a *sector* in a FAT file system. A sector can store up to 512 bytes of data.

Each side of a hard disk platter is divided into a number of concentric circles called *tracks*. Sectors are contained inside these tracks.

A group of sectors together make up one *cluster*. An operating system allocates cluster(s) to a file. Refer to chapter 02 for further study on file systems.

A **floppy disk** is a magnetic storage device which can store up to 1.44 MB of data. The mechanism of data storage on a floppy disk is similar to that of a hard disk. Since data storage capacity of a floppy disk is much lesser than most storage devices available today, it is slowly being phased out.

CD (Compact Disk) and **DVD** (Digital Versatile Disk) are both optical storage devices. Data is stored and read from these devices using laser technology as opposed to electro-magnetic technology used in a hard disk or a floppy disk.

USB Flash drives are small, lightweight storage devices with a USB interface. It consists of a small printed circuit board housed in an outer covering with a protruding USB connector. The drive does not require a separate power source and draws its power from the USB hub of the computer to which it is connected.

Today, these drives can hold gigabytes of data and can be also be used as a booting device in addition to being simply data storage devices. USB drives use the flash memory technology to store data.

This type of memory is non-volatile and solid state but comes with a definite life cycle. Data on these types of memories can be re-written from 10,000-1000,000 times, after which they wear out and become unusable.

Solid state is used to describe electronic devices with no moving parts. This is achieved by using semiconductor technology.

These devices are more reliable due to better resistance to shock, vibration and mechanical wear and tear as compared to technology used in vacuum tubes and transistors.

They also use energy more efficiently than electro - mechanical devices (hard disks) or optical devices (CDs/DVDs)

CF (Compact Flash) **cards** are popular data storage devices widely used in digital cameras and mobile phones. For computer systems, these devices are typically inserted into card readers which connect to the system via a USB or FireWire ports.

Many laptops and desktops computer models also have built in card readers which allow data stored on a CF card to be accessed. The technology used to store information on these cards is the same as USB Flash drives, i.e., flash memory. Like USB flash drives, these devices also do not require a separate power source.

A **tape drive** is a data storage device which uses magnetic tapes for storing data. The advantage of magnetic tape as a storage medium over others is that it has a long life and is cheap. Data access on tape drives is sequential as opposed to random in hard disk drives.

Random access means accessing a data element without having to go through any data element stored before or after it.

Sequential access, on the other hand, means a longer time of access for that element as a reading device has to go through data stored before or after that element as the case may be.

A simple example of a sequential access is a cassette tape containing songs.

If one has to access a particular song, which is recorded in the middle of the cassette, one has to fast forward or rewind to that particular position.

Songs stored on a CD ROM can be randomly accessed. For listening to a particular song, one can simply go to that specific track without having to go to any other track.

Evidentiary value: Needless to say, storage devices are the most important sources of evidence for the cyber crime investigator. They need careful transport and storage so as not to corrupt the data stored on them.

4.8 Peripheral devices

A **modem** allows a computer to access other computers or networks through a telephone line, wireless, or other communications. Modems can be internal as well as external.

A **printer** prints text and images stored in the electronic form onto paper. Printers can be of several types depending on the technology they use, e.g., inkjet, dot matrix, laser, etc. Printers have buffer memory which allows these devices to store multiple documents during the printing process. Some models may even have a hard disk.

A **scanner** converts paper based documents containing images or text into electronic form. These can then be manipulated, viewed or transmitted from one computer to another.

Evidentiary value: The *modem* itself can be potential evidence in Internet based crimes.

A *printer* may contain time stamps and network information if it is connected to a network. In addition, printed documents from a specific printer, ink cartridges and characters superimposed on the printer's roller may also be potential sources of evidence.

In case of a *scanner*, the device itself may be evidence of illegal acts like counterfeiting, forgery etc.

4.9 Other electronic devices

Fax machines can be programmed to store phone numbers. These devices also have the capacity to store several pages of incoming and outgoing document transmissions. The potential evidence in this case may be the stored documents, phone numbers, error logs or the film cartridge involved in printing.

Credit Card Skimmers are devices used for reading the information recorded on credit card magnetic strips at the back of the cards. These strips can hold information relating to the card number, expiry date and name and address of the user, which may all be potential evidence.

Digital Organizers, digital watches and mobile phones can store messages, contact numbers, addresses, appointments and notes which

can all be potential evidence. Certain watches can even synchronize information with computers.

Copiers like printers can hold documents in memory for printing at a later date. Some models may maintain user access details and copying history. Time stamps maintained by copiers, user logs and documents stored in memory can all be potential sources of evidence in a copier.

GPS (Global Positioning Systems) can store travel logs and previous routes used for travel. They can provide information on previous destinations and travel logs which can be potential sources of evidence.

4.10 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.

Component	Description & uses	Potential Evidence
Hard disk	This is the primary data storage device of the suspect computer.	<u>Computer-Created Files</u> System files Swap files Temporary files Backup files Log files Configuration files Printer spool files Cookies Hidden files History files <u>Other evidence</u> Computer date & time BIOS and OS password Deleted files Unallocated space Slack space Free space Metadata
Storage devices	This includes the hard disk(s) of the suspect computer and external disks, floppies,	<u>User-Created Files</u> E-mails & email archives Audio / video files Image files.

	CDs, DVDs, USB disks etc.	Address books Calendar entries Internet bookmarks Favourite sites Database files Spreadsheet files. Document / text files. Compressed files <u>User-Protected Files</u> Encrypted files Password-protected files Steganographic files Misnamed files Hidden & system files
Central Processing Unit	This is the brain of the computer and processes data.	The CPU is evidence in case of theft or counterfeiting
RAM	Stores user's programs and data while the computer is powered on. The information is lost when the computer is powered off / shutdown.	Information such as passwords and encryption keys can be obtained while the computer is powered on. The RAM itself may be evidence in case of theft or counterfeiting.
Smart card	This contains a microprocessor capable of storing encryption keys, passwords, monetary value, digital certificate etc.	Since it is primarily used for access control, it contains important identification and / or authentication information.
Dongle	It is a small device that plugs into a computer port. It is capable of storing encryption keys, passwords, monetary value, digital certificate etc.	Since it is primarily used for access control, it contains important identification and / or authentication information.
Biometric scanner	It is a device, connected to a computer, that recognizes physical characteristics of a person such as fingerprint, retina, voice, face etc.	Since it is primarily used for access control, it contains important identification and / or authentication information.

Digital Cameras	They capture images (and sometimes videos) in a digital format that can easily be transferred to computer.	<ul style="list-style-type: none"> - Photos - Video - Sound - Time stamps - Removable memory card
Personal Digital Assistants	PDAs are small devices that have computing as well as telecommunication features.	<p><u>User-Created Files</u></p> <p>E-mails & email archives Audio / video / image files Address books Calendar entries Internet bookmarks Favourite sites Database files Spreadsheet files. Document / text files. Compressed files</p> <p><u>User-Protected Files</u></p> <p>Encrypted files Password-protected files Steganographic files Misnamed files Hidden & system files</p>

5. Setting up a Cyber Crime Investigation Cell

Cyber crime has made a significant impact on the criminal justice system prevalent throughout the world. Its effects are felt more as nations constantly endeavour to provide quicker and more efficient services to its citizens through the use of cyber space.

Almost all offences in the present time involve the use of computers and other electronic media at some stage of the act being committed by the criminal.

Criminals, realizing the effectiveness of computers and the Internet to successfully perpetrate conventional crimes, are resorting to using them as tools for committing such crimes.

5.1 Need for a Cyber Crime Investigation Cell

A Cyber Crime Investigation Cell is now an essential requirement for any law enforcement agency to tackle not only cyber crimes but also investigate conventional crimes.

Conventional Crime

A disturbing trend that is emerging nowadays is the increasing use of encryption, high-frequency encrypted voice/data links, steganography etc. by terrorists and members of organized crime cartels.

Instances around the world are coming to light where computers and other electronic tools have been used as tools to facilitate the commission of conventional crimes.

Cyber Crime

The widespread growth of cyber crime has affected nations from all across the globe. Incidents of cyber crime have caused extensive loss to a nation's economy. Loss of business profits and disruption of government and other services severely hampers the growth of any economy.

The incidents of cyber crime can range from obscene, threatening and defamatory emails to computer aided sabotage, source code thefts and even attempted cyber murders.

In March 2003, Asian School of Cyber Laws' Computer Emergency Response Team (ASCL-CERT) published the Computer Crime and Abuse Report (India) 2001-02 that analysed 6266 incidents of computer crime and abuse reported by over 600 organisations in India. The highest number of incidents reported was those of Data Theft followed by e-mail abuse, unauthorized access and so on.

The joint survey conducted by Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI), USA highlights the various kinds cyber crimes committed. The highest number of crimes committed was virus attacks followed closely by abuse of Internet Access and Denial of Service.

As can be seen from the reports above, cyber crime has a major impact on the economic growth of a nation. Valuable data is stolen by means of hacking. The various Internet virus attacks that have taken place have caused global losses amounting to billions of dollars. Cyber crime is a phenomenon whose effects are felt at a global level.

5.2 Setting up a Cyber Crime Investigation Cell

To prevent the various cyber crimes that take place every day it is essential to establish a dedicated cell.

As more criminals have started resorting to computers and other electronic media to commit conventional crimes, nations have understood the significant role that a Cyber Crime Investigation Cell plays to help law enforcement agencies to investigate such crimes.

Various nations have already put into place dedicated personnel and infrastructure that exclusively deal with issues of cyber crime.

As realization dawns upon countries on the need to zealously protect their citizens and themselves from becoming victims of cyber crime, they also realize the importance of setting up a dedicated mechanism to counter this menace.

1. Identification of personnel

The identification of key personnel to man the Cyber Crime Investigation Cell is a pre-requisite for setting up such an investigative wing. The personnel would have to undergo initial training to be well equipped to tackle the issues that arise.

However, such training programs should be conducted from time to time to ensure that the personnel are always equipped with the latest information on the tools and techniques to help them tackle cyber crime.

2. Training

The next, and essentially the most crucial step, in setting up a cyber crime cell, involves the identification of the type of training that is required for the personnel that have been assigned to the Cyber Crime Investigation Cell.

Specialized training is a critical pre-requisite to setting up a cell. Training programs are essential for the smooth functioning of a cyber crime cell. With regards to the training of the personnel for the cyber crime cell ASCL offers the **ASCL Certified Cyber Crime Investigator** course.

This course covers the various issues relating to cyber crime investigation. This training is bundled with extensive case studies and practical sessions that would help the participants to master the tools and techniques required for investigating cyber crime.

3. Constant Training & Upgrading Systems

Continuous training ensures that personnel stay in touch with current developments of cyber crime. Such training programs also help the participants in keeping up to date with modern tools and techniques for investigating cyber crimes.

It is essential that the Infrastructure and other systems used in the Cyber Crime Investigation Cell also be checked and audited constantly and upgraded as and when required.

4. Infrastructure

It is important for the Cyber Crime Investigation Cell to have adequate infrastructure for successful examination and analysis of digital evidence. It should be kept in mind that for a cyber crime cell, infrastructure does not only include technical infrastructure but also assets such as adequate working space, dedicated communication lines, a 24 hour high speed internet connection among others which should be made available to the personnel.

The computers should be networked so that various personnel can have access to files residing in other computers in the cyber forensics cell. Stand-alone machines should also be used as they help eliminate the threat of damage to sensitive data through network penetration crimes.

This would include procuring the requisite hardware and software for such examination and analysis.

The **hardware requirements** for the cell include:

- Powerful computer systems with standard peripherals like CD-ROM drives and CD-writers, desktop and laser printers, scanners etc.
- Storage devices for making bit-stream copies or clones of the suspect storage media.

- Card readers for examination of various kinds of cards that store data used for authentication and communication e.g., SMART cards, MicroDrives, GSM SIM cards.
- USB external CD Writers for taking back-up of information retrieved from various storage media.
- A wide array of connectors for connecting various hardware devices.
- Laptop Hard Disk Drive examination tools.

The **software requirements** for the cell include:

- Robust operating system software.
- Other application software facilitating word-processing, spread sheet, electronic mails, multimedia, imaging, etc.
- Case management software for keeping records of the cases being investigated and for tracking case details at short notice.
- Bootable disks to let investigating authorities boot from such disks instead of the suspect's bootable disk.
- Tracking software to detect the location of a computer from which an offence has been committed.
- Spoofing tools for e-mail and SMS spoofing.

Cyber criminals tend to be technically sound and hardly leave any trails for law enforcement personnel to find out or trace their physical location. This necessitates the use of spoofing tools to trap and subsequently induce the suspect to give clues about his actual physical location and thus help law enforcement personnel to ultimately apprehend the suspect.

- Header analyzing software for analysis of email headers.
- Advanced Search software for swiftly locating files containing specified keywords.
- Chain-of-custody software for maintaining a chronological and personnel sequence of evidence handling by the investigating agency
- Steganography software
- Cyber forensic software
- Password cracking tools
- Disc imaging tools
- Data, File and image recovery tools